T.C.

ÇANKIRI KARATEKİN ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ YÖNETİMİ VE BİR REHBER ÖNERİSİ

Ali KAVAK

DOKTORA TEZİ

Danışman

Prof. Dr. Hüseyin ODABAŞ

Çankırı – 2023

T.C.

ÇANKIRI KARATEKİN ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ YÖNETİMİ VE BİR REHBER ÖNERİSİ

Ali KAVAK

DOKTORA TEZİ

Danışman

Prof. Dr. Hüseyin ODABAŞ

Çankırı – 2023

İÇİNDEKİLER

Sayfa

İÇİNDEKİLER ..... **İ**
BİLİMSEL ETİK BİLDİRİMİ ..... **İX**
TEZ KABUL VE ONAY ..... **X**
ÖNSÖZ… ..... **Xİ**
ÖZET … ..... **Xİİİ**
ABSTRACT ..... **XİV**
KISALTMALAR ..... **XV**
TABLO LİSTESİ ..... **XVİ**
ŞEKİL LİSTESİ ..... **XX**
1. GİRİŞ **1**
1.1. Konunun Kavramsal Boyutu 1
1.2. Amaç 7
1.3. Önem 10
1.4. Araştırma Soruları ve Hipotezler 12
1.5. Kapsam ve Sınırlılıklar 13
1.6. Tanımlar 14
1.7. Yöntem 18
1.7.1. Araştırma Modeli ve Çerçevesi 18
1.7.2. Evren ve Örneklem 20
1.7.3. Verilerin Toplanması 23
1.7.4. Verilerin Çözümlenmesi ve Değerlendirilmesi 27
2. BİLGİ GÜVENLİĞİ İLE İLGİLİ TEMEL BİLGİLER **29**
2.1. Bilginin Değeri 29
2.2. Bilgi Varlıkları 33
2.3. Bilgi Varlıklarının Sınıflandırılması ve Etiketlenmesi 36
2.4. Bilgi Sistemleri ve Bileşenleri 43

2.5. Güvenlik İhtiyacı 52
2.6. Bilgi Güvenliği ve Bileşenleri 54
2.7. Bilgi Güvenliğinin Tarihsel Gelişimi 63
2.8. Bilgi Güvenliği İhtiyacı 68
2.8.1. İşlevselliğin Korunması 68
2.8.2. Verilerin Korunması 69
2.8.3. Uygulamaların Güvenliğini Sağlamak 70
2.8.4. Teknolojik Varlıkların Korunması 70
2.9. Bilgi Güvenliği Yönetim Araçları 71
2.9.1. Politikalar 74
2.9.2. Standartlar 76
2.9.3. Rehberler 78
2.9.4. Prosedürler 79
2.10. Bilgi Güvenliği Standartları 79
2.10.1. ISO/IEC 27000 Serisi Standartları 80
2.10.2. NIST SP 800 Serisi Standartları 82
2.10.3. COBIT Bilgi ve Bağlantılı Teknolojiler Kontrol Hedefleri Standardı 82
2.10.4. ITAF Bilgi Güvenliği Denetimi ve Emniyeti Standartları 83
2.10.5. ITIL Bilgi Teknolojisi Altyapı Kütüphanesi 84
2.10.6. SoGP Bilgi Güvenliği İçin İyi Uygulama Standardı 85
2.10.7. IEEE 802 Standartları 86
3. BİLGİ GÜVENLİĞİ TEHDİTLERİ VE ÖNLEMLERİ 88
3.1. Bilgi Güvenliği Tehditlerinin Kaynakları 88
3.2. Bilgi Güvenliği Tehdit Riskleri ve Saldırılar 95
3.3. Bilgi Güvenliği Tehdit Türleri 105
3.3.1. Donanım Güvenliği Tehditleri 105

3.3.2. Yazılım Güvenliği Tehditleri 107
3.3.3. Ağ Güvenlik Açıkları ve Tehditleri 110
3.3.4. Veri Güvenliği Tehditleri 116
3.3.5. Fiziksel ve Çevresel Tehditler 117
3.3.6. İnsan Kaynaklı Tehditler 118
3.4. Bilgi Güvenliği Önlemleri 121
3.4.1. Teknolojik Önlemler 126
3.4.1.1. Donanım Güvenliği Önlemleri 127
3.4.1.2. Yazılım Güvenliği Önlemleri 128
3.4.1.3. Ağ Güvenliği Önlemleri 131
3.4.1.4. Veri Güvenliği Önlemleri 134
3.4.1.5. Fiziksel ve Çevresel Güvenlik Önlemleri 136
3.4.2. Kurumsal (Örgütsel) Önlemler 140
3.4.2.1. Bilgi Güvenliği Politikaları 140
3.4.2.2. Bilgi Güvenliği Prosedürleri ve Kontrolleri 141
3.4.2.3. İdari Araç ve Yöntemler 142
3.4.2.4. Bilgi Güvenliği Farkındalık Çalışmaları 143
4. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ 146
4.1. Bilgi Güvenliği Yönetim Sistemi 146
4.2. Bilgi Güvenliği Yönetim Sistemi Süreç Aşamaları 149
4.2.1. Bilgi Güvenliği Gereksinimlerinin Belirlenmesi 149
4.2.2. Bilgi Güvenliği Risklerinin Değerlendirilmesi ve Düzeltilmesi 149
4.2.3. Bilgi Güvenliği Kontrollerin Seçilmesi ve Uygulanması 150
4.2.4. BGYS' nin Etkinliğinin İzlenmesi, Sürdürülmesi ve İyileştirilmesi 151
4.3. PUKÖ Döngüsü 152
4.4. PUKÖ Döngüsünün Aşamaları ve BGYS ile İlişkisi 153

4.4.1. Planla..... 154

4.4.2. Uygula..... 155

4.4.3. Kontrol Et..... 156

4.4.4. Önlem Al..... 157

4.5. BGYS'nin Başarı Faktörleri ve Faydaları..... 157

5. ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ..... 159

5.1. Üniversite Kütüphanelerinde Bilgi Güvenliğinin Önemi 159

5.2. Üniversite Kütüphanelerinde Bilgi Güvenliği Sorunları ve Önlemleri 164

5.3. Üniversite Kütüphanelerine Ait Bilgi Varlıkları..... 169

5.4. Üniversite Kütüphanelerinde Bilgi Sistemlerinin İşlevi ve Güvenliği 173

5.5. Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi 177

6. TÜRKİYE'DE ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ YÖNETİMİNE İLİŞKİN BULGULAR VE TARTIŞMA181

6.1. Katılımcıların Tanımlayıcı Profillerine İlişkin Bulgular 181

6.2. Üniversite Kütüphanelerinde Bilgi Güvenliği Personeli ve Yönetim Aracının Varlığı 183

6.3. Üniversite Kütüphanelerinde Kullanılan Bilgi Sistemleri 184

6.4. Bilgi Varlıklarının Kritiklik Derecesinin Belirlenmesi..... 187

6.5. Üniversite Kütüphanelerinde Algılanan Bilgi Güvenliği Tehditleri..... 190

6.6. Teknolojik Bilgi Güvenliği Önlemlerine İlişkin Bulgular..... 193

6.6.1. Teknolojik Bilgi Güvenliği Önlemlerinin Genel Uygulanma Düzeyleri... 194

6.6.2. Üniversite Türü Değişkenine Göre Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri 211

6.6.3. Bilgi Güvenliği Personeli Değişkenine Göre Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri..... 217

6.6.4. Bilgi Güvenliği Yönetim Aracı Değişkenine Göre Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri..... 224

6.7. Kurumsal Bilgi Güvenliği Önlemlerine İlişkin Bulgular..... 232

6.7.1. Kurumsal Bilgi Güvenliği Önlemelerinin Genel Uygulanma Düzeyleri... 234

6.7.2. Üniversite Türü Değişkenine Göre Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri ... 247

6.7.3. Bilgi Güvenliği Personeli Değişkenine Göre Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri ... 252

6.7.4. Bilgi Güvenliği Yönetim Aracı Değişkenine Göre Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri ... 258

6.8. Tartışma ... 264

6.8.1. Üniversite Kütüphanelerinde Bilgi Güvenliği Personelinin Varlığına İlişkin Tartışma ... 264

6.8.2. Üniversite Kütüphanelerinde Kullanılan Bilgi Sistemlerinin Önemine İlişkin Tartışma ... 266

6.8.3. Bilgi Varlıklarının Kritiklik Derecesinin Belirlenmesine İlişkin Tartışma 267

6.8.4. Üniversite Kütüphanelerinde Algılanan Bilgi Güvenliği Tehditlerine İlişkin Tartışma ... 268

6.8.5. Teknolojik Güvenlik Önlemlerine İlişkin Tartışma ... 270

6.8.6. Kurumsal Güvenlik Önlemlerine İlişkin Tartışma ... 276

7. ÜNİVERSİTE KÜTÜPHANELERİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) REHBER ÖNERİSİ ... 284

7.1. Planlama Aşaması ... 286

7.1.1. Karar Verme ... 287

7.1.2. BGYS Kurulunun Oluşturulması ... 288

7.1.3. Fark Analizi ... 289

7.1.4. BGYS'nin Hedefleri ve Planlaması ... 290

7.1.5. BGYS Politikası Oluşturma ... 292

7.1.6. BGYS'nin Kapsamı ve Bağlamı ... 293

7.1.7. Varlık Yönetimi ve Envanteri ... 293

7.1.8. Bilgi Varlıklarının Sınıflandırması ve Kritiklik Derecesinin Belirlenmesi 295

7.1.9. Risk Yönetimi ve İşletimi ... 296

7.1.10. Önlemlerin Belirlenmesi ve Uygulanması ... 299

7.1.11. Önlemlerin Uygulanabilirlik Durumu 301
7.1.12. BGYS Dokümantasyon Sistemi 301
7.2. Uygulama Aşaması 305
7.2.1. Seçilen Önlemlerin Uygulanması 305
7.2.2. İhlal Olaylarının Tespiti ve Müdahale 306
7.2.3. Risk işleme 306
7.2.4. Değişiklik Yönetimi 306
7.2.5. İş sürekliliği 307
7.2.6. Farkındalık Çalışmaları 307
7.2.7. Komite Toplantıları 307
7.3. Kontrol Etme Aşaması 307
7.3.1. İç Denetim 308
7.3.2. Yönetimin Gözden Geçirilmesi 311
7.3.3. Dokümanların Gözden Geçirilmesi 312
7.4. Önlem Alma Aşaması 312
7.4.1. Düzeltici Faaliyetler 313
7.4.2. İyileştirme 314
8. SONUÇLAR VE ÖNERİLER 316
8.1. Sonuçlar 316
8.1.1. Bilgi Güvenliği Alt Yapısına ve Tehditlerine İlişkin Sonuçlar 316
8.1.2. Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeylerine İlişkin Sonuçlar 317
8.1.3. Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Düzeylerine İlişkin Sonuçlar 326
8.1.4. Hipotezlere İlişkin Sonuçlar 332
8.2. Öneriler 334
8.2.1. Uygulayıcılara Yönelik Öneriler 334

8.2.2. Araştırmacılara Yönelik Öneriler 336

KAYNAKÇA 338

EKLER …. 364

EK-1. 1: Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi Anket Formu 364

EK-1. 2: Etik Kurul Değerlendirme Formu 371

EK-7. 1: Bilgi Güvenliği Yönetim Sistemi Politikası 372

EK-7. 2: Bilgi Varlıklarının Sınıflandırılması ve Kritiklik Derecesi Politikası 374

EK-7. 3: Bilgi Transferi Politikası 376

EK-7. 4: Fikri Mülkiyet Politikası 377

EK-7. 5: Fiziksel ve Çevresel Güvenlik Politikası 378

EK-7. 6: Güvenli Sistem Mühendisliği Politikası 379

EK-7. 7: İnsan Kaynakları Güvenliği Politikası 380

EK-7. 8: İzleme, Ölçme, Analiz ve Değerlendirme Politikası 381

EK-7. 9: Sürekli İyileştirme Politikası 382

EK-7. 10: Tedarikçi ve Üçüncü Taraf Güvenliği Politikası 383

EK-7. 11: Temiz Masaüstü ve Temiz Ekran Politikası 384

EK-7. 12: Uyum Politikası 385

EK-7. 13: Varlıkların Kabul Edilebilir Kullanımı Politikası 386

EK-7. 14: Ziyaretçi Kabul Politikası 388

EK-7. 15: Bilgi Sınıflandırma ve Etiketleme Prosedürü 389

EK-7. 16: BGYS Doküman Kayıtların Kontrolü Prosedürü 390

EK-7. 17: BGYS Düzeltici Faaliyet Prosedürü 391

EK-7. 18: Eğitim / Farkındalık Eğitimi Prosedürü 392

EK-7. 19: Fikri Mülkiyet Haklarının Korunması Prosedürü 393

EK-7. 20: İç Denetim Prosedürü 394

EK-7. 21: İhlal Olayları Yönetim Prosedürü 395

EK-7. 22: İletişim Prosedürü 397
EK-7. 23: İzleme, Ölçme, Analiz ve Değerlendirme Prosedürü 398
EK-7. 24: Varlık Yönetimi Prosedürü 399
EK-7. 25: Yönetimin Gözden Geçirme (YGG) Prosedürü 400
EK-7. 26: BGYS Dokümanının Kapsam ve Bağlam Dokümanı 401
EK-7. 27:Gizlilik Sözleşmesi Formu 402
EK-7. 28: BGYS Fark Analizi Formu 403
EK-7. 29: Bilgi Güvenliği Risk Belirleme Formu 407
EK-7. 30: İç Denetim Ortak Soru Formu 408
EK-7. 31: BGYS Fark Analizi Değerlendirme Raporu 409
EK-7. 32:Bilgi Varlıkları Envanter Listesi 410
EK-7. 33: BGYS Kurumsal Dokümanlar Listesi 412
EK-7. 34: BGYS Teknik Dokümanlar Listesi 413
EK-7. 35: İhlal Olayı Tespit / Bildirim Formu 414
EK-7. 36: İç Denetim Uygunsuzluk Tespit / Bildirim Formu 415
EK-7. 37: Düzeltici Faaliyet Talep Formu 416
EK-7. 38: BGYS Risk Bildirim ve Talep Formu 417
EK-7. 39: Değişiklik İzleme Formu 418
EK-7. 40: Doküman Revizyon Talep Formu 419
EK-7. 41: Tedarikçi Değerlendirme Formu 420
EK-7. 42: Özgeçmiş 421

BİLİMSEL ETİK BİLDİRİMİ

Doktora tezi olarak hazırladığım *Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi ve Bir Rehber Önerisi* adlı çalışmanın öneri aşamasından sonuçlanmasına kadar geçen süreçte bilimsel etiğe ve akademik kurallara özenle uyduğumu, tez içindeki tüm bilgileri bilimsel ahlak ve gelenek çerçevesinde elde ettiğimi, tez yazım kurallarına uygun olarak hazırladığım bu çalışmamda doğrudan veya dolaylı olarak yaptığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu beyan ederim.

19/06/2023

İmza

Ali KAVAK

TEZ KABUL VE ONAY

ÇANKIRI KARATEKİN ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Ali KAVAK tarafından hazırlanan *Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi ve Bir Rehber Önerisi* başlıklı bu çalışma, *19 / 06 / 2023* tarihinde yapılan tez savunma sınavı sonucunda *oybirliğiyle* başarılı bulunarak jürimiz tarafından *Bilgi ve Belge Yönetimi Anabilim Dalı*'nda *Doktora tezi* olarak kabul edilmiştir.

TEZ JÜRİSİ ÜYELERİ (Unvanı, Adı ve Soyadı)

Danışman	: **Prof. Dr. Hüseyin ODABAŞ**	İmza: ……..
Üye	: **Prof. Dr. Coşkun POLAT**	İmza: ……..
Üye	: **Doç. Dr. Tolga Çakmak**	İmza: ……..
Üye	: **Dr. Öğr. Üyesi İlker KARA**	İmza: ……..
Üye	: **Dr. Öğr. Üyesi Emre TOPRAK**	İmza: ……..

ONAY

Bu Tez, Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Kurulunun 08/06/2023 tarih ve 2023/27-04 sayılı oturumunda belirlenen jüri tarafından kabul edilmiştir.

Prof. Dr. Coşkun POLAT

Enstitü Müdürü

ÖNSÖZ

Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi ve Bir Rehber Önerisi konusu, içinde bulunduğumuz dijital çağda üzerinde durulan önemli konulardan biridir. Özelliklede bilginin merkezi ve kütüphaneler için bu konu daha da önemli bir yer tutmaktadır. Bu nedenle, bu kurumların bilgi güvenliğini sağlama ve koruma konularında etkili yönetim stratejilerine sahip olmaları büyük önem arz etmektedir.

Bu çalışma ile üniversite kütüphanelerindeki bilgi güvenliği yönetiminin mevcut durumu ve eksiklikleri incelenmektedir. Ayrıca, üniversite kütüphanelerinde bilgi güvenliği yönetimine ilişkin kurumsal ve teknolojik uygulamaların durumu tespit edilmektedir. Bu inceleme ve tespitler çerçevesinde çalışma, üniversite kütüphanelerinin bilgi güvenliği yönetimine önemli katkılar sunmaktadır.

Çalışma ile üniversite kütüphanelerinde bilgi güvenliği yönetimi konusunda farkındalık düzeyi, bilgi güvenliği tehditleri ve bu tehditlere karşı belirlenen teknik ve kurumsal önlemlerin düzeyi belirlenerek bu alanda yapılacak çalışmalara ve kütüphanecilik camiasındaki bilgi güvenliği yönetim çalışmalarına katkı sağlanması amaçlamaktadır.

Bu çalışmanın hazırlanması sürecinde Türkiye'de üniversite kütüphanelerinde görev yapan alanında uzman birçok kişinin bilgi ve görüşlerinden yararlanılmıştır. Onlardan elde edilen veriler çerçevesinde konuya ilişkin önemli bulgular ve çıkarımlar elde edilmiştir. Bu bakımdan çalışmanın üniversite kütüphanelerinde bilgi güvenliği yönetimi konusundaki farkındalık düzeyini geliştirmesi, bilgi güvenliğine yönelik daha etkin önlemlerin alınması ve üniversite kütüphaneleri hizmetlerinin daha güvenli bir şekilde yürütülmesi yönleriyle de kütüphanecilik camiasına önemli katkılar sunması beklenmektedir. Ayrıca çalışma kapsamında hazırlanan "Bilgi Güvenliği Yönetim Sistemi Rehberi"nin de bilgi merkezinin bilgi güvenliği yönetim hizmetlerinin planlanması ve yürütülmesi bakımından önemli bir yol haritası olması düşünülmektedir.

Bu itibarla, çalışmanın araştırmacılara ve okuyuculara faydalı ve bilgilendirici olmasını dilerim.

Çalışmanın tamamlanma sürecinde hoşgörüsünü, sabrını, ilgisini, bilgisini ve desteğini hiçbir zaman esirgemeyen çok kıymetli hocam ve tez danışmanım *Prof. Dr. Hüseyin Odabaş*'a; bu zorlu süreçte bilgi ve tecrübeleri ile çalışmama değer katan, desteklerini hiç esirgemeyen tez izleme komitesi üyeleri hocalarım *Doç. Dr. Tolga Çakmak ve Dr. Öğr. Üyesi İlker KARA*'ya; tez savunma jürimde bulunarak bilgi ve tecrübeleri ile çalışmama değerli katkılar sunan *Prof. Dr. Coşkun POLAT* ve *Dr. Öğr. Üyesi Emre TOPRAK* hocalarıma teşekkürlerimi sunarım.

Çalışmanın çeşitli aşamalarında görüş ve önerileriyle katkı sunan akademi ve kütüphane camiasında görev yapan akademisyen ve kütüphaneci dostlarıma; manevi desteklerinden ötürü sevgili eşim Dilek'e, canım oğlum Yiğit Efe'ye ve biricik kızım Elanur'a şükranlarımı sunarım.

19/06/2023

Ali KAVAK

ÖZET

Tezin Başlığı : Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi ve Bir Rehber Önerisi

Tezin Yazarı : Ali KAVAK

Danışman : Prof. Dr. Hüseyin ODABAŞ

Anabilim Dalı : Bilgi ve Belge Yönetimi

Tezin Türü : Doktora

Kabul Tarihi : 19/06/2023

Bilgi merkezleri arasında özgünlükleriyle öne çıkan üniversite kütüphaneleri, bünyelerindeki bilgi varlıklarında kurumsal ve kişisel birçok veri ve bilgiyi barındırmaktadır. Bu nedenle üniversite kütüphanelerinde bilgi varlıklarının güvenliği önemli bir konudur. Bu itibarla araştırmanın amacı, üniversite kütüphanelerinde bilgi güvenliği yönetimi konusunda mevcut durumu ve olası tehditleri incelemek, uygun önlemler ve politikalar önermek ve bu yönetimin iyileştirilmesi için çözüm önerileri sunmaktır.

Araştırmada, nicel araştırma modeli olan tarama yöntemi kullanılmıştır. Araştırmanın evreni Türkiye'de faaliyet gösteren üniversite kütüphanelerinde görev yapan personeldir. Amaçlı örnekleme yöntemi ile bu evren içerisinde belirlenen örnekleme anket uygulaması gerçekleştirilmiştir. Katılımcılardan elde edilen verilere göre, Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin çoğunun "iyi" düzeyde uygulandığına ilişkin katılımcı görüşlerinin yüksek oranlarda olduğu görülmüştür. Fakat bu önlemlerin "hiç uygulanmadığını" veya "kötü" ve "orta" düzeylerde uygulandığını belirten katılımcı görüşlerinin oranlarının da kayda değer düzeylerde olduğu belirlenmiştir. Bu nedenle, üniversite kütüphanelerinde daha etkili ve standart bir bilgi güvenliği yönetim sisteminin oluşturulmasına katkı sağlaması amacıyla çalışma sonunda bir "Bilgi Güvenliği Yönetim Sistemi Rehberi" önerisi sunulmuştur.

Anahtar Kelimeler: Üniversite Kütüphaneleri, Bilgi Güvenliği Yönetimi, Bilgi Güvenliği Rehberi, Kurumsal ve Kişisel Bilgi Güvenliği

ABSTRACT

Thesis Title : Information Security Management in University Libraries and a Guide Proposal

Author : Ali KAVAK

Supervisor : Prof. Dr. Hüseyin ODABAŞ

Department : Information and Records Management

Thesis Type : Ph.D. Dissertation

Date : 19/06/2023

University libraries, distinguished among information centers with their uniqueness, house a multitude of institutional and personal data and information within their information assets. Therefore, ensuring the security of information assets is a crucial issue in university libraries. In this regard, the aim of the research is to examine the current state and potential threats of information security management in university libraries, propose appropriate measures and policies, and provide solutions for improving this management.

The research utilizes a quantitative research model called the scanning method. The population of the study consists of personnel working in university libraries operating in Turkey. Through purposive sampling, a survey was conducted on the determined sample within this population. According to the data obtained from the participants, it is observed that the majority of technological and institutional information security measures in university libraries in Turkey are perceived to be implemented at a "good" level by the participants. However, it was also determined that there were notable percentages of participants who indicated that these measures were "not implemented at all" or implemented at "poor" and "moderate" levels. Therefore, at the end of the study, a "Information Security Management System Guide" is proposed to contribute to the establishment of a more effective and standardized information security management system in university libraries.

Keywords: University Libraries, Information Security Management, Information Security Guide, Corporate and Personal Information Security

KISALTMALAR

ACRL	Association of College ve Research Libraries
ALA	American Library Association
ANSI	American National Standards Institute
BGYS	Bilgi Güvenliği Yönetim Sistemi
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
COBIT	Control Objectives for Information and Technology
ETSI	European Telecommunications Standard Institute
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IBM SPSS	International Business Machines Statistical Package Social Sciences
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFLA	International Federation of Library Associations
ISACA	Information Systems Audit and Control Association
ISF	Information Security Forum
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITAF	Information Technology Assurance Framework
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
LAN	Local Area Network
LISTA	Library, Information Science veTechnology Abstracts
MAN	Metropol Area Network
NIST	National Institute of Standards and Technology
PAN	Personal Area Network
TSE	Türk Standartları Enstitüsü
W3C	World Wide Web Consortium
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language

TABLO LİSTESİ

Tablo No: **Sayfa**

Tablo 1.1: Türkiye'de üniversitelerin kütüphane sayıları 21

Tablo 1.2: Katılımcılara ilişkin demografik bilgiler 22

Tablo 2.1: Bilgi güvenliğinin gelişimindeki önemli tarih ve gelişmeler..... 67

Tablo 3.1: Bilgi güvenliği hizmetleri ve saldırıları 98

Tablo 3.2: Tehdit sınıflandırmaları 101

Tablo 3.3: Yaygın güvenlik politikası zayıflıkları 112

Tablo 3.4: Ağları etkileyen teknoloji zayıflıkları..... 113

Tablo 3.5: Ağları etkileyen yapılandırma zayıflıkları..... 113

Tablo 3.6: Temel güvenlik önlemleri..... 126

Tablo 6.1: Katılımcılara ait demografik bilgiler 181

Tablo 6.2: Üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personel 183

Tablo 6.3: Üniversite kütüphanelerinde bilgi sistemlerinin dağılımı..... 185

Tablo 6.4: Bilginin kritikliği açısından bilgi sistemlerinin önemi 186

Tablo.6.5: Bilgi güvenliği unsurlarının bilginin kritikliğine etkisi 188

Tablo 6.6: Bilgi güvenliği ihlallerinin etki alanları üzerindeki durumu 189

Tablo 6.7: Üniversite kütüphanelerindeki yaygın bilgi güvenliği tehditleri 191

Tablo 6.8: Üniversite kütüphanelerinde yaygın bilgi güvenliği tehdit kategorileri 192

Tablo 6.9: Donanım güvenliği önlemlerinin uygulama düzeyleri 195

Tablo 6.10: Yazılım güvenliği önlemlerinin uygulanma düzeyleri 198

Tablo 6.11: Ağ güvenliği önlemlerinin uygulanma düzeyleri 201

Tablo 6.12: Veri güvenliği önlemlerinin uygulanma düzeyleri 204

Tablo 6.13: Fiziksel ve çevresel güvenlik önlemlerinin uygulanma düzeyleri..... 208

Tablo 6.14: Katılımcıların görev yaptıkları üniversitelerin türüne göre donanım önlemlerinin uygulanma düzeyleri..... 211

Tablo 6.15: Katılımcıların görev yaptıkları üniversitelerin türüne göre yazılım önlemlerinin uygulanma düzeyleri 212

Tablo 6.16: Katılımcıların görev yaptıkları üniversitelerin türüne göre ağ önlemlerinin uygulanma düzeyleri 213

Tablo 6.17: Katılımcıların görev yaptıkları üniversitelerin türüne göre veri önlemlerinin uygulanma düzeyleri 214

Tablo 6.18: Katılımcıların görev yaptıkları üniversitelerin türüne göre fiziksel ve çevresel önlemlerin uygulanma düzeyleri 216

Tablo 6.19: Bilgi güvenliğinden sorumlu personelin varlığına göre donanım önlemlerinin uygulanma düzeyleri 218

Tablo 6.20: Bilgi güvenliğinden sorumlu personelin varlığına göre yazılım önlemlerinin uygulanma düzeyleri 219

Tablo 6.21: Bilgi güvenliğinden sorumlu personelin varlığına göre ağ önlemlerinin uygulanma düzeyleri 220

Tablo 6.22: Bilgi güvenliğinden sorumlu personelin varlığına göre veri önlemlerinin uygulanma düzeyleri 221

Tablo 6.23: Bilgi güvenliğinden sorumlu personelin varlığına göre fiziksel ve çevresel önlemlerin uygulanma düzeyleri 223

Tablo 6.24: Bilgi güvenliği yönetim aracının kullanımına göre donanım önlemlerinin uygulanma düzeyleri 225

Tablo 6.25: Bilgi güvenliği yönetim aracının kullanımına göre yazılım önlemlerinin uygulanma düzeyleri 226

Tablo 6.26: Bilgi güvenliği yönetim aracının kullanımına göre ağ önlemlerinin uygulanma düzeyleri 227

Tablo 6.27 :Bilgi güvenliği yönetim aracının kullanımına göre veri önlemlerinin uygulanma düzeyleri 229

Tablo 6.28: Bilgi güvenliği yönetim aracının kullanımına göre fiziksel ve çevresel önlemlerin uygulanma düzeyleri 231

Tablo 6.29: Bilgi güvenliği politikalarının uygulanma düzeyleri 235

Tablo 6.30: Bilgi güvenliği prosedürlerinin uygulama düzeyleri 239

Tablo 6.31: Bilgi güvenliği idari araç ve yöntemlerinin uygulama düzeyleri 242

Tablo 6.32: Bilgi güvenliği farkındalık çalışmalarının uygulama düzeyleri 244

Tablo 6.33: Katılımcıların görev yaptıkları üniversitelerin türüne göre bilgi güvenliği politikalarının uygulanma düzeyleri 247

Tablo 6.34: Katılımcıların görev yaptıkları üniversitelerin türüne göre bilgi güvenliği prosedürlerinin uygulanma düzeyleri 249

Tablo 6.35: Katılımcıların görev yaptıkları üniversitelerin türüne göre bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeyleri 250

Tablo 6.36: Katılımcıların görev yaptıkları üniversitelerin türüne göre bilgi güvenliği farkındalık çalışmalarının uygulanma düzeyleri 251

Tablo 6.37: Bilgi güvenliğinden sorumlu personelin varlığına göre bilgi güvenliği politikalarının uygulanma düzeyleri 253

Tablo 6.38: Bilgi güvenliğinden sorumlu personelin varlığına göre bilgi güvenliği prosedürlerinin uygulanma düzeyleri 255

Tablo 6.39: Bilgi güvenliğinden sorumlu personelin varlığına göre bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeyleri 256

Tablo 6.40: Bilgi güvenliğinden sorumlu personelin varlığına göre bilgi güvenliği farkındalık çalışmalarının uygulanma düzeyleri 257

Tablo 6.41: Bilgi güvenliği yönetim aracının kullanımına göre bilgi güvenliği politikalarının uygulanma düzeyleri 259

Tablo 6.42: Bilgi güvenliği yönetim aracının kullanımına göre bilgi güvenliği prosedürlerinin uygulanma düzeyleri 261

Tablo 6.43: Bilgi güvenliği yönetim aracının kullanımına göre bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeyleri 262

Tablo 6.44: Bilgi güvenliği yönetim aracının kullanımına göre bilgi güvenliği farkındalık çalışmalarının uygulanma düzeyleri 263

Tablo 7.1: BGYS planlama çizelgesi 292
Tablo 7.2: Tehdit olasılık değerleri 297
Tablo 7.3: Toplam risk değerleri 298
Tablo 7.4: Risk dereceleri 298
Tablo 7.5: Risk işleme planı 299
Tablo 7.6: Uygulanabilirlik durum çizelgesi 301
Tablo 7.7: BGYS doküman şablonu 302
Tablo 7.8: Doküman türlerinin kısaltılmış tür kodları listesi 303
Tablo 7.9: BGYS dokümanları dağıtım çizelgesi 304
Tablo 7.10: BGYS dokümanları saklama süreleri çizelgesi 304
Tablo 7.11: BGYS dokümanları revizyon takip çizelgesi 304
Tablo 7.12: Bilgi güvenliği önlem kontrol listesi 305
Tablo 7.13: İç denetim dokümanları 309
Tablo 7.14: İç denetim planı 309
Tablo 7.15: Uygunsuzluk türleri 311

ŞEKİL LİSTESİ

Şekil No: **Sayfa**

Şekil 1.1: Kütüphane bilgi güvenliği değerlendirme modeli 20

Şekil 1.2: Anket geliştirme süreci 24

Şekil 2.1: Varlık yönetim süreci 36

Şekil 2.2: Bilgi sistemini elemanları 45

Şekil 2.3: Verinin bilgiye dönüşüm süreci 48

Şekil 2.4: Bilgi güvenliği süreç destekleri 53

Şekil 2.5: Bilgi güvenliği ilkeleri 61

Şekil 2.6: Bilgi güvenliği ihlalleri 61

Şekil 2.7: Güvenlik alanları 73

Şekil 2.8: Bilgi güvenliği yönetim araçları 74

Şekil 3.1: Çok boyutlu tehdit sınıflama modeli 100

Şekil 3.2: Bilgi güvenliği tehditleri 105

Şekil 3.3: Yazılım uygulama güvenliğinin unsurları 109

Şekil 3.4: Bilgi güvenliğinin birincil katmanları 119

Şekil 3.5: CERT güvenlik yaşam döngüsü 123

Şekil 3.6: Bilgi güvenliği politikası işlem süreci 141

Şekil 4.1: PUKÖ döngüsü 152

Şekil 4.2: PUKÖ ile BGYS süreçlerinin etkileşimi 154

Şekil 7.1: Kütüphane bilgi güvenliği yönetim distemi PUKÖ döngüsü 286

Şekil 7.2: BGYS organizasyon şeması 289

Şekil 7.3: Varlık yönetim süreci 294

Şekil 7.4: Bilgi varlıklarının kritiklik derecesine etki eden unsurlar 295

Şekil 7.5: Doküman numarası örneği 303

1. GİRİŞ

1.1. Konunun Kavramsal Boyutu

Güvenlik, "toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" (Türk Dil Kurumu, 2021) olarak tanımlanmaktadır. Bu kavram, bir varlığın tehlikelerden uzak olma niteliğini ve durumunu kapsamaktadır. Diğer bir ifadeyle güvenlik, bir nesneyi veya varlığı kasıtlı veya kasıtsız, doğrudan veya dolaylı her türlü tehlikeden korumayı amaçlamaktadır. Güvenliğe duyulan ihtiyaç varlığın içinde bulunduğu faaliyet alanına ve büyüklüğüne göre şekillenmektedir. Örneğin bir devlet halkını, kaynaklarını ve tüm diğer varlıklarını korumak için çok katmanlı ulusal bir güvenlik sistemine ihtiyaç duyarken, bir kurum veya kuruluş ise varlıklarını zararlı unsurlardan korumak için farklı güvenlik işlevlerine sahip güvenlik sistemlerine ihtiyaç duyabilmektedir. Çevresel ve fiziksel güvenlik, kurumsal güvenlik, iletişim ve haberleşme güvenliği, personel güvenliği, ağ güvenliği ve bilgi güvenliği gibi birçok farklı güvenlik sisteminin işler duruma getirilmesi kurumun sürekliliği açısından önemli görülmektedir (Whitman ve Mattord, 2011).

Bilgi, insanın çevresindeki nesneleri ve varlıkları yorumlaması, açıklaması veya yargılaması sonucu oluşan bir üründür. İnsan ile nesne arasında kurulan ilişkiden doğan bilgi, insanlık tarihinin en önemli sermayesi olarak görülmektedir. Bu sermayeyi gelecek kuşaklara sağlıklı biçimde aktarırken mahremiyetlerini korumak kurumsal ve kişisel bağlamda insanlık adına sorumluluk isteyen önemli bir ihtiyaçtır. Bu nedenle veri ve bilgilerin gizlilik, bütünlük ve erişilebilirlik unsurları çerçevesinde korunması önemlidir. Geçmişte bilginin güvenliğine yönelik birtakım önlemler geliştirildiği görülse de günümüzde bu konu üzerinde daha çok durulmaktadır. Gelişmiş ve gelişmekte olan toplumların son yıllarda toplumsal ve kurumsal yapılarında bilgi güvenliğine yönelik çalışmalara daha da önem verdiği anlaşılmaktadır. Teknolojik gelişmelere bağlı olarak kişisel ve kurumsal bilgilerin güvenliğine yönelik artan açıklar kontrol edilemez hale gelmiştir. Bu durum, bilgi güvenliğine yönelik çalışmaların artmasını sağlamıştır. Özellikle bilgi güvenliği yönetim sistemlerine yönelik çalışmalar kurum ve kişilerin üzerinde önemle durdukları bir süreç haline gelmiştir.

Bilgisayar ve ağ teknolojilerindeki gelişmeler, bilginin üretildiği, korunduğu ve iletildiği ortamları da değişikliğe uğratmıştır. Özellikle son yıllarda elektronik ortamlar, bilginin en çok işlendiği ortamlar olmuştur. Bu gelişmeler, bilginin coğrafi ve fiziksel sınırlarını kaldırarak bilgiyi zaman ve mekândan bağımsız bir varlık haline getirdi. Değeri gün geçtikçe daha da artan bilgi, bir güç unsuru olarak devletlerin ve kurumların hatta bireylerin sahip olmak istediği önemli bir varlık durumuna gelmiştir. Bilginin gücüne inanan ve bu gücü kullanmak isteyen kişi ve kurumlar, bilişim ve iletişim teknolojilerine hızlı bir biçimde entegre olarak bu araçları hizmetlerine daha ileri düzeylerde değer katmak için kullanmaya başladılar. Bunula birlikte bu gücün güvenliğini sağlamanın bir gereksinim olduğunu görenler bu gücü güvenilir kılma arayışı içine de girdiler. Bilişim teknolojileri ile doğrudan temas halinde olan sektörler ve bu sektörlere paydaş disiplinler bilgi güvenliği çalışmaları ve uygulamaları konusunda önemli mesafeler aldılar. Bu nedenle bilgisayar ve ağ teknolojileri, bilgi güvenliği çalışmalarının temel yapı taşlarını oluşturmaktadır (Evrin ve Demirer, 2011).

Bilgi güvenliği, en genel ifade ile bilginin izinsiz veya yetkisiz bir biçimde erişiminin, kullanımının, değiştirilmesinin, ifşa edilmesinin, ortadan kaldırılmasının ve hasar verilmesinin önlenmesi olarak tanımlanmaktadır. Gizlilik, bütünlük ve erişilebilirlik, bilgi güvenliğinin vazgeçilmez üç temel unsurunu oluşturmaktadır. Bu üç temel güvenlik unsurundan herhangi birinin zarar görmesi bilgi güvenliği zafiyetinin varlığına işaret eder (Güngör, 2015; Marttin ve Pehlivan, 2010; Slade, 2006).

Kurumlar, faaliyetlerinde meydana gelebilecek olası olumsuzlukları azaltmak ve iş sürekliliklerini ve başarılarını arttırmak için kendileri için önem taşıyan verileri / bilgileri en iyi bir biçimde korunma ihtiyacı duymaktadırlar. Kurumlar, hizmetlerinin ve örgütsel yapılarının sürekliliği açısından önem taşıyan bilgileri tüm tehditlerden ve güvenlik açıklarından korumak için bilgi güvenliği konusunda koruma uygulamaları ve yöntemleri geliştirmektedirler. Sürdürülebilir bir iş politikası amaçlayan kurumlar, varlıklarının devamlılığını sağlamak; kişisel, kurumsal ve paydaşlara ait bilgilerinin mahremiyetini korumak için bilgi varlıklarını iç ve dış tüm tehditlere karşı korunmak zorundadır.

Whitman ve Mattord (2018), bilgi güvenliğinin bir kurumda dört ana görevi üstlendiğini belirtmektedir. Bunları; kurumun faaliyetlerini yürütebilme yeteneğinin korunması, kurumun bilgi sistemlerinde çalışan uygulamalarının performanslarının sağlanması, kurumun teknoloji varlıklarının korunması ve bu varlıklarda üretilen, işlenen ve depolanan verilerin korunması olarak özetlemektedir.

Bilgi güvenliği, bütün kurumlarda olduğu gibi kütüphanelerde ve diğer bilgi merkezlerinde de önemli bir konudur. Bilgi, kütüphane hizmetlerinin temelini oluşturan en önemli varlıktır; güvenliğine önemi nispetince değer verilmeli, güvenilir yöntemler ile yönetilmelidir. Kütüphanelerde bilgi güvenliğinin başarısı yöneticilerin, personelin, kullanıcıların ve diğer paydaşların nitelikli bilgi güvenliği farkındalığına ve bilincine sahip olmalarından geçmektedir. Bu başarıda en önemli rol hiç şüphesiz yöneticilere düşmektedir. Bilgi güvenliğinin ihmal edilmesi, kütüphane hizmetlerinin aksamasına ve telafi edilmesi uzun zaman alabilecek olumsuz sonuçlara yol açabilmektedir. Özellikle teknolojik araçların kütüphane hizmetlerinde daha yaygın olarak kullanılması, bilgi güvenliği yönetimine olan ihtiyacı daha da artırmaktadır (Pathari ve Sonar, 2012).

Bilişim ve iletişim teknolojilerinin hızlı gelişimi, kütüphanelerde kullanılan teknolojik araçların sayısını artırmış ve bu durum kütüphanelerin sahip olduğu bilgi varlıklarına ve bu varlıklar üzerinde kayıtlı veri ve bilgilere yönelik daha fazla güvenlik tehdidi üretmiştir. Bu nedenle bilgi varlıklarına işlenen bilgilerin korunması ve kullanıcılara güvenli bir biçimde iletilmesi giderek zorlaşmaktadır. Kullanıcıların ihtiyaç duyduğu bilgileri karşılamada önemli rol oynayan kütüphaneler, kullandığı ve kullanacağı yeni teknolojik araçlara bağlı olarak hizmetlerinde ve kurumsal yapısında sürekli olarak değişim yaşamaktadır. Bu değişim kütüphanelerin bilgi güvenliği anlayışını da değişime mecbur kılmıştır. Teknolojik bilgi sistemlerinin yoğun bir biçimde kullanılmaya başlanması ile dijital bilgi güvenliği, kütüphaneler için yükselen çalışma alanlarından biri olmuştur. Özellikle kütüphanelerde kullanılmaya başlayan çevrimiçi bilgi sistemleri ile sunulan hizmetlerin daha çok tercih edilmesiyle birlikte birçok güvenlik riski de yaşanmaya başlamıştır. Yüksek maliyetler ile satın alınan bilgi kaynaklarının yanı sıra kurumsal ve kişisel birçok önemli verinin depolandığı bilgi sistemleri, olası tehditlere ve saldırılara maruz kalmaktadır (Da Veiga ve Eloff, 2010; Gillaspy, 2005). Bu tehdit ve saldırıların en az

kayıp ile giderilebilmesi için iyi bir kurumsal bilgi güvenliği yönetim sisteminin geliştirilmesi, uygulanması, değerlendirilmesi ve sürekli olarak iyileştirilmesi gerekmektedir.

Bilgi güvenliğine yönelik tehditlerin genellikle kurumsal bilgi güvenliği yönetimindeki bilgisizlik ve eksikliklerden kaynaklandığı bilinmektedir. Hizmetlerinin çoğunu bilgi sistemleri aracılığıyla yürüten kütüphanelerin bilgi varlıklarına karşı olası saldırılardan korunması amacıyla bilgi güvenliği ile ilgili gelişmeleri sürekli takip etmeleri, kütüphane yöneticilerine ve personeline yönelik bilgi güvenliği farkındalığı ve becerilerini geliştirici çalışmaları yürütmeleri ve ulusal veya uluslararası standartlara uygun bir bilgi güvenliği yönetim sistemini geliştirmeleri gerekmektedir. Kurumsal bilgi güvenliği yönetimi ile üçlü bir bilgi güvenliği kültürü oluşturulur. Bu nedenle kütüphanelerde yöneticilerin tüm personeli ile birlikte kurumsal bilgi güvenliği yönetimi üzerinde önemle durması gerekir (Amini ve diğerleri, 2021; Ismail, 2012; Peltier, 2016; Thomson ve diğerleri, 2006; Workman ve diğerleri, 2008).

Kütüphane bilgi güvenliği yönetim sistemi, bilgi varlıklarının gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması ve bilgi varlıklarının tüm potansiyel tehlikelerden korunması için gereken kontrolleri içermektedir. Kütüphanenin ana kaynakları, personel ve kullanıcı bilgileri, ödünç kayıtları, veritabanı abonelik bilgileri, şifreleri, e-posta adresleri, web sitesi verileri ve kütüphane bilgi sistemleri içerisinde kayıtlı diğer tüm veriler kütüphanelerde korunması gereken bilgi varlıklarını oluşturmaktadır. Bilgi güvenliği yönetiminin uygun güvenlik kontrolleri ile yürütülmemesi, kütüphanelerdeki bu bilgi varlıklarını olası tehditlere maruz bırakmaktadır. Bu durum kütüphanenin kurumsal güvenliğini zafiyete düşürebileceği gibi kütüphane paydaşlarının kişisel güvenliğini de olumsuz etkileyebilir. Daha da önemlisi devletin kamu güvenliğini de zor duruma düşürebilir. Bu nedenle kütüphanelerde uygulanmak üzere uluslararası bilgi güvenliği standartlarına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS)'nin geliştirilmesi önemli bir ihtiyaçtır.

Bilgi, güvenlik, sistem, bilgi güvenliği, bilgi güvenliği yönetimi, bilgi sistemleri, güvenlik politikaları, bilgi güvenliği yönetim sistemleri, bilgi güvenliği standartları, yönergeleri, rehberleri ve prosedürleri, kütüphane bilgi sistemleri, kütüphane güvenlik uygulamaları, güvenlik tehditleri ve önlemleri gibi kavramlar bu

araştırmanın ana omurgasını oluşturan temel terimlerdir. Bu terimler kullanılarak YÖK Tez Merkezi, Türkiye Akademik Arşivi TR Dizin, Harman, Dergi Park, Bilgi Dünyası, Türk Kütüphaneciliği, Springer, Taylor and Francis, Academic Search Ultimate, Business Source Ultimate, ProQuest Dissertations veTheses Global, Cambridge Journals Online, China STM Focus, Emerald Premier eJournal, JSTOR,Informs PubsOnline, MasterFILE Complete, OECD iLibrary, Oxford University Press Journals, Sage Journals Online, Project MUSE, Science Direct, Scopus, Web of Science, WorldCat, Wiley Online Library, İdealonline, Hiperkitap, EBSCO e-Book Collection, ACLS Humanities E-Book, IGI Global e-Books, OECD iLibrary, ProQuest Ebook Central, Springer e-Books, Wiley e-Books, Library, Information Science veTechnology Abstracts (LISTA), Google Akademik, Academia, ResearchGate, IFLA, ALA, ACRL gibi alanda yetkin ulusal ve uluslararası platformlarda alanyazın taraması yapılmıştır. Alanyazın taramasından çalışma konusuna doğrudan veya dolaylı olarak katkı sağlayacağı düşünülen bilimsel kitaplar, tezler, raporlar, bildiriler ve makaleler gibi basılı birincil kaynaklar ile elektronik ortamdaki bilgi kaynaklarına erişim sağlanmıştır.

Her disiplinin uygulama sahasında ele alınan bir uğraş alanı olması nedeniyle bilgi güvenliği konusu ile ilgili akademik camiada geniş bir alanyazının oluştuğu görülmüştür. Buna karşın kütüphanecilik alanı özelinde bu konuya ilişkin çalışmaların yeterli olmadığı fark edilmiştir. Bu nedenle kurumsal bilgi güvenliğine ilişkin diğer disiplinlerde tamamlanmış çalışmalar daha detaylı incelenmiş; bilişim ve iletişim alanlarında hizmet veren kurumların bilgi güvenliğine yönelik oluşturulan çalışmalar üzerinde daha dikkatle durulmuştur. Ayrıca bilgi güvenliğine ilişkin oluşturulmuş standart, model ve rehberler örnek alınarak çalışmanın temel yapısı oluşturulmuştur.

Dünya çapında ulusal standart kuruluşlarının federasyonu olan Uluslararası Standartlar Organizasyonu (ISO) tarafından yayımlanmış “ISO/IEC 27000 Bilgi Güvenliği Standartları” ve diğer uluslararası standart örgütlerinin yayımladığı standartlar, John McCumber’ın geliştirdiği bilgi güvenliği modeli ile ilgi çalışmalar (1991; 2004), Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin hazırlamış olduğu “Bilgi ve İletişim Güvenliği Rehberi” (2020), TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Enstitüsünün hazırladığı “Bilgi Güvenliği

Yönetimi Rehberi: İşletim ve Bakım" (2021), Roesnita Binti Ismail'in akademik kütüphanelerde bilgi güvenliği yönetimine ilişkin çalıştığı "Assessing Information Security Management in Malaysian Academic Libraries" (2012) doktora tezi bu araştırmaya özellikle ampirik verilerin derlenmesi ve değerlendirilmesine doğrudan katkı sağlayan kaynaklardır. Ayrıca International Federation of Library Associations (IFLA) ve American Library Association (ALA) gibi kütüphanecilik alanında faaliyet gösteren önde gelen kuruluşlar trafından bilgi güvenliği ile ilgili doğrudan ve dolaylı olarak bilgi veren belgelerde incelenmiştir.

Bu temel kaynakların yanı sıra konuya ilişkin birçok araştırmanın olduğuda tespit edilmiştir. Türkiye'de farklı hizmet sektörlerinin kurumsal bilgi güvenliği yönetimine ilişkin farklı yöntemler ile hazırladığı bir takım araştırmalar yapılmıştır. (Akdoğan, 2022; Elattresh, 2022; Meral, 2022; Yıldız, 2022; Eren, 2021; Demirok, 2016; Henkoğlu, 2015; Güngör, 2015; Muharremoğlu, 2013; Vural ve Sağiroğlu, 2013; Haklı, 2012; Gemci, 2010; Gülmüş, 2010; Marttin ve Pehlivan, 2010; Mete, 2010; Takçı ve diğerleri, 2010; Tok, 2010; Şahinaslan ve diğerleri, 2009; Çetinkaya, 2008). Özellikle telekomünikasyon ve bankacılık gibi sektörlerin hizmetlerinde ve altyapılarında bilişim teknolojilerinden daha yoğun yararlanılması nedeniyle bu alanlara yönelik bilgi güvenliği yönetimine ilişkin çalışmaların daha yaygın olduğu bilinmektedir. Ayrıca son yıllarda sağlık, hukuk ve finans gibi farklı kamu sektörlerinde de kurumsal bilgi güvenliği yönetimi konusunda çokça araştırmaların yapıldığı gözlemlenmektedir (Çimen, 2021; Filik, 2020; Gürsel, 2019; H. Ö. Kurt, 2019; S. G. Kurt, 2019; Başdinkçi, 2017; Erol, 2016; Aksu, 2014; Şahinaslan, 2010). Bu duruma etki eden en önemli neden bu kurumlarda işlenen veri ve bilgilerin değerinden kaynaklanmaktadır.

Gelişmiş ülkelerde kurumsal bilgi güvenliği ile ilgili araştırmaların ülkemize göre daha erken dönemlerde yapılmaya başladığı ve Türkiye'de bu konunun daha çok kişisel bilgi güvenliği ile birlikte popülerlik kazandığı görülmektedir. Bu nedenle Türkiye'de kurumsal bilgi güvenliği yönetimi ile ilgili çok sayıda araştırma bulunmamakla birlikte, tamamlanan araştırmaların daha çok sağlık, bilişim ve iletişim gibi belirli hizmet sektörlerinde yoğunlaştığı görülmektedir. Kütüphaneler ve diğer bilgi merkezlerinde kurumsal bilgi güvenliği yönetimine ilişkin araştırmaların ise az sayıda olduğu anlaşılmaktadır (Şişkin, 2020; Henkoğlu ve Uçak, 2015;

Öztemiz ve Yılmaz, 2013). Bu durum kütüphane hizmetlerinde yararlanılmakta olan bilgi varlıklarına yönelik riski düzeyinin durumu hakkında belirsizliğin oluşmasına neden olmakta; kişisel, kurumsal ve paydaşlar açısından kritik öneme sahip bilgilerin açığa çıkma olasılığının varlığına işaret etmektedir.

Araştırmada öncelikli olarak araştırmanın kuramsal yapısını oluşturan bilgi güvenliği yönetimine ilişkin varlıklar, bilgi sistemleri tehdit türleri ve kaynakları, bu tehdit türlerine karşı alınacak teknolojik (donanım, yazılım, iş istasyonu, ağ, veri, çevre güvenliği gibi teknik boyutlar) önlemler ile kurumsal (bilgi güvenliği politikası, prosedürleri, araç ve yöntemleri gibi süreç boyutlar) önlemler, bilgi güvenliği yönetim sistemi, bilgi güvenliği değerlendirme modelleri, kriterleri, paketleri ve standartları ve üniversite kütüphanelerinde bilgi güvenliği ile ilgili bilgiler ayrı bölümler halinde verilmektedir. Çalışmanın, kütüphanelerin bilgi güvenliği yönetimine ilişkin kurumsal ve teknolojik açılardan genel durumu ortaya çıkarması bakımında alanyazına zenginlik katacağı düşünülmektedir. Çalışma sonunda bir öneri olarak kütüphane yöneticileri ve bilgi güvenliği uygulayıcılarının yararlanması için geliştirilen bilgi güvenliği yönetim sistemi rehberi, bu çalışmanın en önemli çıktılarından birini oluşturmaktadır.

1.2. Amaç

Kurumlar, hizmetleri doğrultusunda faaliyetlerini yürütürken aynı zamanda iş süreçleri içerisinde bilgi ve belge üretmeye devam etmektedir. Üretilen bilgi ve belgeler, söz konusu faaliyetlerin doğrulanabilmesi ve hizmetlerin sürekliliği bakımlarından güvenli bir biçimde muhafaza edilmelidir. Kurumlarda hizmetlerin sürdürülebilirliği açısından önemli olan bu bilgi ve belgelerin yetkisiz kişilerin eline geçmesi, birçok surunun oluşmasına neden olabilmektedir. Bu nedenle pek çok kurum, hizmetlerinin devamlılığı ve kurumsal itibarları açılarından bilgi sistemlerinde veya fiziksel ortamlarda işledikleri bilgi ve belgelerin gizliliğini, bütünlüğünü ve erişilebilirliğini garanti altına almak için “bilgi güvenliği yönetimi” yaklaşımını önemsemektedir. Özellikle iletişim ve bilgi teknolojilerindeki gelişmelere bağlı olarak ön plana çıkan bilgi güvenliği yönetimi, kurumlar açısından daha da önem arz etmektedir. Gerek kurumsal gerekse kişisel verilerin korunmasında önemli politika ve standartlar içeren bilgi güvenliği yönetimi, günümüzde kurumlar

açısından önemli bir iş süreci olarak sürdürülmektedir. Bilgi hizmetleri sektöründe faaliyet gösteren kütüphaneler açısından değerlendirildiğinde bu konu şüphesiz kamu hizmeti veren diğer kurumlar kadar önemlidir. Bu nedenle kütüphanelerde muhafaza edilen bireysel ve kurumsal bilgilerin kontrollü bir şekilde yönetilmesi kadar bu bilgilerin iyi güvenlik mekanizmaları ile korunması da önemli bir gereksinimdir.

Kütüphaneler, kullanıcılar ile zengin bilgi kaynakları arasında köprü konumundadır. Farklı platform ve kanallarla çeşitli kullanıcı profiline bilgi hizmeti sunmaktadır. Kütüphaneler sahip oldukları bilgileri erişime sunarken ya da diğer kurumlar ile iş birliği sağlarken çeşitli bilgi güvenliği risklerine maruz kalabilmektedir. Özellikle bünyelerindeki bilgi sistemlerine işlenen kurumsal ve kişisel kritik bilgilerin korunması bakımından önemli güvenlik açıklarına maruz kalabilmektedir. Bu nedenle kütüphanelerin bilgi güvenliği risklerini en alt düzeye indirilebilmeleri için iyi bir şekilde planlanmış bilgi güvenliği yönetim sistemini işler duruma getirmeleri gerekmektedir.

Kütüphaneler için bilgi güvenliği yönetim süreci yalnızca bilgilerin toplanması, depolanması, işlenmesi ve dağıtılması sırasındaki gizliliği sağlayan bir mekanizma olarak değerlendirilmemelidir. Çünkü kişisel bilgilerden oluşan kullanıcı ve personel bilgileri de kurumsal bilgiler ile aynı yönetim sürecinde ele alınmalıdır. Bu nedenle, kütüphaneler için bilgi güvenliği, kapsamlı bir şekilde ele alınmalı ve etkili bir bilgi güvenliği yönetim sistemi uygulanmalıdır. Bu sistemin, tüm bilgi varlıklarının korunması, risklerin yönetimi, erişim kontrolü, eğitim ve farkındalık sağlama gibi unsurları kapsaması önemlidir.

Bu bağlamda kütüphanelerde bilgi güvenliği açısından ne gibi sorunlar yaşandığı, bu sorunlara karşı hangi önlemlerin alındığı ve bilgi güvenliği uygulamalarının ne tür prosedür ve standartlar ile ne düzeyde uygulandığının sorgulanması ve araştırılması, kütüphanelerin bireysel ve kurumsal veri ihlali gibi sorunların önlenebilmesi açısından gereklidir. Bu çalışma ile kütüphanelerde etkin bir bilgi güvenliği oluşturabilmek için hangi güvenlik süreçlerinin uygulanması gerektiği, kütüphaneler için fayda sağlayacak bilgi güvenliği standartlarının neler olması gerektiği ve mevcut bilgi güvenliği standartlarının kütüphanelerde neden kullanılması gerektiği gibi pek çok bilgi güvenliği yönetimini kapsayan risk ve iş süreçleri değerlendirilmektedir. Bu itibarla araştırmada kütüphanelerin gerek kurumsal iş süreçlerine yönelik gerekse

kullanıcılarının ve personelinin kişisel bilgilerine yönelik hangi bilgi güvenliği yönetim süreçlerinin planlaması, işletilmesi ve bu konuda hangi standart ve prosedürlerin uygulanması gerektiği üzerinde öneriler sunulmaktadır. Sonuç olarak elde edilen bulgular çerçevesinde ulusal düzeyde kullanılabilecek bir kütüphane bilgi güvenliği yönetim sistemi rehberi sunulmaktadır.

Bu itibarla araştırmanın temel amacı, Türkiye'de üniversite kütüphanelerinin mevcut bilgi güvenliği tehditlerini ve güvenlik açıklarını anlamak, bilgi güvenliği yönetimi ile ilgili uygulanan teknolojik ve kurumsal uygulamaların düzeyini tespit etmek ve bu uygulamaları bir bütün olarak değerlendirerek elde edilen veriler çerçevesinde uygun bir bilgi güvenliği yönetim sistemi rehberi önerisi geliştirmektir. Bu temel amaç doğrultusunda çalışma kapsamında şu alt amaçlara ulaşılması hedeflenmiştir:

- Türkiye'de üniversite kütüphanelerinde yer alan bilgi kaynaklarının depolandığı, aktarıldığı ve işlendiği bilgi varlıklarını ve bu bilgi varlıklarının kritiklik derecesini, işlenen verinin gizlilik, bütünlük ve erişilebilirlik ölçütleri ile bilgi güvenliği ihlallerinin etki alanları açısından tespit etmek;
- Türkiye'de üniversite kütüphanelerinde kullanılan bilgi sistemlerinin durumunu ve bilgi güvenliği açısından önem düzeyini belirlemek;
- Türkiye'de üniversite kütüphanelerinde kurumsal bilgi güvenliği yönetim araçlarının ve bilgi güvenliğinden sorumlu olarak görevlendirilen güvenlik personelinin varlığını belirlemek ve bu iki faktörün bilgi güvenliği yönetimine katkısını incelemek;
- Türkiye'de üniversite kütüphanelerinde algılanan yaygın bilgi güvenliği tehditlerini ve tehdit gruplarını tespit etmek;
- Türkiye'de üniversite kütüphanelerinde uygulanan teknolojik (donanım, yazılım, veri, ağ, fiziksel ve çevresel) ve kurumsal (bilgi güvenliği politikaları, prosedürleri, idari araçları ve farkındalık çalışmaları) güvenlik önlemlerinin uygulanma düzeylerini belirlemek ve bu uygulanma düzeylerinin üniversite türüne, bilgi güvenliği personel varlığına ve kurumsal bilgi güvenliği yönetim aracı kullanım durumuna göre farklılık gösterip göstermediğini belirlemek;

- Türkiye'de üniversite kütüphanelerinde bilgi güvenliği ile ilgili farkındalık düzeyinin durumunu tespit etmek ve bu duruma ilişkin neler yapılması gerektiği hususları üzerinde önerilerde bulunmak;
- Türkiye'de üniversite kütüphanelerinde bilgi güvenliği yönetimine ilişkin uygulanabilir bir bilgi güvenliği yönetim sistemi rehberi önerisinde bulunmaktır.

1.3. Önem

Bilgi ve iletişim teknolojilerindeki gelişmeler kütüphanelerin hizmetlerindeki yapıyı ve sunumları değiştirmektedir. Teknolojik gelişmeler kurumlardaki bilgi ve iletişim sistemlerinin kullanımını daha da arttırmaktadır. Kurumlarda işlenen ve muhafaza edilen bilgiler bilgi sistemleri üzerinden daha çok gerçekleştirilmektedir. Dijitalleşmenin her alanda yoğun bir biçimde hissedildiği günümüzde kütüphaneler de zaman ve mekândan bağımsız bir biçimde hizmet sunmaktadır. Bilgi iletiminde zaman ve mekân olgularının öneminin azalması, hizmetlerini geleneksel yöntemler ile yürüten kütüphaneleri olumsuz etkilemektedir. Bu nedenle kütüphaneler hizmetlerini çağın gereklerine uygun bir biçimde sürdürebilmek için bilgi sistemleri kanallarıyla dijital hizmetlere yönelik çalışmalara hız vermektedir.

Kütüphaneler bilgi ve iletişim teknolojilerini yapılarına hızlı bir biçimde entegre ederken birçok iş ve işlemleri de beraberinde getirmektedir. Geleneksel yöntemlerin yanı sıra dijital bilgi sistemleri ile kullanıcılarına hizmet vermeye başlayan kütüphaneler, bilgi güvenliği açısından yeni sorunlarla karşılaşmakta ve bu sorunların giderilmesi için yeni arayışlar içerisine girmektedirler. Bilgi sistemleri aracılığıyla işlenen, depolanan, aktarılan ve erişilen bilgilerin bütünlüğünün bozulmamasını, gizliliğinin korunmasını ve izinsiz erişilmemesini garanti altına almak için kütüphanelerin nasıl bir bilgi güvenliği yönetiminin uygulanması gerektiğine karar vermesi gerekmektedir.

Kütüphaneler, dijitalleşme ile birlikte birçok güvenlik tehdidine maruz kalabilmektedir. Örneğin dünyanın en eski İncil'inden Dante ve Michelangelo gibi önemli yazarların eserlerine kadar çok sayıda değerli bilgi kaynağına ev sahipliği yapan Vatikan Kütüphanesi, koleksiyonunu dijital ortama aktarma sürecinde birçok siber saldırıya uğramıştır. Kütüphane yönetimi, dijital altyapılarının bilgisayar

korsanları tarafından sürekli tehdit edilmesi nedeniyle başarılı bir saldırı sonucunda belgelerinin çalınabileceği, değiştirilebileceği ve hatta tamamen silinip imha edileceği kaygısıyla yürüttükleri dijitalleşme projesine alanında uzman bir siber güvenlik şirketini dâhil etmiştir (Rudasill ve Moyer, 2004). Kütüphanelere yönelik farklı bir siber saldırı da Hindistan'ın önemli üniversitelerinden biri olan Jawaharlal Nehru Üniversitesinin kütüphane web sitesine yönelik gerçekleştirilmiştir. Bu siber saldırıda ise saldırganlar bilgi sistemlerinde sunulan hizmetleri kesintiye uğratarak kullanıcıları kütüphanenin koleksiyonuna erişimini kısıtlamış, hatta kullanıcılar kütüphanenin web sitesinden saldırganlar tarafından yayınlanan ideolojik sloganlara da maruz kalmışlardır (Pattanaik ve Viswakarma, 2014). Olası benzer sorunlar nedeniyle geniş kullanıcı kitlelerine hizmet sunan kütüphanelerin bilgi sistemlerindeki kurumsal ve kişisel bilgilerin güvenliğini sağlaması zorunlu bir gereklilik olarak görülmektedir. Güvenlik yönetimi yaklaşımı ile tedbir alınmayan bilgi varlıkları ve söz konusu varlıklar üzerinde depolanan veri ve bilgiler, güvenlik açıkları ve tehditleri maruz kalabilme; önemli kayıplar yaşanabilmektedir.

Dünyada kütüphanelerin hizmetleri açısından bilgi güvenliğinin oynadığı hayati rol birçok otorite (IFLA, ACRL, ALA, NIST, ISACA vb.) tarafından kabul edilse de kütüphanecilik alanında yapılan bilgi güvenliği çalışmalarının diğer hizmet alanlarına (sağlık, bankacılık, sigorta, iletişim) nispeten daha az ve yüzeysel olduğu; buna karşın son yıllarda gelişmeler yaşandığı görülmektedir. Bu çalışma, üniversite kütüphanelerinin bilgi sistemlerinde veya fiziksel ortamlarında işlenen bilgi ve verilerin gizlilik, bütünlük ve kullanılabilirlik ölçütleri bakımından ne düzeyde korunduğunun tespit edilmesi ve hangi bilgi güvenliği yöntemlerinin uygulanması gerektiği konusunda önerilerde bulunması açılarından alan yazına önemli bir katkı sağlayacaktır. Sonuç itibariyle söz konusu çalışma ile üniversite kütüphanelerdeki bilgi güvenliği yönetiminin güçlü ve zayıf yönleri belirlenerek bu kurumlarda daha verimli ve güvenli bilgi hizmetlerinin yürütülebilmesi için bilgi güvenliği yönetiminde önceliklerin neler olması gerektiği, ne tür bilgi güvenliği mekanizmalarının geliştirilmesi ve hangi uygulamaların işler haline getirilmesi gerektiği ortaya konulmaktadır.

Türkiye'de üniversite kütüphanelerinin bilgi güvenliği yönetimi ile ilgili mevcut durumun saptandığı ve mevcut duruma ilişkin öneriler getirildiği bu çalışma konu

üzerindeki farkındalığın artmasını sağlayacaktır. Araştırmadan elde edilen bulgular ile Türkiye'de üniversite kütüphanelerinin bilgi güvenliği yönetimi ile ilgili iş süreçlerinin durumu saptanmakta ve söz konusu alanlardaki eksikliklerin görülmesi sağlanmaktadır. Araştırmanın sonuçları, üniversite kütüphanelerinin bilgi güvenliği yönetimi hizmetlerini uluslararası standartlarda yürütebilmeleri ve hizmetlerinde sürekliliği sağlamaları için gerekli bilgileri sunmaktadır. Bu nedenle, bu araştırmanın kütüphaneler için önemi büyüktür ve kütüphanelerdeki bilgi güvenliği konusuna daha fazla odaklanılmasını sağlayacağı düşünülmektedir.

1.4. Araştırma Soruları ve Hipotezler

Araştırma konusunun önemine binaen alanyazında taranan ilgili çalışmalar ve üniversite kütüphanelerinde bilgi güvenliği konulu diğer çalışmalardan elde edilen veriler ışığında araştırmada şu sorulara yanıtlar aranmaktadır:

1. Türkiye'de üniversite kütüphanelerinde kullanılan bilgi sistemleri ve bu sistemlerin bilginin kritikliği açısından korunmasının önemi nedir?
2. Bilgi varlıklarında işlenen veya depolan kritik verilerin veya bilgilerin kritiklik derecesine etki eden faktöreler nelerdir?
3. Türkiye'de üniversite kütüphanelerinde algılanan yaygın bilgi güvenliği tehditleri nelerdir ve bu tehditler en çok hangi unsurlardan kaynaklanmaktadır?
4. Bilgi güvenliği tehditlerine karşı alınan teknolojik bilgi güvenliği önlemlerinin Türkiye'de üniversite kütüphanelerinde uygulanma düzeyleri nedir?
5. Teknolojik bilgi güvenliği önlemlerinin uygulanma düzeylerinde üniversitenin türüne, bilgi güvenliğinden sorumlu personelin varlığına ve kurumsal bilgi güvenliği yönetim aracının kullanımına bağlı olarak farklılıklar oluşmakta mıdır?
6. Bilgi güvenliği tehditlerine karşı alınan kurumsal bilgi güvenliği önlemlerinin Türkiye'de üniversite kütüphanelerinde uygulanma düzeyleri nedir?
7. Kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinde üniversitenin türüne, bilgi güvenliğinden sorumlu personelin varlığına ve kurumsal bilgi

güvenliği yönetim aracının kullanımına bağlı olarak farklılıklar oluşmakta mıdır?

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği yönetimine ilişkin gerek farkındalık düzeyinde gerekse uygulama düzeyinde önemli problemlerin olduğu varsayılmaktadır. Bu problemlerin düzeyi; üniversite kütüphanelerinde çalıştırılan personelin niteliğine ve sayısına, kütüphanelerde kullanılan bilgi sistemlerine, bilgi güvenliğine ayrılan bütçeye, üniversitenin kurumsal yapısına ve düzenine, güvenlik personelinin varlığına ve sayısına, kullanılan güvenlik araç ve gereçlerine, sunulan ağ ve donanım hizmetlerine ve diğer tüm teknik ve kurumsal önlemlere göre farklılıklar gösterebileceği ön görülmektedir.

Çalışma kapsamında belirlenen problem ve araştırma sorularına dayanarak oluşturulan temel hipotezler şu şekilde sıralanmaktadır:

8. Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinde üniversite türleri arasında anlamlı farklılıklar vardır.
9. Türkiye'de üniversite kütüphanelerinde bilgi güvenliği personelinin varlığına bağlı olarak teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinde anlamlı farklılıklar vardır.
10. Türkiye'de üniversite kütüphanelerinde kurumsal bilgi güvenliği yönetim aracının varlığı ve kullanımına bağlı olarak teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinde anlamlı farklılıklar vardır.

1.5. Kapsam ve Sınırlılıklar

Bu çalışmanın kapsamı, Türkiye'de üniversite kütüphanelerinde bilgi güvenliği uygulamaları ve söz konusu uygulamaların durumuna ilişkin verilerle sınırlandırılmıştır. Çalışmada elde edilen bulgular üniversite kütüphanelerinin bilgi güvenliği yönetimine ilişkin durumlarını istatiksel verilerle yansıtmaktadır. Çalışmada amaca dayalı örnekleme yöntemi uygulandığından verilerin toplanmasında öncelikle bilgi güvenliği konusunda yetkinliği olan personel, daha sonra ise kütüphanecilik alanında uzmanlaşmış personel, her ikisinin yokluğunda ise diğer personel türleri arasında kütüphanecilik ile ilgili yetkinliğe sahip personel

tercih edilmiştir. Bu durum çalışmanın örneklem seçimindeki sınırlılığını oluşturmaktadır. Bu nedenle üniversite kütüphanelerinde çalışan personel ile yapılacak anket uygulamasına katılacak kişilerin alanlarında uzman oldukları ve anket maddelerine makul ve geçerli cevaplar verecek bilgi ve tecrübeye sahip oldukları varsayılmaktadır.

Kütüphanecilik hizmetlerinde bilgi güvenliği yönetimi konusu üzerinde yapılan alanyazın taramasında Türkçe kaynağın oldukça sınırlı olduğu gözlemlenmiştir. Diğer yandan Türkiye'de iletişim, haberleşme, güvenlik ve sağlık gibi farklı disiplin mensuplarınca bu konuya ilişkin yapılan çalışmaların daha fazla olduğu görülmektedir. Araştırma kapsamında kullanılan kaynakların büyük çoğunluğunun yabancı alanyazına ve Türkçe kaynakların ise diğer hizmet alanlarında yürütülen bilgi güvenliği çalışmalarına dayanması çalışmanın kavramsal sınırlılığını oluşturmaktadır.

Türkiye'de kütüphanecilik hizmetlerinde bilgi güvenliği yönetimi konusu üzerinde daha önce doğrudan hiç çalışma yapılmamış olması; diğer disiplinler arasında da bu konuya ilişkin çalışmaların azlığı bu çalışmanın tamamlanmasında karşı karşıya kalınan en önemli kısıtlılıklardan biridir. Diğer taraftan bu yönüyle çalışma, bilgi güvenliği konusunda disiplinin uygulama alanlarına ve aynı zamanda alanyazınına katkı sağlayacak potansiyele sahiptir.

1.6. Tanımlar

Veri: İşlenmemiş, fayda sağlayabilmesi için işlenmesi veya yorumlanması gereken ham gerçek olarak ifade edilmektedir. Diğer bir ifadeyle anlamlandırılmamış nesnesi olmayan bir gerçektir. Verinin tanımlanması, incelenmesi, değerlendirilmesi ve sentezlenmesi sonucunda tek başına anlam kazanmasıyla enformasyon oluşmaktadır. Enformasyonun kullanılabilir ve işe yarar bir nesne haline gelmesiyle de bilgi oluşmaktadır. Kısacası veri, bilginin ham halini oluşturmaktadır (Gülseçen, 2012; International Organization for Standardization (ISO), 2018; Öner, 2015; Tonta, 2004). Çalışmada da veri bu anlamıyla anket ve ölçekten elde edilen verileri ifade etmektedir.

Bilgi: Diğer önemli nesneler gibi bir kurum ya da kuruluşun faaliyetleri açısından değerli olan ve dolayısıyla uygun bir biçimde korunması gereken bir varlıktır (ISO,

2015). Bilgi, kâğıt veya farklı ortamlar üzerine işlenmiş anlaşılabilen ve iletilebilen veriler topluluğundan oluşmaktadır. Bu bakımdan bilgi, veri ve enformasyonun üst seviyesini oluşturan varlıktır. Personel, kullanıcı ve kuruma ait politikalar, rehberler, sözleşmeler, mevzuatlar, yazılımlar, sistem mimarileri, teknik alt yapılar gibi tüm bilgi varlıkları o kuruma ait bilgileri oluşturmaktadır. Ayrıca bu bilgileri kayıt altına alan, işleyen, taşıyan, ileten ve çıktı olarak üreten bilgi ve iletişim sistemlerinin her biri de birer bilgi varlığı olarak görülmektedir (Ardıç ve Dulkadir, 2018; ISO, 2018; Öner, 2015).**Bilgi Güvenliği:** Bilginin gizliliği, bütünlüğü ve kullanılabilirliğini sağlamaktadır. Bu temel unsurlara ek olarak özgünlük, hesap verilebilirlik, inkâr etmemek ve güvenirlik gibi diğer unsurlarda dâhil edilebilmektedir. Kurumların faaliyetlerini başarılı bir biçimde sağlamak amacıyla bilgi güvenliği tehdit eden olayların dikkate alınmasını içeren kontrolleri içermektedir. Bilgi ve verilerin yetkisiz kişilere, kuruluşlara ve süreçlere sunulmaması veya ifşa edilmemesi mülkiyetine **gizlilik**, yetkili erişim ile bilginin kendine özgü mahremiyetinin korunmasına, doğruluk ve tamlık özelliğine **bütünlük**, ihtiyaç halinde bilgiye kolay ulaşılmasına ise **erişilebilirlik / kullanılabilirlik** denilmektedir. Bu üç unsur korunacak bilginin temel özelliklerini oluşturmaktadır. Bir kurumun veya kuruluşun bilgi güvenliği bu üç temel unsurunun işler hale getirilmesi ile sağlanabilmektedir. Bilgi güvenliği, belirlenen risk yönetim süreci ile seçilen bilgi varlıklarını korumayı hedeflemektedir. Kurum ve kuruluşlarda belirli bir bilgi güvenliği ve iş hedefine ulaşılmak için politika, prosedür, süreç, kurumsal yapı, yazılım ve donanım dâhil olmak üzere bir dizi kontrolün uygulanması, izlenmesi, gözden geçirilmesi, değerlendirilmesi ve gerektiğinde iyileştirilmesi gerekmektedir. Sonuç itibarıyla belirtilen bilgi güvenliği kontrollerinin bir kuruluşun iş süreçleriyle sonsuz bir biçimde entegre edilmesi beklenmektedir (ISO, 2022a; ISO, 2018).

Varlık / Bilgi Varlığı: Varlık, kurum için değeri olan kavranabilir ve algılanabilir bilgi, yazılım, donanım, hizmet, çevre, itibar, imaj ve çalışan gibi somut ve soyut şeyleri içermektedir. Bilgi varlığı ise bir kurum için değerli olan ve sürekli saklanması ve gizliliğinin sağlanması gereken varlıkları kapsamaktadır. (ISO, 2018; ISO, 2015).

Kütüphaneler açısından bilgi varlıklarını; personel ve kullanıcıların kişisel verilerini içeren her türlü bilgi varlıkları (kullanıcı üyelik formları veya kayıtları, personel

özlük dosyaları, kütüphane uygulamalarındaki kişisel kayıtlar vb. kayıtlı ortamlar), kurumsal bilgi varlıkları (rehberler, raporlar, sözleşmeler, resmi evraklar, politika ve prosedürler vb.), bilgi ve iletişim sistemlerine ait bilgi varlıklar (analiz ve teknik dokümanları, uygulamalar, yazılımlar, lisanslar, veri tabanları, sunucular, ağ cihazları, internet vb.) ve paydaşlara ait bilgi varlıkları olarak gruplandırılabilir.

Bilgi Sistemi: Uygulamaların, hizmetlerin, bilgi teknolojisi varlıklarının veya diğer bilgi işleme bileşenlerinin birleştiği bir küme olarak tanımlanmaktadır (ISO, 2018). Bilgi sistemlerinin tasarım ve geliştirilme aşamalarında bilgi güvenliği her zaman dikkate alınmamaktadır. Bu nedenle kurum ve kuruluşlarının hizmet süreçleri içerisinde kullandığı bilgi sistemleri dolandırıcılık, casusluk, sabotaj, yangın ve sel gibi birçok kaynaktan gelen güvenlik tehditleri ile karşı karşıyadır. Kötü niyetli kod yazılımları, bilgisayar korsanlığı ve hizmet engelleme saldırılarının neden olduğu bilgi sistemlerine ve ağlarına verilen zararlar teknolojik gelişmelere bağlı olarak gün geçtikçe daha da artmakta ve karmaşık bir hale gelmektedir.

Risk: Belirsizliğin hedefler üzerindeki etkisidir. Belirsizlik, bir olayın olma olasılığının veya sonucunun anlaşılması ve bilinmesi ile ilgili bilgi eksikliğini; etki ise beklenen olumlu veya olumsuz durumdan sapmayı göstermektedir. Risk, çevredeki değişikliklerde dâhil bir olayın sonuçları ve meydan gelme olasılığının bir kombinasyonu olarak ifade edilmektedir. BGYS bağlamında **bilgi güvenliği riski**, tehditlerin kuruluşa ait bilgi varlıklarının güvenlik açıklıklarından yararlanarak oluşacak zarar verme potansiyeli ile ilişkilidir (ISO, 2022c; ISO, 2018).

Risk Yönetimi: Bir kuruluşu risk faktörlerine karşı yönlendirmek ve riskleri sistematik bir biçimde kontrol altına almak için yürütülen iletişim, danışmanlık, tanımlama, analiz etme, değerlendirme, izleme ve riski gözden geçirme gibi koordineli faaliyetleri içermektedir (ISO, 2022c; ISO, 2018).

Saldırı: Bir varlığı imha etmek, değiştirmek, ifşa etmek, devre dışı bırakmak, çalmak veya yetkisiz kullanmaktır (ISO, 2018). Kurum ve kuruluşlar tarafından üretilen, korunan ve işlenen bilgi ve veriler güvenlik açıklarına tabi olduğundan her türlü saldırıya maruz kalabilmektedir.

Tehdit: Bir sistem veya kuruluşa zarar verebilecek istenmeyen bir olayın olası nedeni (ISO, 2018) olarak tanımlanmaktadır. Bilgi varlığını bozmaya veya yok

etmeye yönelik gerçekleşen veya gerçekleşebilecek her türlü istenmeyen algı tehdit olarak değerlendirilmektedir. Bu tehditler doğal, çevresel ve insan kaynaklı tehditler olarak birtakım gruplar altında toplanmaktadır. Deprem, sel, yıldırım, yangın, volkanik patlamalar, toprak kayması, çığ, don tehlikesi gibi olaylar doğal tehditler; yazılım hatası, elektrik kesintisi, iletişim arızaları gibi olaylar çevresel tehditler; kasıtlı kasıtsız veriler üzerinde yapılan değiştirme, silme, ekleme veya bu verinin dışarıya sızdırılması, terör veya siber saldırılar, çalışan sabotajı, hırsızlık gibi olaylar ise insan kaynaklı tehditler olarak örneklendirilebilir.

Yönetim Sistemi: Bilgi güvenliği politikaları, süreçleri ve hedefleri oluşturmak ve bu hedeflere ulaşmak için bir organizasyon içerisinde sorumlulukları, yetkileri, ilişkileri ve kendi işlevleri olan kişi veya kişiler kümesi (ISO, 2022a; ISO, 2018) olarak tanımlanmaktadır. Bir yönetim sistemi tek bir disiplin içerisinde oluşabileceği gibi birkaç disiplinin birleşimi içerisinde de oluşabilmektedir. Yönetim sistemi kapsam olarak kuruluşun tamamını veya belirli ve tanımlanmış işlevlerini içerebilmektedir. Kuruluşun yapısı, rolleri, sorumlulukları, planlanması ve çalışması yönetim sisteminin ögelerini oluşturmaktadır. Bilgi güvenliği açısından bir yönetim sistemi; müşterilerinin ve diğer paydaşlarının bilgi güvenliği gereksinimlerini karşılamayı, kuruluşun planlarını ve faaliyetlerini iyileştirmeyi, kuruluşun bilgi güvenliği hedeflerini karşılamayı, bilgi güvenliği ile ilgili ulusal veya uluslararası mevzuat düzenlemelerine ve kurallarına uymayı, bilgi varlıklarını sürekli iyileştirmeyi ve kuruluşu mevcut organizasyonel hedeflere uyumu kolaylaştıracak şekilde yönetmeyi sağlamalıdır.

Bilgi Güvenliği Yönetim Sistemi: Bir kuruluşun bilgi varlıklarını korumak amacıyla oluşturduğu ve yönettiği politikaları, prosedürleri, kılavuzları ve ilgili dokümanları içermektedir. BGYS, bir kuruluşun hedeflerine ulaşabilmesi açısından oluşturduğu sistematik bir yaklaşımdır. Bu sistematik yaklaşım kuruluşun risklerini yönetebilmek ve bu riskleri etkin bir biçimde karşılayabilmek amacıyla tasarlanmış risk kabul düzeylerine dayanmaktadır. Bilgi varlıklarının korunmasına yönelik gereksinimlerin analiz edilmesi ve bu bilgi varlıklarının gerektiği şekilde korunmasını sağlamak için uygun BGYS kontrollerinin (bilgi güvenliği kurmak, uygulamak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirme) uygulanması kuruluşun başarılı faaliyet göstermesine katkıda bulunur (ISO, 2022a; ISO, 2018).

1.7. Yöntem

Bu bölümde, araştırmanın modeli, evreni, örneklemi, yöntemi, veri toplama teknikleri ve verilerin analizi ile ilgili bilgiler yer almaktadır.

1.7.1. Araştırma Modeli ve Çerçevesi

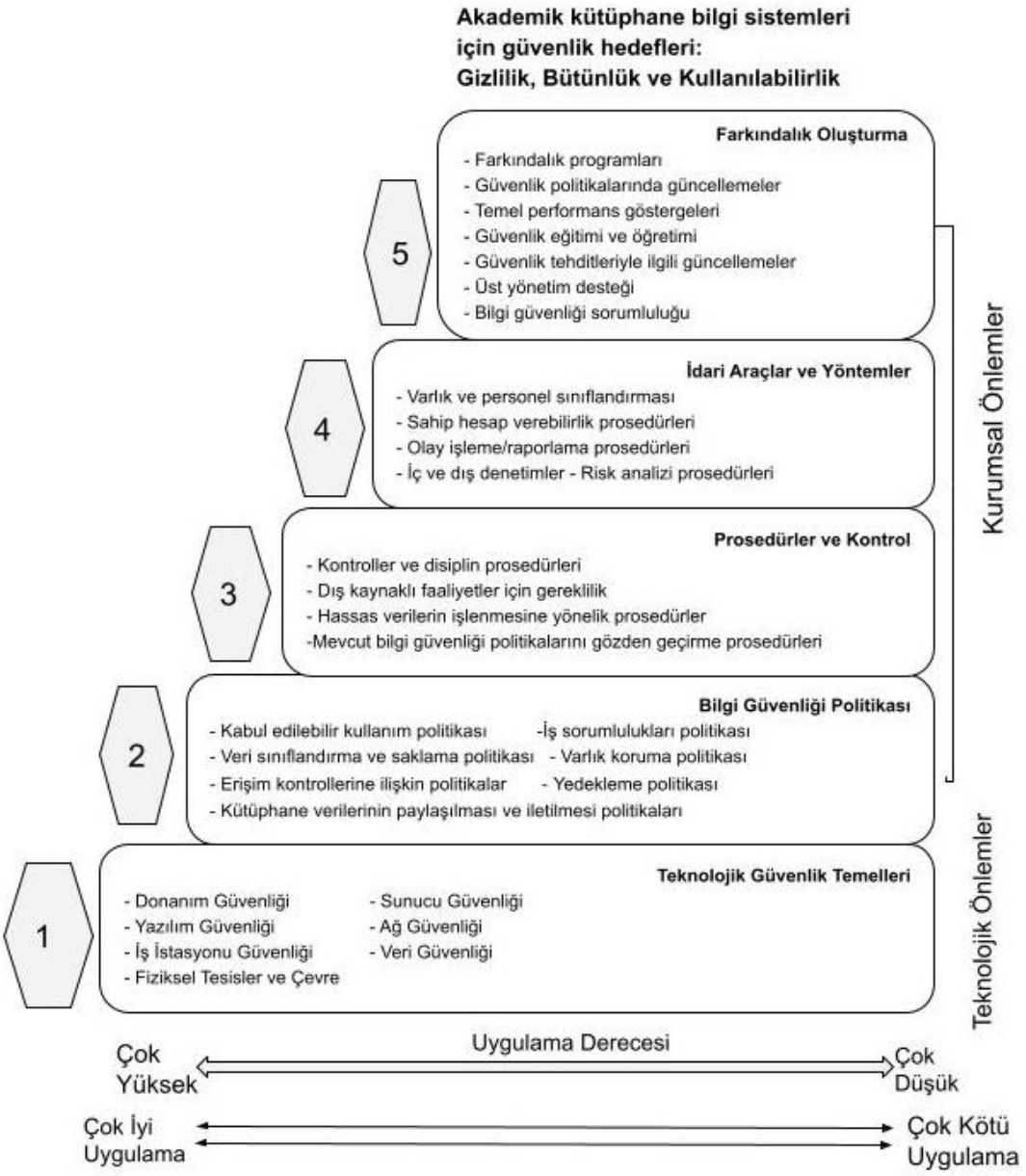
Türkiye'de üniversite kütüphanelerinde bilgi güvenliği yönetimi ile ilgili farkındalığı, bilgi güvenliği tehditlerini ve bu tehditlere karşı belirlenen teknik ve kurumsal önlemlerin düzeyini belirlemek için verilerin toplanmasını amaçlayan bu çalışmada tarama yöntemi kullanılmaktadır. Tarama yöntemi geçmişte ya da halen var olan olayların, olguların, nesnelerin, kurumların veya çeşitli durumların kendi koşulları içerisinde olduğu gibi tanımlanmasını ya da belli özelliklerinin neler olduğunun ortaya çıkarılmasını amaçlayan araştırma yaklaşımıdır (Karasar, 2019; Eşitti, 2018). Tarama araştırmalarında genellikle geniş bir kitleden araştırmacı tarafından belirlenen cevap seçenekleri kullanılarak bilgi toplanır. Genellikle tarama araştırmalarında araştırmacılar, görüşlerin ve özelliklerin neden kaynaklandığından çok örneklemdeki bireyler açısından nasıl dağıldığıyla ilgilenmektedir (Fraenkel ve Wallen, 2006). Sosyal bilimlerde yaygın olarak kullanılan bu araştırma modeli, geniş bir gruptaki verilerin açıklanması, düzenlenmesi, özetlenmesi veya tümünü temsil edecek verilerin bulunması açısından kullanışlı ve uygun bir nicel araştırma desenidir (Çokluk, Şekercioğlu ve Büyüköztürk, 2018; Yazıcıoğlu ve Erdoğan, 2014; Erdoğan, 2012).

Bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini / erişilebilirliğini sağlamak için bilgi varlıklarını tüm potansiyel tehditlerden korunmayı amaçlayan bilgi güvenliği yönetimi, geniş bir kavramsal konu çerçevesine sahiptir. Çalışmanın doğal basamaklarının bütünlük sağlayabilmesi ve araştırma amacını ortaya koyan kavramsal yapının oluşabilmesi için bilgi güvenliği yönetimine ilişkin saptanan anahtar kavramlar ve bu kavramlar arasındaki ilişkiler genel olarak alanyazında genelden özele doğru sıralı bir biçimde açıklanmaktadır. Bu çalışmada, gerek genel bilgi güvenliği yönetimine ilişkin gerekse kütüphane dünyasına özgü bilgi güvenliği kavramları alanyazın taramalarından elde edilen bilgiler ışığında tanımlanarak ve birbiriyle olan ilişkileri açıklanarak araştırmanın temel yapısına, amacına ve önemine uygun bir biçimde sunulmaktadır (Karasar, 2019).

Üniversite kütüphanelerinde bilgi güvenliği yönetiminin etkinliğinin incelendiği bu çalışmanın genel çerçevesi, Şekil 1.1'de verilen model üzerine kurgulanmıştır. Ismail (2012)'in geliştirdiği "Kütüphane Bilgi Güvenliği Değerlendirme Modeli"nde (Şekil 1.1) hem kurumsal hem de teknik önlemlere değinilmekte ve bilgi güvenliği yönetimi beş ana grupta incelenmektedir. Kütüphanelerde teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanmasını değerlendirmek için modelin her adımında birtakım değişkenler önerilmektedir. Ayrıca, model ile uyumlu olarak geliştirilen anket formu ile kütüphanelerde teknolojik ve kurumsal önlemlerin uygulanma düzeylerine ilişkin veriler sağlanmaktadır.

Üniversite kütüphanelerinde bilgi güvenliği uygulamalarının iyi bir biçimde yönetimi için teknolojik ve kurumsal bilgi güvenliği uygulamalarının bir düzen içerisinde gerçekleştirilmesi gerekmektedir. Şekil 1.1'de verilen bu model de, bilgi güvenliği önlemlerinin etkili olabilmesi için örgütsel ölçütler ile teknolojik ölçütlerin bir merdivenin basamağı gibi birlikte değerlendirilmesini göstermektedir. Bu nedenle çalışmada teknolojik ve kurumsal bilgi güvenliği uygulamaları üzerinde yoğun bir biçimde durulmaktadır. İyi bir bilgi güvenliği yönetim sisteminin bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamayı ve korumayı hedefleyen mantıksal bir sırayı takip etmesi gerekmektedir (Ismail, 2012; Eisenberg ve Lawthers, 2008; Sundt, 2006; Berghel, 2005). Bilgi güvenliğinin gizlilik, bütünlük ve kullanılabilirlik ölçütlerinin önemi üzerinde durulan bu çalışma, kütüphanelerdeki bilgileri tehditlerden ve güvenlik açıklarından en etkili bir biçimde korumayı amaçlayan güvenlik önlemlerinin geliştirilmesine rehberlik etmektedir.

Şekil 1.1: Kütüphane bilgi güvenliği değerlendirme modeli



Kaynak: (Ismail, 2012)

1.7.2. Evren ve Örneklem

Araştırma Türkiye'de üniversite kütüphanelerinin bilgi güvenliği tehditlerini ve uygulamalarını tespit etmeyi amaçladığından araştırmanın evrenindeki hedef kişiler arasında, kütüphane hizmetlerinde bilgi işlem sistemlerinin uygulayıcısı ve karar vericisi olan daire başkanları, birim sorumluları, öğretim görevlileri, kütüphaneciler ve bilgi işlem uzmanları bulunmaktadır. Bu kişilerin ortak özelliği, üniversite kütüphanelerinde yürütülen hizmetlerden ve bilgi varlıklarının güvenliğinden ve

muhafaza altına alınmasından doğrudan sorumlu olmalarıdır. Evrendeki tüm üniversite kütüphanelerindeki görevlilerin çalışmaya olan katkılarının homojen bir biçimde sağlanabilmesi için her üniversiteden en az bir kişinin örnekleme dâhil edilmesi amaçlanmıştır. Bu itibarla çalışmanın amacına katkı sağlayacak bilgi açısından zengin ve nitelikli ölçütlere sahip kişilerin belirlenmesi için olasılıklı (tesadüfi) olmayan bir örnekleme yaklaşımı olan "amaca dayalı (yargısal) örnekleme" yöntemi kullanılmıştır (Büyüköztürk ve diğerleri, 2022; Güriş ve Astar, 2014; Yazıcıoğlu ve Erdoğan, 2014). Bu yöntem ile evren parametresindeki benzer özellikteki birim ya da bireylerin seçimi bizzat araştırmacı tarafından özenle gerçekleştirilerek çalışmanın örneklem grubu oluşturulmaktadır.

Amaçlı örnekleme yöntemi, evren içerisinde araştırmanın amacına en güçlü bir biçimde katkı sağlayacağı düşünülen birimlerin seçilmesi yoluyla yapılan örnekleme metodudur. Bu yöntemde örneklemin seçimi araştırmanın amacı ve evrenin özellikleri göz önünde bulundurularak belli ölçütleri karşılayan veya belli özelliklere sahip birimler arasından rastgele olmayacak bir biçimde yapılmaktadır. Patton (1990), amaçlı örnekleme ilgili farklı stratejilerden ve yöntemlerden bahsetmektedir. Bu stratejilerde kullanılacak ölçüt örnekleme, araştırma evreninde belli niteliklere sahip kişiler, olaylar, nesneler ya da durumlar arasından oluşturulmasıdır.

Yükseköğretim Kurumunun Yükseköğretim Bilgi Yönetim Sistemindeki istatistik bilgilerine göre Türkiye'de 130'u devlet, 74'ü vakıf ve 4'ü vakıf yüksekokulu olmak üzere toplamda 208 yükseköğretim kuruluşu bulunmaktadır (YÖK, 2022). Türkiye İstatistik Kurumunun Türkiye'deki kütüphaneler ile ilgi yayınladığı istatistik raporuna göre kütüphanesi olan üniversitelerin niceliksel bilgileri Tablo 1.1'de verilmiştir (TÜİK,2022).

Tablo 1.1: Türkiye'de üniversitelerin kütüphane sayıları

	Devlet Üniversitesi	**Vakıf Üniversitesi**	**Toplam**
Kütüphanesi olan üniversite sayısı	***N***	***N***	***N***
	130	78	208

Kaynak: (TÜİK, 2022)

Araştırma evrenindeki üniversitelerden kurulum aşamasında olan veya bir merkezi kütüphaneye ya da uzman bir kütüphane personeline sahip olmayan ikisi devlet üniversitesi üçü vakıf MYO olmak üzere toplam beş üniversite araştırmanın

örneklem saptama süreçlerine dâhil edilememiştir. Örnekleme dâhil edilmesine rağmen anket uygulamasının yapıldığı dönemde Kahramanmaraş merkezli Türkiye'de meydan gelen iki büyük deprem felaketinden etkilenen iller arasında bulunan üç devlet üniversitesinden çeşitli nedenlerle veri elde edilememiştir. Ayrıca kütüphane yönetiminin anket formuna katılım sağlamak istememesinden dolayı bir devlet üniversitesinden de veri elde edilememiştir. Böylelikle 2022-2023 eğitim ve öğretim yılında faaliyet gösteren Yükseköğretim Kurumunun Yükseköğretim Bilgi Yönetim Sisteminde kayıtlı üniversitelerden 6'sı devlet üniversitesi 3'ü vakıf üniversitesi olmak üzere toplam 9 üniversiteden konuya ilişkin veri elde edilememiştir. Sonuç olarak, 124 devlet üniversitesi ve 75 vakıf üniversitesi olmak üzere toplam 199 üniversiteden çalışmanın konusuna ilişkin veri toplanmıştır.

Araştırmaya katılım sağlayan katılımcıların cinsiyeti, eğitim durumu, çalıştığı üniversitenin türü, üniversite kütüphanesindeki görevi ve iş tecrübesi gibi verilerden oluşan katılımcı demografik bilgileri Tablo 1.2'de verilmiştir.

Tablo 1.2: Katılımcılara ilişkin demografik bilgiler

Demografik Özellikler		**N**	**%**
Cinsiyet	Kadın	117	58,8
	Erkek	82	41,2
Eğitim Durumu	Ön Lisans	1	0,5
	Lisans	121	60,8
	Lisansüstü (Yüksek Lisans/Doktora)	77	38,7
Mezuniyet Programı	Bilgi ve Belge Yönetimi /Kütüphanecilik Arşivcilik/Dokümantasyon Programları	167	83,9
	Bilgisayar / Bilişim / Yazılım Programları	6	3,0
	Diğer	26	13,1
Kütüphanedeki Görev	Daire Başkanı	20	10,1
	Şube Müdürü	12	6,0
	Öğretim Görevlisi	22	11,1
	Kütüphaneci	134	67,3
	Bilgisayar İşletmeni / Bilgi İşlem Uzmanı	5	2,5
	Diğer	6	3
Hizmet Yılı	1 – 5 yıl	71	35,7
	6 – 10 yıl	59	29,6
	11 – 15 yıl	37	18,6
	16 – 20 yıl	18	9,0
	21 yıl ve üzeri	14	7,0
Üniversite Statüsü	Devlet Üniversitesi	124	62,3
	Vakıf Üniversitesi	75	37,7
	Toplam	**199**	**100,0**

Katılımcıların mezun oldukları programa ilişkin "diğer" seçeneğini işaretleyen katılımcıların mezun oldukları programların işletme, iktisat, halkla ilişkiler,

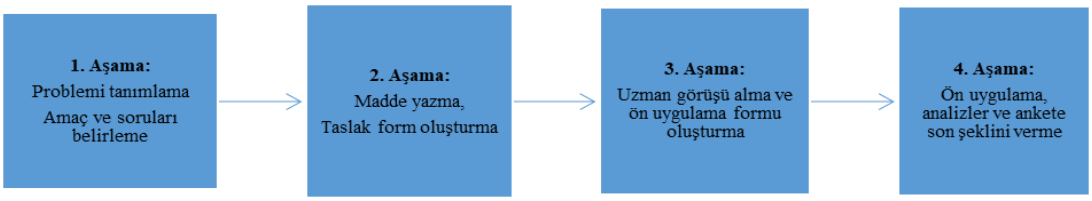
mühendislik ve öğretmenlik bölümleri ile ilgili lisans derecesine sahip programlar; kütüphanede görevi bakımından "diğer" seçeneğini işaretleyen katılımcıların ise şef, genel hizmet ve büro personeli görevleri belirttikleri görülmüştür.

1.7.3. Verilerin Toplanması

Çalışmada veri toplama aracı olarak, araştırmanın amaç ve planına göre düzenlenmiş sorulardan oluşan bir anket formu geliştirilmiştir. Anket sistematik bir veri toplama aracıdır. Araştırma için gerekli olan verilerin belirlenen örneklem gruptan toplanması için oluşturulmuş veri toplama formu olan anket, araştırmacının konuya ilişkin bilgi birikimi ve alanyazındaki benzer çalışmalarda kullanılan anket formlarındaki bilgilere dayanılarak oluşturulmuştur. Alan yazında bilgi güvenliği ile ilişkili çeşitli anket veya ölçeklerin olduğu belirlenmiş (Canoğulları, 2021; Gündüzalp, 2021; CBDDO, 2020; Aslay ve diğerleri, 2019; Genç, 2019; Gürsel, 2019; Onaran, 2019; Güldüren ve diğerleri, 2016; Güldüren, 2015; Güngör, 2015; TÜBİTAK, 2013; Haklı, 2012;) fakat bu ölçme araçları incelendiğinde çoğunun farklı alanlarda yapıldığı görülmüştür. Kütüphanecilik ile ilgili bilgi güvenliği çalışmalarının azda olsa bulunduğu (Şişkin, 2020; Henkoğlu ve Uçak, 2015; Öztemiz ve Yılmaz, 2013) fakat bu çalışmalarda bilgi güvenliğinin daha çok kişisel veri ile ilgili kısımlarına değinildiği görülmüştür. Bu çalışmaya yakın bir çalışma, 2012 yılında yapılan Ismail'in Malezya'da akademik kütüphanelerin bilgi güvenliği durumunu saptamaya yönelik yaptığı doktora tez çalışmasıdır. Ismail'in çalışmasında kullanılan anket formu içerdiği unsurlar bakımından zenginleştirilerek yol haritası olarak kullanılmıştır. Fakat zamanla bu ankette bulunan içerik, teknolojik gelişmelere bağlı olarak güncelliğini yitirmiştir. Konu ile ilgili mevcut anket veya ölçeklerin çalışmanın temel amacına doğrudan katkı sağlamayacağının tespiti üzerine, çalışmanın amacına katkı sağlayacak uygun yeni bir anket formu oluşturulmuştur.

Alanyazına göre anket geliştirme süreci sosyal bilim çalışmalarında kullanılan tüm ölçme araçlarında olduğu gibi belirli aşamalardan geçilerek güvenilir ve geçerli bir anket formu geliştirilmiştir. Anket geliştirme süreci ile ilgili aşamalar Şekil 1.2'de verilmiştir (Büyüköztürk ve diğerleri, 2022).

Şekil 1.2: Anket geliştirme süreci



Kaynak: (Büyüköztürk ve diğerleri, 2022)

Araştırmanın problemlerini iyi tanımlamak ve amaçlarını olabildiğince kesin ve açık bir biçimde elde etmeyi hedeflemek için öncelikle geniş bir alanyazın taraması yapılmıştır. Araştırma kapsamında kullanılacak anket formundaki soruların hazırlanmasında; uluslararası bilgi güvenliği standartları (ISO/IEC 27000, NIST-SP 800, IEEE 802 vb.), ulusal düzeyde hazırlanmış bilgi güvenliği yönetimi ile ilgili rehber, rapor, mevzuat türündeki belgeler ve kütüphanecilik alanında veya diğer alanlarda çalışılmış ulusal veya uluslararası araştırma makaleleri ve tezlerinden yararlanılmıştır. Söz konusu alanyazın çalışmalarından ve mevcut ölçme araçlarından faydalanılarak 1'i açık uçlu, 20'si tek ve çok seçimli ve 125'i likert tipi olmak üzere toplam 146 sorudan oluşan taslak anket formu oluşturulmuştur. Daha sonra anketin kapsam geçerliliğiyle ilgili aşamaya geçilmiştir.

"Ankette yer alan maddeler, ihtiyaç duyulan olgusal ve/veya yargısal verileri kapsamada ve toplamda ne derece yeterlidir?" (Büyüköztürk ve diğerleri, 2022) sorusuna cevap olarak uzman görüşlerine başvurulmuştur. Bu bağlamda Taslak Anket Formu, öncelikle alan uzmanları olan Bilgi ve Belge Yönetimi Bölümü'nden beş öğretim elemanı ve bilgi teknolojileri alanında görev yapan iki öğretim elemanı ve istatistik, ölçme-değerlendirme alan uzmanlarından iki öğretim elemanının görüşlerine sunulmuştur. Uzman görüş ve önerilerine göre bazı maddeler üzerinde değişiklikler ve düzeltmeler yapılmış; gerek araştırmanın amacına uygun olmaması gerekse teknik terminoloji açısından anlaşılması güç olduğuna karar verilen likert tipi 20 madde anket formundan çıkartılmıştır. Ayrıca bir adet tek seçimli soru açık uçlu olarak değiştirilmiştir. Böylelikle kapsam geçerliliği sağlanan taslak anket formu için bir sonraki anket geliştirme aşaması olan pilot (ön) uygulaması uygulanmıştır.

Pilot uygulama ile formun anlaşılırlığı, yanıtların yeterliliği ve amacına uygun olarak çalışıp çalışmadığı tespit edilebilmektedir. Pilot uygulama sonucunda elde edilen geri

bildirimler ve deneyimler, anketin daha iyi bir hale getirilmesi için kullanılabilmektedir. Sonuç olarak bu aşama anketin taslak formundaki problemlerini belirlemek ve gerekli düzeltmeleri yapmak için kritik bir öneme sahiptir. Bu süreç, anketin nihai versiyonunun oluşturulması için önemli bir adımdır (Büyüköztürk ve diğerleri, 2022). Bu bağlamda, Türkiye'de üniversite kütüphanelerinde görev yapan daire başkanı, birim sorumlusu, öğretim görevlisi, kütüphaneci ve bilgi işlem uzmanı personeli arasından 18 katılımcı ile taslak anket formunun pilot uygulaması yapılmıştır.

Ön uygulamadan elde edilen verilere göre, katılımcıların anket formunu 20-30 dakika arasında cevapladıkları belirlenmiş ve anket formunun uygulama süresinin ortalama 25 dakika gibi bir süre de cevaplanacağını anlaşılmıştır. Bu durum araştırmacının 30 dakika olarak düşündüğü anketin cevaplanma süresini karşıladığını ortaya koymuştur. Katılımcıların anket formunda anlamadıkları ya da anlaşılma güçlüğü çektikleri maddeler ile anket formunda çıkarılmasını ya da eklenmesini düşündükleri uzman ve danışman önerilerine göre 1 adet çok seçimli maddenin seçeneklerine yeni bir seçeneğin eklenmesi ve 1'i tek seçimli ve 1'i çok seçimli olmak üzere 2 tane daha kapalı uçlu sorunun ankete eklenmesinin uygun olacağı belirlenmiştir. Ayrıca anlaşılmayan maddelerin daha sade ve anlaşılır biçimde düzenlenmesi için görüş birliğine varılmıştır.

Sonuç olarak, anket geliştirme sürecindeki tüm aşamalardan elde edilen değerlendirmeler çerçevesinde anket formunun son şekli oluşmuştur. Kapsam geçerliliği çalışması sonucunda oluşturulan 2'si açık uçlu, 20'si tek ve çok seçimli ve 104'ü likert tipi dereceleme sorusu olmak üzere toplam 126 maddeden oluşan veri toplama aracı geliştirilmiştir (EK-1.1). Bu anket formunun örneklem gruba uygulanabilmesi ile ilgili olarak Çankırı Karatekin Üniversitesinden Etik Kurul Onayı alınmıştır (EK-1.2).

Söz konusu bu veri toplama aracının likert tipi dereceleme sorularından oluşan kısımda, 5'i teknolojik güvenlik (donanım, yazılım, ağ, veri, fiziksel çevre) ve 4'ü kurumsal güvenlik (güvenlik politikası, prosedürü, idari araçları ve farkındalık çalışmaları) olmak üzere toplamda 9 boyut altında 104 adet likert tipi madde yer almaktadır. Bu maddeler teknolojik ve kurumsal güvenlik önlemlerinin uygulamada var olup olmadığı ve varsa hangi düzeyde uygulanmakta olduğu ile ilgili mevcut

durumun belirlenmesi amacıyla kullanılmıştır. Maddelerin uygulama düzeylerine ilişkin durumu istatistiksel olarak veren derecelendirme seçenekleri şu biçimde sıralanmaktadır:

- Yok / Hiç uygulanmamakta,
- Var / Çok kötü düzeyde uygulanmakta,
- Var / Kötü düzeyde uygulanmakta,
- Var / Orta düzeyde uygulanmakta,
- Var / İyi düzeyde uygulanmakta,
- Var / Çok iyi düzeyde uygulanmakta,

Bu seçenekler yolu ile elde edilecek veriler çerçevesinde, üniversite kütüphanelerinde bilgi güvenliği önlemleri "hiç uygulanmamaktadır", "kötü düzeylerde uygulanmaktadır", "orta düzeylerde uygulanmaktadır" ve "iyi düzeylerde uygulanmaktadır" olarak değerlendirilmektedir.

Ayrıca boyutlar altında verilen maddelerde sunulan bilgiye ilişkin herhangi bir bilgisi olmayan ya da o maddedeki önlemin kurumunda uygulanması veya varlığı ile ilgili tereddüt yaşayan katılımcıların da olacağı düşüncesiyle bu derecelendirme seçeneklerine ek olarak "fikrim yok" seçeneği de eklenmiştir. "Fikrim yok" seçeneği, bir katılımcının belirli bir madde hakkında yeterli bilgiye sahip olmadığını kabul etmesini ve diğer katılımcıların cevaplarını etkilememek veya o maddenin boş bırakılmaması sağlamak amacıyla araştırmacılar tarafından önerilen bir çözüm seçeneğidir (Dursun ve Alnıaçık, 2019; Krosnick ve Fabrigar, 1997). "Fikrim yok" seçeneğinin sunulması, katılımcının hafızasını yoklayarak, o maddenin içeriği hakkında bilgi sahibi olup olmadığını araştıracağı ve sonucunda o bilgiye sahip olmadığını öngördüğünde "fikrim yok" seçeneğini işaretleyeceği varsayımına dayanmaktadır. Bu seçenek, katılımcının maddenin içeriği hakkında bir değerlendirme yapmadan eksik bilgi durumunu ifade edebilmesini sağlamaktadır (Krosnick ve Presser, 2010).

Geliştirilen anket formunun uygulanmasında, bilgisayar yoluyla uygulama yöntemi kullanılmıştır. Bu yöntemde, öncelikle anket formundaki maddeler web ortamındaki anket paket uygulaması üzerine işlenmiştir. Sonra, Türkiye'deki üniversite kütüphanelerinin web sayfaları üzerinden örnekleme yöntemine uygun kütüphane çalışanları belirlenmiştir. Örneklem grup içerisine dâhil edilen kişilerin mail ve iletişim bilgileri, görev yaptıkları üniversite kütüphanelerinin web sayfaları

üzerinden edinilmiş ve bu kişiler ile öncelikle iletişime geçilerek çalışmanın amacı, önemi ve anket formunun içeriği hakkında bilgiler verilmiştir. Bu iletişimler neticesinde örneklem içerisinde değerlendirilen kişinin araştırmanın amacına en uygun örneklem olabileceği teyit edilmesi üzerine kendisine anket formunun katılım linki kurumsal veya kişisel e-postaları üzerinden iletilmiştir. İletişim kurulan kişi, araştırmanın amacına uygun örneklem olmadığını belirtmesi durumunda o kütüphane içerisinde araştırmaya katkı sağlayabileceği düşünülen kişinin bilgileri edinilmiş ve aynı şekilde bu katılımcıya da anket formunun katılım linki iletilmiştir. Ankete katılım sağlanıp sağlanmadığı kontrolüne ilişkin ise katılımcılar ile tekrar iletişime geçilmiştir.

1.7.4. Verilerin Çözümlenmesi ve Değerlendirilmesi

Araştırma kapsamında uygulanan anket formundan elde edilen veriler IBM SPSS 26.0 programı ile analiz edilerek değerlendirilmiştir. Türkiye'de üniversite kütüphanelerin tanımlayıcı profilini, bilgi güvenliği tehditlerini ve uygulamalarını tespit etmek için anketten elde edilen veriler bu program üzerine işlenerek betimsel istatistikler gerçekleştirilmiştir.

Verilerin niteliğini incelemek ve hangi analiz tekniklerinin kullanılacağına karar vermek, doğru sonuçlar elde etmek için önemlidir. Verilerin niteliği, analiz sürecinde kullanılacak yöntemleri belirler. Üniversite kütüphanelerinde donanım güvenliği, yazılım güvenliği, ağ güvenliği, veri güvenliği, fiziksel ve çevresel güvenlik, bilgi güvenliği politikaları, prosedürleri, idari araç ve yöntemleri ve bilgi güvenliği farkındalık çalışmaları kategorileri altında gruplandırılan teknolojik ve kurumsal güvenlik önlemlerinin uygulama düzeyleri hakkında katılımcılardan elde edilen verilerin frekans (*f*) dağılımları ayrı ayrı incelenmiştir. Ayrıca bu güvenlik önlemlerin uygulama düzeyleri arasında katılımcıların görev yaptığı üniversite türüne göre, üniversite kütüphanelerinde görevlendirilen sorumlu bir bilgi güvenliği personelinin varlığına göre ve bir bilgi güvenliği yönetim aracının kullanımına göre farklılıkların tespiti için ki-kare (X^2) testi uygulanmıştır.

Ki-kare testi, veri analizinde yaygın bir şekilde kullanılan ve farklı problemlere uyan bir sınamadır (Gürbüz ve Şahin, 2018). İki kategorik değişken arasında anlamlı bir ilişki olup olmadığını test etmektedir (İslamoğlu ve Alnıaçık, 2019). Bu test, iki

kategorik değişkenin oluşturduğu çapraz tablodaki gözlenen değerler ile bu değişkenler arasında herhangi bir bağıntı olmadığı durumda ortaya çıkması beklenen değerler arasındaki farklılığı test etmektedir (Coşkun ve diğerleri, 2019; Karasar, 2019). Ki-kare testleri ile ölçümlenen değişkenler arasındaki ilişkinin anlamlı olup olmadığı anlaşılmaktadır (Aziz, 2018). Anlamlılık değeri 0,05'ten küçük ise iki değişkenin birbirinden bağımsız olduğu hipotezi reddedilir ve aralarında bir şekilde bir bağlantı olduğu kabul edilmektedir. Bu ilişkinin ne oranda güçlü olduğu ise Ki-kare testinin türevi niteliğindeki "Phi, Cramer's V, Contingensy coefficient" değerlerine bakılarak elde edilmektedir. Ki-kare testindeki anlamlılık değerlerine bakılırken hücrelerin %20'sinden fazlasında 5'ten küçük beklenen frekans yoksa "Pearsan ki-kare" değerine, varsa en küçük beklenen değere göre "Fisher's exact test değeri kullanılmıştır (İslamoğlu ve Alnıaçık, 2019).

2. BİLGİ GÜVENLİĞİ İLE İLGİLİ TEMEL BİLGİLER

Bu bölümde, bilgi güvenliği yönetimine ilişkin temel kavramlar hakkında açıklamalar yapılmaktadır. Bilgi güvenliği ile ilişkili olan bu temel kavramlar bilgi güvenliği ekseninde alanyazında yapılan çalışmalardan derlenerek oluşturulmuştur. Bilgi güvenliği yönetimine ilişkin genel bir bakış açısı oluşturmak için bilgi ve güvenlik temel kavramları ile ilişkili konular üzerinde değerlendirmeler yapılmaktadır.

2.1. Bilginin Değeri

Bilgi, insanların düşünce, tecrübe, deneyim ve araştırmaları sonucunda elde ettikleri anlamlandırılmış verilerdir. İnsanlar bilgi sayesinde varlıkları anlamlandırmakta, sorunları çözebilmekte, yeni fikirler üretebilmekte ve geliştirebilmektedir. Bilgi, insanlığın ilerlemesine ve evrimine katkı sağlayan canlı bir varlık gibidir. Bir ortamda üretilir, zamanla gelişir ve daha geçerli yeni bir bilgi ile geçerliliğini kaybedebilir.

Bilgi, insanlığa büyük faydalar sağlayan değerli bir hazinedir. Davis ve Olson (1985)'un ifade ettiği gibi "Bilgi, alıcı için anlamlı olan ve mevcut veya ileriye dönük eylem ve kararlarda algılanan değeri olan işlenmiş verilerdir." Bilginin değeri, insanların kararlar alabilmesi, sorunları çözebilmesi veya hedeflerine ulaşabilmesiyle doğrudan ilişkilidir. Ancak bu değerin korunabilmesi için bilginin güvenliği de büyük önem taşır. Bilgi, istenmeyen kişilerin eline geçtiğinde kötüye kullanılabilir veya yanlış anlaşılabilir. Bu nedenle, bilginin güvenliği ve gizliliği sağlanmalı, yetkisiz erişimlere karşı korunmalı ve doğru şekilde paylaşılmalıdır. Bilgi güvenliği, teknik önlemler, güvenlik politikaları, eğitim ve farkındalık gibi çeşitli yöntemlerle sağlanabilir. Böylelikle, bilginin değeri korunurken insanların güvenle kullanabilmesi sağlanmış olur.

Bilgi, bulunduğu ortama, zamana ve değerlendirdiği varlığa göre farklı anlamlar kazanabilir. Kişisel, kurumsal, toplumsal, ekonomik vb. birçok farklı alanda bilginin anlamı ve değeri farklılık gösterebilmektedir. Kişisel düzeyde isim, adres, hesap bilgileri özel ve gizli bilgileri ifade edebilmektedir. Bu tür bilgilerin gizliliği ve

güvenliği önemlidir, çünkü kötü niyetli kişilerin eline geçtiğinde kişisel mahremiyeti tehlikeye atabilmektedir. Kurumsal düzeyde ise bilgi, bir kurumun değerli varlıklarını temsil etmektedir. Basılı evraklar, elektronik belgeler, müşteri bilgileri, iş süreçleri, stratejik bilgiler gibi birçok kurumsal bilgi varlığını kapsamaktadır. Bu tür bilgilerin gizliliği, bütünlüğü ve erişimine ilişkin güvenlik önlemleri, kurumların başarıları ve rekabet avantajları açısından büyük önem taşımaktadır. Toplumsal düzeyde bilgi, bilimsel araştırmalar, kültürel miras, tarihî kaynaklar, kamu hizmetleri gibi birçok alanda değer taşımaktadır. Bu bilgilerin de korunması, paylaşılması ve erişilebilir olması, toplumun ilerlemesi, eğitim düzeyinin artması ve kültürel zenginliğin sürdürülmesi açısından önemlidir. Ekonomik düzeyde ise bilgi, işletmelerin rekabet avantajı elde etmesine yardımcı olmaktadır. Bilgiye dayalı ekonomi çağında, yeni fikirler, yenilikler ve teknolojik bilgi, şirketlerin büyümesi ve sürdürülebilirliği için kritik öneme sahiptir. Bilginin korunması, yenilikçilik ve ticari sırların korunması, şirketlerin rekabet gücünü artırmaktadır (Fidan, 2016; Gülseçen, 2012; Tonta, 2004). Sonuç olarak, bilgi farklı alanlarda farklı anlamlar kazanabilmekte ve insanlık için fayda veya zarar doğurabilecek bir güç olarak değerlendirilmektedir. Bu nedenle bilginin güvenliği, gizliliği, bütünlüğü ve erişimi her seviyede önem taşımakta ve söz konusu işlevlere yönelik uygun önlemlerin alınması gerekmektedir.

Bilginin olmazsa olmaz özellikleri bulunmaktadır. Bu özellikler, bilginin güvenliğini ön plana çıkarmaktadır. Bunlar (Chopra ve Chaudhary, 2020);

- Gizlilik: Yalnızca erişim haklarına sahip veya yetkili kişilerin bilgileri kullanmasını ifade eder. Örneğin, kişilere ait banka bilgileri veya kütüphane üyelik bilgileri gizli bilgilerdir. Bu nedenle bu bilgilere yalnızca yetkili kişilerin erişmesi ve bu konuda güvenlik tedbirlerinin alınması önemlidir.
- Bütünlük: Herhangi bir konu/kişi/kurum vb. alanla sınırlı bilgilerin eksiksizliğini ifade etmektedir. Kaydedilen bilgilerim eksiksiz olması ve bozulmaması gerekir. Örneğin veri tabanına kaydedilen bilgilerin kaydedildiği şekilde erişilmesi gereklidir.
- Kullanılabilirlik: Bilgi gerektiğinde kullanılabilir olmalıdır. Örneğin, birkaç yıl önce buluta kaydedilen verilere ihtiyaç duyulduğunda,

zamana/değişime/eskimeye dayalı sorunlara maruz kalmadan kullanılabilir olmalıdır.

- Doğruluk: Verilen kararlar bilginin doğruluğuna bağlıdır. Bu nedenle bilginin doğruluğu önemlidir. Örneğin, deneyimli bir ekip üyesi projenin zaman çizelgesini öngörür ve bütçe bu bilgilere dayanılarak tahsis edilir. Fakat bu bilgilerin doğruluğu zedelenmişse proje gecikmelerine hatta sonlanmasına neden olabilir.
- Özgünlük: Bilginin değiştirilmemiş ilk orijinal halini ifade etmektedir. Örneğin, müşteriye bir durum raporu sunuluyorsa bu raporun özgün olması önemlidir.

Günümüz teknolojisinin sürekli değişimi, bilginin içerik ve biçiminini de değiştirmektedir. Bu durum bilginin gelecekte yeni içerik ve biçimlerde karşımıza çıkacağını göstermektedir. İnsanlığın ilk dönemlerinden itibaren uzun zamanlar boyunca daha çok sözel iletişim süreçlerinde akışkan olarak dolaşan bilgi, günümüzde çok farklı ortamlarda üretilmekte, yönetilmekte, iletilmekte ve muhafaza edilmektedir. Bu bağlamda bilgi, insanlığın ilk dönemlerinden günümüze kadar farklı anlamlarda ve biçimlerde kendine yer bulmuştur. Örneğin kurumsal bilginin bulunduğu ortam ve biçimler şu şekilde sıralanmaktadır (Güler ve Furat, 2022):

- Elektronik veya basılı ortamda oluşturulan ve muhafaza edilen belgeler,
- İletişim hatlarında, toplantılarda, görüşmelerde vb. sözlü olarak konuşulan önemli bilgiler,
- Sunucu veya istemci bilgisayar ortamlarındaki bilgi ve belgeler,
- CD/DVD, sabit disk, flaş bellek gibi depolama cihazlarında tutulan veri, bilgi ve belgeler,
- Evrak dolapları ve arşivlerde muhafaza edilen dosya ve belgeler,
- Ağlar üzerindeki kuruma ait bilgiler,
- Elektronik posta içinde yer alan bilgiler,
- Faks, telefon cihazı gibi teknolojik gereçler ile iletilen bilgiler,
- Personel ve müşterilere ait kişisel bilgiler,
- Kurum için önemli diğer veri ve bilgilerdir.

Bilgiye her disiplin içinde farklı anlamlar yüklenebilmektedir. Bilgi üzerine inşa edilmemiş bir disiplinden bahsetmek mümkün değildir. Felsefi olarak bilen (özne/süje) ile bilinen (nesne/obje) uyumu içerisinde tanımlanan bilginin, her disiplin için farklı anlamlar kazanmasının nedeni kendi varlıklarıyla kendi bilgisini oluşturmasından kaynaklanmaktadır. Bu itibarla kütüphaneler açısından bakıldığında "Bilgi nedir?" sorusuna verilen veya verilecek cevabın da farklı olduğunu görülebilir. Kütüphanecilik disiplinin temel nesnesi konumunda olan bilgi, bilginin bilgisi olarak daha da farklı bir anlam kazanmaktadır. İçeriğinde bir nesne olgusu barındıran bilgi, kütüphanecilik disiplininde bir nesne konumuna geçmektedir. Kütüphanecilik disiplininin temel varlığı olarak kabul edilen bilgi, kütüphanelerin varoluş nedeni olarak anlam kazanmaktadır (Keseroğlu, 2010; Yontar, 2000).

İnsanın duygu ve düşüncelerinin yazılı bir belge olarak toplanıp, düzenlendiği ve korunduğu yer olan kütüphaneler, "bilgi" kavramı ile birlikte anılan tüm işlem ve süreçlerin merkezinde yer alır. Kütüphanelerin varlık nedeni ve hizmetlerinin merkezinde olan bilgi, bir nesne olarak seçilir, sağlanır, düzenlenir ve tekrar bir bilgi olarak kullanıcıların erişimine sunulur. Yazının icadı ile kayıt altına alınan bilginin korunması ve depolanması için oluşan kütüphaneler, içerisinde barındırdığı bilgi dermelerini birer nesne olarak tekrar insanlığın bilgisine sunmaktadır. İnsanoğlunun ürettiği bilgi, tarih boyunca farklı ortamlarda değişim geçirerek kütüphanelerin koleksiyonlarını oluşturan nesnelere dönüşmüştür. Başlangıçta kil tabletler gibi taşınabilir malzemeler üzerine yazılan bilgiler zamanla kâğıt gibi daha pratik ve erişilebilir bir ortama taşınmıştır. Gelişen teknolojiyle birlikte ise bilgi sayısal ortamlarda saklanmaya ve paylaşılmaya başlanmıştır. Bu değişim süreci, bilginin farklı ortamlarda ve formatlarda var olmasını sağlamış ve kütüphanelerin çok çeşitli kaynakları bir araya getirerek toplumun erişimine sunmasına olanak sağlamıştır (Güler ve Furat, 2022; Gülseçen, 2012).

Kurumsal, toplumsal, dinsel, sanatsal, bilimsel, algısal, teknik, gündelik ve felsefi bilgi gibi her türden bilgiyi içerisinde barındıran kütüphaneler açısından bilgi kavramı, en kısa tabirle "bilginin bilgisi" olarak tanımlanabilir. Çünkü kütüphaneler, başkaları tarafından üretilmiş ve bilgi taşıyıcıları üzerinde kayıtlı olan mevcut bilginin, bilgi hizmetleri çerçevesinde işlenerek (üst verisi oluşturularak) tekrar kullanıcının erişimine sunulmasını kapsamaktadır. Kütüphaneler bu bağlamda özgün

bir yeni bilgi ortaya koymamaktadır. Sadece dermeyi oluşturan bilgi materyalleri hakkında bir takım sınıflama ve kataloglama verileri oluşturulmaktadır. Kütüphaneci veya bilgi uzmanları tarafından kütüphane dermesine sağlanan bir bilgi materyalinin içeriğine bağlı olarak oluşturulan sınıflandırma bilgisi, mevcut bilginin bir üst verisi olarak üretilen yeni bilgiyi oluşturmaktadır. Bu nedenle kütüphaneler bilgi kavramının anlamına bir üst anlam kazandırmaktadır. Fakat üretilen bu bilginin bireysel, kurumsal ya da toplumsal mı olduğu konusundaki tartışmaları beraberinde getirdiği görülmektedir. Kütüphanelerde üretilen bu bilgilerin toplum yararına üretildiği düşünüldüğünde birer toplumsal bilgi, bu bilgiyi üretenin kişisel bilgi donanımı açısından düşünüldüğünde ise bireysel bir bilgi, kurumsal yönetim politikaları ve standartları çerçevesinde oluşturulduğu düşünülürse kurumsal bilgi olarak karşımıza çıkmaktadır. Ayrıca bu bilgiler sadece bir derme çerçevesinde kütüphanelerde bir bilgi olarak bulunmamaktadır. Derme unsurunun yanı sıra kullanıcı, personel, bütçe, bina ve son yıllarda üzerinde özellikle durulan teknoloji unsurları ile kütüphaneler, bir bütün olarak önemli bilgileri içinde barındıran bilgi merkezleridir. Bu bağlamda kütüphanecilik disiplini açısından düşünüldüğünde bilgi özetle, "var olan bilgi materyalinin belirlenmiş kurallar çerçevesinde yeniden biçimlenerek kavramlaştırıldığı üst veri" olarak tanımlanabilir (Külcü, 2000; Keseroğlu, 2010; 2005; Öner, 2005; Karakaş,1991).

2.2. Bilgi Varlıkları

Toplumun her katmanında çok çeşitli amaçlarla üreyen bilginin bir kısmı, gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarının faaliyetleri sonucunda oluşmaktadır. Bu çıktıların işlenmesi, iletilmesi, korunması, saklanması ve sürekliliğinin sağlanması süreçlerinde birtakım varlıklar ile ilişkisi bulunmaktadır. Bilginin ilişki içerisinde bulunduğu bu varlıklar bilgi varlıkları olarak kabul edilmektedir. Bilgi varlıkları içerisinde bilginin kendisi ile birlikte bulunduğu ortamda önemli yer tutmaktadır. Hatta bu ortamların bulunduğu alanlar ve erişimi için kullanılan ağ ve iletişim sistemleri de bilgi varlıkları içerisinde yer almaktadır.

Bu itibarla varlık; kurum için değeri olan kavranabilir ve algılanabilir bilgi, yazılım, donanım, hizmet, çevre, itibar, imaj ve çalışan gibi somut ve soyut şeyler olarak tanımlanmaktadır. Bilgi varlığı ise bir kurum için değerli olan ve sürekli saklanması

ve gizliliğinin sağlanması gereken varlıklar olarak tanımlanmaktadır (ISO, 2015; ISO, 2018).

Kurum veya kişiler için maddi ve manevi değere sahip olan tüm unsurlar, bilgi varlığı kapsamında değerlendirilmekte ve bu nedenle güvenliğinin sağlanması gerekmektedir. Bilgi varlıkları, bir kurumun veya kişinin faaliyetlerini sürdürmek, rekabet avantajı elde etmek, müşteri ilişkilerini yönetmek ve itibarını korumak için kullandığı önemli varlıklardır.

Bilgi varlıkları çeşitli şekillerde ortaya çıkabilir. Bunlar, ticari sırlar, patentler, telif hakları, finansal bilgiler, müşteri verileri, stratejik planlar, iş sürekliliği planları, çalışan bilgileri, üretim süreçleri gibi yazılı veya elektronik dokümanlar olabilir. Bu dokümanlar haricinde dosyalar, raporlar, veri tabanları, personel dosyaları, müşteri bilgileri, politikalar, iş süreçleri, iletişim ağları, sistem odaları, bilgisayar, ağ, telefon, sunucu, switch, yazıcı, mobil cihazlar gibi bilişim sistemleri ve donanımlar da bilgi varlıkları içerisinde değerlendirilmektedir. Ayrıca, bir kurumun veya kişinin itibarı ve marka değeri de önemli bir bilgi varlığı olarak kabul edilmektedir.

ISO 27001 (2022)'de varlık yönetimine ilişkin varlıkların sorumluluğuna yönelik kontroller listelenmektedir. Varlıkların sorumluluğu, kuruluşun varlıklarını tespit etmeyi ve uygun koruma sorumluluklarını tanımlamayı amaçlamaktadır. Bu başlık altında listelenen kontroller şu şekilde sıralanmaktadır:

- Varlıkların envanteri: Bilgi ve bilgi işleme olanakları ile ilgili varlıklar belirlenmeli ve bu varlıkların bir envanteri çıkarılmalı ve yönetilmelidir.
- Varlıkların sahipliği: Envanterde tutulan tüm varlıklara sahip sorumlu atamalar yapılmalıdır.
- Varlıkların kabul edilebilir kullanımı: Bilgi ve bilgi işleme tesisleri ile ilgili varlıklarını kabul edilebilir kullanımına dair kurallar belirlenmeli, yazılı hale getirilmeli ve uygulanmalıdır.
- Varlıkların iadesi: Tüm çalışanlar ve dış tarafların kullanıcıları, istihdamlarının, sözleşme veya anlaşmalarının sonlandırılmasının ardından ellerinde olan tüm kurumsal varlıkları ifade etmelidirler.

Kurum ve kuruluşların faaliyetlerinde olumlu olumsuz her türlü etkiye sahip olan bilgi varlıklarının belirlenmesi önemlidir. Varlık envanterinin oluşturulmasında,

hangi bilgi varlığı türünün hangi kapsamda değerlendirilmesi gerektiğini belirlemek önemlidir. Bu envanter genellikle yazılım ve donanım kategorilerine odaklanarak, diğer bilgi varlıklarının önemini yeterince yansıtmayabilir. Bilgi varlıkları, yazılım, donanım, ağ altyapısı, yapısal varlıklar (bina, tesis, saha), personel, destek hizmetleri (ısıtma, havalandırma, enerji vb.) gibi çeşitli kategorilerde değerlendirilmelidir. Bilgi varlıklarının envanterinin hatalı veya eksik belirlenmesi, kurumların risk analizi gibi önemli faaliyetlerin etkilenmesine neden olabilir. Bu nedenle, kapsamlı bir envanter oluşturmak ve tüm bilgi varlıklarını dikkate almak önemlidir (Kim ve Solomon, 2018).

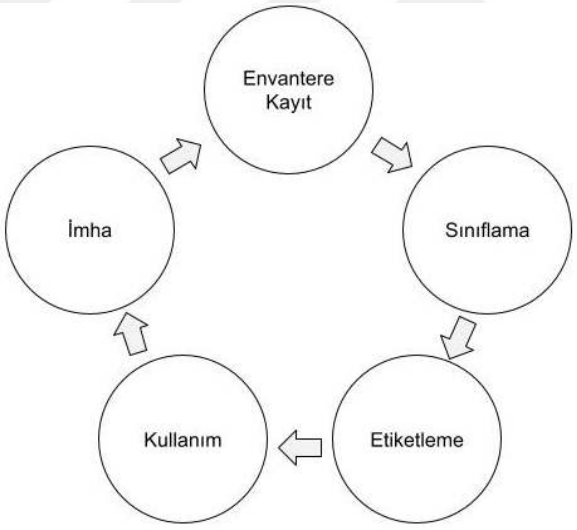
Bilgi varlıkları; bilginin içeriğine, niteliğine, erişime sunulmasına, iletilmesine, bulunduğu ortama ve muhafaza altına alınmasına göre farklı kategorilerde sınıflandırılmaktadır. Bilgi varlıklarının eksik veya hatalı tespit edilmesi, kurum ve kuruluşların risk analizleri başta olmak üzere birçok süreçlerinde hatalar oluşturabilmektedir. Varlık gruplandırmaları genel olarak şu şekilde kategorilendirilmektedir (Çubukçu, 2018):

- **Donanımlar:** Bilgisayarlar, sunucular, yazıcılar, dizüstü bilgisayarlar, bellek aygıtları, telefonlar, mobil aygıtlar, modem, switch, iletişim araçları vb. teknolojik cihazlardır.
- **Yazılımlar:** Sistem, uygulama, grafik yazılımları, yazılım geliştirme araçları vb. uygulamaları içermektedir.
- **Ağlar:** İnternet, yerel ağlar vb. iletişim ağlarını kapsamaktadır.
- **Bilgiler:** Elektronik dosyalar, çizim dosyaları, resimler, basılı dokümanlar, evraklar, anlaşmalar gibi dijital donanımlar üzerindeki dosyalar ve kâğıt üzerindeki bilgilerdir.
- **Fiziksel Tesis ve Ortamlar:** Sitem odası, arşiv odası, ısıtma ve aydınlatma cihazları vb. fiziksel ve çevresel bölümleri içermektedir.
- **Hizmetler:** Danışmanlık hizmetleri, iletişim hizmetleri, teknik destek hizmetleri vb. kurumsal faaliyetlerden oluşmaktadır.
- **Personel ve Müşteri:** Bilgi varlıklarına sahip ve kullanan kişilerin bilgilerini içermektedir.
- **Soyut varlıklar:** Kurum veya kuruluşa ait imaj ve itibar gibi değerlerdir.

- **Süreçler:** Bilgi işlem, finans, satın alma, insan kaynakları gibi süreçleri kapsamaktadır. İş süreçlerinin korunması ve kurumun iş sürekliliğinin sağlanması bakımından çok önemlidir. Bilgi güvenliği yönetim sisteminde iş süreçlerine çok önem verilmektedir. Bu nedenle süreçler de bir varlık olarak kabul edilmektedir.

Kurumun bilgi varlıklarının belirlenip envantere kayıt edilmesi ile başlayıp varlığın sınıflandırılması ve etiketlendirilmesi ile devam eden ve belirli bir süre sonra varlık ömrünü tamamlayarak imha etme süreci ile sona eren faaliyetler dizisine varlık yönetim süreci denilmektedir. Tüm bilgi varlıkları, bu yönetim sürecine göre işlerliklerine devam etmekte ve son bulmaktadır. Varlık yönetim süreci Şekil 2.1'de gösterilmektedir (Çubukçu, 2018):

Şekil 2.1: Varlık yönetim süreci



Kaynak: (Çubukçu, 2018)

2.3. Bilgi Varlıklarının Sınıflandırılması ve Etiketlenmesi

Bilgi ve iletişim teknolojilerinin gelişmesi ve kullanımlarının yaygınlaşması, bilgiyi ve bilgi ile ilişkili bütün nesneleri ve varlıkları değerli konuma getirmiştir. Özellikle bilgisayar ve internetin her ortamda kullanılması bilginin değerini daha da arttırmıştır. Bu teknolojilerin kullanıldığı bütün ortamlarda bilgi hızlı ve kolay bir biçimde daha çok insana ulaşmaya başlamıştır. Fakat niceliği artan bilginin paylaşılmasından kaynaklı birtakım olumsuzluklar da oluşmaya başlamıştır.

Özellikle yetkisiz ve izinsiz bilgi erişimleri bilgi varlığı sahiplerine ciddi zararlar vermeye başlamış; bu durum kişisel bilgi güvenliğinden ulusal bilgi güvenliğine geniş bir ortamı etkisi altına almıştır. Bilgi varlıklarının maruz kaldığı bu tehditler bilgi paylaşımında yeni düzenlemelerin yapılması gerekliliğini ortaya çıkarmıştır.

Bilginin paylaşım ve erişim süreçlerinde karşı karşıya kalınan riskler ve tehditler, bilgi varlıklarının gizlilik derecelerine göre sınıflandırma gereksinimini gerektirmektedir. Bilgi varlıklarının bulunduğu ortamlar, içerdiği bilgiler ve bu bilgilerin kapsamı, değeri, kullanım amacı, aidiyeti gibi birtakım özellikler dikkate alınarak bu varlıkların gizlilik dereceleri oluşturulmaktadır. Bu derecelendirme kriterleri ve sınıflandırmaları kurumdan kuruma değişebildiği gibi en genel sınıflandırma kategorilerini düzenleyen ülkeler arasında da değişebilmektedir. Örneğin Türkiye'de bilgi varlıklarının gizlilik derecelendirmesi genelde dört grupta (çok gizli, gizli, özel, hizmete özel) sınıflandırırken; ABD de ise üç grupta (çok gizli, gizli, özel) sınıflandırılmaktadır (Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkında Esaslar Hakkında Yönetmelik, 2022; Classified National Security Information, 2009).

Bilgi, bir kuruluşun en değerli varlığıdır. Bu varlıkları değer, duyarlılık ve kritiklik gibi belirli standartlara göre tanımlamak bilgi güvenliği açısından sağlam bir temel oluşturmaktadır. Veri sınıflandırılmasının iyi bir biçimde planlanması bilgi güvenliği risk yönetimi, yasal uygunluk ve verinin yaşam döngüsü açılarından önemli görülmektedir (Aggarwal, 2015).

Bilgi sınıflandırmada amaç, bilginin kurum için önemi derecesinde uygun seviyede korunmasını temin etmektir. ISO/IEC 27001 (2022a)'de varlık yönetimine ilişkin bilgi sınıflandırılmasına ilişkin kontroller şu başlıklar altında listelenmektedir:

- Bilgi sınıflandırması: Bilgi, yasal şartları, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyeti bibi özelliklerine göre sınıflandırılmalıdır.
- Bilgi etiketlemesi: Bilgi etiketleme için uygun bir prosedür kümesi kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.

- Varlıkların kullanımı: Varlıkların kullanımı için prosedürler, kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.

Kurumsal bilgilerin sınıflandırılması, belirli veri türlerinin korunmasını hedefleyen düzenlemelere dayanmaktadır. Bu sınıflandırma genellikle kişisel bilgiler, finansal bilgiler, sağlık bilgileri gibi değerli veri kategorilerini içermektedir. Verileri bu kategorileri göz önünde bulundurarak sınıflandırmak için şu kriterler dikkate alınmaktadır (Kim ve Solomon, 2018):

- Değer: Bilginin değerini yansıtan faktörler arasında kuruluşun itibarı, rakiplerin bilgiye erişim değeri, bilginin değiştirilmesi veya kaybedilmesi durumunda ortaya çıkacak maliyet gibi unsurlar bulunmaktadır. Bu ölçütlere dayanarak bilginin değeri belirlenmektedir.
- Duyarlılık: Bilgilerin bütünlüğünün ve erişiminin ihlal edilmesinin kurum üzerindeki etkisini ölçerek duyarlılık düzeyi belirlenmektedir. Bu ölçüt, pazar kaybı, güvenilirlik, itibar, maddi kayıplar ve sorumluluk gibi birçok yönden değerlendirilebilmektedir. Kurumlar, bu faktörleri dikkate alarak bilginin duyarlılık seviyesini belirlemekte ve uygun koruma önlemlerini seçmektedir.
- Kritiklik: Bilginin kuruluş misyonu açısından öneminin ölçüsünü yansıtmaktadır. "Bilgi kaybolursa veya ifşa olursa kuruluşa ne olur?" sorusunun sonuçlarını belirleyen ölçüttür.

Bilgi güvenliği kapsamında kurumsal bilgi varlıklarının sınıflandırılması, özetle bir kurumun sahip olduğu verilerin değer, duyarlılık ve kritiklik seviyelerine göre kategorize (gizli, harici ve dâhili bilgi) edilmesi olarak tanımlanabilir. Sağlıklı bir kurumsal bilgi sınıflandırması, kurumun belirlediği politika ve yönergeler çerçevesinde verilerin işlenmesini kolaylaştırmaktadır. Bu sınıflandırma, verilerin doğru bir şekilde kategorize edilmesini, önem derecelerinin belirlenmesini ve uygun güvenlik önlemlerinin alınmasını sağlamaktadır. Kurumsal bilgi sınıflandırmasında iyi bir risk değerlendirmesinin yapılması da önem arz etmektedir. Sınıflandırılma aşamasında verinin kritiklik seviyesinin belirlenmesi verinin çalınması, değiştirilmesi veya yok edilmesi kapsamında kurumda oluşabilecek etkileri en aza indirgemektedir. Bu açıdan kurumun bilgi güvenliği risk profili ve kültürü önemli rol oynamaktadır.

Kurumlar, farklı derecelere sahip kurumsal bilgi sınıflandırma şemalarını kullanmaktadır. Çoğu kurum, bilgilerin gizliliğini ve bütünlüğünü sağlamaya yönelik bilgi sınıflandırma şemalarını öncelikli olarak benimsemektedir. Bilgi sahibi kurumlar, doğru bir şekilde sınıflandırılan ve uygun erişim kontrolleriyle sunulan verilere güvendiklerinden emin olmak için belirli periyotlarla bilgi sınıflandırma sistemlerini gözden geçirmelidir. Kurumsal bilgilerin önem derecesi basit düzeyde şu üç kategoride gruplandırılmaktadır (Whitman ve Mattord, 2018).

- Gizli Bilgi: Kurum içerisinde sıkı bir biçimde kontrol altında tutulması gereken hassas bilgileri içermektedir. Bu kategori içerisinde sınıflandırılmış bilgiye erişim belirli şartlara bağlanmaktadır. Bu sınıflama sistemindeki bilgiler, "özel" veya "hassas" bilgi olarak da adlandırılmaktadır.
- Dâhili Bilgi: Gizli bilgi kategorisindeki ölçütleri karşılamayan tüm kurum içi bilgiler bu kategori içerisinde değerlendirilmektedir. Bu kategoride sınıflandırılan bilgiler yalnızca kurum çalışanları, yetkili yükleniciler ve diğer üçüncü şahıslar tarafından görüntülenebilmektedir.
- Harici Bilgi: Yönetim tarafından kamuya açıklanmak üzere onaylanmış tüm bilgileri kapsamaktadır.

Bilgi güvenliğine en çok değer veren devletlerin başında gelen ABD'de, Information Security Oversight Office (ISOO) tarafından gizli bilgilerin sınıflandırılmasına yönelik hazırlanan "Classified National Security Information" adlı kararname başkanlık emri ile yürütülmektedir. Bu yasal belge, ABD'de ulusal güvenlik bilgilerinin korunmasına, sınıflandırılmasına ve gizliliğinin sağlanmasına yönelik tek tip bir sınıflama sistemi işletmektedir. Bu kararnamede bilgilerin sınıflandırması ile ilgili standartlar ve düzeyler şu biçimde sıralanmaktadır (U.S. Department of Justice, 2009):

Sınıflandırma Standartları;

- Yetkili bir sınıflandırma otoritesi tarafından gerçekleştirilir.
- Sınıflandırma otoritesi, Birleşik Devletler Hükümetine ait olan veya onun için üretilen bilgilerin kontrolünün yine Birleşik Devletler Hükümetine ait olduğunu belirler.

- Sınıflandırılacak bilgiler, aşağıdaki kategorilerden birine veya birkaçına girmelidir:
    - Askeri planlar, silah sistemleri veya operasyonlar,
    - Yabancı hükümet bilgileri,
    - İstihbarat faaliyetleri, istihbarat kaynakları veya yöntemleri veya kriptoloji,
    - Amerika Birleşik Devletleri'nin dış ilişkileri veya dış faaliyetleriyle ilgili konular, ulusal güvenlikle ilgili bilimsel, teknolojik ve ekonomik konular,
    - Nükleer materyalleri veya tesisleri korumaya yönelik programlar,
    - Ulusal güvenlikle ilgili sistemlerin, kurulumların, altyapıların, projelerin, planların veya koruma hizmetlerinin zayıflıkları veya yetenekleri,
    - Kitle imha silahlarının geliştirilmesi, üretilmesi ve kullanılması gibi konular,
- Yetkili sınıflandırma otoritesi, bilginin izinsiz olarak ifşa edilmesi durumunda, ulusal güvenliğe zarar vermesinin makul bir şekilde beklenebileceği olası zararı tanımlar.

Sınıflandırma Düzeyleri;

- Çok Gizli (Top Secret): İfşası halinde ulusal güvenliğe son derece ağır hasarlar vermesi beklenen bilgilere uygulanır.
- Gizli (Secret): İfşası halinde ulusal güvenliğe ciddi zararlar vermesi makul olarak beklenen bilgilere uygulanır.
- Özel (Confidential): İfşası halinde ulusal güvenliğe zarar vermesi makul bir şekilde beklenen bilgilere uygulanır.

Bu sınıflama sisteminde bilgiler, "beşikten mezara" tabirine eşdeğer biçimde koruma altına alınmaktadır. Diğer bir ifadeyle, kişilere veya kurumlara ait gizli bilgiler resmi olarak açıklanana kadar bilgi güvenliği kapsamında koruma altına alınmaktadır. Devlet ayrıca ilgili bilgi kategorilerine ait bilgileri korumak için personel bilgilendirme ve değerlendirme raporları gibi bazı özel sınıflama derecelendirmelerini de uygulamaktadır (Kaiser, 2008).

NATO, “Security Within The North Atlantic Treaty Organization” isimli dokümanda gizli bilgilerin güvenlik sınıflandırılmasını dört kategoride ele almaktadır. Bu sınıflandırma, NATO üyesi devletlerin güvenliğine zarar gelmemesi için bilgilerin korunmasını amaçlamaktadır. Bu bilgi sınıflandırma sistemi şu şekilde sıralanmaktadır (North Atlantic Council, 2002):

- Kozmik Çok Gizli (Cosmic Top Secret): Yetkisiz ifşası, NATO’ya son derecede ağır zarar veren bilgileri içerir.
- NATO Gizli (NATO Secret): Yetkisiz ifşası, NATO’ya ciddi zarar veren bilgileri içerir.
- NATO Özel (NATO Confidential): Yetkisiz ifşası, NATO’ya zarar veren bilgileri içerir.
- NATO Hizmete Özel (NATO Restricted): Yetkisiz ifşası, NATO’nun menfaatlerine ya da etkinliğine zarar veren bilgileri içerir.

NATO’da güvenlik sınıflandırmasına tabi olmayan bilgiler “NATO Tasnif Dışı (NATO Unclassified)” ve “Kamuya Açıklanabilir Bilgiler” olarak nitelendirilmektedir. Örneğin, NATO ile ilgili haberler ve NATO’nun basın açıklamaları kamuya açıklanabilir bilgi niteliğinde olduğu için herhangi bir gizlilik ibaresi taşımamaktadır. Nato Tasnif Dışı ibaresi taşıyan bilgiler ise resmi maksatta kullanabilmektedir. Bu sınıftaki belgelerde “yayım kısıtlama ya da idari” ibareler kullanılarak bilgilerin açıklanması özel kurallara tabi kılınmıştır.

Avrupa Birliği (AB), gizli bilgilerin korunmasına yönelik kapsamlı bir güvenlik sisteminin kurulmasını öngören “The Security Rules for Protecting EU Classified Information” adında bir konsey kararı yayımlamıştır. Bu doküman ile Avrupa Birliğinin veya bir veya daha fazla üye devletin çıkarlarına zarar verebilecek herhangi bir bilginin veya materyalin ifşası önlenmeye çalışılmaktadır. Bilgi ve belgelerin güvenlik sınıflandırmaları dört kategoriye tabi tutulmaktadır (Council of the European Union, 2013):

- AB Çok Gizli (EU Top Secret) :Yetkisiz ifşa, Avrupa Birliğinin ya da en az bir üye devletin temel çıkarlarına son derecede ağır zarar veren bilgileri ve materyalleri içerir.

- AB Gizli (EU Secret): Yetkisiz ifşa, Avrupa Birliğinin ya da en az bir üye devletin temel çıkarlarına ciddi veren bilgileri ve materyalleri içerir.
- AB Özel (Confidential): Yetkisiz ifşa, Avrupa Birliğinin ya da en az bir üye devletin temel çıkarlarına zarar vermesi muhtemel olan bilgileri ve materyalleri içerir.
- NATO Hizmete Özel (NATO Restricted): Yetkisiz ifşa, Avrupa Birliğinin ya da en az bir üye devletin çıkarları açısından dezavantaj oluşturması muhtemel olan bilgileri ve materyalleri içerir.

Avrupa Birliğinde kullanılmakta olan bu sınıflandırmada belirtilen kategorilere ek olarak sınıflandırılmış bilginin hangi faaliyet alanına ait olduğunu belirlemek, bu bilgiyi özel bir dağıtıma tabi tutmak ve erişimini kısıtlamak amacıyla "ikaz (caveat)" ve "kod (code)" işaretlemeleri de kullanılmaktadır.

Türkiye'de gizlilik dereceli yazılara ilişkin sınıflandırmalar "Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022)" ile düzenlenmektedir. Kamu kurum ve kuruluşları yürüttükleri faaliyetlerde üretilen bilgi ve belgelerin gizlilik derecelendirmelerini bu yasal doküman çerçevesinde düzenlemektedir. Genel kuralları korunmakla birlikte sonraki yıllarda yeni düzenlemeler ile güncellenen bu doküman esasları günümüzde de yürütülmektedir. Bu dokümana göre Türkiye'de bilgi ve belgelerin gizlilik dereceleri dört kategoride sınırlanmaktadır:

- Çok Gizli: Müsaadesiz açıklandığı takdirde, millî menfaatlere hayati bakımdan son derece büyük zarar verecek olan ve güvenlik bakımından olağanüstü önemi haiz mesaj ve dokümanları kapsar.
- Gizli: Müsaadesiz açıklandığı takdirde, millî güvenliğe, prestij ve menfaatlere ciddi suretle zara verecek ve diğer yandan, yabancı bir devlete geniş faydalar temin edecek mahiyette olan mesaj ve dokümanları kapsar.
- Özel: Müsaadesiz açıklandığı takdirde milli menfaate ve prestijine zarar verecek veya bir şahsın zarar görmesine veya yabancı bir devlete fayda telkin edici mahiyette olan mesaj ve dokümanları kapsar.
- Hizmete Özel: Çok gizli, gizli ve özel gizlilik dereceleriyle korunması gerekmeyen ve fakat bilmesi gerekenlerden başkasının bilmesine lüzum görülmeyen mesaj ve dokümanları kapsar.

İlgili mevzuatta bu gizlilik dereceleri ile belirtilmeyen "Tasnif Dışı" ibaresine de ayrı bir kategoride yer verilmektedir. Bu grupta değerlendirilen bilgi ve belgeler gizlilik derecesi içerisinde değerlendirilmediğinden, belgelerin üzerlerine veya üst verilerine yazılmamaktadır. Ayrıca elektronik ortamda gizlilik derecesi taşıyan belgelerin üretilmesine ilişkin yeni düzenlemeler yürütülmektedir. Yeni düzenlemeler ile "Hizmete Özel" haricindeki diğer gruplarda yer alan gizlilik dereceli belgelerin elektronik ortamda üretilmesinin önüne geçilmiştir. Böylelikle kamu kurum ve kuruluşların "Hizmete Özel" nitelikteki belgelerinin elektronik ortamda işlem görmesi sağlanmıştır (Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, 2014)

Varlıkların etiketlendirilmesi, sınıflandırılmaya uygun bir biçimde varlıkların üzerinde veya gizli yerlerinde renklendirme, yazma veya dijital kimliklendirme ile yapılmaktadır. Örneğin dolaplara ya da klasörlere içerdiği evraklara veya bilgilere göre etiketler yapıştırılmaktadır. Elektronik dosyalarda alt ve üst başlık alanlarında sınıflandırma bilgisine uygun etiket bilgileri (gizli, çok gizli, şirkete özel vb.) ile sağlanmaktadır. Etiketleme işlemi bilgisayar donanımları üzerindeki varlıklar için çok kullanılmamakta olsa da harici disk, flash bellek, cd gibi aygıtlar üzerine bilgi değerine göre etiketleme yapılmaktadır. Sonuç olarak, kurumlar envanterindeki tüm bilgi varlıklarını geliştirdikleri bilgi güvenliği politikalarına ve prosedürlerine göre sınıflandırmakta ve etiketlemektedir (Çubukçu, 2018).

2.4. Bilgi Sistemleri ve Bileşenleri

ISO/IEC 27000:2018'de bilgi sistemi; uygulamaların, hizmetlerin, bilgi teknolojisi varlıklarının veya diğer bilgi işleme bileşenlerinin birleştiği bir küme olarak tanımlanmaktadır. Bilgi sistemi, bir kurumun veya örgütün bilgi üretme, toplama, kaydetme, saklama, işleme, görüntüleme ve aktarma gibi bir dizi işlevi yerine getirmek için kullanılan insan kaynağı ve teknoloji bütünüdür. Girdi, işlem ve çıktı olmak üzere üç temel aşamadan oluşan bilgi sistemleri, kurumların hizmetlerinin yürütülmesinde büyük kolaylıklar sağlamaktadır. Kurum içinden veya dışından girdi olarak sağlanan verilerin birtakım işlem sürecinden geçirilerek yararlı ve uygun bir çıktıya dönüşmesini sağlayan bu sistemlerin önemli bir özelliği ise, sistemin tekrar çalışabilmesini sağlayan geribildirim özelliğine sahip olmasıdır (Anameriç, 2005).

Bilgi sistemleri, kurum veya kişiler için veri toplama, işleme ve depolama gibi faaliyetlerin yürütüldüğü donanım, yazılım, ağ ve diğer sitemlerin birleşiminden oluşmaktadır. Bu itibarla bilgi sistemini ve içinde depolanan verileri koruyan faaliyetlerin toplamına bilgi sistemleri güvenliği denilmektedir. Devletler bu tür sistemleri bir takım yasal çalışmalar ile koruma altına almaya çalışmaktadır. Organizasyonlar bilgi sistemlerinde yaygın olarak yer alan bilgi türlerini (isim adres, doğum tarihi, sosyal güvenlik numarası, banka hesap numaraları, kamu hizmeti numaraları, sigorta poliçesi numaraları gibi bireylere özgü kişisel bilgiler; ticari sır, ürün geliştirme bilgileri, satış ve pazarlama stratejileri, finansal kayıtlar, telif hakları ve patentler gibi kurumsal fikri mülkiyet bilgileri; online bankacılık, online sağlık ve sigorta talepleri, e-ticaret ve e-devlet hizmetleri, çevrimiçi eğitim hizmetleri gibi online işlemler; ulusal güvenlik, askeri ve savunma bakanlığı stratejilerini içeren devlet fikri mülkiyet bilgileri) gözden geçirerek bunlara uygun güvenlik tedbirleri geliştirmektedirler (Kim ve Solomon, 2018).

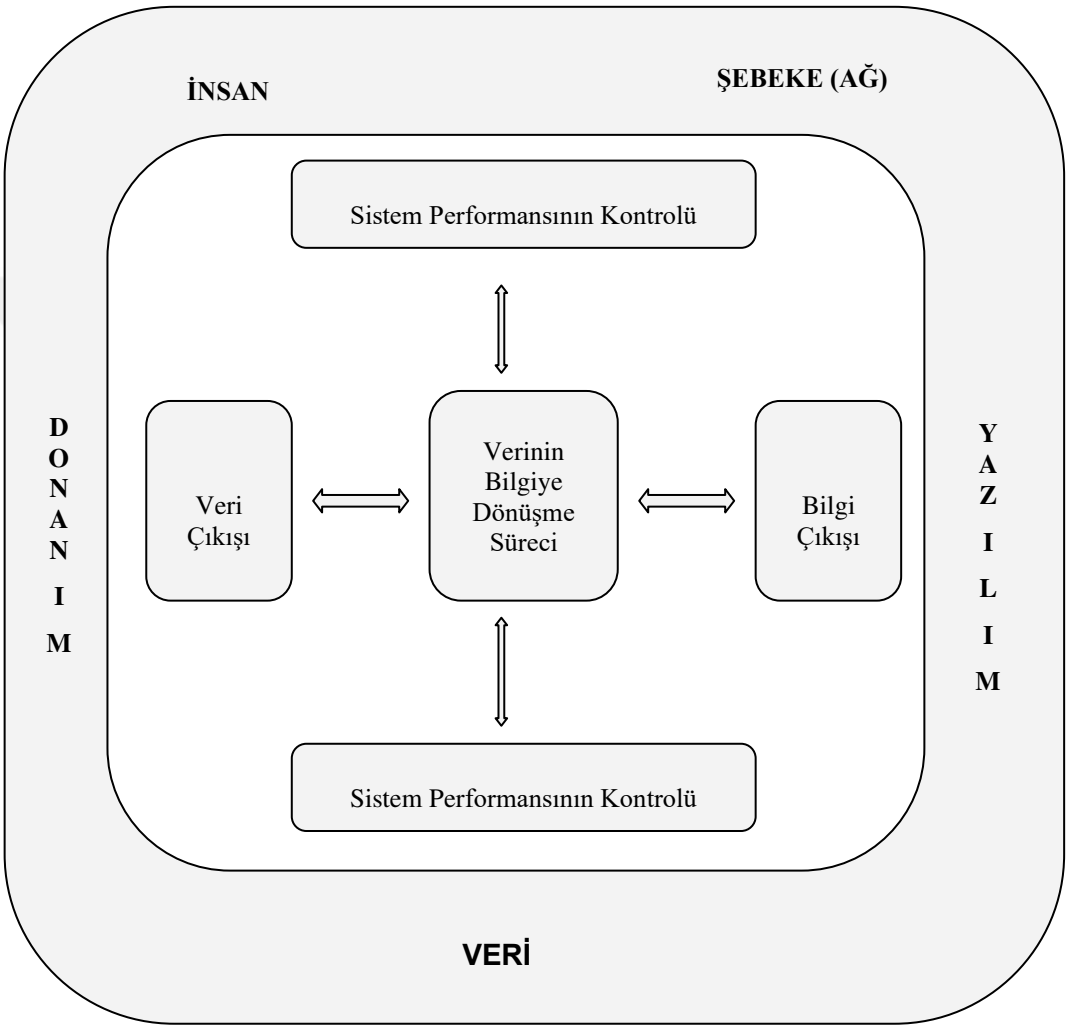
Bilgi sistemlerinin tasarım ve geliştirme aşamalarında bilgi güvenliği her zaman yeterince gözetilememektedir. Bu durum, kurumlar ve kuruluşlar tarafından kullanılan bilgi sistemlerinin çeşitli güvenlik tehditleriyle karşı karşıya kalmasına neden olmaktadır. Dolandırıcılık, casusluk, sabotaj, yangın ve sel gibi çeşitli kaynaklardan gelen güvenlik tehditleri, bu bilgi sistemlerine ve ağlara zarar verebilir. Kötü niyetli yazılımlar, bilgisayar korsanları ve hizmet engelleme saldırıları gibi unsurların yol açtığı zararlar, teknolojik ilerlemelerle birlikte giderek artmakta ve daha karmaşık bir hal almaktadır.

Bu bağlamda, bilgi güvenliği önlemleri ve stratejileri, bilgi sistemlerinin tasarım ve geliştirme süreçlerinde aktif olarak dikkate alınmalıdır. Güvenlik açıklarının belirlenmesi ve bunlara karşı koruyucu tedbirlerin alınması, bilgi sistemlerinin ve verilerin korunmasında hayati bir rol oynamaktadır.

Bilgi sistemi, veri kaynaklarını girdi olarak alıp süreçten geçiren ve çıktı olarak bilgi ürünlerini ortaya çıkaran bir sistemdir. Şekil 2.2'de görüldüğü üzere bilgi sistemi, veriyi bilgiye dönüştürmek için girdi, süreç, çıktı, saklama ve kontrol faaliyetlerini yerine getirirken insan, donanım, yazılım, veri ve ağ kaynaklarını kullanmaktadır. Beş ana kaynaktan oluştuğu görülen bu bilgi sistemi modeli, kurumlardaki bilgi

sistemlerinin çoğunda önemli rol oynamaktadır. Bilgi güvenliği yönetim sisteminde yer alan bu kaynaklar ana eleman olarak bilgi güvenliği sürecini etkilemektedir (O'Brien ve Marakas, 2006).

Şekil 2.2: Bilgi sistemini elemanları



Kaynak: (O'Brien ve Marakas, 2006).

Vacca, (2009), bilgi sistemleri güvenliğini; mantıksal güvenlik, fiziksel güvenlik ve çevre güvenliği olmak üzere üç ana bölüme ayırmaktadır. Mantıksal güvenlik, bilgi sistemlerinin uygulama ve iletişim ağları güvenliğini oluşturan unsurları ve bu unsurlar üzerinde maruz kalabileceği tehditleri kapsamaktadır. Fiziksel güvenlik, bilgi sistemlerinin alt yapısını oluşturan sunucu ve istemci donanımlarını, sistem

odası, bulunduğu yapıyı, güç hatlarını ve diğer fiziksel bileşenlerin güvenliğini kapsamaktadır. Çevre güvenliği ise fiziksel güvenlik ile birlikte işlemektedir. Bilgi sistemini barındıran bina, alan veya kampüs gibi sınırları belli olan bir çevre üzerinde etki eden beşeri veya doğal tehditleri kapsamaktadır.

Ayrıca bilgi sistemi, sadece bilgisayar donanımından oluşmayan birden fazla bileşene sahip insan, prosedür ve teknoloji kümesi olarak ifade eden Whitman ve Mattord (2018, 2019), bilgi sistemlerinin bileşenlerini yazılım, donanım, veri, ağ, prosedür ve insan olarak sıralamaktadır. Bu bileşenlerin yüklendiği görev ve özelliklerine ait bilgiler sırasıyla aşağıda verilmiştir.

Bilgi sistemlerinin bileşenlerinden biri olan yazılım, program uygulamalarını, işletim sistemlerini ve çeşitli yardımcı komut programları içermektedir. Yazılım, bilgi sistemi içerisinde en zor bileşen olarak görülmektedir. Yazılım programlaması sırasında oluşan hataların kullanılması, bilgi saldırılarının önemli bir bölümünü oluşturmaktadır. Bu hatalar ile dolu bozuk yazılımlar, günlük yaşamın birçok alanlarını olumsuz etkilemektedir. Bilgi teknolojisi endüstrisinde bu bozuk yazılımlardaki hataları, zayıflıkları ve diğer temel sorunları bildiren çok sayıda raporlar yayınlamaktadır (Redwine, 2006).

Yazılım, bir kurumdaki bilgi sistemlerinin can damarını oluşturmaktadır. Yazılım projeleri yönetiminde oluşan zaman, maliyet ve insan gücü kısıtlamaları ne yazık ki bilgi güvenliği açıklarına neden olabilecek bilgi sistemlerinin oluşmasına neden olmaktadır. Yazılım projelerinde bilgi güvenliği en baştan itibaren düşünülmesi ve bu gerçeklikte projelerin yürütülmesi gerektiği vurgulanmasına rağmen, bu durum genellikle bir düşünce olarak uygulanmaktadır. Bu biçimde üretilen yazılım programlarına sahip bilgi sistemleri kazara veya kasıtlı saldırıların kolay bir hedefi durumuna gelmektedir (Mead, Shoemaker ve Woody, 2015).

Yazılımların kullanılmaya başlandığı ilk yıllarda kaliteli ve olgun yazılım üretme düşüncesi, son yıllarda güvenli yazılım geliştirme anlayışına dönüşmüştür. Bu gelişmedeki en büyük etki bilgi sistemlerindeki yazılım kaynaklı artan güvenlik açıklarıdır. Artan bu güvenlik tehditlerini en aza indirgemek, yazılım geliştiricilerine yeni maliyetler yüklemektedir. Yazılım geliştirme sürecinde yapılan hataların erken bir süreçte farkına varılarak düzeltilmesi, ileri süreçlerde farkına varılan açıklara göre

daha az maliyet oluşturacağı yazılım geliştiricileri tarafından yaygın bir biçimde kabul edilen ilke olarak görülmektedir. Bu ilke, güvenli yazılım geliştirme sürecinde maliyetin ne derecede önemli olduğunu göstermektedir. Maliyet dışında güvenli yazılım geliştirme sürecine etki eden dokuz temel güvenlik konusu bulunmaktadır (Özbilgin ve Özlü, 2010):

- Girdi Denetleme: Bir sistem veya programın kullanıcıdan alınan verileri doğrulamak ve geçerli olup olmadığını kontrol etmek için yapılan bir süreçtir.
- Kimlik Doğrulama: Bilgi varlıklarının (kullanıcı, donanım veya bir uygulama programı gibi) kimlik doğrulama yöntemlerinin kontrolünden geçmesidir.
- Yetkilendirme: Kimlik doğrulama sonrasında kullanıcının erişim haklarının belirlendiği ve kontrolünün gerçekleştiği aşamadır.
- Konfigürasyon Yönetimi: Yazılım uygulaması ile ilgili hassas bilgilerin nitelendirildiği, şifrelenerek muhafaza edildiği ve bu dosyalara erişim kayıtlarının tutulduğu işlemleri kapsamaktadır. Örneğin bir veri tabanına erişim için gerekli bilgileri muhafaza eden dosyalar bu kapsamda işlemektedir.
- Hassas Bilgi: Yazılım güvenliği için uygulama sahibi ile geliştiricisinin işin niteliğine uygun hassas bilgileri içeren bir politika oluşturmalıdır.
- Kriptografi: Bilginin korunması için şifrelenmeli ve zamanla gözden geçirilerek güncellenmelidir.
- Parametre Manipülasyonu: Dağıtık algoritmaların modülleri arasında yer alan parametrelerin değiştirilmesi ile oluşan saldırıdır.
- Hata Yönetimi: Bazı teknolojiler hataları kullanarak hata yönetimi gerçekleştirmektedirler.
- Kayıt Tutma ve Denetim: Uygulama sürecine ilişkin şablon tanımlanmalı ve sürekli denetim altında tutulmalıdır.

Donanım, yazılım bileşenine ev sahipliği yapan, verileri depolayan ve aktaran, bilgi girişi ve çıkışı için ara yüzler sağlayan teknolojik varlıklardır. Donanımlar, bilgi sistemlerinin işlerliğini devam ettiren teknolojik ürünlerdir. Bu ürünler her geçen gün gelişmekte ve kullanımları daha da yaygınlaşmaktadır. Çoğu bilgi sisteminin bilgi güvenliği düzeyini garanti edemeyen donanım platformları üzerine kurulmuş sınırsız erişim noktaları bulunmaktadır (Whitman ve Mattord, 2018). Bu kapsamda

donanımları fiziksel birer varlık olarak ele alan ve bu varlıkları fiziksel tehditlerden korumasını sağlayan fiziksel güvenlik politikaları oluşturulmaktadır. Fiziksel güvenlik ihlalleri, bilgi kayıplarına neden olacağından bilgisayarların ve diğer donanımların fiziksel konumlarını korumak önemlidir.

Bilgi sistemlerinin fiziksel boyutunu oluşturan donanım bileşeni, kurum ve kuruluşların faaliyetlerinde önemli yere sahiptir. Birçok kuruluş hangi bilgi sistemi donanımlarına sahip olduklarını bilmemektedir. Kuruluş içerisinde hangi donanımın hangi bölüm veya çalışan tarafından kullanıldığına ilişkin donanım envanterinin bulunmaması, bilgi sistemlerinin güvenliği açısından ciddi bir boşluktur. Donanım envanterlerinin belirlenmemesi yangın, arıza veya hırsızlık gibi herhangi bir fiziksel güvenlik tehdidine karşı alınacak önlemlerin yavaşlamasına neden olabilmektedir. Fiziksel veya diğer güvenlik tehditlerinden etkilenen donanımın aidiyet bilgilerini tespit edememek, o donanımın güvenliğine ilişkin alınacak önlemleri de engellemektedir (Kim ve Solomon, 2018).

Veri, işlenmemiş ham bilgidir. Veri ile bilgi kavramları alanyazında çokça karıştırılmakta ve aralarındaki fark tanımlarla ortaya konulmaktadır. Bilgi (information), verinin işlenmiş anlamlı halidir (Şekil 2.3). Bilgi sistemlerinde veri denilince akla ilk olarak bu sistemlerde yer alan anlamlı bilgiler gelse de aslında bir bilgi sistemi için veri ham gerçektir. Bu anlam karmaşasından dolayı veri ile bilgi terimleri günümüzde çokça karıştırılmakta hatta birbirlerinin yerine kullanıldığı görülmektedir.

Şekil 2.3: Verinin bilgiye dönüşüm süreci

Veri, bir grup sayı, harf, metin, resim, ses kaydı gibi bir takım özel karakterlerden oluşmaktadır. Örneğin, 102829577899 numarası bir banka hesap numarası, bir üniversiteye ait kayıt numarası, bir kişiye ait kimlik numarası veya bir güvenlik numarası olabilir. Bu örnekteki sayı grubu gibi bir grup sayı veya harften oluşmuş veri ham bir gerçeği yansıtmaktadır. Bu nedenle veri olarak adlandırılmaktadır. Bilgi ise, verilerin işlenmesi sonucu oluşan verinin anlamlı duruma gelmiş halidir. Bilgi,

karar vermeyi sağlayan ilgili veriler grubundan oluşmaktadır. Başka bir ifadeyle, bilgi verilere açıklık getirmektedir (Chopra ve Chaudhary, 2020).

Bilgi sistemleri tarafından işlenen, depolanan ve iletilen verilerin korunması gerekmektedir. Veriler, bir kuruluşun en değerli bilgi varlıklarıdır. Bu varlıklar kötü ve yetkisiz kullanım amaçlı saldırıların ana hedefinde bulunmaktadır. Bu nedenle son yıllarda bilgi sistemlerinin güvenliğini daha da arttırmak amacıyla veritabanı yönetim sistemlerinin kullanıldığı görülmektedir. Veritabanlarının doğru uygulanması, verilerin güvenliğini daha da arttırmaktadır. Fakat birçok bilgi sisteminin veritabanı yönetim sisteminin güvenlik özelliklerinden tam olarak yararlanmadığı ve bazı durumlarda geleneksel dosya sistemlerinden daha az güvenli olacak biçimde uygulandığı ifade edilmektedir (Kim ve Solomon, 2018). Bu nedenle güvenli veritabanı uygulamalarının geliştirilememesi ve uygulanamaması kâğıt ve dosya gibi fiziksel formlarda bulunan bilgilerin güvenliğini elektronik ve bilgisayar tabanlı sistemlerdeki dijital bilgiler kadar önemli duruma getirmektedir.

Ağ, artan bilgi güvenliği gereksiniminde büyük paya sahip olan bilgi sistemi bileşenidir. Yerel ağ bağlantıları ile birbirine bağlanan bilgi sistemlerinde ortaya çıkan güvenlik sorunları, internet gibi geniş ağ yapıları ile hızla artmaktadır. Ağ işlevleri ile donatılan bilgisayar teknolojisini kullanarak bilgilerini daha erişilebilir duruma getirmek isteyen kurumlar, daha çok güvenlik tehdidiyle karşı karşıya gelmektedir. Ağların zayıf noktaları kullanılarak yapılan saldırılar neticesinde değerli olan bilgilere yetkisiz erişim sağlanabilmektedir. Ayrıca kurum çalışanlarının bilinçsizce yaptıkları hatalar veya kasıtlı eylemler neticesinde birçok bilgi ağlar üzerinden yetkisiz kişilerin eline geçmekte ve kötüye kullanılmaktadır. Bu durum dış dünya ile irtibatını ağ yapıları üzerinden sağlayan kurumların güvenlik anlayışlarını değiştirme zorlamaktadır.

Bilgi sistemlerine izinsiz girişleri tespit etmek ve devam eden tehlikeleri haberdar etmek için geliştirilen ağ güvenliği uygulamaları ve politikaları bilgi güvenliği açısından önemlidir (Karaarslan, Teke ve Şengonca, 2003). Güvenlik duvarı ve şifreleme gibi uygulamalar ile ağların güvenli kullanımına ilişkin kuralları belirleyen politikalar bilgilerin korunmasında önem arz etmektedir. Güvenlik politikası olmadan güvenli bir ağ yapısından bahsetmek mümkün değildir. Ağ güvenlik politikaları, bilgi sistemlerinde olası bir güvenlik sorunu ile karşılaşmadan önce

oluşturulması ve uygulanması gerekmektedir. Bu nedenle bir güvenlik politikası oluşturulmadan güvenli bir bilgisayar ağı kullanımının gerçekleştirmesi doğru bulunmamaktadır. Ağ güvenlik politikaları, kurum ve kuruluşların yapılarına, faaliyetlerine, gereksinimlerine ve kullanılan ağların özelliklerine göre değişiklik gösterebilmektedir. Bilgi ve ağ güvenlik politikalarından bahsedildiğinde birçok politikanın olduğu görülmektedir. Çünkü bu politikalar bilgi sistemlerinde kullanılan teknolojiye ve faaliyet alanlarına özgü olabilmektedir. Ağ güvenliğine ilişkin oluşturulan başlıca temel politikalar şu şekilde sıralanmaktadır (SANS Institute, 2021):

- Kabul edilebilir kullanım politikası
- Kabul edilebilir şifreleme politikası
- Uzaktan erişim politikası
- Yönlendirici ve anahtar güvenlik politikası
- Web uygulaması güvenlik politikası
- Ağ güvenlik duvarı politikası
- İnternet ağı politikası
- Şifre koruma politikası
- İş istasyonu güvenliği politikası

Prosedürler, politika ve standartların sağlıklı bir biçimde nasıl kullanılacağını belirleyen yazılı talimatlardır. Bir güvenlik sisteminin gereksinimini, sürecini ve amacını belirleyen sistematik eylemlerden oluşmaktadır. Bilgi sistemlerine ait güvenlik kontrollerinin eylem planını, kurulumunu, denenmesini ve denetimini içermektedir. Kurumların bilgi güvenliği için oluşturulan en güçlü dokümanlardan biridir. Bilgi sistemlerinin güvenliği kapsamında sıklıkla gözden kaçırılan bir bileşen olarak görülmektedir (Kim ve Solomon, 2018).

Bir organizasyona ait bilgi güvenliği prosedürünün yetkisiz kullanıcılar tarafından ele geçirilmesi bilgilerin bütünlüğü açısından tehdit oluşturmaktadır. Örneğin, bir bankanın danışmanın bilgisayar merkezi güvenlik prosedürlerini kullanarak fonların nasıl aktarılacağı ile ilgili bilgileri öğrenmesi ve milyonlarca doları kendi hesabına havale etmesi bu bileşenin ne derecede önemli olduğunu göstermektedir. Çoğu kuruluş, bilgi sistemlerine erişebilmeleri için güvenlik prosedürlerini çalışanları ile paylaşmaktadır. Ancak bu prosedürlerin güvenli bir biçimde kullanılmasında

kuruluşlar genellikle başarısız olmaktadır. Kuruluşlar, bu durumun önüne geçebilmek için bilgi güvenliği organizasyonlarından eğitim destekleri almakta ve çalışanlarını bu konuda sürekli denetim altında tutmaktadır. Çalışanları güvenli koruma prosedürleri konusunda eğitmek, bilgi sistemini fiziksel olarak güvence altına almak kadar önemli görülmektedir (Whitman ve Mattord, 2018). Sonuç itibariyle kurumların bilgi sistemleri için oluşturulan bu prosedürler de kendi başına sadece bir bilgi konumunda bulunmaktadır. Bu nedenle prosedürlerde belirlenen talimat bilgilerinin de diğer tüm kritik bilgiler gibi bir kuruluş çalışanları arasında sağlıklı kullanımını destekleyecek eğitimlerin verilmesi önem arz etmektedir.

İnsan bileşeni ise, bilgi sistemlerinin güvenliği konusunda göz ardı edilmesine rağmen bilgi güvenliği için her zaman tehdit riski taşıyan unsur olarak kabul edilmektedir. İnsan varoluşundan itibaren yaşamını sürdürebilme mücadelesinde çevresine tehdit oluşturduğu gibi kendisi için de tehdit oluşturabilmektedir. Bu durum günümüzde de en üst seviyede gerçekleşmektedir. İnsan, kurumların bilgi güvenliği programlarındaki en zayıf halkadır. İnsan unsurunun bilgi sistemlerine yanlışlıkla veya isteyerek zarar vermesini önlemek için eğitilmesi gerekmektedir. Eğitim-öğretim, politika ve teknoloji olguları düzgün bir biçimde kullanılmadıkça insan unsuru bilgi güvenliği yönetiminde en zayıf halka olarak varlığını sürdürecektir.

Sosyal mühendislik faaliyetleriyle insanlar psikolojik manipülasyon altına alınabilmektedir (Hatfield, 2019). Psikolojik manipülasyon, insanları kendi bilgileri dışında veya istemedikleri hâlde etkileme veya yönlendirme eylemidir. “Kişinin çıkarlarına uygun olabilecek veya olmayabilecek bir eylemde bulunmasını etkileyen herhangi bir eylem” (Security Through Education, 2021) olarak tanımlanan sosyal mühendislik, bilgi güvenliği bağlamında ise eylemleri gerçekleştirmeye veya gizli bilgileri ifşa etmeye yönelik olarak insanların psikolojik manipülasyonu olarak tanımlanmaktadır (Siberay, 2021). Belirli bir sistem veya bilgiye erişim sağlamak amacıyla, insanlara güven duygusu aşılayarak bilgi güvenliği tehdidi oluşturulmaktadır. Bu yöntem, planlı bir dizi adımdan oluşması ve geleneksel hile yöntemlerinden farklı olmasıyla öne çıkmaktadır. Temelde, hedef kişilerin güvenini kazanarak, onları manipüle ederek veya kandırarak sisteme veya bilgilere erişim sağlanmaya çalışılmaktadır. Bu şekilde, insanların doğal güven duygusu ve istekleri

kullanılarak bilgi güvenliği açığı oluşturulmaktadır. Bu yöntem, toplumsal mühendislikle karıştırılmamalıdır, çünkü toplumsal mühendislik daha geniş bir kavramdır ve farklı taktikler ve stratejiler içermektedir.

İnsanlar, hizmet ettikleri kurumlardaki bilgi güvenliği kültürüne büyük etkileri bulunmaktadır. Lim ve diğerleri (2009), bilgi güvenliği kültürünü "her türden bilginin korunmasına katkıda bulunan bir kuruluştaki davranış kalıplarının toplamıdır" olarak ifade etmektedir. İnsanların kurumsal bilgi güvenliği kültürüne olumlu yönde bir katkı sağlamadıkları, genellikle kurumsal bilgi güvenliği çıkarlarını göz ardı eden eylemler içerisinde bulundukları belirtilmektedir (Andersson ve diğerleri, 2014). Bu nedenle araştırmalarda bilgi güvenliği kültürünün geliştirilmesi ve bu yönde bir takım adımların atılması gerekliliği savunulmaktadır (Anderson, 2008; Schlienger ve Teufel, 2003). Bunlar şu şekilde sıralanmaktadır:

- Ön değerlendirme: Kurum çalışanları arasındaki bilgi güvenliği farkındalığının düzeyinin belirlenmesi ve mevcut bilgi güvenliği politikasını analiz edilmesi.
- Stratejik planlama: Bilgi güvenliği farkındalığının daha iyi oluşması için net hedefleri içeren programların belirlenmesi.
- Operatif planlama: Kurum içi iletişim, çalışanların güvenlik bilinci, yönetimin katılımı ve eğitim programlarına dayalı iyi bir güvenlik kültürünün oluşturulması.
- Uygulama: Yönetimin ve çalışanların katılımının, kurum üyeleri arasındaki iletişimin ve tüm kurum üyelerine bilgi güvenliği eğitim kurslarının sağlanması.
- Son değerlendirme: Uygulama aşamasında programlanan bilgi güvenliği kültürünün değerlendirilmesi.

2.5. Güvenlik İhtiyacı

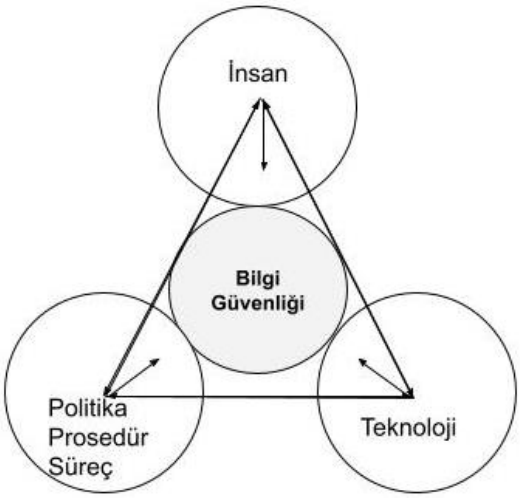
Güvenlik, koruma amacıyla uygulanan tedbirlerin yönetimidir. Kasıtlı veya kasıtsız her türlü zarar verici durumlara karşı oluşturulan koruma, güvenliğin nihai amacıdır. Ana yapısı koruma eyleminden oluşan güvenlik kavramı, birçok alanda kullanılan bir terim olup kullanıldığı alana göre anlamsal değişikliklere uğramaktadır. Ulusal güvenlik, kurumsal güvenlik, sosyal güvenlik, kişisel güvenlik, fiziksel güvenlik,

bilgi ve iletişim güvenliği gibi birçok alanda farklı yapılara sahip olabilmektedir. Örneğin ulusal güvenlik, bir devletin egemenliğini, kaynaklarını, varlıklarını ve insanlarını koruyan çok katmanlı bir güvenlik yapısına sahiptir. Aynı biçimde bir kuruluşun da uygun bir güvenlik düzeyine sahip olması çok katmanlı bir güvenlik sistemini gerektirir. Başarılı bir kuruluş operasyonlarını, işlevlerini, fiziksel altyapısını, çalışanlarını, müşterilerini, iletişim sistemlerini ve bilgilerini korumak için birden çok güvenlik katmanına ihtiyaç duymaktadır. Bu bakımdan güvenlik çok yönlü bir koruma sistemidir. Çeşitli alanlarda çeşitli koruma mekanizmaları ile kullanılan bu kavram temelde olumsuzluklara karşı alınan önlemlerin bütününü oluşturmaktadır (Whitman ve Mattord, 2018).

Flip (2019), çalışmalarında, bir kurumun işletmesi ve sürekliliği için o kurumun güvenliğinin ve kontrolünün öncelikli duruma getirilmesi gerektiğini vurgulamaktadır. Güvenlik, bilgi sistemlerine yetkisiz erişim sonucunda yapılacak değişikliği, hırsızlığı ve fiziksel hasarı önlemek için kullanılan politika, prosedür ve teknik önlemleri ifade etmektedir. Kontroller ise, kuruluşun varlıklarının güvenliğini, kayıtlarının güvenirliğini ve yönetim standartlarında operasyonel bağlılığı sağlayan yöntemler, politikalar ve organizasyonel prosedürleri kapsamaktadır.

Nayak ve Rao (2014), güvenliği süreklilik arz eden bir süreç olarak ifade etmektedir. İnsan, politika, prosedür, süreç ve teknolojiyi kapsamaktadır. Bunlar bilgi güvenliğinin destek elemanları olarak sürecin sürekliliğini sağlamaktadır (Şekil 2.4).

Şekil 2.4: Bilgi güvenliği süreç destekleri



Kaynak: (Nayak ve Rao, 2014)

İnsan bilgi güvenliğinin önemli ve unutulmaz bir parçasıdır. Etkin bir bilgi güvenliği politikası, kuruluştaki yöneticilerin ve çalışanların rol ve sorumluluklarının net bir biçimde belirlenmesi ve atanmasını içermektedir. İnsan olmadan herhangi bir bilgi güvenliği sürecinin yürütülme olasılığı yoktur. İnsanlar, bilgi güvenliğinin en güçlü dayanaklarıdır. Ancak farkındalık eksikliği ve bilinçsizlik insanı bilgi güvenliğinde zayıf konuma getirmektedir. Sosyal mühendislik saldırılarına ve diğer kötü amaçlı saldırılara yatkındırlar. Bu nedenle, güçlü bilgi güvenliği için farkındalıkların, becerilerin ve olumlu katılımların arttırılması sağlanmalıdır.

Bilişim ve teknolojik gelişmelere bağlı olarak bilginin sınırı genişlemiş, bilgisayar ve ağlar ile birlikte bilgi herkesin kolayca ulaşabileceği hale gelmiştir. Öyle ki kişiler veya kurumlar için önem arz eden bilgiler de bu bilgi ortamları içerisinde yetkisiz kullanıma açık hale gelebilmektedir. Gizli ve korunması gereken bilgilerin yetkisiz kişilerin eline geçmesi bilgi ve iletişim sistemleri ile daha da kolaylaşmıştır. Bu itibarla teknolojik sistemlerin açıklarına karşın bilginin güvenliğini sağlamak daha da önem kazanmıştır.

İletişim teknolojilerindeki sınır tanımaz gelişmeler bilginin güvenli ortamlarda tutulmasını zorlaştırmaktadır. Dünyanın herhangi bir yerinden yapılan siber saldırılar ile en güvenilir ortamda tutulan bilgiler bile yetkisiz kullanıcıların erişimine maruz kalabilmektedir. Bu nedenle bilginin güvenliğine yönelik çalışmaların daha da önem kazandırdığı açık bir biçimde görülmektedir. Özellikle son yıllarda bilgi güvenliği ile ilgili yapılan çalışmalar, güvenlik terimine yeni bir anlam kazandırmak ile birlikte bilginin ne derecede önemli bir duruma geldiğini de göstermektedir. Bu araştırma kapsamında ifade edilecek olan güvenlik kavramı ile genellikle kütüphane bilgi sistemleri tarafından yönetilen bilgilerin bütünlüğünü, gizliliğini ve erişilebilirliğini sağlamak için uygulanan teknolojik ve yönetsel prosedürler anlatılmaktadır.

2.6. Bilgi Güvenliği ve Bileşenleri

Bilgi güvenliği, hassas ve değerli bilgilerin yetkisiz erişim, değişiklik, ifşa veya yok edilme gibi olumsuz etkilerden korunmasını sağlayan bir dizi önlem ve uygulamaları içeren güvenlik alanıdır. Bilgi güvenliği, bilginin gizlilik, bütünlük ve erişilebilirlik unsurlarını koruyarak, bilgi varlıklarının güvenliğini sağlamayı hedeflemektedir. En kısa tabirle bilgi güvenliği, bilgilerin güvenliğinin sistemli bir biçimde sağlanması

olarak tanımlanabilir. Türü veya içeriğine bakılmaksızın bir bilgi varlığı kişi veya kuruma zarar veriyorsa mutlaka o bilgi varlığının güvenliğini sağlamak gerekir. Bu nedenle bilginin güvenliğini sağlamak, gerek kişisel gereksek kurumsal anlamda önem arz etmektedir.

Bilgi güvenliği, elektronik veya basılı ortamlardaki bilgilerin veya verilerin saklanması ve iletilmesi sırasında izinsiz erişim gibi oluşabilecek risklere karşı alınan veya alınacak önlemleri ve tedbirleri kapsamaktadır. Bilginin güvenliğinin sağlanabilmesi için kuruma veya varlığa uygun güvenlik politikalarının belirlenmesi ve uygulanması gerekmektedir. Bilgi güvenliği politikaları ile kişi veya kurumların faaliyetlerinin sorgulanması, erişimlerinin izlenmesi, işlem kayıtlarının tutulup değerlendirilmesi ve veri silme işlemlerinin sınırlandırılması gibi bazı kullanım şekilleri belirlenmektedir. Bu bakımdan bilgi güvenliği, bilgi ve bilişim ile ilgili güvenlik konularını detaylı olarak ele alan güvenlik biliminin bir alt alanı olarak incelenmektedir (Canbek ve Sağıroğlu, 2006).

McCumber (2004), geliştirdiği bilgi güvenliği modelinde bilgi güvenliğini "bilgi ve iletişim sistemlerinin yetkisiz erişim ve kullanımından kaynaklı bilginin gizliliğine, bütünlüğüne ve kullanılabilirliğine zarar vermeye yönelik yapılan kötü niyetli girişimlere karşı sağlanacak koruma" olarak tanımlamaktadır.

Whitman ve Mattord (2019), bilgi güvenliğini, örgütün işlerliğini devam ettirmek ve teknolojik sistemlerin güvenli bir şekilde çalışmasını sağlamak için örgüte ait kurumsal bilgilerin ve kullanılan teknolojik bilgi sistemlerinin korunması olarak tanımlamaktadır.

Bilgi güvenliği, bilgilerin olası her türlü tehlike ve tehdide karşı korumasının sistemli bir biçimde sağlanmasıdır. Bilgiyi kullanan, depolayan, ileten sistemler ve donanımların fiziksel durumları da dâhil olmak üzere bilginin ve kritik unsurların her türlü zarar verici durumdan korunması olarak tanımlanan bilgi güvenliği, bilginin üç kritik özelliği olan gizlilik, bütünlük ve kullanılabilirlik bileşenlerinin korunmasını sağlamaktadır. Bu bilgi güvenliği bileşenleri, makinalaştırılmış bir bilgi ortamındaki tüm güvenlik endişelerini temsil etmektedir (North Atlantic Council, 2002).

Bilgi güvenliği, bilgi varlıklarının bütünlüğüne, kullanılabilirliğine ve gizliliğine yönelik her türlü olası saldırıları ve tehditleri önlemek amacıyla bilgi sistemlerinde

yer alan güvenlik açıklarının tespit edilerek kapatılmasını kapsamaktadır. Bilgi güvenliği, tanım olarak basit bir güvenlik yönetimi olarak görülse de teknolojik gelişmelere paralel olarak çeşitlenen saldırıların karmaşıklığı bilgi güvenliğinin kapsamını genişletmekte ve tehditlere karşı alınan önlemleri zorlaştırmaktadır. Bu nedenle bilgi güvenliği faaliyetlerinin etkin ve güncel tutabilmek için bu sistemlere karşı oluşabilecek potansiyel risk ve tedbirlerin neler olabileceğini de öngörmek ve bilmek gerekir.

Bilgi güvenliği, kişisel cihazlardan kurumsal ve ulusal alanlardaki tüm bilgi sistemlerine ve teknoloji altyapılarına kadar uzanan tüm bilgi sistemlerini kapsayan güvenlik anlayışıdır. Günümüzde bilgi güvenliği denilince akla gelen ilk kavramlar bilgi sistemi ve teknolojik altyapısıdır. Kullanıcının bilgi teknolojileri ile etkileşimini sağlayan bilgi sistemleri bilgiye erişimde teknik destek hizmeti sunan en önemli teknolojik ürünlerin başında gelmektedir. Ayrıca bilgi güvenliği açısından önemli olan kritik altyapıları da bulunmaktadır. Bu teknolojik altyapılar ile bilgi sistemlerinin avantajlarının yanı sıra dezavantajları da bulunmaktadır. Bilgi hırsızlığı veya ifşası bu dezavantajların başında gelmektedir. Bu nedenle bilgi güvenliği, bilgi sistemlerinin kullanımı ile önemini her geçen gün daha da artmaktadır (Güngör, 2015).

Bilgi güvenliğinin temel amacı, bilgi sistemlerinde yürütülen hizmetlerin kesintisiz ve güvenli bir biçimde yürütülmesidir. Ayrıca bilgi varlıklarının yetkisiz erişim ve kullanımlarının önüne geçilerek kurumsal imaj ve güvenirliğinin sağlanması da diğer temel amaç ve öncelikleri arasında yer almaktadır.

Kuruluşlar, uygun işlev ve seviyelerde bilgi güvenliği amaçlarını belirlemesi gerekmektedir. Belirlenen bu bilgi güvenliği amaçları bilgi güvenliği politikası ile tutarlı olmalı, uygulanabilir bilgi güvenliği şartlarını ve risk değerlendirme sonuçlarını dikkate almalı, ölçülebilmeli, ilgililere duyurulması ve uygun bir biçimde güncellenmesi gerekir. Bilgi güvenliği amaçlarını nasıl başaracağını planlarken ne yapacağını, hangi kaynakların gerekli olacağı, ne zaman tamamlanacağı ve sonuçlarının nasıl değerlendirileceği eylemlerinin belirlemelidir. Kuruluşlar, yukarıda belirtilen hususları dikkate alarak belirledikleri amaçları, hazırladıkları ilgili dokümanlarda muhafaza etmektedir (ISO,2022a).

Bilgi güvenliği, kişileri veya kurumları kötü niyetli ve yanlış yönlendirilmiş saldırılara karşı korumak için esastır. Bu bağlamda "Bilgiyi korumak neden önemlidir?" sorusu çoğu bilgi güvenliği çalışmalarının temelini oluşturmaktadır. Özellikle teknolojik cihazlarda kullanılan, depolanan ve transfer edilen bilgiler, önem derecelerine göre sınıflandırılmakta ve bu sınıflandırma derecelerine göre güvenlikleri sağlanmaya çalışılmaktadır.

Son yıllarda küresel anlamda hizmet sunan kurum ve kuruluşlarda yaşanan bilgi güvenliği ihlalleri "Bilgiyi korumak neden önemlidir?" sorusunu daha da önemli kılmıştır. Günümüzde ve gelecekte bilgi güvenliğinin önemini daha da ön planda tutulması gerektiğini kanıtlayan bilgi güvenliği ihlallerine ilişkin birkaç örnek olay aşağıda sıralanmaktadır:

- Yahoo, 2013 yılında gerçekleşen bir siber saldırı sonucunda büyük bir veri ihlaline uğradığını açıklamıştır. Bu ihlalde, tahminen 3 milyar kullanıcının hesap bilgileri etkilenmiştir. Saldırganlar, kullanıcıların isimleri, e-posta adresleri, şifrelerinin kırılamayan kısımları, telefon numaraları ve bazı durumlarda güvenlik sorularına verilen yanıtlar gibi kişisel bilgilere erişim sağlamışlardır. Yahoo, kullanıcılarına ihlalle ilgili bilgi vermiş ve etkilenen hesapların şifrelerini sıfırlamalarını, güvenlik ayarlarını gözden geçirmelerini ve şüpheli faaliyetleri bildirmelerini önermiştir. Ayrıca, olayın ardından Yahoo, güvenlik önlemlerini güçlendirme ve benzer durumların tekrar yaşanmasını engelleme adına önlemler almıştır. Bu durumun artık güvenli parola seçmenin tek başına bir işe yaramadığını, bilgilerin güvende kalması için yeterli olmadığını göstermektedir (Kuchler, 2017)
- eBay, 2014 yılında gerçekleşen bir siber saldırı sonucunda 150 milyona yakın kullanıcısının kullanıcı bilgilerinin çalındığını bildirmiştir. Saldırı sonucunda, kullanıcıların tam adları, şifreleri, e-posta adresleri, adresleri, telefon numaraları ve doğum tarihleri gibi kişisel bilgileri ele geçirilmiştir. eBay çalışanlarının kimlik bilgilerini kullanarak hackerler tarafından şirket ağına 7 ay gibi uzun bir süre fark edilmeden sürdürülen bu saldırı, bilgi güvenliğinin tüm yönleriyle neden değerli olduğunu göstermiştir (Mishkin ve Kuchler, 2014)

- Heartland Ödeme Sistemleri, 2008 yılında büyük bir güvenlik ihlali yaşadığını duyurmuştur. Bu ihlal, kredi ve banka kartı verilerini içeren bir saldırıydı. Heartland, o dönemde 650'den fazla finansal hizmet şirketi tarafından verilen 100 milyondan fazla kredi kartının ödeme işlemlerini gerçekleştiriyordu. İhlal şirkete 147.6 milyon dolara mal olmuş. Bu olayın ardından Heartland Payment Systems, güvenlik önlemlerini artırmak için önemli adımlar atmıştır. Ödeme işlem ağını daha güvenli hale getirmek, kart bilgilerini daha iyi korumak ve benzer saldırıların tekrar yaşanmasını önlemek için sektör standartlarına uygun güvenlik protokolleri benimsemiştir. Aynı zamanda, kredi kartı sektöründe güvenlik ve veri koruma standartlarının geliştirilmesine katkıda bulunmuştur (Twentyman, 2015).
- Sony PlayStation Network, 2011 yılında büyük bir güvenlik ihlali yaşadığını duyurmuştur. Bu ihlal, kullanıcılarının hesap bilgilerinin çalındığı bir saldırıydı. Saldırganlar, kullanıcı adları, adresler, şifreler ve hatta bazı durumlarda kredi kartı verileri gibi hassas bilgilere erişim sağlamışlardır. Ağ birkaç haftalığına kapatılmış. Birleşik Krallık Bilgi Komisyonu Ofisi tarafından bu olay "Veri Koruma Yasasının ciddi bir ihlali" olarak değerlendirilmiş ve şirket 250.000 İngiliz Sterlini para cezasına çarptırılmıştır. Olaydan kaynaklanan davaları çözmek için 15 milyon dolar harcayan Sony, ihlalin ardından güvenlik protokollerini güçlendirmek için önemli adımlar atmıştır. Şifreleme ve güvenlik sistemlerini geliştirmiş, güvenlik yazılımı ve izleme araçları kullanmış ve kullanıcıların hesaplarını daha iyi korumak için önlemler almıştır. Ayrıca, müşterilerin bilgilerini daha iyi korumak için genel veri güvenliği uygulamalarını iyileştirmiştir (Twentyman, 2015).
- Target, 2013 yılında büyük bir indirim perakendecisi olarak faaliyet gösteren bir şirkettir ve o yıl önemli bir güvenlik ihlali yaşamıştır. Saldırganlar, Target'in bilgi sistemlerine sızarak müşterilere ait hassas bilgileri ele geçirmişlerdir. Bu ihlal sonucunda, yaklaşık 40 milyon ödeme kartı bilgisi ve 70 milyon diğer kayda ait bilgi çalındığı duyurulmuştur. Çalınan bilgiler arasında müşterilerin e-posta adresleri, telefon numaraları ve bazı durumlarda kişisel kimlik bilgileri de bulunmaktadır. Bunun üzerine şirketin CEO'su

istifa etmiş ve şirket en son mali raporunda ihlalle ilgili maliyetlerin toplam 252 milyon dolar olduğunu açıklamıştır (Kuchler, 2014)

- Yine ABD'de büyük bir perakendeci şirketi olan Home Depot, 2014 yılında hacklenmesi sonucunda 50 milyondan fazla müşteri kredi kartı numarası ve e-postasının çalındığını bildirmiştir. Şirket, ihlalin 43 milyon dolara mal olduğunu açıklamıştır. Güvenlik ihlali, müşteriler arasında güven kaybına ve endişeye neden olmuştur. Ancak, olaydan sonra alınan önlemler ve güvenlik iyileştirmeleri, benzer saldırıların tekrar yaşanmasını önlemek ve müşteri bilgilerini daha iyi korumak için önemli bir deneyim olmuştur. (Kuchler, 2014).
- ABD sağlık sigortası şirketi olan Anthem'in 2015 yılında bilgi güvenliği ihlaline uğramış ve 78,8 milyon insanın tıbbi verilerinin çalındığını duyurmuştur (Twentyman, 2015).
- Uber, 2016 yılında büyük bir veri ihlali yaşadığını açıklamıştır. Bu ihlal sonucunda, kayıt altında tutulan 57 milyon kullanıcı ve 600 bin sürücüye ait kişisel verilerin bilgisayar korsanları tarafından çalındığı belirlenmiştir. Uber, veri ihlali olayını fark ettikten sonra hemen olayı yetkililere bildirmiş ve etkilenen kullanıcılara durumu açıklamıştır. Bununla birlikte, Uber, olayın gizli tutulması amacıyla bilgisayar korsanlarına 100 bin dolarlık bir ödeme yapmıştır. Bu olay daha sonra kamuoyuna duyurulmuş ve Uber'in veri ihlali iddialarını çözmek için 148 milyon dolarlık bir ödeme yaptığı ortaya çıkmıştır (Bond ve Yuk, 2018; Hook ve Kuchler, 2017).
- 2017 yılında İngiltere'deki Ulusal Sağlık Sevisi (National Health Service), önemli bir siber saldırıya maruz kalmıştır. Bu saldırıda, bilgisayar korsanları tarafından WanaCrypt adlı fidye yazılımı kullanılarak gerçekleştirilen bir saldırı gerçekleşmiştir. Saldırganlar, kullanıcılara e-posta eki olarak gönderilen mesajlar aracılığıyla fidye yazılımını yaymışlardır. Bu fidye yazılımı, bilgisayarlardaki verileri şifrelemekte ve kullanıcılardan bitcoin gibi kripto paraları ödeme yapmalarını talep etmektedir. Yaklaşık 200.000 bilgisayarın şifrelendiği bu saldırı sonucunda 112 milyon dolardan fazla zararla sonuçlanmıştır (Murgia ve Neville, 2017).

- Equifax, ABD'de faaliyet gösteren bir kredi raporu sağlayıcısıdır ve 2017 yılında büyük bir veri ihlali yaşamıştır. İhlal sonucunda, 145 milyon kişinin kişisel bilgileri, sosyal güvenlik numaraları, kredi kartı bilgileri vb. çalınmıştır (Alımcı, 2022).
- Marriott International, 2018 yılında Starwood otel zincirini satın almasından önceki yıllarda gerçekleşen bir veri ihlalini ortaya çıkarmıştır. Bu ihlal sonucunda, 500 milyondan fazla müşterinin kişisel bilgileri, rezervasyon detayları ve kredi kartı bilgileri etkilenmiştir (Yanarışık, 2020).
- Facebook, kullanıcıların kişisel verilerinin izinsiz olarak toplandığı ve kötüye kullanıldığı bir skandalla karşı karşıya kalmıştır. Cambridge Analytica adlı bir şirket, Facebook üzerinden milyonlarca kullanıcının verisini toplayarak seçimlerdeki propaganda çalışmalarında kullanmıştır (Güden, 2019).
- Capital One, 2019 yılında büyük bir veri ihlali yaşamıştır. Bu ihlal sonucunda, 100 milyonun üzerinde müşterinin kişisel bilgileri, kredi kartı başvuruları, sosyal güvenlik numaraları vb. çalınmıştır (Solmaz, 2022).
- SolarWinds, bir yazılım sağlayıcısı olarak bilinir ve 2020 yılında önemli bir siber saldırıya maruz kalmıştır. Saldırganlar, SolarWinds'in sistemine sızarak bir güvenlik güncellemesi aracılığıyla birçok büyük kuruluşun bilgi sistemlerine erişim sağlamışlardır. Bu olay, birçok hükümet kurumu ve özel sektör kuruluşunu etkilemiştir (Çınar ve Yıldırım, 2020).

Bu örnek olaylar bilgi güvenliği çalışmalarının ne derecede önemli olduğunu ortaya koymaktadır. Teknolojik gelişmeler bilginin değerini arttırırken bir taraftan da olumsuzlukları beraberinde getirmektedir. Değerli olan bilgi ve bu bilgileri depolayan bilgi sistemleri bilgisayar korsanları tarafından maddi bir kazanç olarak değerlendirilmektedir. Bu durum bilgi güvenliği yönetim sistemini ön plana çıkarmaktadır.

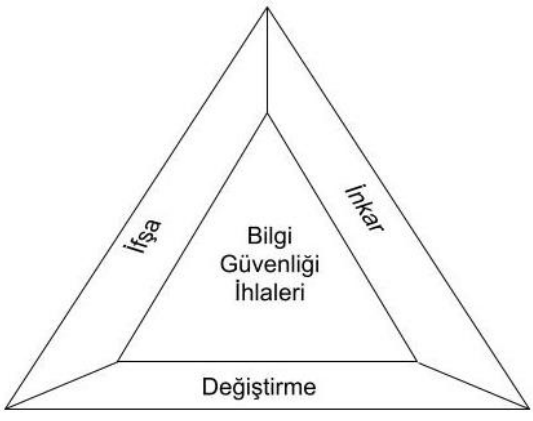
Bilgi güvenliği, kurumdaki her paydaş tarafından kurum kültürü olarak benimsenmesi gereken bir güvenlik yaklaşımıdır. Kurum yönetiminden sorumlu yöneticilerin bilgi güvenliğine yönelik politika ve prosedürleri planlaması, geliştirmesi ve tüm paydaşlar tarafından uygulanabilir duruma getirmesi gerekir. Bu bağlamda her kurumda kurumsal bir bilgi güvenliği yönetim organizasyonu kurulmalı ve bu organizasyonun iş süreçleri yine aynı çerçeve içerisinde

desteklenmelidir. Böylelikle kurumlar, süreklilikleri açısından büyük öneme sahip bilgilerini koruyarak yetkisiz ve izinsiz erişimleri engeller. Bilgi güvenliği mekanizmaları ile önemli bilgilerin mahrem sınırların dışına çıkması engellenerek rekabet üstünlükleri ve iş sürekliliği sağlanır. Ayrıca bilgi ve iletişim teknolojilerinin verimli kullanımını sağlayarak paydaşlara güven ortamı sağlanır.

Bilgi güvenliği gizlilik, bütünlük ve kullanılabilirlik/erişilebilirlik bileşenlerinden oluşmaktadır. McCumber (1991), bilgi güvenliği modeli çalışmasındaki "bilginin karakteristiği" başlığı altında bu üç ana unsur üzerinde durmaktadır. Daha sonraki dönemlerde yapılan çalışmalarda bu üç bileşene yeni bileşenlerin eklendiği görünse de McCumber (2004), geliştirdiği modelin 2004 yılındaki değerlendirmesinde bu yeni unsurların bilgi bütünlüğünün bir yüzü olarak değerlendirilmesi gerektiğini belirtmektedir. Bu itibarla McCumber'ın geliştirmiş olduğu model günümüzde de güncelliğini korumakta olup bilgi güvenliği çalışmalarında yoğun olarak kullanılmaktadır. Bu modelde genel olarak gizlilik, bütünlük ve kullanılabilirlik/erişilebilirlik bileşenleri üzerinde durulduğu görülmektedir. Solomon ve Chapple (2004)'nin "Information security illuminated" adlı çalışmalarında bilgi güvenliğinin bu üç unsur çevresinde geliştiğini ifade etmektedirler (Şekil 2.5). Ayrıca bu çalışmada bu üç unsura karşı gelişen unsurlar da belirtilmektedir. İfşa, değiştirme ve inkâr üçlüsü olarak adlandırılan bu unsurlar ise Şekil 2.6'da gösterilmektedir.

Şekil 2.5: Bilgi güvenliği ilkeleri

Şekil 2.6: Bilgi güvenliği ihlalleri



Kaynak: (Solomon ve Chapple, 2004)

Gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability) kavramları, bilgi güvenliğini sağlamak üzere kullanılan ve üzerinde en çok durulan bileşenlerdir:

- **Gizlilik:** Bilgi sistemlerindeki değerli ve gizli bilgilerin yetkisiz kişilerin eline geçmesinin engellenmesidir. Böylelikle bilgileri kullanması uygun görülen kullanıcıların bilgi sistemlerine güvenli bir biçimde erişimleri sağlanmaktadır. Disk, CD, DVD gibi statik ortamlar ile internet, intranet gibi ağ yapısından oluşan dinamik ortamlar üzerinden erişim sağlanan bilgilerin gizliliğini sağlamak bilgi güvenliği yönetiminin önemli bir amacıdır. Saldırganlar, bilgi sistemlerindeki güvenlik açıklarını kullanarak gizli bilgilere veya verilere birçok saldırı yoluyla erişebilmektedir. Örneğin, şifre dosyalarının yer aldığı veritabanları, sosyal mühendislik yöntemleri ile çalınmakta ve bu şifreler ile birçok veri dosyası kırılarak bilgiler ifşa olmaktadır.
- **Bütünlük:** Bilgilerin yetkisiz kişilerce çalınması, silinmesi, değiştirilmesi veya farklı bir biçimde zarar verilmesi tehditlerine karşı orijinal içeriğin korunmasını sağlayan bileşendir. Bilginin ilk ve orijinal haliyle bir bütün olarak göndericiden alıcısına ulaştırılmasıyla bütünlük bileşenin işlevi sağlanmaktadır (Fussell, 2005). Bu bileşen bilgi sistemlerinde veya diğer ortamlarda bulunan bilgilerin orijinal içeriğinin bozulmadan eksiksiz ve doğru bir biçimde kullanıcıların erişimine sunulabilmesini amaçlamaktadır. Kısaca kasıtlı veya kazara gerçekleştirilen olumsuz eylemlere karşı bilginin bozulmamasını sağlamayı kapsamaktadır.
- **Kullanılabilirlik / Erişilebilirlik:** Bilgilerin erişim yetkisi olan kişilerce erişilebilirliğini ve ihtiyaç duyulduğu zaman kullanıma hazır olma durumunu ifade etmektedir. Bilgilerin bulunduğu ortamda çıkabilecek olası bir sorunda bile erişilebilir kılınması bilgi güvenliğinin kullanılabilirlik bileşenin gereğidir. Kullanılabilirlik, bilgiyi kurallar veya standartlar dâhilinde erişime sunabilmektir. Bu bileşenin odağında kullanıcılar bulunmakta olup her

kullanıcının kendisine sağlanan haklar dâhilinde bilgi sistemlerindeki veya ortamlarındaki bilgilere yetkileri dâhilinde erişilebilmektedir.

Kullanılabilirlik, hizmetlerin ve bileşenlerin kullanıcı topluluğu için sürekli olarak erişilebilir olmasını gerektiren bilgi güvenliği alanıdır. Bir hizmet veya bileşen kullanılamıyorsa, gizlilik ve bütünlük anlamsızdır. Kullanılabilirlik, bilgi hizmetlerinin son kullanıcılar tarafından erişilebilir olması için var olması gereken temel bileşendir. Bilgi sistemlerini, iç ve dış tehditlere karşı korumayı hedefleyen bu bileşen sayesinde, erişim yetkilerine sahip kullanıcılar orjinal bilgilere veya verilere zamanında ve hızlı bir biçimde erişebilmektedir. Sistemlerin eğitimsiz ve bilinçsiz personel tarafından kullanılması veya yapılandırılması, yazılımlardaki hatalar, sistemin yanlış kurgulanması ve doğal tehditler gibi faktörler bilgi sistemlerinin erişilebilirliğini etkileyebilmektedir. Erişilebilirliğin sürekliliğini sağlamak için fiziksel önlemlerin yanı sıra güvenlik duvarı, saldırı tespit sistemi ve antivirüs yazılımları gibi teknolojik önlemlerinde alınması zaruri bir durumdur. Özellikle, bilgi sistemlerinin erişilebilirliğini sağlayan ağ sistemlerinin korunması için alınan önlemler bu bileşen için çok değerlidir (Fussell, 2005).

Bu üç bileşenin yanı sıra güvenilirlik (reliability), emniyet (safety), erişim denetimi (access control) ve hesap verebilirlik (accountability) gibi bileşenlerin de alanyazında ifade edildiği görülmektedir. Ayrıca bilgi güvenliğinden ziyade daha çok elektronik ticaret güvenliği ile birlikte kendiliğinden gelişen doğruluk ve inkâr edilemezlik bileşenleri de birçok çalışmada kullanılmaktadır (Güngör, 2015). Bilgi güvenliği üzerine farklı güvenlik bileşenlerinin oluştuğu görülse de bu bileşenler klasik bilgi güvenliğinin üç ana bileşeni olan gizlilik, bütünlük ve kullanılabilirlik bileşenlerini desteklemek amacıyla ortaya çıkmıştır.

2.7. Bilgi Güvenliğinin Tarihsel Gelişimi

Güvenlik kavramının alt unsuru olarak gelişen bilgi güvenliği, 20. yüzyılın sonlarına kadar genellikle basılı ortamlarda kayıtlı bulunan bilgilerin fiziksel güvenliği ile ilgili faaliyetleri kapsamaktadır. Ancak, bilgi ve iletişim teknolojilerindeki ilerlemelerle birlikte bilgi güvenliği uygulamaları yeni bir boyut kazanmıştır. Bilginin elektronik

ortamlarda üretilmesi, iletilmesi ve muhafaza edilmeye başlanması ile birlikte bilgi güvenliği ile ilgili uygulamalar da değişime uğramıştır. Hızla artan elektronik bilgi miktarı, yeni güvenlik önlemlerinin geliştirilmesini gerektirmiştir. Elektronik ortamlardaki bilgilerin güvenliği basılı ortamlardaki bilgilerin güvenliğine göre daha farklı yöntemleri içerdiği için bilgi güvenliği üzerinde geliştirilen her araç ve model üzerinde köklü değişimler yaşanmıştır. Özellikle internete dayalı bilgi çağı olarak adlandırılan 21. yüzyıl, bilgi güvenliğinde büyük bir değişim ve dönüşüm dönemine işaret etmektedir.

Bilgi güvenliğinin gerçek anlamdaki tarihi gelişimi, bilgisayarın icadıyla birlikte başlamaktadır. Bilgisayar güvenliği, ilk zamanlarda bilgisayar teknolojisinin fiziksel tehditlere karşı korunması ihtiyacından doğmuştur. Fiziksel güvenlik önlemleri, bilgisayar sistemlerinin donanım bileşenlerini hırsızlık, hasar veya doğal afetlerden korumayı amaçlamaktadır. Daha sonraki süreçte bilgisayar sistemlerinin karmaşık hale gelmesiyle birlikte, bilgisayar güvenliği kavramı tüm tehditlere karşı koruma sağlama ihtiyacını kapsamaya başlamıştır. Bu tehditler arasında kötü amaçlı yazılımlar, siber saldırılar, veri sızıntıları, kimlik avı gibi unsurlar yer almaktadır. Bilgisayar güvenliği kavramı bilgilerin korunması kapsamında genişledikçe zamanla mevcut bilgi güvenliği kavramına dönüşmüştür (Whitman ve Mattord, 2019).

Birinci Dünya Savaşı sırasında kâğıt ortamında bulunan belgelerin büyük bir çoğunluğunun yok edilmeye başlanması ile bilgilerin saklanması ve korunması için yeni bir kayıt ortamına ihtiyaç duyulmuştur. O zamana kadar bilginin saklanması ve korunması için yalnızca fiziksel ortamlara başvurmuştur. 1930'lar bilginin depolama şeklinin fizikselden dijitale dönüştüğü yıllar olarak bilgi güvenliğinde bir dönüm noktası olarak görülmektedir. Alman mühendis Arthur Scherbius tarafından şifreleme ve şifre çözme teknikleri için geliştirilen ENİGMA ilk güvenli bilgi sistemi olarak geliştirilmiştir. 1932 yılında Konrad ArpanZuse tarafından icat edilen ilk elektromanyetik bilgisayar Z1 Computer, 1942 yılında icat edilen ilk elektronik dijital bilgisayar, 1946 yılında Amerikan askeri çalışmaları için geliştirilen ENİAC-I ve daha sonraki yıllarda gelişen diğer bilgisayar teknolojileri bilginin kayıt ortamını dijital ortama hızlı bir şekilde taşımıştır. İlk ana bilgisayarların ve ENİGMA gibi kriptografik cihazların gelişimi ve kullanımı bilgisayar güvenliğine duyulan ihtiyacı daha da artırmıştır. Devletler ve kurumlar bu gibi teknolojik cihazları ve hizmet

ettikleri görevleri korumak için birden fazla güvenlik seviyeleri oluşturmaya başlamıştır (Suganthy ve Maiti, 2014).

Bilgi güvenliği ilk yıllarda ağırlık olarak fiziksel güvenlik ve basit belgelerin korunması gibi yüzeysel bir süreçte yürümekteydi. 1960'lı yıllarda daha karmaşık, gelişmiş ve özel görevleri yerine getirmek için geliştirilen bilgisayarın çevrimiçi hale gelmesiyle birlikte bilgi güvenliğinin üstlendiği görevler genişletmiştir. 1968 yılında Department of Defense's Advanced Research Project Agency (ARPA)'in geliştirdiği ARPANET ile bilgisayarlar arasında çevrimiçi bilgi paylaşımı sağlamış ve sonraki yıllarda popüler hale gelen ARPANET, daha geniş kullanım alanına yayılmıştır. 1973 yılında internetin öncüsü olan Robert M. Metcalfe, ARPANET'i güvenli bir ağ haline getirmek için ağ üzerindeki temel sorunları belirlemiş ve yerel ağ protokolü olan Ethernet'i geliştirmiştir. ARPANET kullanımında artan kullanıcı sayısı nedeniyle bilgisayar güvenliği ihlallerinin sıklığında da artış görülmüştür. Bu durum yeni bir güvenlik kavramı olan ağ güvenliği kavramını da ortaya çıkarmıştır ("Planning the ARPANET: 1967-1968", 2021; Crocker, 2019).

Bilgi işlem cihazlarının fiziksel korumasının ötesinde yeni güvenlik kontrollerini içeren RAND Report R-609 dokümanı, 1970 yılında RAND Corporation tarafından Birleşik Devletler Savunma Bakanlığı için oluşturulmuş güvenlik standartları belgesidir. Bu rapor, bilgisayar güvenliğinin yönetim ve politika konularının rollerini tanımlayan ilk doküman olma özelliğine sahiptir. Bilgisayarlı bir veri işleme sisteminin korunması için gerekli olan çok katmanlı güvenlik kontrolleri ve mekanizmalarını tanımlayan bu doküman, yaklaşık on yıl boyunca sınıflandırılmış ve günümüzün bilgisayar güvenliği çalışmalarını başlatan belge olarak kabul edilmiştir. Bilgisayar güvenliği tarihinde önemli bir konuma sahip olan bu doküman, bilgisayar güvenliğinin fiziksel koruma kapsamını aşağıda sıralanan maddeleri içerecek şekilde genişletilmiştir (Ware, 1979):

- Bilgisayarlar üzerinde bulunan verilerin güvence altına alınması,
- Bu verilerin rastgele ve yetkisiz erişiminin sınırlandırılması,
- Bilgi güvenliği sürecine kuruluşun farklı seviyelerdeki personelin dâhil edilmesi.

1979 yılında dosyaları ve bilgisayarları bozan ilk bilgisayar solucanının keşfedilmesi;

1982 yılında ilk Apple virüsünün Apple DOS işletim sistemine saldırması ve bunları 1986 yılında bilgi güvenliğini tehdit eden ilk PC virüsünün tespitinin izlemesi bilgi güvenliği gelişim tarihi açısından önemli dönüm noktaları olarak kabul edilmektedir (Suganthy ve Maiti, 2014).

1990'lı yıllarda kurumların bilgisayar ve internet kullanımlarında yaşanan gelişmeler, hatta internetin halka açık hale getirilerek tüm dünyada yaygın bir biçimde kullanılmaya başlanması bilgi güvenliğinin önemini daha da arttırmıştır. İnternet ve bilgisayar teknolojisi yönetim, finans, pazarlama, savunma, sağlık, bilgi gibi birçok sektördeki faaliyetlerin hızlanmasını ve gelişmesini sağlarken diğer taraftan da bu sektörlerdeki bilgi güvenliğini sağlama yeteneğini giderek zayıflatmıştır. Böylelikle bilgisayarlarda depolanan önemli ve kritik bilgiler güvenlik tehditlerine daha fazla maruz kalmaya başlamıştır. 20. yüzyılın sonlarında yaşanan iletişim ve bilgi teknolojilerindeki bu hızlı gelişmeler devletleri ve kurumları tedirgin etmiştir. Devletler, kurumlar hatta kişiler için önem derecesi yüksek bilgilere yetkisiz kişilerce ağlar üzerinden daha kolay erişilmesi, bilgi güvenliği konusunda ileri seviyede önlemlerin alınmasına neden olmuştur (Whitman ve Mattord, 2018).

21. yüzyılda internet, güvenli olmayan milyonlarca bilgisayar ağını ve milyarlarca bilgisayar sistemini sürekli iletişim halinde tutmaktadır. Bu nedenle bilgisayarlarda depolanan bilgilerin güvenliği bağlı oldukları diğer bilgisayarların güvenlik düzeyine bağlı duruma gelmektedir. Artan siber saldırı tehditleri, devletlerin ve kurumların kamu ve diğer kritik altyapı hizmetlerinde kullandığı bilgisayarlı sistemlerin savunma ihtiyacının farkındalığını arttırmıştır. Özellikle ulusal savunma için bilgi güvenliğinin önemli olduğunun farkına varılması, devletler tarafından bilgi güvenliği çalışmalarını daha da arttırmıştır. Artan bir diğer endişe ise, ulus devletlerin bilgi savaşına girme tehdididir. İş ve kişisel bilgi sistemlerinin savunmasız oldukları zamanlarda yaşanacak olan bilgi kaybı olasılıkları devletleri tedirgin etmektedir. Bu kapsamda gelişmiş devletler bilgi güvenliği ile ilgili yasal düzenlemelere giderek ulusun çıkarlarını koruma altına almaya başlamıştır.

Bilgi ve iletişim teknolojilerinin gelişmesi ve kullanımlarının hızla yayılması bilgi güvenliği ihtiyacını artıran en büyük etkenlerin başında gelmektedir. Bilgi güvenliğine olan ihtiyaç her geçen gün daha da artmış ve bu konuda birçok çalışma yapılmaya başlanmıştır. Bilgi güvenliğinin gelişimine katkı sağlayan önemli

çalışmalar bulunmaktadır. Bu çalışmaların yapıldığı tarihler bilgi güvenliği açısından çok önemli tarihler olarak kabul edilmektedir. Bu tarih ve çalışmalara ilişkin bilgiler Tablo 2.1'de sunulmaktadır.

Tablo 2.1: Bilgi güvenliğinin gelişimindeki önemli tarih ve gelişmeler

Tarih	Doküman
1968	Maurice V. Wilkes' in Time-sharing Computer Systems adlı kitabı, bilgisayarların şifre güvenliği üzerine önemli bilgiler sunmaktadır (Wilkes, 1975).
1970	RAND şirketi tarafından çalışılan ve 1979'da Willis H. Ware tarafından sınıflandırılan - RAND Report R-609 raporu, bilgi güvenliği ihtiyacını belirleyen ilk çalışma olarak tanınmaktadır (Ware, 2009).
1973	R. Schell, P. Downey ve G. Popek yazarları tarafından yayımlanan Preliminary Notes on the Design of Secure Military Computer Systems dokümanında askeri sistemlerde devam eden bilgi güvenliği çalışmalarına ek güvenlik ihtiyaçları incelemektedir (Schell, Downey ve Popek, 1973).
1975	Birleşik Devletler Federal Hükümeti tarafından kullanılan bilgi sistemlerinin güvenlik kategorilerini oluşturan "Federal Information Processing Standard (FIPS-199)" adlı standart (Radack, 2004).
1978	Richard Bisbey ve Dennis Hollingworth'ın ARPA projesinin işletim sistemi güvenliğinin güvenlik açıklarını daha iyi anlamak ve mevcut sistemdeki otomatik güvenlik açıklarını algılama tekniklerini incelemek için yayınan "Protection Analysis: Final Report" dokümanı (Bisbey ve Hollingworth, 1978).
1979	Robert Morris ve Ken Thompson'un uzaktan erişilen çevrimiçi sistemlerdeki şifre güvenliği şeması tasarımı hakkındaki incelemelerinin yayınlandığı "Password Security: A Case History" adlı makaleleri (Morris ve Thompson, 1979).
1979	Dennis M. Ritchie'nin güvenli kullanıcı / grup kimlikleri ve bilgi sistemlerinde karşılaşılan sorunlar üzerine yayınladığı "Protection of Data File contents" ve "On the Security of UNIX" adlı makaleleri (Ritchie, 1979a, 1979b).
1982	ABD Savunma Bakanlığının Rainbow serisi olarak bilinen "Trusted Computer Security (TCSED)" belgeleri (United States Government Department of Defense, 1985).
1984	F. T. Grampp ve R. Morris'in UNIX işletim sistemindeki güvenlik tehlikelerini ve bunlara karşı korunma yollarını inceledikleri "The UNIX System: UNIX Operating System Security" adlı rapor (Grampp ve Morris, 1984).
1984	J. A. Reeds ve P. J. Weinberger'in şifre çözme yönteminin ana hatlarını ve bir güçlendirilmiş algoritma önerisi sundukları "The UNIX system: File security and the UNIX system crypt command"adlı makale (Reeds ve Weinberger, 1984).
1992	ABD Deniz Araştırma Laboratuvarında çalışan İnternet Mühendisliği Görev Gücü Araştırmacılarının geliştirdiği ve günümüzde de IPSEC güvenliği olarak bilinen Simple Internet Protocol Plus (SIPP) Security protokolleri (Deering, 1993).
2009	Uluslararsı Standardizasyon Orgonizasyonu terafından ilk olarak 1995 yılında BS 7799-1 ve 1998 yılında ise BS 7799-2 olarak yayımlanmış, 2000 yılında ISO 17799 standartları olarak yayınlanmıştır. 2009 yılında ise ISO/IEC 27000 standartlar ailesi olarak yayınlandı (ISO, 2018).

2.8. Bilgi Güvenliği İhtiyacı

Bilgi güvenliği programının temel misyonu, bilgi varlıklarının güvenli ve faydalı kalmasını sağlamaktır. Kurum ve kuruluşlar değerli olan bilgi varlıklarını korumak için yüksek oranda para ve zaman harcamaktadır. Bilgi varlıklarına yönelik mevcut veya potansiyel tehditler olmasaydı, bunlara karşı harcanan kaynaklar bilgi sistemlerin geliştirilmesinde kullanabilirdi. Fakat bilgi varlıklarına yönelik saldırı tehditlerinin sürekliliği ve karmaşıklığı bilgi güvenliğine duyulan ihtiyacı artırmaktadır. Whitman ve Mattord (2018)'a göre bilgi güvenliği, bilgi varlıklarının güvenli ve yararlı kalmasını sağlamak için dört önemli işlevi yerine getiren süreçte işlemektedir:

- Kurumun işleyiş kabiliyetini muhafaza etmek.
- Kurumun ürettiği, topladığı ve kullandığı fiziksel veya elektronik tüm veri ve bilgileri korunmak.
- Kurumun bilgi teknolojileri sistemlerinde çalışan donanım ve uygulamaların güvenli çalışmasını sağlamak.
- Kurumun teknolojik varlıklarını korumak.

2.8.1. İşlevselliğin Korunması

Kurumun işlevselliğin korunmasında genel yönetim, bilgi teknolojileri yönetimi ve bilgi güvenliği yönetimi önemlidir. Bu üç yönetim topluluğu, kurumun işlev görme yeteneğini koruyan bilgi güvenliği programının kolaylaştırılmasından sorumlu tutulmaktadır. Kurumlar bilgi güvenliği programlarını teknik olarak karmaşık bir görev algıladıkları için uygulamaktan çekinmektedir Bilgi güvenliği uygulamasının aslında teknik işlemlerden çok yönetim ile ilgili olduğu göz ardı edilmektedir. Bilgi güvenliği yönetimi, politika ve teknolojik alt yapıdan çok yönetimin uygulanması ile ilgilidir.

Bilgi güvenliği alanında ünlü bir araştırmacı olan (Wood, 2004), sıkı bir bilgi güvenliği yönetiminin teknolojik güvenlik önlemlerinden daha önemli olduğunu belirtmektedir. Birçok insanın bilgi güvenliği sorununa yönelik çözümün teknolojik önlemlerle giderileceği düşüncesinden ziyade, çalışmalarında bilgi güvenliği yönetimini ön planda tutarak yönetim konusunda öneriler sunmaktadır. Bilgi

güvenliği algısının yıllar içinde çok değiştiğini ve sonuç olarak artık ekip tabanlı bir yaklaşımın gerektiğini savunmaktadır. Organizasyon içerisindeki bu ekibin ise iyi bir yönetim ile yönlendirilmesinin önemli olduğunu vurgulamaktadır.

Kurumların işlevselliklerinin korunmasında yönetim topluluklarının önemli olduğu ve bilgi güvenliği sorunlarına sadece teknik çözümlerle yaklaşmanın yeterli olmayacağı anlaşılmaktadır. Her alanda olduğu gibi bilgi güvenliği programlarının uygulanmasında da iyi bir yönetim anlayışının, kurumların iş etkinliği ve iş maliyeti açısından önemli olduğu görülmektedir.

2.8.2. Verilerin Korunması

Veri, bir kurumun varlığı için en değerli bilgi varlığıdır. Veri olamadan kurum iş potansiyelini ve müşterilere değer sağlama yeteneğini kaybetmektedir. İçinde bulunduğumuz çağda modern bir kurumun tüm hizmetleri bilgi sistemlerine dayanmaktadır. Bilgi sistemleri içinde barındırdıkları veriler, kurumların işlevselliğini sağlamaktadır. Bu nedenle veri güvenliği bilgi güvenliği yönetiminin kritik bir yönünü oluşturmaktadır. Değerli veri, yetkisiz kişileri bilgi sistemlerini sabote etmeye ve bozmaya motive etmektedir. Fakat etkili bir bilgi güvenliği yönetimi, toplanan ve kullanılan verilerin bütünlüğünü ve değerini korumaktadır (Wood, 2004).

Kurumlar, kritik ve değerli verilerinin çoğunu, veri tabanı yönetim sistemleri olarak bilinen uzman veri yönetim yazılımları tarafından yönetilen veri tabanlarında depolamaktadır. Veri tabanı yönetim sistemi tarafından yönetilen verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini koruma süreci veri tabanı güvenliği olarak bilinmektedir. Veri tabanı güvenliğinde birçok bilgi güvenliği alanında olduğu gibi yönetim, teknik ve fiziksel kontroller gibi çeşitli denetim yaklaşımları uygulanmaktadır. Yönetsel kontroller politika, prosedür ve yönetim uygulamalarını; teknik kontroller kimlik doğrulama, uygulama güvenliği, yedekleme, kurtarma, şifreleme ve bütünlük gibi güvenlik boyutlarını; fiziksel kontroller ise yangın söndürme sistemleri, kilit mekanizmaları, kamera, güvenlik kapısı ve diğer fiziksel güvenlik donanımlarını içermektedir.

2.8.3. Uygulamaların Güvenliğini Sağlamak

Günümüzde kurumlar verimliliklerini artırmak için hizmetlerine uyumlu uygulamalara sahip olma çabasındadır. İşletim sistemi platformları, belirli operasyonel uygulamalar, e-posta ve kısa mesaj gibi anlık mesajlaşma uygulamaları modern bir kurumun altyapısını oluşturan teknolojik unsurlarını oluşturmaktadır. Kurumlar bu uygulamaları bir servis sağlayıcısından edinebileceği gibi kendi içyapısından da sağlayabilmektedir (Whitman ve Mattord, 2018). Kurumlar bu uygulama altyapısını kurduktan sonra, bunların güvenliğini sağlayıcı yönetim yapısı oluşturmak zorundadır. Uygulamaların güvenliğini sağlamak, kurumun işlevselliği açısından önemlidir.

Bilgi teknolojileriyle gelişen elektronik uygulamalar, kurumların tüm faaliyetlerini etkilemekte ve kolaylaştırmaktadır. Diğer taraftan da güvenlik tehditlerini beraberinde getirmektedir. Kurumların hatta kişilerin sahip oldukları önemli bilgiler, bilgi hırsızları ve kötü niyetli çalışanlarca dışarıya sızdırılmaktadır. Bu durum kurumların hizmetlerinde aksamalar oluşturabilmektedir. Hatta hizmetlerin tamamının durmasına da neden olabilmektedir. Bu nedenle bilgi teknolojilerine bağlı olarak gelişen modern kurumlar, bilgi güvenliği yönetimine önemli derecede ihtiyaç duymaktadırlar.

Elektronik platform ve uygulamalar ile faaliyetlerini yürüten kurumlar, güvenlik ihlallerine ve suiistimallerine uğramakta ve her geçen gün bu güvenlik ihlallerine yenileri eklenmektedir. Örneğin dijital bilgi hizmeti sunan bir kütüphanenin bilgi sistemlerinde kayıtlı kullanıcı bilgilerinin çalınması, kullanıcıları birtakım olumsuz durumlara düşürebileceği gibi kurumun da itibarını zedeleyecektir. Bu gibi güvenlik tehditlerinden etkilenmemek veya etki düzeyini en aza indirgemek için kurumlar üzerlerine düşen bilgi güvenliği ile ilgili sorumlulukları yerine getirmelidir. Bu bağlamda kurumların bilgi güvenliği yönetimine önem vermesi ve bilgi güvenliği kültürünün tüm çalışanlarda ve paydaşlarda oluşturulması gerekmektedir.

2.8.4. Teknolojik Varlıkların Korunması

Kurumlar iş performanslarını arttırmak için sundukları hizmetlerin veya faaliyetlerin kapsamına ve niteliğine uygun güvenli bilgi sistemi donanımları kullanmaktadırlar.

Bu donanımlar güvenlik açıklarını da beraberinde getirmektedir. Artan teknolojik varlık kullanımı, kurumların güvenlik anlayışını da değişime itmektedir. Aksi takdirde sahip olduğu teknolojik varlıklar faydadan çok zarara dönüşebilmektedir. Kullanılan her bir teknolojik varlık ayrı bir güvenlik önleminin alınmasını mecbur kılmaktadır (Whitman ve Mattord, 2018).

Kurumlar, değişen ihtiyaçlarını karşılayacak şekilde büyürken yeni teknolojik varlıklarını da bünyelerine katmaktadırlar. Bu teknolojik varlıkları kullanmak kadar onların güvenliğini sağlamak da önemlidir. Bu da sağlam bir bilgi güvenliği yönetiminden geçmektedir. Örneğin izinsiz giriş algılama ve önleme sistemini hizmetlerinde kullanmaya başlayan bir kurum, bu sisteme tanımladığı verilerin de güvenliğini sağlaması gerekmektedir. Aksi takdirde bu sisteme tanımlanan kurumsal ve kişisel veriler bilgi hırsızları tarafından çalınarak hem kurumun faaliyetleri zarar görebilmekte hem de personel ve müşterilerin kişisel bilgileri kötü amaçlı kullanabilmektedir.

Suç olarak bilgi teknolojileri, kurumlara kazandırdığı yeni yöntem ve beceriler ile bilgi güvenliği açısından da önemli rol durumuna gelmektedir. Özellikle bilgisayar ve internet gibi yeni teknolojiler, kurumların bilgi güvenliği yönetimine yeni boyutlar kazandırmaktadır. Örneğin, bilgi teknolojileri hizmetlerini sunmanın yeni yollarından biri olan bulut tabanlı hizmetler, kurumsal bilgilere yeni riskler getirmektedir. Bu ve buna benzer yeni teknolojik varlıklar beraberinde getirdiği riskler ile bilginin nasıl korunacağına ilişkin endişeleri artırmaktadır. Bu durum kurumsal bilgi güvenliği yönetimine olan ihtiyacı daha da önemli hale getirmektedir.

2.9. Bilgi Güvenliği Yönetim Araçları

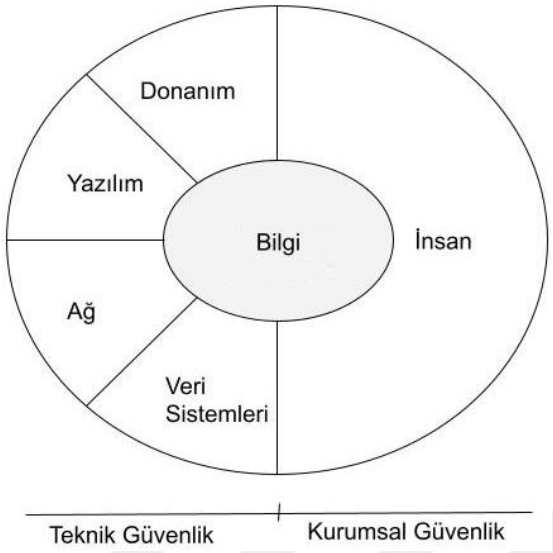
Günümüzde kurumlar faaliyetlerini, yasalar, yönetmelikler, gereksinimler, hedefler, rakipler ve ortaklar gibi birçok karmaşık uygulama ve sistem içerisinde sürdürmektedir. Ayrıca iş ilişkileri, verimlilik, moral, ekonomik durum ve performans gibi durumlarda kurumların faaliyetlerine etki etmektedir. Kurumlar bu karmaşık ortamda yönetimlerin faaliyetlerini başarılı bir şekilde sürdürebilmesi için yönetimin genel güvenlik yaklaşımları ile donatılan dokümanlar geliştirmesi ve yayınlaması gerekmektedir. Güvenlik profesyonellerinden oluşan bir ekibin görüşleri ile geliştirilen bu güvenlik dokümanları, amaç ve uygulamalara göre politikalar,

standartlar, prosedürler, yönergeler ve diğer temel güvenlik dokümanları olarak değişik formlarda oluşturulmaktadır. Bu güvenlik dokümanları; uyumluluk izleme, erişim kontrolü, eğitim, güvenlik bilinci, gizlilik, analiz ve diğer konularla ilgili olarak güvenlik uzmanları tarafımdan kontrol edilmektedir. Bu nedenle geliştirilen bu dokümanların güvenlik uygulamalarının hedeflerine uygun şekilde olması için bilgi güvenlik uzmanı yeterliliklerine sahip olmanız gerekmektedir (Kim ve Solomon, 2018).

Güvenlik uygulamalarına ait dokümanlar bir organizasyonun gücünü ve kültürel yapısını belirlemektedir. Bu uygulamaların başında politikalar gelmektedir. Politikalar, kurumun üst düzey değerlerini ve hedeflerini içermektedir. Standartlar, yönergeler, prosedürler ve kılavuzlar ise politikayı destekleyen güvenlik uygulamalarıdır. Sağlam ve nitelikli bir bilgi güvenliği programı, politika ile başlamakta ve son bulmaktadır. Bilgi güvenliği politikası, kurumun bilgi varlıklarının güvenliğini koruyacak şekilde faaliyetlerin sürekliliğini zorunlu kılan bir yönetim aracıdır. Güvenlik ilkeleri, yürütülmesi en az maliyetli bir denetimdir; fakat doğru biçimde uygulanması zordur. Oluşturulmaları ve yaygınlaştırılmaları sadece yönetim ekibinin zamanına ve çabasına bağlı olduğundan düşük maliyetlere sahiptir. Fakat bu güvenlik araçlarının uygulanması teknik sistem, insan, zaman ve mekân gibi birçok unsura bağlı olduğundan doğru bir biçimde uygulanmayı zorlaştırır (Whitman ve Mattord, 2018).

Bilgi ile bilgiye erişim sağlayanlar arasında koruma düzeyleri ve katmanları bulunmaktadır. Bu koruma düzeylerinin etki dereceleri farklılık göstermektedir. Şekil 2.7'de de görüldüğü üzere bilgi güvenliği yönetimi, teknik güvenlik önlemlerinden ziyade çoğunlukla kurumsal güvenlik önlemlerine dayanmaktadır. Güvenlik politikaları, prosedürleri, planları, farkındalık çalışmaları ve idari araçlar kurumsal güvenlik önlemlerini oluşturmaktadır. Bu kurumsal güvenlik önlemlerin temel amacı, teknik güvenlik güvenliğinin işleyişinin bir düzen içerisinde yürütülmesini sağlamaktır. Örneğin bilgiye erişmek isteyenler güvenlik politikalarına göre tasarlanmış teknik (sistem, ağ, internet vb.) güvenlik katmanlarından geçerek bilgiye erişim sağlayabilmektedirler (Whitman ve Mattord, 2019).

Şekil 2.7: Güvenlik alanları



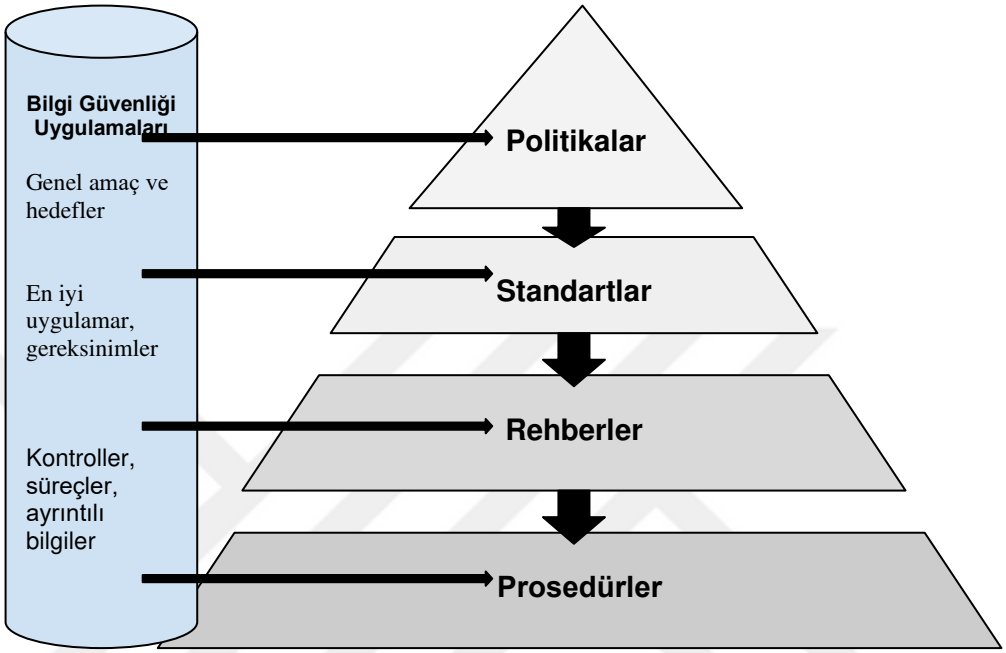
Kaynak: (Whitman ve Mattord, 2019)

Bilgi güvenliği yönetiminde kurumsal araçlar bulunmaktadır. Bunlar politikalar, standartlar, rehberler ve prosedürler gibi bir kurumun bilgi varlıklarını korumak için benimsediği önlemlerdir. Bu kavramlar birbirleriyle ilişkilidir ve bir bütün olarak bilgi güvenliği yönetimini desteklemektedir. Politikalar kurumun bilgi güvenliği hedeflerini ve taahhütlerini belirten resmi belgelerdir. Bu belgeler ile kurumun bilgi güvenliği amaçları ve genel stratejileri belirlemektedir. Standartlar, belirli bir sektörde veya endüstride kabul gören en iyi uygulamaları, gereksinimleri ve prosedürleri içeren belgelerdir. Bunlar genellikle uluslararası standartlar veya sektörel standartlar olabilmektedir. Rehberler, bir kurumun bilgi güvenliği politikalarını ve standartlarını uygulamasına yardımcı olmaktadır. Prosedürler ise bir kurumun belirli bir faaliyetinin veya sürecinin nasıl gerçekleştireceğini açıklayan adımları içermektedir (Whitman ve Mattord, 2019).

Özetle, politikalar kurumun bilgi güvenliğindeki genel amaçları ve taahhütleri belirtirken, standartlar belirli gereksinimleri ve en iyi uygulamaları sağlamaktadır. Rehberler, kurumların bilgi güvenliği yönetimine pratik bilgi ve öneriler sunarken, prosedürler günlük işleyişteki adımları ve talimatları belirlemektedir. Tüm bu unsurlar bir araya gelerek, kurumun bilgi güvenliği yönetimine katkıda bulunarak bilgi varlıklarını koruması sağlanmaktadır. Şekil 2.8'de bilgi güvenliği kurumsal

yönetim araçlarını oluşturan politikalar, standartlar, prosedürler ve yönergeler arasındaki ilişki gösterilmektedir

Şekil 2.8: Bilgi güvenliği yönetim araçları



Kaynak: (Whitman ve Mattord, 2019)

Politika, bir sistemin üst düzeyde güvenlik hedeflerini ve değerlerini içermektedir. Standartlar, rehberler, yönergeler ve prosedürler ise politikanın ayrıntılarını ifade etmektedir. Şekil 2.8'de politikaların piramidin en üstünde yer aldığı görülmektedir; politikanın en üst katmanda yer alması diğer güvenlik araçlarından daha değerli olduğunu göstermez, diğerlerinin genel ve özetlenmiş çıktıları olduğunu anlatır. Politikalar daha genel ve stratejik bilgiler içerdiğinden hiyerarşinin üstünde yer almaktadır. Diğer güvenlik araçları ise işleyişe ait ayrıntıları ve taktikleri belirleyen detaylı kurumsal araçlardır.

2.9.1. Politikalar

Politika, kuruluşun yönetim felsefesinin resmi durumunu ifade etmektedir. Politikalar, kurumlar için kabul edilebilir ve kabul edilemez davranışları belirleyen kuralları içermektedir Bilgi güvenliği politikası da kuruluşun bilgi güvenliği felsefesini temsil etmektedir. Kurumlar, bilgi güvenliği ortamlarına ilişkin ilke ve

yöntemlerin belirlenmesi için politikalar oluşturulmaktadır. Bu politikalar kurumun bilgi güvenliği profilinin planlanması, yönetimi ve kontrolleri için temel dayanak oluşturmaktadır. Politikaların oluşturulmasının ardından bu politikaların uygulanması için gerekli teknolojilerin belirlenmesi ve prosedürlerin geliştirilmesi gerekmektedir (Whitman ve Mattord, 2019).

Güvenlik politikaları, yönetimin amaç ve hedeflerini belgelendirmektedir. Kurumun güvenlik ihtiyaçlarını ve bu ihtiyaçları karşılama konusundaki kararlılıklarını açıklamaktadır. Güvenlik politikaları, kurumun güvenlik konusundaki temel gereksinim ve ilkelerinin kısa özeti olarak yönetim tarafından belirlenmiş güvenlik uzmanları ve dış güvenlik paydaşları tarafından kuruluşun amaç ve hedefleri doğrultusunda hazırlanmaktadır. Hazırlanan bir politika çok karmaşıksa yönetim bu politikayı kabul etmekte ve onaylamakta zorlanmaktadır. Bu nedenle politikalar kısa ve net olmak zorundadır. Örneğin, iyi bir güvenlik politikası "Kuruluşunuzun geleceği için güvenlik önemlidir" veya "Ürünlerimizde / hizmetlerimizde güvenlik en önemli görevimizdir." gibi ifadelerle yöneticilere güvenlik konusunda karar vermeleri için ihtiyaç duydukları rehberliği net bir biçimde sağlamalıdır (Henkoğlu, 2022; Köksoy, 2020).

Güvenlik politikaları ayrıca kurumun yasalara, düzenlemelere ve gereken özen ve durum tespiti için belirlenen standartlara ne kadar uyduğunu değerlendirmesine yardımcı olmaktadır. Güvenlikle ilgili herhangi bir politikanın temel amacı riski azaltmaktır (Ahmet, 2021). Politika, kuruluşun çabalarına odaklanmasına yardımcı olmaktadır. Politikalar; anlaşılamaz, kullanılamaz, uygulanamaz ve güncellenemez ise önemini yitirmektedir. Politikaların çalışanlarca farkında olunması ve erişilebilir olması önemlidir. Politikaların özellikle günün şartlarına uygun yeni politikalar ile güncellenmesi ve bu yeni politikaların çalışanlara duyurulması gerekmektedir. Güvenlik politikası, tüm çalışanların kuruluşun değer verdiği varlıkları ve ilkeleri anlamalarına yardımcı olmaktadır. Açık ve nitelikli bir güvenlik politikası, çalışanların kuruluşun varlıklarına saygılı olma olasılığını arttırmaktadır. Çünkü çalışanlar politikaları kuruluşun ciddiye aldığı kadar değerli bulmakta ve uygulamaktadırlar (Kim ve Solomon, 2018).

Politika, etkili bir bilgi güvenliği programının temel dayanağını oluşturmaktadır. Wood (1997), politikaların bilgi güvenliği alanında gerçekleşen neredeyse tüm

sürecin merkezinde yer alan temel kurumsal araç işlevi konumunda olduğunu belirtmektedir. Örneğin, Bir kuruluşta net bir şekilde belirlenmemiş bir bilgi güvenliği politikası olduğunda, güvenlik duvarının güvenli bir şekilde yüklenmesini beklemek zor olabilir. Bilgi güvenliği politikası, güvenlik duvarının nasıl yapılandırılacağı, hangi trafiği engelleyeceği veya izin vereceği gibi önemli parametreleri belirleyen temel bir rehberdir. Bu nedenle, güvenlik duvarının etkili bir şekilde çalışması ve kuruluşun güvenlik hedeflerine uygun olması için net bir bilgi güvenliği politikasının varlığı önemlidir.

Sonuç olarak politikaların en önemli işlevi; kurumları olumsuz olaylardan korurken çalışanları kabul edilebilir ve kabul edilemez davranışlar konusunda bilgilendirmektir. Politika, çalışanların verimliliğini artırmak ve potansiyel olumsuz durumları önlemek için geliştirilmektedir. Politikaların doğru ve anlaşılır bir şekilde uygulanamaması, kuruma zarar verebilir. Bilgisizlik, kaza ve kasıt gibi üç önemli durum, çalışanları veya paydaşları etik olmayan ve yasa dışı eylemlere itebilir. Bilgi güvenliğinde ilk caydırıcı önlem, bilgisizliği ortadan kaldırmaktır. Bu nedenle, tüm çalışanların ve paydaşların kuruluşun bilgi güvenliği politikaları ve ilgili belgeleri konusunda bilgilendirilmesi ve eğitilmesi gerekmektedir. Eğitim ve farkındalık programları, çalışanların ve diğer paydaşların politika bilgisini güçlendirir.

2.9.2. Standartlar

Standart, kullanıcıların hizmetlerden maksimum işlevi, hedefi veya faydayı elde etmelerini sağlamak için bir kurum tarafından uygulanması gereken teknik özellikleri belirlemektedir. Bu nedenle birçok kurum, kuruluş, dernek ve konsorsiyum ilgili hizmet alanlarına yönelik standartların geliştirilmesinde hayati role üstlenmektedirler (Syafrizal, Selamat ve Zakaria, 2020).

ISO (2018), standartları belirli bir bağlamda bir kılavuz, model veya örnek olarak en uygun sonuçların elde edilmesine yardımcı olan genel bir anlaşmaya dayalı olarak yapılan ve bir tüzel kişilik tarafından doğrulanan belgeler veya kurallar bütünü olarak tanımlamaktadır. Genel ifade ile standartlar; ürünlerin, hizmetlerin ve sistemlerin güvenliğini, tutarlılığını ve güvenilirliğini sağlamayı amaçlayan özellikleri, prosedürleri ve yönergeleri tanımlayan belgeler olarak belirtilmektedir. Standartlar,

kullanıcı taleplerini, teknoloji ve kaynakların sınırlamalarını ve güvenlik doğrulama gereksinimlerini karşılamaktadır (Taherdoost, 2022).

Standartlar, hizmetlerin, ürünlerin ve sistemlerin güvenliğini, güvenilirliğini ve tutarlılığını sağlamak için prosedürleri ve yönergeleri belirleyen belgelerdir. Bu belgeler, bir şirket veya ülke tarafından özel bir standart veya yerel düzenleme standardı olarak geliştirilebilmektedir. Uygulayıcı kuruluş tarafından yasal veya düzenleyici hükümler içeren bu kılavuzlar, içeriğinde bulunmayan gereksinimleri tamamlamak ve güçlendirmek için diğer standartlarla birlikte kullanılabilmektedir. Bazı standartlar her tür işletmeye ve devlet kurumuna açıkken, bazıları ise kapalı konumda olabilmektedir. Diğer bir ifadeyle bazı standartlar belirli sektörlere veya işletmelere özgü olabilmektedir. Kısacası standartlar, süreci tamamlamak için belirlenen yöntemleri açıklayarak yapılması gereken kuralları vermektedir (Taherdoost, 2022).

Bilgi sistemlerinin temelinde yer alan yazılımları ve donanımları tek bir üreticiden tedarik etmek imkânsız görülmektedir. Günümüzde kuruluşlar kendi bilgi teknoloji alt yapılarını farklı üreticilerden tedarik etmekte ve bu ürünlerin birlikte çalışmalarını sağlamak amacıyla standartlardan yararlanmaktadır. Standartlar, yazılım ve donanım üreticileri için rekabetçi bir pazar oluşturmakta ve bu pazarın devamlılığı için gerekli görülmektedir. Bilgi işlem ortamındaki ürünlerin birlikte çalışmalarını sağlamak için oluşturulan standartlar, temel uygulama belgeleri arasında bulunmaktadır. Bu nedenle birçok kurum ve kuruluş bilgi teknoloji ürünlerinin birlikte kullanımından güvenliğine kadar olan süreçleri yürütmek için standartlar geliştirmekte ve bu standartları teknolojik gelişme ve gereksinimlere göre güncellemekte ve geliştirmektedir.

Standartlar, kurumların güvenlik politikası hedeflerini yerine getirmek için gereksinim duydukları çözümleri içermektedir. Standartları benimsemenin birçok faydası bulunmaktadır. Fakat kurumlar her yönetim süreci için kendi standardını oluşturmak zorunda değildir. Çünkü ulusak veya uluslararası düzeyde çalışan gücenilir organizasyonların oluşturduğu standartlar benimsenebilir ve bunlar kurumun iş süreçlerine uyarlanarak kullanılabilmektedir. Standartlar ayrıca kurumun genelinde ortak bir güvenlik temeli oluşturmaktadır. Bu ortak güvenlik anlayışı, kurum içerisinde tüm birim ve çalışanların aynı güvenlik olguları içerisinde

kalmalarına yardımcı olmaktadır. Tüm birim ve çalışanların uyumlu bir güvenlik anlayışı içerisinde kalmaları için gereken planlara sahip olmalarını sağlamaktadır (Kim ve Solomon, 2018).

Standartların dezavantajlarından biri, kırılgan bir yapıya sahip olmalarıdır. Bir kuruluşun bilgi sistemine dâhil edilen hatalı bir ürün, tüm bilgi sistemini ve varlıklarını riske atabilir. Özellikle üretici veya satıcı tarafından desteklenmeyen veya bakımı ve lisansı maliyetli olan bir ürünün kullanılması durumunda, tek bir güvenlik standardının uygulanması yetersiz kalabilir. Bu nedenle, ürünler standartlara göre değerlendirilirken alternatif seçeneklerin de incelenmesi önemlidir. Bilgi sisteminde sorun çıkması durumunda, zararın en aza indirilmesi ve kesintilerin önlenmesi için alternatif ürünlerle garanti altına alınması, standartların etkili bir şekilde uygulanması açısından büyük önem taşır.

2.9.3. Rehberler

Rehberler, kuruluşların belirli bir konuda yönergeler, tavsiyeler ve pratik bilgiler sunan dokümanlardır. Bu dokümanlar, bir kuruluşun belirli bir teknoloji, süreç veya uygulama alanında en iyi uygulamaları takip etmesine yardımcı olmaktadır. Rehberler, genellikle bir teknoloji standardının uygulanması, sistem yapılandırması, güvenlik politikası uyumu, veri yönetimi veya iş süreçleri gibi konuları kapsamaktadır. Bu dokümanlar, kuruluş içindeki çalışanlara ve sistem yöneticilerine nasıl hareket etmeleri gerektiği konusunda yol göstermektedir (Kim ve Solomon, 2018).

Rehberler, genellikle sektör standartları, mevzuat veya uluslararası en iyi uygulamalar temelinde oluşturulur. Bu dokümanlar, teknik ayrıntıları, adım adım talimatları, örnek senaryoları ve önerilen yapılandırmaları içerebilmektedir. Bu dokümanlar, kuruluşun kendi ihtiyaçlarına ve hedeflerine uyacak şekilde özelleştirilebilir. Her kuruluşun kendi rehber dokümanlarını oluşturması veya harici kaynaklardan temin etmesi mümkündür.

Rehber dokümanları, kuruluşun güvenlik, uyumluluk ve operasyonel etkinlik gibi alanlarda kılavuzluk etmek ve en iyi uygulamaları takip etmek için önemli bir kaynak olarak kullanılmaktadır. Bu dokümanlar, kuruluşun süreçlerini

standartlaştırmak, hataları önlemek ve uyum sağlamak için değerli bir kurumsal güvenlik aracıdır.

2.9.4. Prosedürler

Prosedürler, bir güvenlik gereksinimini, sürecini veya amacını gerçekleştirmek için aşama aşama yürütülen sistematik eylemleri içermektedir. Bu dokümanlar, güvenlik politikasının sistemli olarak sürdürülmesi için mevcut en güçlü güvenlik araçlarındandır. Kuruluşların iş yapma biçimleri ile ilgili süreçleri belirlemekte ve güvenlik politikasının yürütülmesinde karşılaşılabilecek riskleri en aza indirgemektedir.

Bir politikanın veya standardın amacına uygun olarak uygulanmasını sağlayan prosedürlerde görevlerin tamamlanması için yapılması gereken aşamaları tanımlamaktadır. Böylelikle kriz anlarında olası hataları azaltmakta, önemli görev basamaklarını gözden geçirilmesini garanti altına almakta, güvence kontrollerinin yürütülmesi sürecinde müdahale alanları sağlanmaktadır. Prosedürler, güvenlik politikaları ve standartları gibi zorunlu güvenlik araçlarındandır (Kim ve Solomon, 2018).

2.10. Bilgi Güvenliği Standartları

Bilgi güvenliği standartları, kuruluşların bilgi sistemleri ve varlıklarının güvenliğini sağlamak için kullanılan kurumsal ve teknik yöntemleri içeren belgelerdir. Bu standartlar, verinin işlendiği, iletildiği ve depolandığı ortamlardaki kullanıcılar, ağ altyapısı, yazılım, donanım, süreçler ve bilgilerin güvenliğini amaçlamaktadır. Bilgi güvenliği standartlarının temel amacı, kurumsal veya kişisel bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak ve siber saldırıların neden olduğu riskleri en aza indirmektir. Bu standartlar, çeşitli güvenlik kontrollerini, süreçlerini, prosedürlerini, yönergelerini ve talimatlarını içerir ve kuruluşlara temel sağlamaktadır (Karie ve diğerleri, 2021). Bilgi güvenliği standartları, kuruluşlara güvenlik alanında en iyi uygulamaları sunarak siber güvenlik tehditlerinden ve risklerden korunmalarına yardımcı olmaktadır. Bu standartlar, güvenlik uzmanları tarafından önerilen ve kabul görmüş güvenlik önlemlerini içermektedir (Knapp ve diğerleri, 2017).

Bilgi güvenliği yönetimine ilişkin uluslararası düzeyde önemli standartlar bulunmaktadır. Bilgi güvenliği yönetiminde daha çok kabul gören bilgi güvenliği yönetimi çerçeveleri ve standartları şunlardır:

- ISO/IEC 27000 Serisi Bilgi Güvenliği Standartlar Ailesi
- NIST Özel Yayınları 800 Serisi
- COBIT - Bilgi ve Bağlantılı Teknolojiler Kontrol Hedefleri
- ITAF Bilgi Güvenliği Denetimi ve Emniyet standartları
- ITIL - Bilgi Teknolojisi Altyapı Kütüphanesi
- SoGP Bilgi Güvenliği İçin İyi Uygulama Standardı

Bu standart ve çerçevelerden kurumlar kendi hizmet düzeylerine göre yararlanmaktadırlar. Örneğin, detaylı kurumsal bilgi güvenliği tanımlamasını yapmak için ISO/IEC 27000 serisi bilgi güvenliği standartlarından, bilgi teknolojileri işlemeleri ve iş akışı entegrasyonu için kullanılabilecek en iyi uygulamaları ITIL'den, denetim ve kontrol modelleri için COBIT'ten ve bilgisayar güvenliği için ise NIST'ten yararlanabilmektedirler.

Bu bilgi güvenliği yönetim çereçeveleri ve standartları, çalışmanın temel hedeflerine ulaşmak için üniversite kütüphanelerinde hangi tür bilgi güvenliği uygulamalarının geliştirilmesi ve uygulanması konusundaki süreçlerin belirlenmesine yönelik önemli bilgiler sunmaktadır. Bu itibarla bu standartlar bilgi güvenliği alanında yeni bilgilerin keşfedilmesi, mevcut sorunların çözülmesi ve en iyi uygulamaların geliştirilmesi açısından çalışmaya büyük katkılar sağlamaktadır. Üniversite kütüphanelerinin bilg güvenliği yönetimi süreçlerini geliştirmelerine yardımcı olabilmek ve yeni değerlendirme yöntemleri, araçları veya modelleri geliştirilebilmek için çalışmanın uygulama aşamasında yapılacak çalışmalara rehberlik etmektedir.

Aşağıda bu standartlar üzerinde kısaca bilgiler verilmektedir.

2.10.1. ISO/IEC 27000 Serisi Standartları

ISO/IEC 27000 serisi bilgi güvenliği standartları, bilgi güvenliği yönetim sistemlerini oluşturmak ve sertifikalandırmak için kullanılan uluslararası standartlardır. Uluslararası Standardizasyon Örgütü (International Organization for Standardization) ve Uluslararası Elektroteknik Komisyonu (International

Electrotechnical Commission) tarafından ortaklaşa geliştirilmişlerdir. ISMS (Information Security Management System) Standartlar Ailesi veya kısaca ISO27k olarak da bilinmektedir. Bu standartlar ailesi; bilgi güvenliği yönetimi, risk yönetimi ve kontrollerin uygulanması hakkında öneriler sunmaktadır. Bu standartlar, bilgi güvenliği yönetim sistemini oluşturmasına ve uygulamasına rehberlik etmektedir. Kurum ve kuruluşlar, ISO/IEC 27000 serisi standartlarının çerçevesinde belirtilen gereksinimlere uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) oluşturabilir ve uygulayabilirler. Kuruluşlara bilgi güvenliği politikaları, süreçler, prosedürler ve kontrolleri geliştirme konusunda rehberlik etmektedir (Blokdyk, 2020).

Bu standartlar, finansal bilgiler, fikri mülkiyetler, personel ve müşteri bilgileri veya üçüncü taraflarca kendilerine emanet edilen bilgiler gibi bilgi varlıklarının güvenliğini sağlamak için bir çerçeve sunmaktadır. Bilgi varlıklarının korunması ve bilgi güvenliğinin sağlanması için küresel kabul görmüş en iyi uygulamaları içermektedirler. Kuruluşlar, bu standartlar çerçevesinde yönergeleri takip ederek bilgi güvenliği risklerini azaltabilir, müşteri ve paydaş güvenini artırabilir ve yasal ve düzenleyici gereksinimlere uyum sağlayabilir.

Kurum ve kuruluşlar, bu standartlar çerçevesinde geliştirilen belgeler ile finansal bilgilerinin, fikri mülkiyetlerinin, personel ve müşteri bilgilerinin veya üçüncü taraflarca kendilerine emanet edilen bilgilerin veya bilgi varlıklarının güvenliğini yönetmek için bir çerçeve geliştirebilmekte ve uygulayabilmektedir. Bu standartlar, bilgilerin korunması için geliştirilen BGYS'lerinin bağımsız bir biçimde değerlendirmesine de katkı sunmaktadır.

27000 serisi standartlarının temeli, İngiliz Standartları olarak da bilinen BS-7799 adı ile yayınlanmış standart çerçevesine dayanmaktadır. Bu standartlar ilk olarak 1995 yılında BS 7799-1 ve 1998 yılında ise BS 7799-2 olarak yayımlanmış, daha sonraki yıllarda ise ISO tarafından revize edilerek 2000 yılında ISO 17799 standartları olarak yayınlanmıştır. 2009 yılında ise ISO/IEC 27000 standartlar ailesi olarak yayınlandı ve günümüze kadar çeşitli güncellemeler geçirmiştir.

Bu standart ailesi, uygulama biçimine göre çeşitli belgeler altın yayımlanmakta ve sürekli olarak güncellenmektedir Her bir standart, belirli bir konuya odaklanarak

kuruluşlara rehberlik sağlamakta ve bilgi güvenliği yönetimi süreçlerinin ve kontrollerinin etkili bir şekilde uygulanmasına yardımcı olmaktadır. Bu standartlar, kuruluşların bilgi güvenliği alanında en iyi uygulamaları takip etmelerine ve riskleri yönetmelerine olanak sağlamaktadır.

2.10.2. NIST SP 800 Serisi Standartları

Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technogy), tarafından kuruluşların siber güvenlik risklerini yönetmelerine yardımcı olmak için siber tehditleri ele alan ve kuruluşların hizmetlerini destekleyen bir dizi güvenlik standardı ve rehberlik dokümanlarıdır. NIST SP 800 serisi standartları, siber güvenlik uygulamaları, bilgi güvenliği yönetimi, risk değerlendirme, risk işleme ve kontrol önlemlerinin belirlenmesi gibi faaliyetler için uluslararası kabul görmüş yayınları arasında yer almaktadır. Bu serinin amacı, bilgi güvenliği ve siber güvenlik alanında en iyi uygulamaları, yöntemleri ve kontrolleri tanımlamak ve yaymak ve kuruluşlara rehberlik etmektir. NIST Özel Yayınlar 800 serisi olarak tanınan bu dokümanlar, bilgi sistemlerinin güvenlik faaliyetleri için rehberlik sağlayan pek çok standardı kapsamaktadır (Calder, 2018).

NIST SP 800 standartlar serisinde çok sayıda rehberlik ve yönergeleri içeren ve geniş bir yelpazede bilgi güvenliği konularını kapsayan standartlar bulunmaktadır. NIST SP 800 Serisi, hem ABD hükümeti hem de uluslararası alanda faaliyet gösteren kuruluşlar tarafından sıklıkla kullanılan önemli bir kaynaktır. Bilgi güvenliği yönetimi ve uygulamaları konusunda standartlaşmış yaklaşımlar sunmaktadır. (NIST, 2022a):

2.10.3. COBIT Bilgi ve Bağlantılı Teknolojiler Kontrol Hedefleri Standardı

Bilgi Sistemleri Denetim ve Kontrol Derneği (Information Systems Audit and Control Association - ISACA) tarafından bilgi teknolojisi yönetimi için oluşturulan COBIT (Control Objectives for Information and Technology), bilgi ve bağlantılı teknolojilerin yönetimi için bir çerçeve olarak kullanılan bir dizi standart ve rehberlikler bütünüdür. COBIT, bilgi teknolojileri yönetimi, bilgi güvenliği, risk

yönetimi ve iş sürekliliği gibi alanlarda en iyi uygulamaları ve kontrol hedeflerini tanımlamaktadır (ISACA, 2019).

COBIT, ilk olarak 1996'da piyasaya sürüldü ve en son sürümü 2019'da yayımlanmıştır. Bu dokümanlar, kuruluşların bilgi ve bağlantılı teknolojileri etkili bir şekilde yönetmelerine yardımcı olmak için çeşitli kontrol hedefleri ve en iyi uygulamalar sunmaktadır. İşletme hedeflerini desteklemek, riskleri yönetmek, kaynakları etkin bir şekilde kullanmak, bilgi ve teknoloji ile ilgili faaliyetleri izlemek ve performansı değerlendirmek için çeşitli kontrol hedefleri sağlamaktadır. Bu kontrol hedefleri, bilgi güvenliği, süreç performansı, risk yönetimi, kaynak yönetimi ve işbirliği gibi alanlarda odaklanmaktadır. Kuruluşların bilgi ve bağlantılı teknolojilerle ilgili süreçleri ve kontrolleri kurmalarını, uygulamalarını ve iyileştirmelerini sağlamayı amaçlayan COBİT, ayrıca kuruluşlar arasında bir dil ve anlayış sağlayarak paydaşlar arasında etkili iletişimi ve işbirliğini teşvik etmektedir (ISACA, 2018).

COBIT'in kontrol hedeflerini açıklayan bir standardı kesin olarak COBIT 5 olarak bilinmektedir. Bu standart, organizasyonların bilgi teknolojileri süreçlerini etkin bir şekilde yönetmelerini, riskleri azaltmalarını ve hedeflere ulaşmalarını sağlamak için bir dizi kontrol hedefi sunmaktadır.

COBIT 5, planlama ve organizasyon, edinme ve uygulama, teslim ve destek, izleme ve değerlendirme, iş sürekliliği ve risk optimizasyonu olmak üzere beş ana hedef kategorisine dayanan 37 kontrol hedefini tanımlamaktadır. Bu kontrol hedefleri, organizasyonların bilgi teknolojilerini etkili bir şekilde yönetmelerine ve kontrol etmelerine yardımcı olmaktadır. COBIT, bilgi teknolojileri hizmetlerinin iş gereksinimlerine uygun olarak sağlanmasını, risklerin yönetilmesini ve stratejik hedeflere ulaşılmasını desteklemektedir (ISACA, 2019).

2.10.4. ITAF Bilgi Güvenliği Denetimi ve Emniyeti Standartları

ITAF (Information Technology Assurance Framework), bilgi güvenliği denetimi ve emniyeti için bir standartlar setidir. ITAF, ISACA tarafından geliştirilmiş ve bilgi teknolojileri denetimini desteklemek amacıyla kullanılan bir çerçevedir. Denetim ve güvenlik görevlilerinin planlanması, yerine getirilmesi ve raporlanması teknikleri ve kılavuzlarını sunmaktadır. Standart üç kategoriye ayrılmaktadır. 100 serisi genel

standartları, 1200 serisi performans standartlarını, 1400 serisi ise raporlama standartlarını oluşturmaktadır.

ITAF standartları, bilgi güvenliği denetimi sürecinde izlenmesi gereken adımları, en iyi uygulamaları ve kontrol hedeflerini tanımlamaktadır. Bu standartlar, denetim profesyonellerine, bilgi güvenliği kontrolünün etkin bir şekilde yapılmasına yardımcı olur ve riskleri azaltmaya yönelik öneriler sunmaktadır.

ITAF, şu bileşenlerden oluşmaktadır (ISACA, 2022):

- Genel Kontroller: Bilgi sistemlerinin güvenliğini ve işletimini etkileyen genel kontrolleri içerir. Örnek olarak, fiziksel güvenlik önlemleri, erişim kontrolü ve değişiklik yönetimi gibi konular bulunur.
- Uygulama Kontrolleri: Uygulama sistemlerinin güvenliğini ve işletimini etkileyen kontrolleri içerir. Örnek olarak, veri girişi kontrolleri, yetkilendirme mekanizmaları ve veritabanı yönetimi gibi konular bulunur.
- Operasyon Kontrolleri: Bilgi teknolojileri operasyonlarının güvenliğini ve işletimini etkileyen kontrolleri içerir. Örnek olarak, sistem izleme, yedekleme ve geri yükleme, olay yönetimi gibi konular bulunur.
- Bilgi Güvenliği Kontrolleri: Bilgi güvenliği yönetimine yönelik kontrolleri içerir. Örnek olarak, politika ve prosedürlerin oluşturulması, risk değerlendirmesi, olay yanıtı ve felaket kurtarma gibi konular bulunur.

ITAF standartları, denetim profesyonellerine bilgi güvenliği denetim sürecini yönlendirmek için bir çerçeve sunmaktadır. Bu standartlar, işletmelerin bilgi güvenliği uygulamalarını değerlendirmelerine ve geliştirmelerine yardımcı olmaktadır.

2.10.5. ITIL Bilgi Teknolojisi Altyapı Kütüphanesi

ITIL (Information Technology Infrastructure Library), bilgi teknolojisi hizmet yönetimi alanında bir dizi en iyi uygulamalar ve kılavuzlardan oluşan bir çerçevedir. ITIL, bilgi teknolojileri hizmetlerinin etkili bir şekilde tasarlanması, yönetilmesi ve iyileştirilmesi için rehberlik sağlamaktadır. ITIL, işletmelerin BT hizmetlerini müşteri odaklı, süreç odaklı ve en iyi uygulamalara dayalı bir şekilde yönetmelerine yardımcı olmaktadır. ITIL'in ana hedefleri arasında, hizmet kalitesinin artırılması,

maliyetlerin azaltılması, risklerin yönetilmesi ve müşteri memnuniyetinin sağlanması yer alır.

ITIL, bir dizi yayından oluşan ve farklı alanlara odaklanan bir kütüphane olarak sunulmaktadır. Bu yayınlar, bilgi teknolojileri hizmet yönetimi süreçlerini, rolleri, sorumlulukları ve en iyi uygulamaları açıklamaktadır. Aşağıda ITIL'in temel kitaplarından bazıları bulunmaktadır (Gallacher ve Morris, 2012).

- ITIL Hizmet Stratejisi: Bilgi teknolojileri hizmetlerinin stratejik planlamasına odaklanmakta ve hizmet portföyü yönetimi, finansal yönetim ve risk yönetimi gibi konuları kapsamaktadır.
- ITIL Hizmet Tasarımı: BT hizmetlerinin tasarımına odaklanmakta ve hizmet kataloğu yönetimi, süreç tasarımı, hizmet seviyesi yönetimi gibi konuları kapsamaktadır.
- ITIL Hizmet Geçişi: Bilgi teknolojileri hizmetlerinin geçiş sürecine odaklanmakta ve değişiklik yönetimi, sürüm ve dağıtım yönetimi gibi konuları kapsamaktadır.
- ITIL Hizmet İşletimi: Bilgi teknolojileri hizmetlerinin günlük işletme ve yönetimine odaklanır ve olay yönetimi, problem yönetimi, erişim yönetimi gibi konuları kapsar.
- ITIL Sürekli Hizmet İyileştirme: Bilgi teknolojileri hizmetlerinin sürekli olarak geliştirilmesine odaklanmakta ve performans yönetimi, hizmet ölçümü, sürekli iyileştirme süreci gibi konuları kapsamaktadır.

ITIL, kurumların bilgi teknolojileri hizmetlerini daha etkin ve verimli bir şekilde yönetmelerine yardımcı olmaktadır. İşletmeler, ITIL'in en iyi uygulamalarını benimseyerek süreçlerini iyileştirebilir, hizmet kalitesini artırabilir ve müşteri memnuniyetini sağlayabilir.

2.10.6. SoGP Bilgi Güvenliği İçin İyi Uygulama Standardı

SoGP (Standard of Good Practice for Information Security) standardı ilk olarak 1996 yılında Bilgi Güvenliği Forumu (The Information Security Forum - ISF) tarafından yayımlanmıştır. Bilgi güvenliği için en iyi uygulamaların ayrıntılı bir dokümantasyonunu temsil etmektedir. Standart iki yılda bir yayınlanmakta ve revize

edilmektedir. Ücretsiz olarak kullanılabilen İyi Uygulama Standardı, ISO/IEC 27002 ve COBIT v4.1'den türetilmiştir. Bu standartlar ve hem araştırmaya hem de gerçek dünya deneyimine dayanan işlevsel bir bilgi güvenliği metodolojisini ana hatlarıyla belirtmektedir (Whitman ve Mattord, 2019).

SoGP İyi Uygulama Standardı Standartı, altı temel güvenlik hususunu ele almaktadır:

- Bilgisayar kurulumları; esas olarak bilgi teknolojisi uzmanlarını hedeflemekte ve kritik iş uygulamalarını destekleyen donanım ve yazılımları ele almaktadır.
- Kritik iş uygulamaları; kuruluşun faaliyetlerinin bağlı olduğu uygulamalardır. Bu yön öncelikle iş süreçlerinden sorumlu kişileri ve sistem jeneratörlerini hedef almaktadır.
- Güvenlik yönetimi; güvenlikle ilgili karar vericileri ve denetçileri hedef almaktadır. Kuruluş genelinde güvenlik uygulamalarıyla ilgili olarak yönetim düzeyinde karar vermeyi yönetmektedir.
- Ağlar; benzersiz güvenlik açıkları nedeniyle özel bir kategori oluşturmaktadır. Bu güvenlik hususu, genellikle ağ yöneticileri, ağ hizmeti uzmanları ve ağ hizmeti sağlayıcılarının güvenliği hedeflenmekte ve bir kuruluşun ağ oluşturma gereksinimlerinin doğasını ve uygulamasını ele almaktadır.
- Sistem geliştirme; sistem geliştiricilerine hitap etmekte olup sistem gereksinimlerinin tanımlanması, tasarımı ve uygulanması ile ilgilenmektedir.
- Son kullanıcı ortamı; son kullanıcı ortamlarında çalışan işletme yöneticilerini ve bireylerin güvenliği hedeflenmektedir.

2.10.7. IEEE 802 Standartları

IEEE 802 standartları, kablosuz ağlar, Ethernet ve yerel alan ağı (LAN) teknolojileri gibi bilgisayar ağlarıyla ilgili teknik spesifikasyonları belirlemek için kullanılan bir dizi standarttır. Elektrik ve Elektronik Mühendisleri Derneği (Institute of Electrical and Electronics Engineers - IEEE) tarafından geliştirilen bu standartlar, bilgisayar ağlarının uyumlu ve etkin çalışmasını sağlamak amacıyla oluşturulmuştur.

IEEE 802 standartları, farklı katmanlarda çalışan ağ protokollerini kapsar. Aşağıda, bazı önemli IEEE 802 standartlarının örneklerini bulabilirsiniz (Guo ve Congdon, 2021):

- IEEE 802.3 (Ethernet): Kablolu yerel alan ağlarında (LAN) kullanılan Ethernet standartlarını belirlemektedir. Bu standartlar, veri iletimi için çerçeve yapısını, veri hızlarını ve ağ topolojilerini tanımlamaktadır.
- IEEE 802.11 (Wi-Fi): Kablosuz yerel alan ağlarında (WLAN) kullanılan Wi-Fi standartlarını belirlemektedir. Bu standartlar, kablosuz ağ bağlantısını, frekans bantlarını, güvenlik protokollerini ve hızları tanımlamaktadır.
- IEEE 802.15 (Bluetooth): Kablosuz kişisel alan ağlarında (PAN) kullanılan Bluetooth standartlarını belirlemektedir. Bu standartlar, kısa mesafeli kablosuz iletişimi, bağlantı protokollerini ve güvenlik özelliklerini tanımlamaktadır.
- IEEE 802.16 (WiMAX): Geniş alan ağlarında (WAN) kullanılan WiMAX standartlarını belirletendir. Bu standartlar, yüksek hızlı kablosuz internet erişimini, veri hızlarını ve mesafeleri tanımlamaktadır.
- IEEE 802.1 (LAN/MAN Yönetimi): Yerel alan ağları (LAN) ve geniş alan ağları (MAN) yönetimi için standartlar oluşturulmaktadır. Bu standartlar, ağ yapılandırması, ağ yönetimi protokolleri ve ağ güvenliği gibi konuları kapsamaktadır.

IEEE 802 standartları, bilgisayar ağlarının uyumlu bir şekilde çalışmasını sağlamakta ve farklı cihazların birbirleriyle iletişim kurabilmesini sağlayan ortak bir dil oluşturulmaktadır. Bu standartlar, ağ teknolojilerinin gelişmesine ve ilerlemesine katkıda bulunmakta ve endüstri genelinde kabul görmektedir.

3. BİLGİ GÜVENLİĞİ TEHDİTLERİ VE ÖNLEMLERİ

3.1. Bilgi Güvenliği Tehditlerinin Kaynakları

Tehdit, kurum faaliyetlerini ve bilgi varlıklarını olumsuz yönde etkileyebilecek herhangi bir olay veya durumdur. Saldırı ise bilgiye ve onu destekleyen sistemlere zarar verebilecek veya başka şekilde tehlikeye atabilecek kasıtlı veya kasıtsız eylemdir (ISO, 2018).

Bilgi güvenliği tehdit kaynakları birçok şekilde kategorize edilmektedir. Bu gruplandırmaların önemli yollarından biri tehdidin kökenine dayanmaktadır ki bunlar iç tehdit kaynakları ve dış tehdit kaynakları olarak gruplandırılmaktadır. Aynı şekilde bu tehdit kaynakları donanım, yazılım, ağ, veri, iletişim, sosyal, ekonomik, insan ve fiziksel tehdit katmanlarına göre de kategorize edilebilmektedir.

Nayak ve Rao (2014)'ya göre tehdit kaynakları iç ve dış tehditler olarak iki grup altında ele alınmaktadır. İç tehditler kurum içindeki bilgi ve kaynak yetersizliklerinden kaynaklanmaktadır. İç tehditler daha çok insan kaynaklı tehditlerdir. Özellikle kurum çalışanlarının kasıtlı veya kasıtsız eylemleri iç tehditlerin temel nedenidir. Bu temel kaynağın teknolojik ve fiziksel güvenlik katmanlarına etkisi iç tehditlerin oluşumunda önemli rol oynamaktadır. İnsan kaynaklı başlıca tehditler dolandırıcılık, bilgilerin kötüye kullanılması ve bilgilerin yok edilmesidir. Bunun gibi birçok iç kaynaklı tehdidin şu nedenlerden kaynaklandığı belirtilmektedir:

- **Zayıf bilgi güvenlik politikaları:** Güvenlik politikalarının güçlü niteliklere sahip olması önemlidir. Bilgi güvenliği politikalarının kuruluşun faaliyetleri ve işlevleri ile birebir örtüşmesi gerekmektedir. Gizli bilgilerin yetkisi olmayan kişiler veya gruplarla kasıtlı veya kasıtsız olarak paylaşılması, kimlik doğrulama veya yetkilendirme işlemlerinin yetkisiz kişilerin erişimine sunulması, müşteri veya tedarikçi bilgilerin izinsiz paylaşılması, bilgi güvenliği yönetimi rol ve sorumlulukların net bir biçimde belirlenmemesi, görevlerin uygun biçimde ayrılmaması gibi zayıf bilgi güvenliği uygulamaları bilgi güvenliğini ciddi şekilde etkileyebilir ve çeşitli risklerin ortaya çıkmasına neden olabilir. Bu nedenle, güvenlik politikalarının gözden

geçirilmesi, uygun önlemlerin alınması ve personelin bilgi güvenliği konusunda eğitilmesi önemlidir. Aksi takdirde, bu gibi zayıf güvenlik eylemleri bilgilerin kötüye kullanılmasına, imha edilmesine, sahtekârlığa ve görevin kötüye kullanılmasına neden olabilmektedir.

- **Zayıf bilgi güvenlik yönetimi:** Bilgi güvenliği politikalarının iyi bir biçimde uygulanması güçlü bir yönetim anlayışından geçmektedir. Yönetimin güvenlik politikalarını iyi bir biçimde planlaması, uygulaması ve sürekli denetim altında tutması gerekir. Bilgi sistemlerinde ve uygulamalarında tanımlanan zayıf yönetici ve kullanıcı şifrelerinin belirlenmesi, yerel ağa veya donanımlara erişim kısıtlamalarının planlanmaması, çalışanların kişisel cihazlarından veya kimliği doğrulanmamış ağlardan bilgi sistemlerine erişimlerinin kısıtlanmaması, USB gibi harici kişisel aygıtların bilgi sistemlerine erişimlerinin denetlenmemesi, yüklenici veya tedarikçi tarafların sistemlere erişimlerinin kısıtlanmaması, güvenirliği denetlenmemiş sistemlerin veya uygulamaların mevcut sistemlere entegre edilmesi, denetimsiz web sitesi hizmetinin verilmesi, güvenilir olmayan yazılım veya uygulama indirmelerine müsaade edilmesi, sınırsız ve denetimsiz uzaktan erişim izinlerinin tanımlanması, kimlik avı, korsan saldırıları gibi saldırılara karşı alınan tedbirlerin yetersizliği, telif hakkı ile ilgili çalışmalara yeterince önem verilmemesi gibi birçok güvenlik yönetim anlayışının yetersizliğinden kaynaklı eylemler oluşabilmektedir. Bu eylemler bilgi hırsızlığı, yetkisiz erişim ve sistem saldırıları gibi birçok tehdide neden olabilmektedir.
- **Kullanıcıların bilgi güvenliği becerilerindeki eksiklikler:** Gerek çalışanlar gerekse müşterilerin bilgi güvenliği becerilerini gereken seviyede tutmak önemlidir. Kurum her ne kadar iyi bir bilgi güvenliği politikası uygulasa da bu politikanın kullanıcılara da iyi bir biçimde benimsetilmesi gerekmektedir. Kullanıcılar, bilgi güvenliği farkındalık eğitimleri ve etkinlikleri ile desteklenmelidir. Kullanıcıların şifreleme veya parola konusundaki bilgisizlikleri, bilgi varlıklarının uygun kullanımı, kullanıcı kimliklerinin veya şifrelerinin yetkisiz kişilerle paylaşılması, sosyal mühendislik saldırılarına karşı farkındalığın eksikliği, kimlik avı gibi saldırıların önemsenmemesi, kötü amaçlı saldırı tehditlerini barındıran yazılım,

uygulama, yardımcı program ve araçların indirilmesi ve kullanılması, itibar kaybına veya yasal ihlallere yol açabilecek uygunsuz e-posta iletilmesi, messenger veya skype gibi haberleşme uygulamalarının yanlış kullanımı, güvenlik yapılandırmalarının gevşetilmesi ve uygun olmayan güvenlik yapılandırmalarının kullanılması, güvenlik hatalarını görmezden gelerek işlemlerin devam ettirilmesi gibi başlıca olumsuz eylemler kullanıcıların bilgi güvenliği becerilerindeki eksikliklerden kaynaklanmaktadır. Bu eylemler gizli bilgilerin ifşa olmasına, sistemlere yetkisiz erişimlerin oluşmasına, itibar kaybına ve dolandırıcılık gibi tehditlere neden olabilmektedir.

Dış tehditler, kurum veya organizasyonun faaliyet gösterdiği ortam ve çevreden kaynaklanmaktadır. Donanım tehditleri, yazılım tehditleri, ağ ve iletişim tehditleri, yasal tehditler, ülkenin içinde bulunduğu duruma bağlı sosyo-ekonomik tehditler ve bilgisayar korsanlığından kaynaklanan insan ile ilgili tehditler başlıca dış tehdit kaynakları olarak değerlendirilmektedir.

International Telecommunication Union (2020) organizasyonu tarafından yayınlanan telekomünikasyon standartları belgesinde bilgi güvenliği tehdit kaynaklarının etki, karakter, aktör ve kökenlerine göre farklılaştığı vurgulamaktadır. Bilgi güvenliği tehditleri; kazayla ve kasten tehditler, aktif veya pasif tehditler, tehdit kaynağı, tehdit aktörü ve güvenlik açığı grupları altında incelenmektedir. Bir bilgi varlığının güvenliğini tehdit eden bilinçli eylemler kasıtlı tehditler altında değerlendirilirken, fiziksel hatalar veya yazılım ve donanım arızaları kazayla ortaya çıkan kasıtsız tehdit grubu altında değerlendirilmektedir. Verilerin yok edilmesi, değiştirilmesi veya veriyi depolayan donanımın imha edilmesi gibi bilgi sisteminin işletimine dair değişiklikler aktif tehdit grubu altında değerlendirilirken, bilgi sistemlerinin kaynaklarını etkilemeden sadece bilgi toplamayı amaçlayan tehditler ise pasif tehditler olarak değerlendirilmektedir. Tehdidi gerçekleştiren birey veya gruplar tehdit kaynağının aktörleri olarak ifade edilmektedir. Bu aktörlerin sistemlerdeki güvenlik açıklarını tespit ederek saldırıya geçtikleri bilinmektedir. Bu güvenlik açıkları ve tehditleri, zayıf güvenlik yönetimi ile birlikte çalışanların bilgi güvenliği farkındalıklarının yetersizliğinden kaynaklanmaktadır.

Volonino, Robinson ve Volonino (2004) ve Vaast (2007)'ın çalışmalarında da bilgi güvenliği tehdit kaynakları, iç ve dış eylemler altında gruplandırmaktadır. Dış

kaynaklı tehditlerin, bilgisayar korsanları, kötü amaçlı yazılım yüklemeleri, eski çalışanların saldırıları, virüsler, reklam yazılımları ve davetsiz misafir eylemleri gibi dışarıdan gelen saldırıları kapsadığı; iç kaynaklı tehditlerin ise yönetim ve personelin bazı merak, umursamazlık, kötü niyet, bilgisizlik ve kötü zaman ve süreç yönetimi gibi eylem ve tutumlarından kaynaklandığı belirtilmektedir.

Tehdidi bir bilgi sisteminin veya kurumsal bilgi varlığının zarar görmesine sebep olan veya olabilecek istenmeyen bir eylem olarak tanımlayan Tekerek (2008), her tehdidin arkasında gizli bir kaynağın olduğunu ve bu kaynağın da bilgi sistemlerindeki güvenlik boşluklarından yararlandığını vurgulamaktadır. Tekerek (2008)'te tehditleri, iç ve dış kaynaklı olmak üzere iki ana grup altında toplandığını belirtmektedir. Bu ana grupları da kendi içerisinde fiziksel tehditler, insan kaynaklı tehditler, donanım ve yazılım kaynaklı tehditler, ağ kaynaklı tehditler, güvenlik boşlukları ve eğitim eksikliğinden kaynaklanan tehditler olarak sınıflandırmaktadır.

Bilgi sistemlerine zarar veren güvenlik ihlalleri ve zafiyetlerin farklı kaynaklardan ortaya çıkabileceğini belirten Güldüren (2015), tehdit kaynaklarını şu başlıklar altında gruplandırmaktadır:

- Doğal afetler veya teknik arızalara bağlı tehditler,
- Prosedür yetersizliklerine bağlı tehditler,
- İnsan hatalarından kaynaklanan tehditler,
- Zararlı yazılımlardan kaynaklanan tehditler.

Gawde (2010), güvenlik tehditlerinin çoğunun çalışanların e-posta ekine yanlış dosya ekleme ve gönderme, sosyal mühendislik saldırılarını görmezden gelme, kurum dışındaki bir bilgisayara klasörlerin paylaşması, zayıf şifrelerin kullanılması ve paylaşılması gibi bilgi güvenliği bilincinden yoksun eylemlerden kaynaklandığını belirtmektedir. Bilgi sistemlerinin, kurumun tüm operasyonlarını etkileyen çok önemli bir yere sahip olduğunu ve bu nedenle yönetimin bu sistemleri kurumun en değerli bilgi varlıkları arasında kabul etmesi ve onları korumak için gerekli önlemlerin alınması gerektiğini vurgulamaktadır.

Whitman ve Mattord (2018) ise, bilgi güvenliği tehdit kaynaklarını on iki kategori altında değerlendirdikleri nedenlerden kaynaklandığını ifade etmektedirler. Bu kategoriler şu şekilde sıralanmaktadır:

- **Fikri mülkiyet tavizleri:** Telif hakları, ticari sırlar, markalar veya patentler gibi fikri mülkiyet hakları uygun bir biçimde korunur. Bu maddi olmayan bilgi varlıkları bilgi hırsızları tarafından saldırılara uğramaktadır. Fikri mülkiyetin yetkisiz olarak kullanılmaya çalışılması bilgi güvenliği için önemli bir tehdit oluşturmaktadır.
- **Hizmet kalitesindeki sapmalar:** Genellikle bir servis sağlayıcısı tarafından kaynaklanan ve kurum içerisinde olumsuz bir olaya neden olan hizmet aksamalarından oluşmaktadır. Bilgi sistemleri; elektrik şebekeleri, veri ve iletişim ağları, servis sağlayıcıları, donanım tedarikçileri, hatta temizlik personelleri olmak üzere birçok operasyonel ve destek sisteminin uyumlu ve sağlıklı bir biçimde çalışmasına bağlıdır. Örneğin, internet servisinin kesintiye uğraması kurumun hizmetini olumsuz etkilemektedir. Bilgi sistemlerini destekleyen diğer servis ve sistemlerin güvenliğini sağlamak kurumun hizmet kalitesini güvence altına alınmasını sağlamaktadır. İnternet hizmeti sorunları, iletişim ve diğer hizmet sağlayıcı sorunları ve enerji kaynakları sorunları gibi birçok sorun kurumların hizmet kalitesinde sapmalara neden olmaktadır.
- **Casusluk ve yetkisiz işlemler:** Bilgilerin gizliliğini ihlal eden yaygın bir saldırı kategorisidir. Yetkisiz bir kişinin gizli bilgilere erişim sağlaması, casusluk veya izinsiz giriş olarak tanımlanmaktadır. Bilgi güvenliği alanında sıkça söz edilen bu tehdit grubu, kurumların da en çok çekindiği tehdit türleri arasında yer almaktadır. Saldırganlar, bilgi sistemlerine işlenen bilgilere çeşitli bilişim yöntemleri ile yetkisiz bir biçimde erişilebilmektedir. Bilgi sistemlerine izinsiz ve çoğu zaman yasa dışı olarak erişim sağlayan hackerler bu kategoride en çok üzerinde durulan kişilerdir. Özellikle şifre kırma saldırıları ile bilgi sistemlerine sızan ve sistemleri ele geçiren hackerler kurumları bilgi güvenliği açısından en çok zorlayan yasadışı gruplar olarak bilinmektedir. Aslında yetenekli bilişim uzmanı olarak bilinen hackerler, yaptıkları saldırılar ile günümüzde daha çok yasadışı eylemler gerçekleştiren gruplar olarak tanınmaktadır.
- **Doğal Afetler:** Yangın, sel, deprem, yıldırım, kasırga, fırtına, tsunami hatta böcek veya kemirgen saldırıları, statik elektrik ve toz gibi doğal tehditler

insanların hayatlarını tehdit ederken, bilginin işlendiği ve muhafaza edildiği sistemleri ve varlıkları da olumsuz yönde etkilemektedir. Ayrıca bu kategori tehditler arasında mücbir sebep olarak adlandırılan sivil itaatsizlik ve savaş eylemleri de yer almaktadır. Doğal güçlerin tehditlerinden kaçınmak mümkün olmadığından kurumlar karşılaşabilecekleri hasarları en aza indirgemek için önleme, müdahale, iş sürekliliği ve kurtarma planları gibi acil durum planlarını hazırlamaları önemlidir.

- **İnsan hatası ve başarısızlığı:** Yetkili bir kullanıcının kasıtlı veya kötü niyetli bir amacı olmadan ya da bilgisizliğinden ötürü gerçekleştirdiği tehditleri içermektedir. Bu tür tehditler kurumların bilgi sistemlerine zarar verebilmekte ve bilgi kayıplarına neden olabilmektedir. Benzer hatalar, müşterilerin veya diğer paydaşların kurumun güvenlik politikalarına uymamasından da kaynaklanabilmektedir. Deneyimsizlik, yanlış eğitim, yanlış tahminler, başarı veya başarısızlık hırsı, baskı gibi durumlar bilgi güvenliği ile ilgili hatalara neden olan birkaç olumsuz eylem ve tutum arasında yer alır. Sebep ne olursa olsun zararsız görülen hatalar bile bir kurum için büyük olumsuzluklara neden olabilmektedir. Bir kurumun bilgi güvenliğine yönelik en büyük tehditlerinden biri, bilgiye en yakın potansiyel tehdit ajanları oldukları için kendi çalışanlarıdır. Çünkü çalışanlar, kurumun faaliyetlerini yürütürken aynı zamanda kurumun veri ve bilgilerini de kullanmaktadır.
- **Bilgi gaspı:** Bilgi varlıklarındaki değerli bilgilerin maddi kazanç elde edilmek amacıyla yetkisiz kişilerce çalınması eylemlerinden oluşmaktadır. Bilgi gaspında bulunan kişiler, gasp ettikleri bilgilerin kurum aleyhine ifşa edilmemesi veya kuruma geri iade edilmesi için maddi kazançlar elde etmeyi amaçlamaktadırlar. Bu grup altında son yıllarda fidye yazılımı olarak bilinen kötü amaçlı yazılım araçları çokça kullanılmaktadır. Bu saldırılar genellikle kimlik avı ve sosyal mühendislik gibi saldırılar sonucunda mağdur tarafın bilgi sisteminde çalıştırılan kötücül yazılımlarla sağlanmaktadır.
- **Sabotaj ve vandalizm:** Bir kurumun bilgi varlığını yok etmek veya imajına zarar vermek amacıyla bilgi sistemlerinin kasıtlı olarak sabote edilmesini içeren vandalizm eylemlerinden oluşan tehdit kategorisidir. Bu tehdit kategorisinde bilgi sistemlerine karşı gerçekleştirilen küçük bir vandalizm

eyleminden organize edilmiş sabotaja kadar birçok tehdit yer almaktadır. Bu tür eylemlerin mali açıdan etkilerinin yanı sıra kurumun imajı açısından etkisi de önemli görülmektedir. Özellikle kurumların dünyaya açılan yüzü olan web sitelerine yapılan saldırılar, kurumların mali değerlerini ve imajlarını sarsabilmektedir. Örneğin, bilgi ve siber güvenliği alanında eğitimler düzenleyerek kurum ve kuruluşlara profesyonel eğitim hizmeti sunan SANS Enstitüsünün web sitesine 13 Temmuz 2001 tarihinde Flutti Bunni olarak bilinen bir grup tarafından yapılan saldırı enstitü tarafından utanç vericiydi. Saldırgan grup tarafından enstitünün web ana sayfasında yayınlanan "Size güvenliği öğretmek için bu adamlara gerçekten güvenir misiniz?" sloganı kurumun imajına ve itibarına zarar vermiştir (SANS, 2021).

- **Yazılım saldırıları:** Kurumların bilgi sistemlerini ele geçirmek veya bilgi varlıklarını yok etmek amacıyla saldırganlar tarafından üretilen zararlı yazılımlar tarafından gerçekleştirilen tehdit grubudur. Bu tür yazılımlar bilgi sistemlerinin kullanımlarında aksamalar oluşturabildiği gibi bilgi güvenliği zafiyeti de oluşturabilmektedir. Kurumun bağlı sistemlerine yayılarak bilgi ve veri hırsızlığı gerçekleştirilen bu tür yazılımların birçok çeşidi bulunmaktadır. Virüsleri, solucanları ve truva atlarını içeren kötü amaçlı yazılım saldırıları, arka ve tuzak kapılar ve bakım kancaları gibi saldırılar, hizmet reddi saldırıları, e-posta saldırıları ve iletişim durdurma saldırıları bu grubun içerisinde yer alan bilgi güvenliği tehdit kaynaklarıdır.
- **Donanım arızaları ve hataları:** Bilgi sistemlerinin kullandığı donanımlardaki teknik kusurlar, bilgi güvenliğinde beklenmeyen olumsuz sonuçlara neden olabilmektedir. Bu kusurlar, donanımların beklenen parametrelerin dışında çalışmasına neden olarak bilgi sistemlerini tehlikeye düşürmektedir. Bazıları kurumun ana terminal donanımlarında yer aldıkları için bilgi sisteminde kurtulamaz kayıplara neden olabilmektedir. Bazıları ise zaman zaman ortaya çıkarak sistemin kullanılabilirliğinde aksamalara neden olabilmektedir.
- **Yazılım arızaları ve hataları:** Bilgi sistemleri tarafından kullanılan yazılımlar, kullanılabilirlik kaybına veya bilgilere yetkisiz erişime yol açabilecek arızalara yol açan olası ve kasıtsız hatalar ile kullanıma

sunulmaktadır. Bazı yazılım ve donanım kombinasyonlarının kusurlarının denetlenmemesi yeni arızaların ve hataların oluşmasına neden olmaktadır. Güvenlik denetimlerini geçen kusurlu yazılımlar ciddi bilgi güvenliği ihlallerini beraberinde getirmektedir.

- **Teknolojik eskime:** Eskimiş veya teknolojik uyumluluğunu yitirmiş altyapı, bilgi sistemlerinin kullanılabilirlik kaybına veya bilgi sistemlerine yetkisiz erişime neden olabilmektedir. Bilgi sistemlerinin kullandığı altyapı teknolojisinin güncel teknolojiye uygun olmamasına bağlı saldırılara maruz kalabilmekte ve bilgi güvenliği riski artmaktadır. Bu durum yönetim tarafından dikkate alınarak eski teknolojik altyapının yeni teknolojik altyapı araçları ile desteklenmesi veya yenilenmesi gerekir. Yönetimin stratejik planlamasının içeriğinde kullanılan teknolojiye ait kullanılabilirlik analizlerinin yer alması, bu tür güvenlik tehditi riskini en aza indirmektedir.
- **Hırsızlık:** Hırsızlık, genellikle yazılım saldırıları, casusluk veya izinsiz giriş, bilgi gaspı ve fikri mülkiyete verilen tacizlerle örtüşen bir tehdit kategorisidir. Bilgi hırsızlığı çok çeşitli saldırılardan kaynaklanabilmektedir. Bilginin değerini azaltan bu gruptaki eylemler, fiziksel ve elektronik olmak üzere iki yolla gerçekleşmektedir. Fiziksel hırsızlık, kilitli kapılar, eğitimli güvenlik personeli ve alarm sistemleri gibi çeşitli önlemler kullanılarak kontrol edilmeye çalışılmaktadır. Fakat elektronik hırsızlığı kontrol etmek veya yönetmek daha karmaşık bir sorundur. Örneğin bir fiziksel hırsızlık sonucunda kayıp olan bilgi varlığı kolayca tespit edilebilirken, elektronik ortamdaki bir bilgi hırsızlığını tespit etmek her zaman kolay olmamaktadır. Elektronik bilgi hırsızlığında rol oynayan saldırganlar, girişim izlerini dikkatli bir biçimde kapatarak işlenen suçun çok geç fark edilebilmesini hatta hiç fark edilmemesini sağlayabilmektedirler.

3.2. Bilgi Güvenliği Tehdit Riskleri ve Saldırılar

Güvenlik planlamalarında öncelikli olarak neyin korunması gerektiğini anlamak ve bilmek temel olgudur. Bu durum bilgi güvenliği için de aynı temel olguya dayanmaktadır. Kurumların bilgi güvenliği tehditlerine karşı kendilerini savunabilmesi için ilgili güvenlik önlemlerini planlamadan önce hangi bilgi

varlıklarını hangi düzeyde koruması gerektiğini bilmesi gerekmektedir. Bilgi sistemlerini oluşturan donanımlar, uygulamalar, bilgisayar sistemleri ve ağları gibi tüm varlıkların hangi olası tehditler altında bulunduğunun bilinmesi gerekir. Bu güvenlik tehditlerinin farkında olunması, kurumun itibarı ve değeri için önemlidir (Muharremoğlu, 2013).

Kurumlar faaliyetlerinin devamlılığı için işledikleri bilgileri, tehdit ve saldırılardan koruması gerekmektedir. Bu koruma sürecini işletebilmesi için ise bazı öncelikleri yerine getirmesi gerekir. Öncelikle korunacak bilgileri ve bunların işlendiği ve muhafaza edildiği sistemleri kısacası kendi öz bilgi varlığını tanıması gerekir. Daha sonra ise bu varlıklarının karşılaşabileceği tehdit ve saldırıları belirlemesi ve bunları tanıması gerekir. Yönetimin bilgi güvenliği konusunda sağlam kararlar alabilmesi için kurumun verilerine, çalışanlarına, uygulamalarına ve bilgi sistemlerine yönelik gerçekleşebilecek tehditler hakkında bilgi sahibi olması bilgi güvenliğinin en önemli işlevidir (Solmaz, 2022).

Tehditler, bilgi varlıkları için her zaman potansiyel riski temsil etmektedir. Bu potansiyel risk bilgi varlığına karşı olumsuz sonuçlar doğurabilecek saldırı eylemine dönüşebilmektedir. Tehditler, güvenlik kontrollerinin sağlıklı yapılmadığı zaman güvenlik açıklarından yararlanarak bilgi varlıklarına zarar verici eylemlere dönüşebilmektedir. Tehditler, bilgi varlıkları üzerinde her zaman potansiyel risk barındırmaktadır. Tehditlerin aksine saldırılar ise yalnızca belirli bir eylemin kayba neden olabileceği durumlarda kendini göstermektedir. Örneğin, bilgi sistemlerinden bir verinin kaybolma veya çalınma riski birçok kurumda potansiyel bir tehdit riskini oluştururken, sadece bir bilgi kaybı ve buna bağlı kayıp riski gerçek bir saldırı sürecinde gerçekleşmektedir. (Whitman ve Mattord, 2019).

Jones ve Ashenden, (2005), bilgi güvenliği tehdit riskinin değerlendirilmesinde önemli adımların olduğunu ve bunların şu şekilde sıralandığını belirtmektedir:

- Korunması gereken bilgi varlıklarının belirlenmesi,
- Varlıkların kuruluşlar açısından ne derecede değerli olduğunun bilinmesi,
- Hizmetlerin yürütülmesinde etkin olan her bir bilgi varlığının maruz kalacağı olası tehditlerin belirlenmesi,

- Bilgi varlıklara karşı oluşan tehditlerin ne şekilde önlenmeye çalışılacağının planlanması,
- Saldırıların hizmetleri nasıl etkileyeceğinin araştırılması,
- Oluşacak zararların etkilerini düşürmek için yapılacak eylemlerin araştırılması,
- Tehditleri minimum seviyede tutmak için önlemlerin planlanması.

Tehdit çok geniş bir terimdir. Tehditler, güvenlik açıkları ve saldırılar bağlamında tartışıldığında daha belirgin hale gelmektedir. Tehdit, güvenlik açığı bağlamında incelendiğinde daha spesifik durumda değerlendirilmektedir (Slade, 2006). Güvenlik açığı ve tehdit terimlerinin tanımları farklılık göstermektedir ve bu terimler için evrensel olarak kabul edilmiş hiçbir tanım bulunmamaktadır (Schneier, 2015; Igure ve Williams, 2008; Slade, 2006; Bishop, 2005; Denning, 1999). Tehditler geneldir, güvenlik açıkları ise sistemde kullanılan koruyucu önlemlere bağlı olduklarından çevreye özgüdür (Furnell, 2007).

ISO 27000 standardına göre tehdit, bir sistem veya kuruluşa zarar verebilecek istenmeyen bir olayın olası nedeni olarak tanımlanmaktadır. Bir organizasyon tarafından işlenen ve depolanan tüm bilgiler saldırı, doğa olayları ve hatalar gibi tehditlere ve kullanıma bağlı olarak güvenlik açıklarına tabidir (ISO, 2018).

Güvenlik açığı, bir varlık veya kontrolün (riski değiştiren herhangi bir süreç, ilke, cihaz, uygulama veya diğer eylemler) bir veya daha fazla tehdit tarafından istismar edilme zayıflığıdır (ISO, 2018). Güvenlik açıkları daha çok donanım, yazılım, ağ gibi teknolojik altyapı varlıklarında oluştuğu belirtilmektedir (Pipkin, 2000). Spesifik olarak bir bilgi sistemi tehdidi, istenmeyen sonuçlara yol açabilmekte ve bilgi sistemlerindeki güvenlik açığından kaynaklanan bir tehlikeye neden olmaktadır. Örneğin, doğal afetler veya insan hataları gibi spesifik tehditler, bilgi varlıklarının istismar edilmesine yol açabilecek güvenlik açıklarına neden olabilmektedir (Muharremoğlu, 2013).

Slade (2006), tehdidin tek başına bir sisteme zarar veremeyeceğini ancak başarılı bir saldırının zarar verebileceğini belirtmektedir. Saldırı, bir varlığı imha etmek, ifşa etmek, değiştirmek, devre dışı bırakmak, yetkisiz erişim elde etmek için güvenlik

kontrollerini atlatarak güvenlik tehdidinin gerçekleştirilmesi olarak da bilinen bir eylemdir (ISO, 2018).

Değişen ve gelişen teknolojiler, bilgi sistemlerine yapılan saldırıları daha karmaşık ve anlaşılmaz hale getirmektedir. Maiwald (2004) çalışmasında, kurumlarda bilgi güvenliği hizmetlerinin etkin bir şekilde kullanılabilmesi için uygun güvenlik planlamasının gerekliliğini vurgulamakta ve bu planlamanın kurumların saldırılara karşı dirençli olmalarını sağlayabileceğini belirtmektedir. Bu planlama Tablo 3.1'de gösterilmektedir

Tablo 3.1: Bilgi güvenliği hizmetleri ve saldırıları

Saldırı	Güvenlik Hizmeti			
	Gizlilik	Bütünlük	Kullanılabilirlik	Hesap Verilebilirlik
Erişim	X			X
Değiştirme		X		X
Hizmet Engelleme			X	
Reddetme		X		X

Bilgi sistemleri, çeşitli tehdit türlerine maruz kalarak farklı zararlara yol açabilmektedir. Bu durum, kurumlarda önemli finansal kayıplara neden olabilmektedir. Bilgi güvenliği tehditleri, küçük kayıplardan tüm bilgi sistemlerinin çökmesine kadar değişen zararlara neden olabilmektedir. Tehditler etkileri türlerine önemli ölçüde değişiklik gösterir; bazıları veri gizliliğini veya bütünlüğünü etkilerken bazıları sistem kullanılabilirliğini etkileyebilmektedir. Tablo 3.1'de de belirtildiği üzere, farklı saldırı türlerinin bilgi sistemlerindeki güvenlik hizmetlerini farklı boyutları ile etkileyebilmektedir. Bu nedenle her saldırı türüne uygun güvenlik önlemlerini almasını gerekmektedir.

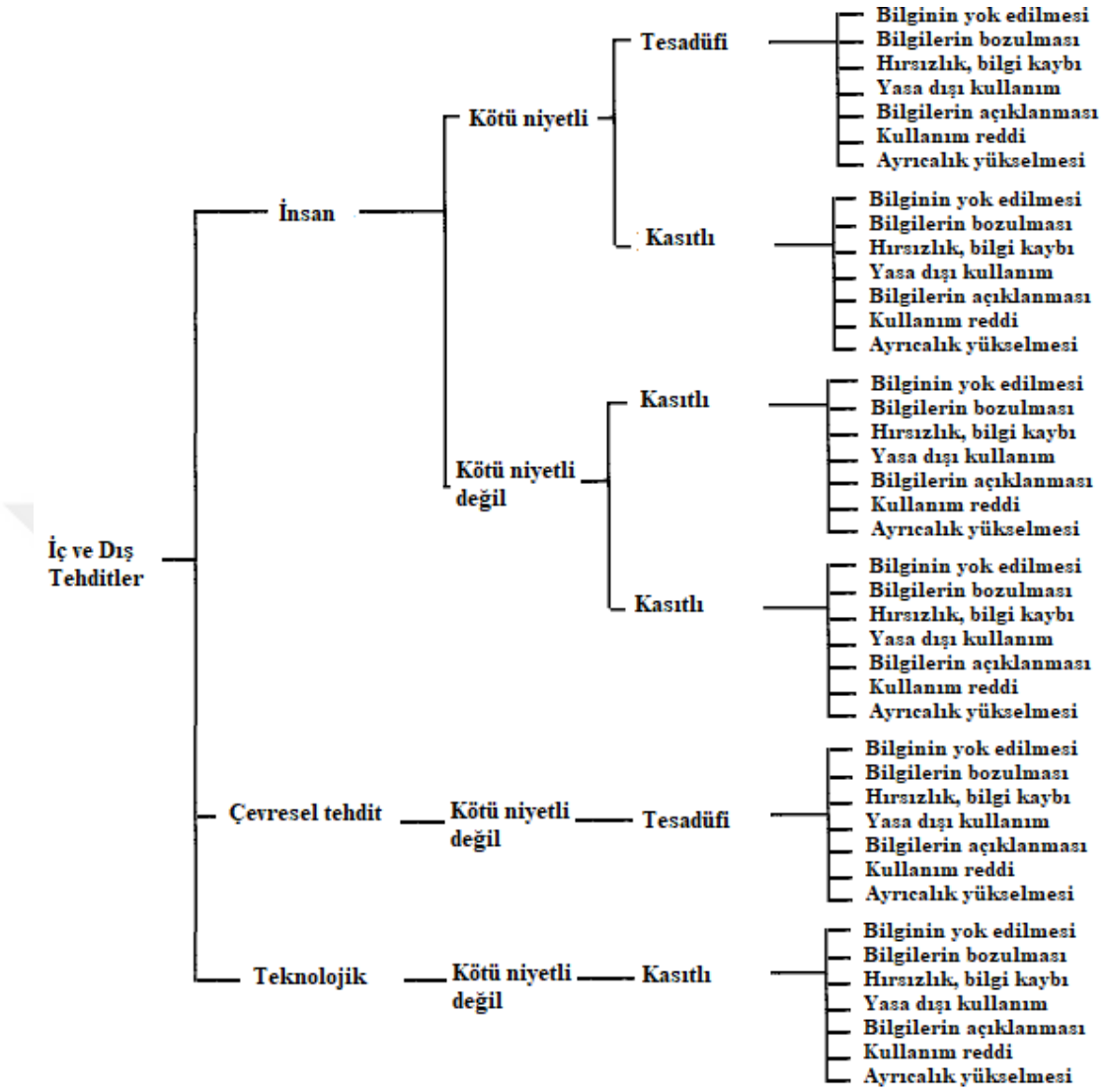
Kurumlar, uygun bilgi güvenliği yönetim stratejileriyle bilgi varlıklarına yönelik tehditleri belirlemek ve bu tehditlerle mücadele etmek için gerekli güvenlik mekanizmalarını planlamak ve uygulamak zorundadır. Bilgi güvenliği tehdit ve saldırılarına karşı iyi bir güvenlik anlayışın geliştirilmesi kurumun sürekliliği ve itibarı için önem arz etmektedir.

Kurumlar günümüzde bilgi teknolojilerine olan bağımlılıklarını artırmakta ve kullandıkları bilgi sistemlerini daha karmaşık hale getirmektedir. İş süreçleri, iletişim, veri depolama ve paylaşım gibi birçok önemli faaliyet, bilgi teknolojilerine bağlı bu karmaşık bilgi sistemleri üzerinden yürütülmektedir. Bu durum, güvenlik önlemleri zayıf olana kurumları bu sistemlere yönelik tehditlere karşı daha savunmasız hale getirmektedir. Bilgi teknolojileri alanındaki hızlı gelişmeler bilgi sistemlerine yönelik tehditleri sürekli değiştirmekte ve arttırmaktadır (Özgü, 2013).

Whitman (2003), yeni teknolojilerin piyasaya sürülmesi ile birlikte bilgi güvenliği tehditlerinin tanımlanmasında değişikliklerin olduğunu belirtmiştir. Bu değişikliklere bağlı olarak kurumların bilgi güvenliği anlayışında köklü değişimler yaşanacağını vurgulayarak gelecek ile ilgili bilgi güvenliği tereddütlerini vurgulamıştır.

Jouini, Rabai ve Aissa (2014)'nın birlikte çalıştığı bilişim sistemlerinde güvenlik tehditlerinin sınıflandırılması ile ilgili çalışmada, bilgi sistemi güvenlik riskleri sınıflandırmasının farklı kriterleri ele alınmakta ve birçok tehdit sınıflandırma modeli incelenmektedir. Bilgi sistemlerine yönelik gerçekleşen tehditlerin zamanla değiştiği vurgulanmakta ve bu nedenle tehdit etkisi yerine tehdit sınıfı etkisinin belirlenmesine olanak sağlayan bir güvenlik tehdidi sınıflandırma modeli önerisinde bulunulmaktadır. Şekil 3.1'de gösterilen bu modelde, tüm tehdit sınıflandırma ilkelerini destekleyen ve kuruluşların bilgi güvenliği stratejilerini uygulamalarına yardımcı olan bir sınıflandırma mimarisi sunulmaktadır.

Şekil 3.1: Çok boyutlu tehdit sınıflama modeli



Kaynak: (Jouini ve diğerleri, 2014)

Bilgi sistemlerine yönelik gerçekleşen tehditlerin sayısı, türleri ve gücü her geçen gün daha da artmaktadır. Bu nedenle tehditlerin çeşitlerine ilişkin güncel bir liste sunmakta mümkün olamamaktadır. Fakat tehdit kategorilerini inceleyen araştırmacıların sunduğu tehdit sınıflandırmaları bulunmaktadır (Wang, 2009; Swiderski ve Snyder, 2004; Bishop, 2002; Shirey, 1994).

Tablo 3.2: Tehdit sınıflandırmaları

Sınıflandırma	**Sınıflandırma İçeriği**
Security Architecture for Internet Protocols. A Guide for Protocol Designs and Standards (Shirey, 1994)	İfşa - Aldatma –Kesinti / Bozma -Gasp
Computer Security: Art and Science (Bishop, 2002)	Gözetleme - Değişiklik/Değiştirme -Reddetme - Alındı reddi - Geciktirme- Hizmet Reddi
Computer Network Security: Theory and Practice (Wang, 2009)	Gizlice dinleme- Kriptoanaliz - Şifre Kırma - Kimlik Sahtekârlığı - Arabellek Taşması İstismarları - İnkâr etme - Saldırı - Trafik Analizi - Hizmet Reddi - Kötü Amaçlı Yazılım
Threat Modeling (Swiderski ve Snyder, 2004)	Dolandırma / Kandırma - Tahrifat - İtibar - Bilgilerin Açıklanması - Hizmet Reddi - Ayrıcalığı Yükseltilmesi
The WASC Threat Classification v2.0 report (WASC, 2007)	Yetki - Müşteri Saldırıları - Kimlik Doğrulama - Komut Yürütme - Bilgilerin Açıklanması - Mantıksal Saldırılar
E-business Information Systems Security Design Paradigm and Model (Nachtigal, 2009)	Çalışmada, en çok tartışılan tehdit ve saldırı çeşitleri ile birlikte birçok saldırı türü, saldırı sınıfları, saldırganların hedefleri, saldırı teknikleri ve saldırıların olası sonuçları üzerinde durmaktadır.

Tablo 3.2'de de görüldüğü üzere bilgi güvenliği tehditlerini analiz etmek için birçok araştırmacı kendi sınıflama sistemlerini ortaya koymaktadır. Shirey (1994) çalışmasında, internet protokollerine yönelik olarak ifşa, aldatma, kesinti/bozma ve gasp gibi tehditlerin belirtildiği görülmektedir.

Bishop (2002), çalışmasında bilgisayar güvenliği alanında karşılaşılan saldırı ve zayıflıkları ifade etmektedir. Bilgi güvenliği tehditlerini; değişiklik/değiştirme, reddetme, alındı reddi, geciktirme, hizmet reddi kategorileri altında incelemektedir. Bilgisayar sistemlerini ve ağlarını bu güvenlik tehditlerinden korumanın önemi üzerinde duran araştırmacı, bilgisayar güvenliğinin kolay bir sanat ya da basit bir bilim olarak görülmemesi gerektiğini savunmaktadır.

Wang (2009), ağ güvenliği tehditlerine yönelik son gelişmeleri ve bu tehditlere karşı pratik çözümleri derinlemesine incelendiği çalışmasında, ağ güvenliğine genel bakış sunmakta ve tehdit sınıflandırmasını detaylandırmaktadır. Bu sınıflandırmada tehditlerin mevcut ve olası sonuçlarına da yer vermektedir.

Swiderski ve Snyder (2004), sistem güvenliğine yönelik riskleri belirlemek, değerlendirmek ve azaltmak için yapılandırılmış bir tehdit modelleme yaklaşımı üzerinde durmaktadır. Çalışmada ele alınan tehdit sınıflandırması, Shirey sınıflandırmasının bir uzantısı durumunda olup tipik bir sonuca dayalı yeterince kapsamlı sınıflandırmadır. Tehdit türlerinin farklı varlık türlerine uygulanabilirliğini ve farklı tehdit türlerine karşı karşılık gelen kontrol önlemlerini değerlendirmek için kullanılan bu sınıflandırma modeli, bilgi güvenliği yönetim çalışmalarına pratik bir biçimde entegre edilebilmektedir. Bu tehdit modellemesi, saldırganların bilgi sistemlerini nasıl değerlendirdiklerini göstererek saldırıların tahmin edilmesine yardımcı olmaktadır.

Web Uygulaması Güvenlik Konsorsiyumu tarafından sunulan tehdit sınıflandırması, bir web sitesinin güvenliğine yönelik tehditleri netleştirmek ve düzenlemek için oluşturulmuştur. Çalışma, bir web sitesinin verilerinin veya kullanıcılarının güvenliğinin ihlal edilmesine yol açabilecek saldırıları ve zayıflıkları özetlemektedir. Birçok kuruluş (IBM, HP, WhiteHat Güvenliği, Pozitif Teknolojiler (MaxPatrol) ve Hizmetler, Qualys, F5, HoneyApps, OWASP) tarafından kullanılan bu çalışma ile uygulama geliştiricileri, güvenlik uzmanları, yazılım satıcıları ve uyumluluk denetçileri web güvenliğiyle ilgili sorunlarda tutarlı bir dil ve tanımlara erişim becerisine sahip olabilmektedir. Bu sınıflandırmanın kapsamı, yalnızca potansiyel saldırı yöntemini değil, aynı zamanda ilgili sonuçları ve karşı önlemleri de içeren kapsamlı bir tehdit sınıflandırması sunmaktadır (WASC, 2007).

Nachtigal (2009), bilgi teknolojilerindeki gelişmelerle birlikte sürekli olarak yeni saldırı türlerinin geliştirildiğini ve bu nedenle belirli tehdit örnekleri listelemeye çalışmak yerine genel saldırı kategorilerinin belirlenmesi gerektiğini savunmaktadır. Saldırıların genellikle tek bir tehdit kategorisiyle ilişkili olmadığını, birden fazla tehdit kategorisine bağlı olarak oluşabileceğini belirtmektedir. Çalışmasında en çok tartışılan tehdit ve saldırı çeşitleri ile birlikte birçok saldırı türü ve sınıfları, saldırganların hedefleri, saldırı teknikleri ve saldırıların olası sonuçları başlıkları üzerinde durmaktadır. Bu başlıklar altında incelediği bilgi güvenliği tehdit ve saldırılarına ilişkin bilgileri şu biçimde sıralamaktadır:

Saldırı sınıfları;

- Kötü amaçlı yazılım saldırıları: Virüsler, solucanlar, truva atları, casus yazılımlar gibi birçok kasıtlı kötü amaçlı yazılım saldırılarıdır.
- Hizmet reddi (DoS veya DDoS) saldırıları: Yetkisiz taraflardan kaynaklanan faaliyetlerin doğrudan bir sonucu olarak meşru erişimin engellendiği veya önlendiği bir saldırı biçimidir.
- Sosyal mühendislik saldırıları: Meşru kullanıcıların güvenlik politikasını çiğnemesini sağlamak için sahtekârlık, dolandırıcılık veya diğer sosyal ve psikolojik bir takım olumsuz eylemlerin kullanılmasıdır.
- Dâhili saldırılar: Genellikle normalden daha yüksek erişime sahip olan bir çalışanın veya başka bir güvenilir kişinin olumsuz eylemlerin kapsar.
- Kimliğe bürünme (sahte kimlik) saldırıları: Yetkili kullanıcı kılığında bir sisteme erişim elde etme girişimidir.
- Bilgisayar korsanlığı (hacker) saldırıları: Yetenekli bilişim uzmanları veya vasıfsız kişiler tarafından güvenlik sistemlerini kırılması saldırılarıdır.
- Uygulama hatalarına bağlı saldırılar: Geliştirilmekte olan bir uygulamanın hatalarından yararlanılması sonucunda oluşan güvenlik politikası gereksinimleriyle uyumlu olmayan bir saldırıdır.

Saldırıların hedefleri;

- Taciz: Bir rakibe doğrudan, şahsen veya e-posta gibi bir araç ile istenmeyen tehdit edici veya yaralayıcı mesajlar gönderilmesi amacı gütmektedir.
- Siber terörizm: Terörist gruplar ve bireyler tarafından ulaşmak istedikleri düşünce ve eylemleri gerçekleştirmek hedefi ile yapılan saldırılardır.
- Siyasi veya endüstriyel ağ casusluğu: Ağ destekli casusluk faaliyetlerini hedeflemektedir.

Saldırı teknikleri;

- Arabellek taşması: Aşırı girdinin kendisine ayrılan bellek alanını aştığı ve potansiyel olarak programın isteğe bağlı kod yürütmesine veya işlemsel denetimi isteğe bağlı bir bellek konumuna geçirmesine neden olan yaygın bir programlama saldırı tekniğidir.

- SQL enjeksiyonu: SQL deyimlerinde kullanılan parametreleri değiştiren bir saldırı tekniğidir.
- Zararlı e-posta gönderme: İstenmeyen, alakasız veya uygunsuz mesajların, özellikle ticari reklamların, ayrım gözetmeksizin toplu miktarlarda gönderilmesi yolu ile yapılan bir saldırı türüdür.
- Paket koklama: Bir ağ içindeki bir saldırgan tarafından ağ hakkında bilgi toplamak için kullanılan trafik izleme metodudur.
- Yanıltma / Maskeleme: Yetkili bir kullanıcı gibi davranarak bilgi sistemine erişim sağlama girişimidir.
- Tanımlama bilgilerinin kötüye kullanılması: Çerezlerde yer alan bilgilerin meşru olmayan amaçlarla kullanılmasıdır.
- Yönlendirme tablosu zehirlenmesi: yönlendirme protokolü tarafından iletilen yönlendirme bilgilerinin kötü niyetli şekilde değiştirilerek yönlendirme tablolarının yanlış veya hatalı bilgilerle güncellenmesi sürecidir.
- Kimlik avı: Spam veya diğer genel gönderiler yoluyla çok sayıda kişiye sahtekârlık amaçlı bir mesajın gönderilerek kişisel ve finansal bilgilerinin ele geçirilmek istenmesidir.
- SMiShing veya SMS saldırıları: SMS yoluyla gerçekleştirilen dolandırıcılık ve sahtekârlık girişimlerini ifade eder. Telefon kullanıcılarına gönderilen yanıltıcı SMS mesajları aracılığıyla kişisel bilgileri çalmayı, zararlı yazılımların indirilmesini sağlamayı veya başka kötü niyetli amaçları gerçekleştirmeyi amaçlar.
- Vishing veya sesli dolandırıcılık: Telefon aracılığıyla gerçekleştirilen dolandırıcılık ve sahtekârlık girişimlerini ifade eder. Sesli iletişim kanallarını kullanarak kullanıcıları manipüle etmeyi ve kişisel bilgilerini çalmayı hedefler.
- DNS (Alan Adı Sistemi) korsanlığı: İnternetin büyük bir bölümünü etkileme potansiyeli olan DNS altyapısına yapılan bir saldırıdır.

Saldırıların olası sonuçları;

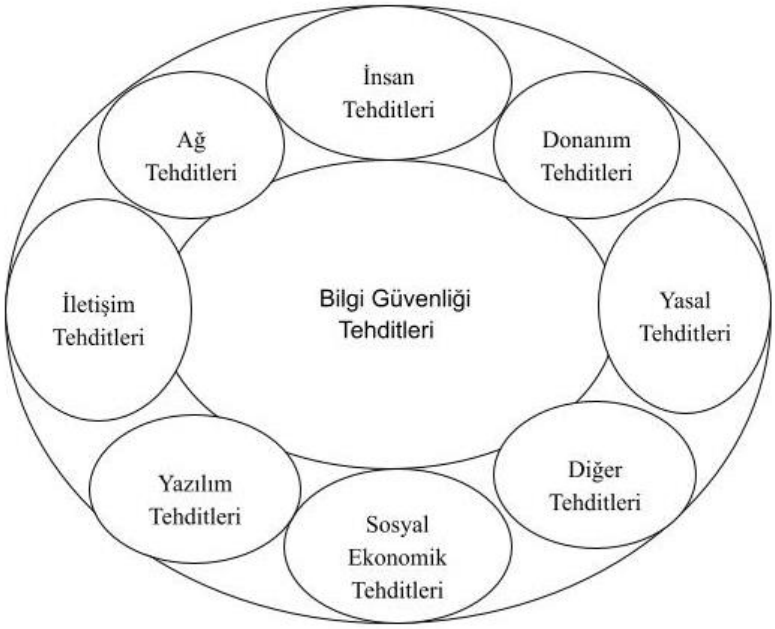
- Yazılım bozulması ve değiştirilmesi,
- Donanım arızası,
- Veri bozulması, değiştirilmesi, teşhir edilmesi ve hırsızlığı,

- Kimlik hırsızı,
- Fikri mülkiyet hırsızlığı,
- Finansal kayıp,
- İtibar zedelenmesi,
- Bilgi sistemlerinin ve alt yapının zarar görmesi.

3.3. Bilgi Güvenliği Tehdit Türleri

Bilgi güvenliği tehditleri birçok başlık altında sınıflandırılmaktadır. Belli başlı tehdit türleri Şekil 3.2'de gösterilmektedir.

Şekil 3.2: Bilgi güvenliği tehditleri



Kaynak: (Nayak ve Rao, 2014)

3.3.1. Donanım Güvenliği Tehditleri

Donanım güvenliği, başlarda fiziksel tehditlere karşı gelişen bir kavramsal çerçeveye sahipken; günümüzde bu çerçeve teknolojik gelişmelere bağlı olarak daha da genişlemiştir. Özellikle bilgi işlem cihazlarının ağlar ile birbirlerine olan bağlantılarının artması, donanım güvenliği üzerinde yapılan çalışmaları hızlandırmıştır. Son yirmi yılda bilgi işlem cihazlarının güvenlikleri ağlar üzerinden yapılan saldırılar ile kırılmakta ve bu durum donanım güvenliği zafiyetini arttırmaktadır. Saldırganlar, donanım güvenliği zafiyetlerinden yararlanarak

yaptıkları saldırılar ile bilgi sistemlerinin kontrolünü ele geçirmekte ve bilgilerin gizliliğine, bütünlüğüne ve kullanılabilirliğine zararlar vermektedirler. Güvenlik uzmanları, bu donanım güvenlik zafiyetlerini tespit etmek ve bilinen donanım saldırılarına karşı donanım tasarımını güçlendirmek için koruma teknikleri geliştirmede ciddi derecede çaba sarf edilmektedirler (Hu ve diğerleri, 2020). Donanım güvenliğine karşı gelişen tehditlere ve olası sonuçları olan saldırılara karşı sürekli yeni önlemler ve güvenlik tasarımları geliştirilmektedir. Bu döngü sürekli olarak kendini güncellenmekte ve yenilemektedir.

Bilgisayar ve internet teknolojisinden önce bilgi güvenliği, hassas gizli bilgilerin depolaması için korunan kilitli bir dolap veya oda gibi fiziksel alanlar olarak ele alınmaktadır. Fakat bilgisayar ve internetin yaygın kullanımı bilgi güvenliği uygulamalarını ve kontrollerini büyük değişikliğe uğratmıştır. Bilgisayar ve ağ iletişiminin gelişmesi ve kullanımının yaygınlaşması, bu sistemler üzerinde depolanan verilerin korunması için otomatik güvenlik araçlarının geliştirilmesini ve kullanılmasını zorunlu hale getirmiştir. Bilgi güvenliğine duyulan bu ihtiyaç, bilgi sistemlerinin ve verilerin kamuya açık telefon ve veri ağları üzerinden erişildiği ve iletildiği internetin ortaya çıkmasıyla daha da artmıştır (Karaarslan ve diğerleri, 2003).

Ismail (2012), donanımların güvenliği üzerinde etkisi olan tehditleri ve saldırıları şu başlıklar altında özetlemektedir:

- Deprem, yangın, sel ve yıldırım gibi doğal afetler,
- Sıcaklık veya iklimdeki değişimlere bağlı tehditler,
- Hırsızlık ve vandalizm gibi saldırılar,
- Kötü niyetli izinsiz giriş ve imha saldırıları,
- Yönlendiriciler veya güvenlik duvarlarından kaynaklanan tehditler,
- Donanımın imalatından kaynaklanan tehditler,
- İklimlendirme cihazlarından kaynaklanan tehditler,
- Telekomünikasyon veya enerji gibi temel altyapı hizmetlerin durmasından kaynaklanan tehditler,
- Elektromanyetik saldırılar,
- İletişim ekipmanı ve cihazlarının arızalanmasına bağlı hatalar,
- Yetkisiz donanım kurulumu ve bakım hataları,

- Fiziksel sabotaj veya bilgi işlem ekipmanlarının kasıtlı imhası.

3.3.2. Yazılım Güvenliği Tehditleri

Yazılım geliştirme, bilgi güvenliği açısında özel dikkat gerektirmektedir. Uygulamalar, kullanıcıların ve müşterilerin verilerine erişmek için saldırganlar tarafından en yaygın kullanılan güvenlik alanını oluşturmaktadır. Bu yönde gerçekleşebilecek saldırılar hem veri hem de sistem süreçlerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyebilmektedir. Bu tür güvenlik tehditlerini ve saldırılarını önlemek için iyi bir yazılım güvenliği politikasının geliştirilmesi önemlidir. Bir kurumda benimsenen yazılım güvenliği geliştirme modeli veya politikası ne olursa olsun, yazılım veya uygulamaların aşağıdaki güvenlik kontrollerine ve hedeflerine sahip olması gerekmektedir (Whitman ve Mattord, 2018):

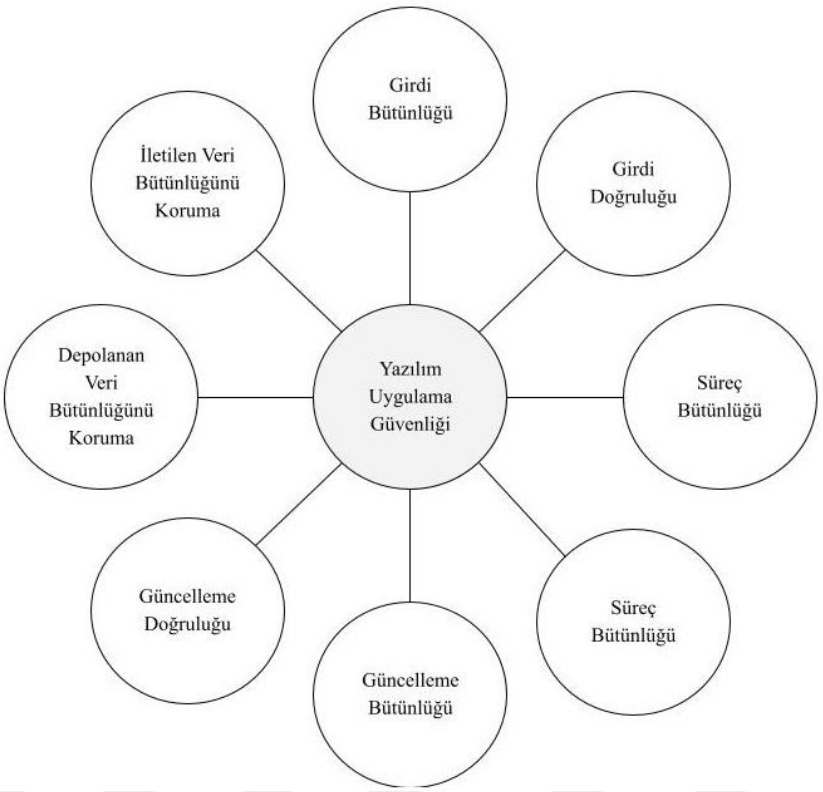
- Kullanıcı kimlik doğrulamasını denetlemelidir.
- Kullanıcı yetkilendirmesini (ayrıcalık düzeyini) denetlemelidir.
- Sistem arızası durumunda veri tabanı bütünlüğünü kurtarma prosedürlerine sahip olmalıdır.
- Uygulama, gerçekleşen hataları ve özel durumları sürekli olarak işlenmelidir. İşlenmeyen bir hata veya özel durum uygulamanın güvenliğini azaltabilir. Standart yanıtlarla tüm hataları ve istisnaları açıklayıcı yaklaşımlar sunmalıdır.
- Kullanıcılara tutarlı bir hata yanıtı veren anlaşılır yönergelere sahip olmalıdır.
- Uygulamaya başka bir kaynaktan dâhil edilen tüm girdiler, güvenirliği doğrulamadan asla kabul etmemelidir. Verilerin doğrulaması başarısız olursa bu verilerin uygulamaya dâhil edilmesi engellemelidir. İstemcideki ve sunucudaki verilerin doğrulanması önemlidir. Saldırganlar, genellikle verilerin istemciden sunucuya aktarılması sırasında değiştirebilir. Bu nedenle verilerin sunucuda tekrar doğrulanması, verilerin geçerli ve güvenli olduğundan emin olunması gerekmektedir.
- Güvenli yapılandırmanın temel dayanakları tanımlanmalıdır. Uygulamayı son kullanıcılarının kullanımına bırakmadan önce güvenli bir başlangıç noktasını tanımlayan belgelenmiş bir yapılandırma ayarları kümesi sağlanmalıdır.

- Uygulamayı güvende tutacak yapılandırma ayarlarını değiştirme konusunda rehberlik hizmeti sunulmalıdır. Ayrıca uygulamanın güvenliğini arttırıcı harici denetimlerin eklenmesi konusunda rehberlik sağlanmalıdır.
- Uygulamanın yeni gelişmelere karşı güvenlik düzeltme yamaları ile desteklenir olmasını temin etmelidir. Ayrıca uygulama kullanıcılarına sık sık güvenlik yamaları sağlanmalı, bu yamaları uygulama işlemlerini yönetmek için uygun bir yöntem sunulmalıdır.

Yazılım uygulamasının gerçekleştirdiği işlev önemlidir ve kullanıcıların beklentilerini karşılamalıdır. Bir yazılımın gereksinimlere uygun çalışması ve istenen görevleri yerine getirmesi beklenir. Bununla birlikte, yazılımın gereksinimlerin ötesinde fazladan özelliklere sahip olması, kullanıcılar için karmaşıklık veya gereksiz karmaşıklık yaratabilir. Bu nedenle, yazılım uygulaması, gereksinimleri tam ve etkili bir şekilde yerine getirmesiyle tanınmalıdır. Nayak ve Rao (2014), yazılım uygulamalarının sekiz güvenlik unsuruna sahip olması gerektiğini vurgulamaktadır (Şekil 3.3). Ayrıca yazılım uygulamaları üzerinde etkisi olabilecek tehdit ve saldırıları şu biçimde özetlemektedir:

- Sömürülen ve hatalara yol açan yazılım kusurları,
- Virüsler, solucanlar, truva atları gibi kötü amaçlı yazılımlar,
- Bot ve botnet gibi yazılım ajanları,
- Geçersiz kılınan yazılım girdileri,
- Kimlik doğrulama saldırıları,
- Yanlış yazılım yapılandırmalarının kullanılması,
- Oturum yönetimi ile ilgili sorunlar,
- Uygulamalar tarafından işlenen uygunsuz ve istisnai hatalar,
- Arabellek taşması,
- Uygulamalar tarafından yanlış işlenen şifreleme,
- Parametre manipülasyonları,
- İşletim sistemi ile ilgili sorunlar ve güvenlik kusurları.

Şekil 3.3: Yazılım uygulama güvenliğinin unsurları



Kaynak: (Nayak ve Rao, 2014)

Whitman ve Mattord (2018) ise yazılım saldırılarını; kötü amaçlı yazılımlar (virüsler, solucanlar, Truva atları, polimorfik saldırılar vb.), arka kapı saldırıları, hizmet reddi (DOS) ve dağıtılmış hizmet reddi (DDOS) saldırıları, e-mail saldırıları, iletişim durdurma saldırıları, teknik yazılım arızaları ve hataları olarak sınıflandırılmaktadır.

Bu saldırı türleri arasında yer alan özellikle kötü amaçlı yazılımlar (malware) çokça karşılaşılan yazılım saldırısıdır. İstenmeyen eylemleri gerçekleştirmek için özel tasarlanmış bilgisayar yazılımları ile yapılmaktadır. Bu tür yazılım tehditlerine kötü amaçlı kod (malicious code) olarak da adlandırılmaktadır. Yönlendirme saldırıları ve hizmet reddi saldırıları gibi yazılım kullanan diğer saldırılar da bu tür yazılım tehditleri altında yer almaktadır. Bu yazılım bileşenleri ve programları hedeflenen sistemlere zarar vermek, yok etmek veya hizmeti reddetmek için tasarlanmaktadır. Bu tür saldırılar, bilgi sistemlerindeki bilgileri yok etmek, zarar vermek veya çalmak amacıyla virüsleri, solucanları, Truva atlarını, polimorfik tehditleri ve etkin web komut dosyalarını kullanmaktadır Özellikle, sıfır gün saldırısı, kötü amaçlı yazılım

saldırıları arasında önemli bir saldırı türü olarak bilinmektedir. Sıfır gün saldırısı, bilgisayar korsanlarının sistemlere saldırmak için kullanabileceği, yakın zamanda keşfedilen güvenlik açıklarını tanımlayan geniş bir terimdir. Bilgisayar korsanları, geliştiricilerin sorunu çözme şansı bulmadan önce bu açıktan yararlanarak yaptıkları saldırı, sıfır gün saldırısı olarak gerçekleşmektedir (Bilge ve Dumitras, 2013; Whitman ve Mattord, 2018).

3.3.3. Ağ Güvenlik Açıkları ve Tehditleri

Bilgi ve iletişim teknolojilerindeki gelişmeler, ağların büyümesine ve ilerlemesine katkıda bulunmuştur. Kablosuz ağ teknolojisi gibi yenilikler, kullanıcıların mobil cihazlarla bağlantı kurma esnekliğini artırmış ve iletişim imkânlarını genişletmiştir. Ancak, bu gelişmeler aynı zamanda güvenlik açıklarını da beraberinde getirmiştir. Ağların büyümesi ve karmaşıklığı, bilgisayarların ve diğer teknolojik cihazların kontrolünü zorlaştırmıştır. Ağdaki çok sayıda cihazın yönetimi, izlenmesi ve güvenlik önlemlerinin uygulanması daha karmaşık hale gelmiştir. Bu durum, ağın güvenliği açısından önemli bir zorluk oluşturmaktadır (Smith, 2021).

Güvenlik, ağ yapısında daha da önemli hale gelmiştir. Artan sayıda cihazın ağa bağlanması, hassas verilerin iletilmesi ve depolanması, güvenlik sürecinin öncelikli bir konu haline gelmesini sağlamıştır. Bilgisayar korsanları, kötü amaçlı yazılımlar ve diğer tehditler, ağların güvenliğini tehlikeye atabilmektedir. Bu nedenle kurumlar ve bireyler, ağlarını korumak için güvenlik önlemlerini geliştirmelidir. Bu önlemler arasında güvenlik duvarları, ağ güvenlik protokolleri, güçlü şifreleme yöntemleri, güncel yazılım ve donanım güncellemeleri, erişim kontrolü ve yetkilendirme gibi önlemler yer alabilmektedir. Ayrıca, personelin güvenlik eğitimine tabi tutulması ve güvenlik politikalarının oluşturulması da önemlidir (Çınar ve Yıldırım, 2020).

Ağ güvenliği, ağların sürdürülebilirliği, veri gizliliği ve bütünlüğü, kullanılabilirlik ve iş sürekliliği açısından kritik bir unsurdur. Bu nedenle, ağ güvenliği ile ilgili risklerin belirlenmesi, analiz edilmesi ve uygun güvenlik önlemlerinin alınması, ağların güvenliğini sağlamak için önemli adımlar arasında yer almaktadır.

Ağlardaki çok sayıda bilgisayar, ağ aygıtı, protokol ve uygulama, bilgi güvenliği için ciddi bir tehdit oluşturabilir. Herhangi bir zayıf nokta veya savunmasızlık, kötü niyetli kişilerin veya hackerların ağa sızmasına ve bilgileri çalmalarına veya sistemi

zarar vermelerine olanak sağlayabilir. Bu nedenle, ağların güvenliği için proaktif bir yaklaşım benimsenmelidir. Ağ yöneticileri, güvenlik açıklarını düzeltmek, düzenli güvenlik taramaları yapmak, güvenlik duvarları, güncel yazılım ve donanım kullanmak, erişim kontrolleri ve kimlik doğrulama mekanizmaları uygulamak gibi önlemler almalıdır. Ayrıca, kullanıcıların güvenlik bilincini artırmak ve güvenlik politikalarına uygun davranmalarını sağlamak da önemlidir. Eğitim ve farkındalık programları, kullanıcıların güvenlik tehditlerini tanımalarına ve güvenli davranışlar sergilemelerine yardımcı olabilmektedir.

Sonuç olarak, ağ güvenliği için sürekli bir çaba gerekmektedir. Bilgisayar korsanlarının ve kötü niyetli kullanıcıların sürekli olarak yeni saldırı yöntemleri geliştirdiği göz önünde bulundurulmalı ve güvenlik önlemleri buna göre güncellenmelidir.

Ağ tehditleri, ağda var olan herhangi bir güvenlik açığından yararlanılarak meydana gelebilecek bir olaydır. Nayak ve Rao (2014), ağ güvenliği ile ilgili güvenlik olaylarını güvenlik açığı, tehdit ve saldırı grupları altında incelemektedir:

Ağ güvenlik açıkları: Bilgisayar sistemleri, ağlar veya yazılımların savunmasız veya eksik yönleri, bilgi güvenliği açısından zayıf noktalar olarak adlandırılır. Bu zayıf noktalar, kötü niyetli kişilerin veya saldırganların ağlar üzerinden bilgi sistemlerine izinsiz erişim sağlaması, hassas bilgilere ulaşması veya sistemde istenmeyen faaliyetlerde bulunması için bir fırsat sunabilmektedir. Güvenlik açıkları genellikle hatalı kodlama, yanlış yapılandırma, güncelleme eksikliği veya bilinmeyen bir güvenlik zafiyeti sonucunda ortaya çıkabilmektedir. Bu açıklar, kötü amaçlı yazılımların, virüslerin, solucanların veya diğer saldırı vektörlerinin sisteme sızması veya saldırı gerçekleştirmesi için kullanılabilmektedir.

Güvenlik açıklarının önlenmesi veya azaltılması için çeşitli yöntemler vardır. Bunlar, düzenli güvenlik güncellemeleri yapmak, güvenlik açıklarını tespit etmek ve düzeltmek için güvenlik taramaları yapmak, güçlü parolalar ve yetkilendirme politikaları kullanmak, güvenlik duvarları ve antivirüs yazılımları gibi koruyucu önlemleri uygulamaktır. Bununla birlikte, güvenlik açıklarının tamamen ortadan kaldırılması her zaman mümkün olmayabilir. Bu nedenle, güvenlik açıklarının tespit edilmesi ve hızla düzeltilmesi önemlidir. Ayrıca, sistemlerin sürekli izlenmesi ve

güvenlik politikalarının güncellenmesi gerekmektedir. Güvenlik açıklarına karşı bilinçli olmak, düzenli güncellemeler yapmak ve güvenlik en iyi uygulamalarını takip etmek, güvenlik açıklarının etkilerini minimize etmede önemli bir adımdır.

Ağlarda güvenlik açıklıklarının oluşmasına neden olan zayıflıklar bulunmaktadır. Bunlar; güvenlik politikası zayıflığı, teknoloji zayıflığı, yapılandırma zayıflığı olmak üzere üç grupta toplanmaktadır.

Bazı yaygın güvenlik politikası zayıflıkları Tablo 3.3'te özetlemektedir.

Tablo 3.3: Yaygın güvenlik politikası zayıflıkları

Zayıflıklar	Açıklama
Yazılı bir güvenlik politikasının olmaması	Kuruluş genelinde bilgi güvenlik tehditlerine yol açabilir. Bilgisizlik nedeniyle bilgi güvenliğini tehlikeye atabilecek hatalar oluşabilir. Kötü niyetli kasıtlı eylemler, bilgisizlik eylemleri olarak gizlenebilir.
Donanım ve yazılım yüklemeleri veya güncellemeleri için bir güvenlik politikasının olmaması	Bilgi hırsızlığına yol açabilecek yetkisiz kurulumlara, saldırıya açık onaylanmamış değişikliklere ve kötü amaçlı yazılım bulaşmalarına yol açabilir. Yetkisiz donanım ve yazılım yüklemeleri bilgilerde yetkisiz değişikliklere, ağ çökmelerine ve kişisel kazanç için ağın kasıtlı olarak kötüye kullanılmasına neden olabilir.
Afetle mücadele ve iş sürekliliği planlarının olmaması	Afet sırasında karışıklığa neden olabilir. Afetlere karşı etkili ve verimli bir planın olmaması itibar kaybına, iş kaybına veya müşteri kaybına neden olabilir.
Acil müdahale ekibinin olmaması	Güvenlik olaylarını veya krizlerini yönetememek, bazen sorunu çözmek yerine durumu daha da karmaşık hale getirebilir.
Resmi varlıkların kullanımına ilişkin politikanın olmaması	Resmi varlıkların kötüye kullanılmasına, kötü amaçlı yazılımların bulaşmasına, itibar ve verimlilik kaybına neden olabilir.
Uzaktan veya evden çalışma ile ilgili politikanı olmaması	Ağa bağlanmak için kişisel makinelerin kullanılması, veri hırsızlığına veya ofis ağına kötü amaçlı yazılımların bulaşmasına neden olabilir.

Kaynak: (Nayak ve Rao, 2014)

Ağlardaki tüm veri trafiği kötü amaçlı değildir. Sadece trafiğe tanımlanan güvenlik ilkeleri tarafından izin verilir veya reddedilir. Saldırganlar, teknoloji politikasının zayıflığından yararlanarak güvenlik ihlallerine yol açabilecek politika kurallarını atlayabilmektedir. Tablo 3.4'te protokol zayıflıkları, işletim sistemi zayıflıkları ve ağ ekipmanı zayıflıklarını içeren teknoloji zayıflıklarına ilişkin bilgiler açıklanmaktadır.

Tablo 3.4: Ağları etkileyen teknoloji zayıflıkları

Zayıflıklar	**Açıklama**
TCP/IP Uygulamaları ve protokolleri	HTTP, FTP, SNMP, SMTP, TCP, IP ve DNS standartlara ve teknik özelliklere göre uygulanır.
İşletim sistemi	Microsoft Windows, Apple Macintosh, IBM OS/2, UNIX ve diğer işletim sistemlerinde çeşitli güvenlik sorunları olabilmekte ve güvenlik zafiyetine neden olabilmektedir.
Ağ cihazı	Bir veya daha fazla protokol katmanına katılan ağın ayrı bir bileşenidir. Varsayılan parolaların değiştirilmemesi veya güçlü parola gereksiniminin olmaması, kimlik doğrulama zayıflıkları, güvenlik duvarı açıkları ve kullanıcı zayıflıkları gibi parola zayıflıkları görülür.

Kaynak: (Nayak ve Rao, 2014)

Ağ yöneticilerinin, güvenlik tehditlerini önlemek için ağları ve ağ cihazlarını yapılandırmada yeterli becerilere sahip olması gerekmektedir. Tablo 3.5'te olası yapılandırma zayıflıklarından bazılarını açıklamaktadır.

Tablo 3.5: Ağları etkileyen yapılandırma zayıflıkları

Zayıflıklar	**Açıklamalar**
Kullanıcı hesapları	Cihazlarda saklanan kullanıcı hesaplarının güvenliği sağlanmalıdır. Kullanıcı adlarını ve parolaları açığa çıkarmak bir güvenlik tehdidi olabilir.
Şifreler	Parola politikası kullanıcı düzeyinde uygulanmalıdır. Sunucular, yönlendiriciler, veritabanları gibi büyük cihazların şifreleri, kuruluşun BT politikası tarafından belirlenen şifre politikasına uygun olarak belirlenmelidir. Varsayılan şifrelerin devam etmesine izin verilmemelidir. Şifre gizliliği korunmalıdır. Bu parolalar, bir yönetici kuruluştan ayrıldığında veya periyodik olarak değiştirilmelidir.
TCP bağlantı noktalarının ve internet hizmetlerinin yapılandırılması	Hangi uygulama hizmetlerine hangi amaçlarla izin verileceğini tanımlayan bir politikaya sahip olunmalıdır. Bu konuda netlik olmaması, Java Script ve VB Script gibi saldırıya açık olanlardan bazılarının etkinleştirilmesi veya riskleri anlamadan uzak servislerin etkinleştirilmesi yaygın bir sorundur.
Varsayılan ayarları	Ağ yöneticileri cihazların varsayılan politikasını değiştirmezlerse, varsayılan parolaların herkes tarafından bilinmesi gibi ciddi güvenlik tehditlerine neden olabilir.
Güvenlik ve ağ cihazlarının yanlış yapılandırılması	Güvenlik duvarı ve diğer ağ cihazlarının yanlış yapılandırılması ciddi güvenlik sorunlarına neden olabilir. Örneğin, erişim listelerinin yanlış yapılandırılması, yönlendirme protokolünde ciddi güvenlik tehditlerine neden olabilir.

Kaynak: (Nayak ve Rao, 2014)

Ağ tehditleri: Veri hırsızlığı veya verilerin yetkisiz değiştirilmesi gibi güvenlik açıklarından yararlanma ve varlıklara saldırı nedeniyle ters gidebilecek olayları

kapsamaktadır. İç tehditler ve dış tehditler, olmak üzere iki ana tehdit grubu altında incelenmektedir.

İç tehditler, ağ ve ağ kaynaklarına uygun erişimi olan, ağ altyapısını iyi bilen, güvenlik uygulamalarını bilen ve anlayan kurum içindeki kişiler tarafından oluşan tehditlerdir. Bu kişiler kuruluş içerisindeki bilgilere zaten hâkim olduğu için kimliklerini gizleyerek bilgi sistemlerine saldırıların düzenlenmesine imkân tanımaktadırlar. Bilgi güvenliği olaylarının çoğunluğu kuruluş içindeki erişim ve bilgilerin kötüye kullanılmasından kaynaklandığı bilinmektedir.

Dış tehditler, kuruluş dışından gelen tehditlerdir. Bu tür tehdit sınıfında bulunan kişiler, ağ kaynaklarına yetkili erişime sahip olmamalarına rağmen kaynaklara zarar verme veya kâr amacıyla ağ ve ağ sistemlerine yetkisiz erişim sağlayarak saldırılar düzenlemektedir.

Saldırı: Ağın zarar görmesine, güvenliğini engellemeye veya ihlal etmeye yönelik yetkisiz bir eylemdir. Saldırganlar, saldırıya açık olan sunucular veya masaüstü bilgisayarlar gibi uç nokta cihazlar üzerinden ağ ve ağ kaynaklarına zarar vermek için saldırı eyleminde bulunarak gizli ve değerli bilgileri ele geçirmektedir.

Saldırganlar, güvenlik politikaları tarafından belirlenen ağ kurallarını kötüye kullanmaktadır. Ağ saldırıları keşif, hizmet reddi / dağıtılmış hizmet reddi ve diğer ağ saldırıları olmak üzere üç ana kategoride incelenmektedir.

Saldırganın bir saldırıyı etkili bir şekilde başlatabilmesi için ağda kullanılan donanım, yazılım ve topolojisi hakkında bilgi sahibi olması gerekir. Bu bilgi keşif adı verilen ağ tarama işlemi ile gerçekleştirilmektedir. Keşif, kendi başına bir saldırı değildir; ağ veya ağ kaynaklarının zayıflıklarının saldırgana bildirilmesine izin vererek ciddi bir güvenlik tehdidine neden olabilir. Daha çok bir bilgi toplama görevi olan keşif saldırıları, ağ üzerinde hiçbir etkiye sahip olmadığı için önemli bir süre tespit edilememektedir.

Hizmet reddi saldırısının amacı, bellek kullanımını zorlayan yönlendiriciler ve anahtarlar ile sunucunun kapasitesini aşan, sunucuyu bunaltan veya çökerten büyük miktarda ağ trafiği oluşturularak ağ kaynaklarını kullanıcılar için erişilemez hale getirmektedir. Bu tür saldırılar bazı durumlarda belirli bir cihazı hedeflemekte ve sistemin askıda kalmasına neden olabilmektedir.

Keşif ve dağıtılmış hizmet reddi saldırı kategorilerinin dışında ağ güvenliğine ciddi zararlar verebilecek başka saldırılar da bulunmaktadır. Yaygın olanlar kullanılan bu tehditlerden bazıları, kimlik sahtekârlığı saldırıları, adres çözümleme protokolü saldırıları, HTTP ve SSH tüneli oluşturma ve oturum kaçırma gibi saldırı türleridir.

Ağ saldırılarına karşı alınacak önlemlerden bir kısmı şu şekilde sıralanmaktadır (Solmaz, 2022, TÜBİTAK, 2013; Muharremoğlu, 2013; Tuncay (2013); Yüksel, 2007) :

- Tüm varsayılan parolalar güçlü parolalarla değiştirilmelidir.
- Güvenli oturum kimliği kullanılmalıdır.
- Oturum zaman aşımı, uygulamada karşılaşabilecek risklere göre ayarlanmalıdır.
- Tüm ağ ekipmanları uygun konfigürasyon ve yamalar ile sağlamlaştırılmalıdır.
- Oturum kaçırma gibi saldırıları önlemek için sağlam savunma uygulamaları kullanılmalıdır.
- Karmaşık oturum kimliği ve parolaları oluşturulmalıdır.
- Dijital sertifika veya VPN, TLS ile SSL gibi şifreli anlaşmalar kullanılmalıdır.
- Çerezlerde kayıtlı kullanıcı adı ve parola gibi küçük veri parçalarını içeren kritik bilgiler saklanmamalıdır.
- Yardımcı programlar ve araçlar dâhil olmak üzere kullanılan tüm yazılımların yamalandığından veya güncellendiğinden emin olunmalıdır.
- Anlaşılması kolay ve net güvenlik politikaları belirlenmelidir.
- Çalışanlar arasında hangi durumların yanlış gidebileceği ve onlardan ne beklendiği konusunda farkındalık oluşturulmalıdır.
- Tüm sistemler için aynı kullanıcı adı ve parolalar olmamalı, farklı olanlar kullanılmalıdır.
- Kullanım sona erdikten sonra oturum kapatılmalıdır.
- Hassas işlem oturumlarından sonra çerezlerin, geçmişin ve çevrimdışı içeriğin kaldırıldığından emin olunmalıdır.
- Şüpheli e-postalardaki linkler tıklanmamalıdır.

3.3.4. Veri Güvenliği Tehditleri

Veri güvenliği; şirketler, kuruluşlar, devlet yetkilileri ve hatta kişisel kullanıcılar için büyük bir öneme sahiptir. Verilerin yetkisiz kişiler tarafından erişilmesi, değiştirilmesi veya kötüye kullanılması, ciddi sonuçlara yol açabilmektedir. Veri güvenliği tehditleri, verilerin güvenliğini tehlikeye atan çeşitli durumları ve saldırı yöntemlerini içermektedir. Bu tehditler, verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyebilir.

ISO (2022) belgesinde verilere yönelik tehditleri, bilgilerin veya bilgi varlıklarının yok edilmesi, değiştirilmesi, çalınması, kaybedilmesi ve hizmetlerin kesilmesi olarak değerlendirilmektedir. Veri güvenliği, veri tabanlarında, ağ sunucularında veya kişisel bilgisayarlarda bulunan kişisel veya kurumsal verilerin bozulmaması, yetkisiz erişime karşı korunması ve gizliliğinin sağlanması uygulamalarını kapsamaktadır.

Ismail (2012), veri güvenliğini tehlikeye düşürebilecek tehditleri genel itibariyle şu şekilde sıralamaktadır:

- Bir bilgisayar sistemine giriş öncesinde veya sırasında verilerin karıştırılması veya değiştirilmesi,
- Yanlış güncelleme, depolama veya yedekleme prosedürleri nedeniyle veri kaybı,
- Veri manipülasyonu,
- Güncelleme veya dağıtımda gecikme,
- Doğal afet nedeniyle tahribat,
- Web saldırısı yoluyla kullanıcıların hassas verilerinin ifşa edilmesi,
- Başka kimliğe bürünme veya sosyal mühendislik,
- Kullanıcı verilerinin veya mahremiyetin ifşa edilmesi,
- Kötü amaçlı yazılım ve kod saldırıları,
- Kullanıcı kimliğinin gizlenmesi,
- Parola saldırıları, çözümleme, çalma, kimlik avı ve site trafiği yönlendirme,
- Özel verilerin çalınması,
- Yetkisiz erişim,
- İzinsiz veri kopyalama,
- Yetkisiz veri aktarımı,

- Verilerin yetkisiz, kazara ifşa edilmesi, değiştirilmesi.

3.3.5. Fiziksel ve Çevresel Tehditler

Fiziksel ve çevresel güvenlik, bilgi güvenliği yönetiminin önemli bir unsuru olarak göz ardı edilmemelidir. Donanımların fiziksel güvenliği sağlanmadığında, çeşitli tehditlere karşı savunmasız hale gelebilirler. Bilgi sistemlerinin ana unsurlardan biri olan donanımların fiziksel tehditlerden korunamaması, bu donanımlar üzerinden bulunan verilerin ve yazılımların korunamamasıdır. Bu nedenle bilgi güvenliği yönetiminde fiziksel ve çevresel tehditlerin belirlenmesi ve bu tehditlere karşı önlemlerin alınması önemli görülmektedir. Fiziksel güvenlik, binalara, bilgisayar odalarına ve içindeki cihazlara kimin erişebileceği ile ilgili olduğu kadar doğal afetler ile ilgili tehditleri de içermektedir.

Bir güvenlik programına dâhil edilmesi gereken en yaygın fiziksel tehdit sorunu, doğal afet ve hırsızlıktır. Doğal ve insan yapımı çevre sorunlarının neden olduğu doğal felaketler, bilgisayar ekipmanlarının, fiziksel altyapı varlıklarının ve kayıtlı verilerin tahrip olmasına veya yok olmasına neden olabilmektedir. Yangın, su baskını, ani elektrik artışları ve elektrik kesintileri nedeniyle de bilgi sistemleri zarar görebilmekte ve veriler imha olabilmektedir. Bunun yanı sıra kimyasal, radyolojik ve biyolojik tehlikeler de bilgi sistemlerine zarar verebilmektedir (Vacca, 2012).

Stewart, Chapple ve Gibson, (2005), en yaygın fiziksel tehdit türlerini şu biçimde sıralamaktadır:

- Yangın ve duman,
- Sel ve su baskını,
- Yer hareketleri (depremler, toprak kaymaları veya volkanlar),
- Hava olayları (rüzgâr, fırtına, şimşek, yağmur, kar veya dolu),
- Sabotaj veya vandalizm,
- Patlama veya imha,
- Bina çökmesi,
- Zehirli malzemeler,
- Altyapı hizmeti kaybı (güç, ısıtma, soğutma, hava veya su),
- Ekipman arızası,
- Personel kaybı (grevler, hastalık, erişim veya ulaşım).

Fiziksel güvenlik, kasıtlı veya kasıtsız tehditlere karşı geleneksel korumaları içermektedir. Bu tehditler insan kaynaklı veya doğal olaylar olabilir. Bu nedenle, kurum personeline bu tür tehditlere karşı acil müdahalenin önemini anlatmak ve eylemlerinin sorumluluğunu benimsetmek önemlidir.

3.3.6. İnsan Kaynaklı Tehditler

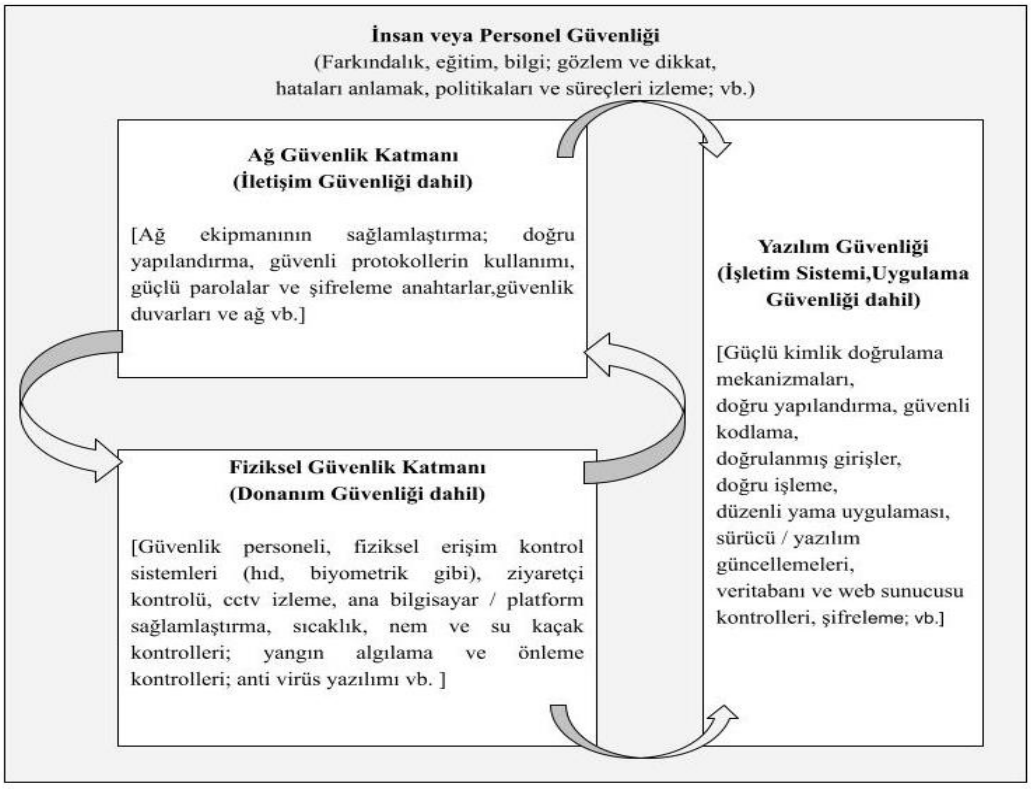
İnsan veya personel güvenliği, bilgi güvenliğinin diğer bir önemli unsurudur. Fakat bilgi güvenliği alanında yapılan çalışmalarda insan faktörünün ikinci planda tutulduğu görülmektedir. Hâlbuki bilgi güvenliğinde en zayıf halka insan kaynaklı tehditlerdir. Kurumlardaki hizmet altyapısı, yönetim, denetim ve teknolojik tüm alanlardaki başarı insan unsuruna bağlı gerçekleşmektedir. Bu nedenle insan bileşeni, bilgi güvenliği anlayışının bir bileşeni olmaktan ziyade ana unsuru durumuna gelerek diğer tüm bilgi güvenliği bileşenlerini etkilemektedir. Personeli motive etmek, bilgi güvenliği risklerinden haberdar etmek ve onları bilgi güvenliği uygulamalarına dâhil etmek bilgi güvenliği yönetiminin vazgeçilmez amaçlarını oluşturmaktadır. Bu nedenle personel, kullanıcı, müşteri, yüklenici ve tedarikçi hangi pozisyonda olursa olsun insan bileşeni bilgi güvenlik yönetiminin en önemli yapı taşını oluşturmaktadır (Chopra ve Chaudhary, 2020).

Bilgi güvenliğinde en zayıf halkanın insan faktörü olduğu göz önünde bulundurulduğunda, hem güvenlik tedbirlerinin uygulanmasında hem de uygulanan güvenlik tedbirlerinin denetlenmesinde görev alacak kurum personelinin belirli bir yetkinliğe sahip olması önem arz etmektedir. Bu çerçevede, bilgi güvenliği ile ilgili eğitimler planlanmalı ve personelin bilgi güvenliği bilincinin gelişimine katkı sağlayacak uygulamalar hayata geçirilmelidir. Bilgi güvenliği eğitimlerinin sadece teorik bilgi vermekten ziyade, personelin ilgili alanda pratik becerisini arttıracak uygulamaları içermesi önemlidir. Bu kapsamda planlanacak eğitimlerde katılımcıların öğrendikleri bilgiyi beceriye dönüştürmesi sağlanmalıdır (CBDDO, 2020).

İnsan ve personel güvenliği, yukarıda üzerinde durulan diğer önemli bilgi güvenliği katmanlarının bileşenlerinden herhangi birinin planlanması, uygulanması, izlenmesi, denetlenmesi, saptanması, düzeltilmesi ve değiştirilmesine yönelik politikalar, prosedürleri ve süreçleri desteklemektedir. Çeşitli katmanlar arasındaki uygun

koordinasyon ve riskler ile fırsatların farklı katmanlara dağılımını sağlayan bu güvenlik katmanındaki uygulamalar, maliyet etkinliğine, kullanım kolaylığına, bilgi güvenliğinin verimliliğine bağlı olarak değişmektedir (Nayak ve Rao, 2014). Şekil 3.4'te insan bileşeni ile diğer bileşenler arasındaki etkileşimi gösteren bilgi güvenliği katmanlarının bağlam diyagramı gösterilmektedir.

Şekil 3.4: Bilgi güvenliğinin birincil katmanları



Kaynak: (Nayak ve Rao, 2014)

Zayıf parola seçimi, verilerin çöp kutusuna taşınması, yetkisiz yazılım yükleme, yetkisiz kullanıcılar tarafından erişim ve sosyal mühendislik, disiplinsizlik gibi birçok insana bağlı hatalar bilgi sistemlerinin güvenliğini riske atmaktır. Veri girişi hataları veya dikkatsizlik dâhil olmak üzere insan kaynaklı hatalar, genellikle tehdit olarak görülmese de potansiyel tehdit kaynağını olarak meydana gelme olasılıkları yüksektir. Personelin veya kullanıcıların bilgi sistemlerinde gerçekleştirdikleri hatalı eylemler verilerin bütünlüğünü, kullanılabilirliğini, gizliliğini ve güvenilirliğini tehdit edebilmektedir (Nayak ve Rao, 2014; Kim ve Solomon, 2018; Whitman ve Mattord, 2018, 2019; Smith, 2019).

Kim ve Solomon (2018), bilgi güvenlik ihlallerinin büyük bir kısmının kurum içinde çalışanların eylemlerinden kaynaklandığını ortaya koymaktadır. Çalışanların bilgi güvenliği suiistimalleri, kurum üzerinde verimlilik kaybı, gelir kaybı, yasal yükümlülükler gibi çeşitli olumsuz etkilere neden olabilmektedir. Bu nedenle, kurumların bilgi güvenliğine bağlı kayıpları en aza indirmek ve hizmetlerinin devamlılığını sürdürebilmesi için çalışanlarına yönelik uygun güvenlik politikaları geliştirmesi ve uygulaması gerekmektedir.

Whitman ve Mattord (2018)'da benzer biçimde, kurum çalışanlarının bilgi sistemlere daha hâkim olmasından dolayı çalışanlar tarafından hassas bilgi sistemlerine karşı yapılacak sabotaj riskinin altını çizmektedir. Kurum çalışanlarının sahip oldukları bilgi, onlara kuruluşun bilgi sistemlerini sabote etme fırsatları sağlamaktadır. Çalışanlar, donanım ve altyapıyı yok etme, verilerin değiştirilmesi, hatalı verilerin girilmesi, yazılımın silinmesi, verilerin silinmesi, virüs yerleştirmek gibi sabote eylemlerle bilgi sistemlerinin güvenliğine karşı tehdit oluşturabilmektedir. Bilgi sistemlerini tehdit eden insan hatalarının ciddiyetine ilişkin raporlara ve bulgulara rağmen bu tür tehditlerin bilgi sistemlerinin güvenliği için önemli bir unsur olarak yeterli seviyede ele alınmadığı vurgulanmamaktadır.

Bilgi güvenliği tehditlerinde en zayıf unsur olarak görülen insan hatalarına karşı kurumların önlemler geliştirilmesi gerektiği üzerinde duran Irmak ve Baz (2019), kurum hizmetlerine uygun oluşturulan bilgi güvenliği politikaları ile tehdit risklerinin minimum seviyelere indirgeneceği belirtilmektedir. Truva atı, oltalama, omuz sörfü, çöp karıştırma, telefonla arama, farklı kimliklere bürünme, gelişmiş siber tehditler, fiziksel zarar ve hırsızlık ve oltalama gibi çeşitli sosyal mühendislik atakları ile kurumların ve kişilerin zafiyetlerinden yararlanılarak gizli ve nitelikli bilgilerin elde edilmesine yönelik yapılan saldırılar, insan kaynaklı bilgi güvenliği tehditlerin başında geldiğini vurgulanmaktadır.

Chopra ve Chaudhary (2020), doğru personel seçiminin ve eğitiminin bilgi güvenliği açısından önemi üzerinde durmaktadır. Kurum yöneticilerinin, yeni personel veya paydaşların kurum bilgilerine erişmeden önce onlara bilgi güvenliği politikaları ve önlemleri hakkında farkındalık sağlatması konusunda sorumluluk almaları gerektiğini vurgulamaktadır. Yeni personel seçimi aşamasında, doğru beceri, deneyim ve eğitime sahip adayların tercih edilmesi önemlidir. Bilgi güvenliği

konusunda uzmanlığa sahip olan veya bu alanda deneyimli adaylar, kurumun bilgi varlıklarını ve sistemlerini korumak için daha etkili olabilirler. Ayrıca, yeni personelin rolleri ve yetkilendirmeleri doğru şekilde belirlenmeli ve bu rollerde görevlendirilmelidir. Örneğin, hassas verilere erişimi olan bir pozisyona getirilecek bir çalışanın, bilgi güvenliği konusunda bilinçli ve güvenilir olması gerekmektedir.

ISO/IEC 27001 (2022) belgesinde kuruma istihdam edilecek personelin ilgili yasalara, yönetmeliklere ve etik kurallara uygun olarak kontrollerinin yapılması gerektiği vurgulanmaktadır. Bu kontrollerin personel tarafından erişilecek bilgilerin sınıflandırılması ve algılanan risklerle orantılı olarak gerçekleştirilmesi gerektiği belirtilmektedir. Böylelikle seçilen personelin kuruluş, müşteriler ve diğer çalışanlar için risk oluşturabilecek sahte kimliğe veya ciddi bir suç geçmişine sahip olmaması sağlanır. Bu nedenle, kurumların insan kaynakları departmanları bu konuda önemli rol üstlenmektedirler.

Birçok araştırma, bilgi güvenliği ihlalleriyle ilgili olarak teknik yönleri ele alırken, insan faktörünün önemini göz ardı etmektedir. Ancak, kurumsal sistemlerin ve bireysel hayatın güvenliği için kişisel davranışların temel olduğu bir gerçektir. Teknik önlemler ve zorunlu kontroller elbette önemlidir ve güvenliğin sağlanmasında kritik bir rol oynarlar. Ancak bu önlemlerin etkin bir şekilde uygulanması ve istismar edilmemesi için insan faktörünün dikkate alınması gerekmektedir. İnsanlar, güvenlik politikalarına uyma, güçlü parolalar kullanma, güvenli internet tarama alışkanlıklarını benimseme gibi kişisel davranışlarıyla güvenliği sağlayabilirler (Workman ve diğerleri, 2008).

3.4. Bilgi Güvenliği Önlemleri

Bilgi güvenliği tehditlerine karşı önlemler; caydırıcı, önleyici, düzeltici, soruşturucu ve kurtarıcı güvenlik kontrollerini kapsamaktadır. Bilgi varlıklarına karşı olası tehditlerin en aza indirgenmesi veya tamamen ortadan kaldırılması için teknik ve kurumsal bilgi güvenliği önlemeleri planlanmakta ve uygulanmaktadır. Bu nedenle bilgi güvenliği tehditlerine karşı önlemler yalnızca teknolojik değil, aynı zamanda idari uygulamaları da içermektedir. Bir kuruluşun varlıklarının, süreçlerinin ve iletişimlerinin güvenliğini sağlamak için teknolojik güvenlik kontrollerinin yanı sıra insan unsurunun da sürece dâhil edilmesi önemlidir. Alanyazında, insanların

rollerine, süreç yönetimine ve teknik uygulamalara dikkat çekilen bilgi güvenliği ilkeleri ve uygulamalarından bahsedilmektedir (Whitman ve Mattord, 2019; Kim ve Solomon, 2018; Seferoğlu ve diğerleri, 2018; Güngör, 2015; Mead ve diğerleri, 2015; Muharremoğlu, 2013; Ismail, 2012; Vaast, 2007; Volonino ve diğerleri, 2004).

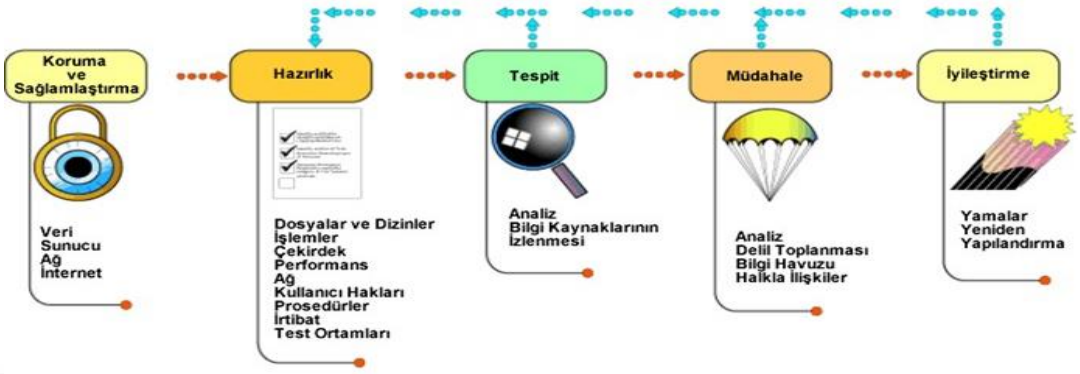
Bilgi güvenliğinde teknoloji, süreç ve insan bileşenlerinin göz önünde bulundurulması son derece önemlidir. İnsan faktörü, bilgi güvenliği sürecinde en zayıf halka olarak kabul edilir, çünkü insanlar hatalar yapabilir, ihmalkârlık gösterebilir veya kötü niyetli davranışlarda bulunabilirler. Bu nedenle, güvenlik önlemleri tasarlarken ve uygularken insan faktörünü dikkate almak önemlidir. İnsanların bilgi güvenliği konusunda eğitilmeleri ve bilgilendirilmeleri gerekmektedir. Bilgi güvenliği politikaları ve prosedürleri ile bilgi sistemi kullanıcılarının güvenlik sorumluluklarını netleştirmek önemlidir. Bu politikalar, kullanıcıların bilgisayar sistemlerini güncel tutmalarını, düzenli yedekleme yapmalarını, güvenlik yazılımlarını güncellemelerini ve diğer güvenlik önlemlerini takip etmelerini sağlar (Gülmüş, 2010).

Bilgi güvenliği yaşayan bir süreç olarak devamlılığını sağlamaktadır. Teknolojik gelişmeler ve tehditlerin değişimi, güvenlik önlemlerinin sürekli olarak güncellenmesini ve iyileştirilmesini gerektirir. Bir zamanlar güvenli kabul edilen bir sistem, teknolojik değişimler veya yeni tehditlerle karşılaştığında güvenliğini korumakta zorlanabilir. Bu nedenle, bilgi güvenliği çalışmalarında güvenlik yaşam döngüsü modelleri kullanılır. Bu modeller, güvenlik sürecinin planlama, uygulama, denetleme ve iyileştirme aşamalarını içermektedir. Bu aşamaların sürekli olarak tekrarlanması, güvenlik önlemlerinin sürekliliğini sağlamaktadır. Güvenlik yaşam döngüsü modelleri, tehdit analizi yapma, risk değerlendirmesi, güvenlik politikalarının ve prosedürlerinin oluşturulması, teknik önlemlerin uygulanması, sürekli izleme ve denetleme gibi adımları içermektedir. Bu adımlar, güvenlik açıklarını tespit etmeyi, tehditlere karşı korunmayı sağlamayı ve meydana gelen olaylardan ders çıkararak güvenlik önlemlerini sürekli olarak iyileştirmeyi amaçlar (Tekerek, 2008).

Computer Emergency Response Team tarafından önerilen CERT Güvenlik Yaşam Döngüsü Modeli (Şekil 3.5), bilgi güvenliği yönetiminde kabul görmüş önemli yaklaşımlardan biridir (Riebe ve diğerleri, 2021). Bu güvenlik yaşam döngüsü

sağlamlaştırma, hazırlık, saldırı tespiti, müdahale ve iyileştirme adımlarından oluşmaktadır.

Şekil 3.5: CERT güvenlik yaşam döngüsü



Kaynak: (Yazıcı ve Şener, 2003)

CERT Güvenlik yaşam döngüsünün ilk aşaması olan sağlamlaştırma aşamasında, bilinen tehditlere ve saldırılara karşı bilgi sistemlerinin güvenliğini artırmaya yönelik önlemler alınmaktadır. Bu önlemler;

- Ağ aktif cihazlarının ve bilgisayar sistemlerinin yazılım güncellemelerinin gerçekleştirilmesi,
- Ön tanımlı parolaların ve anahtar sözcüklerin değiştirilmesi,
- Gerekli olmayan yazılımların durdurulması, gereksiz yazılımların kurulmaması,
- Kullanıcılara yetkilerinin gerektirdiği kadar izin verilmesi,
- Tek kullanımlık parola düzeneklerinin kurulması,
- Sürekli kullanılan parolaların denetlenmesi, zayıf parola atamalarının engellenmesi,
- Akıllı kart, hardware-token, biyometrik denetimlerin kullanımının tercih edilmesi, bunlar kullanılmıyorsa S/Key gibi parola düzeneklerinin kullanılması,
- Yedekleme ve geri yükleme düzeneğinin kurulması ve düzenli aralıklarla denetlenmesi,
- Antivirüs programlarının kullanılması ve düzenli güncellemelerin gerçekleştirilmesi,

- Sunucu yazılımları için üreticiler tarafından tavsiye edilen güvenlik ayarlarının yapılması,
- Güvenlik düzeyine göre ağ bölümlendirmesi,
- Bu aşamada alınan önlemlerin bilinen tehditleri ve saldırıları engellediğinin yeterli olup olmadığını denetlemek için zafiyet tarama yazılımlarının kullanılması olarak sıralanmaktadır.

Hazırlık aşamasında, bir önceki aşama olan hazırlama aşamasında oluşturulan güvenli ortamın bilinmeyen tehdit ve saldırılara karşı korunması için gerekli hazırlıklar yapılmaktadır. Bu aşamada;

- İşletim sistemlerinin olabildiğince çok kayıt üretiminin sağlanması,
- Ağ aktif cihazlarının kayıt düzeneklerinin aktif hale getirilmesi,
- Tüm kayıtların ağ üzerinde merkezi bir sunucuda toplanması,
- Merkezi kayıtların güvenliğinin sağlanması,
- Kayıtları tutabilecek diğer uygulamaların (veritabanı, e-posta, DNS, web, uygulama sunucuları) belirlenmesi ve kayıtlarının merkezileştirilmesi,
- Merkezileştirilmeyen kayıtların belirlenmesi ve bunlar için izlenecek yöntemin tespiti,
- Ağ veya sunucu temelli saldırı tespit sistemlerinin kurulması ve normal olmayan durumlar ile bilindik saldırıların tespit edilmesinin sağlanması,
- Dosya bütünlük denetleyici sistemlerinin kurulması,
- Saptanmamış saldırıları cezbetmek, yanıltmak, oyalamak ve tespit edilmelerini kolaylaştırmak için tuzak sistemlerin kurulması işlemleri yürütülmektedir.

Tespit aşamasında, bilgi sistemleri ve ağlar üzerindeki yetkisiz ya da şüpheli olaylar tespit edilerek hangilerine detaylı inceleme veya müdahale edileceğinin değerlendirilmesi yapılmaktadır. Bu aşamada;

- Tutulan kayıtların düzenli olarak incelenmesi ve şüpheli kayıtların belirlenmesi,
- Kayıtlarda saldırı izi olabilecek girdilerin, kayıtlar arası tutarsızlıkların ve kayıtlarda zaman almamalarının aranması,

- Saldırı tespit sistemleri ve diğer sistemlerin verdiği alarmların incelenmesi işlemleri yürütülmektedir.

Müdahale aşamasında, tespit aşamasında değerlendirilen şüpheli olayların detaylı olarak incelenmesi, müdahale edilmesi ve çözümlenmesi amaçlanmaktadır. Bu aşamada;

- Kayıtlar arasında ilişkilerin aranması,
- Saldırıdan emin olduktan sonra ilgili birim ve kuruluşlar (kurum yönetimi, ilgili acil durum müdahale ekibi, saldırı kaynağı olan ağı işleten kuruluş, savcılık, basın, vb.) ile bilgi paylaşımı,
- Saldırının nasıl gerçekleştiğinin çözümlenmesi,
- Saldırıya ilişkin kayıtların topluca yedeklenmesi işlemleri yürütülmektedir.

Son aşama olan iyileştirme aşamasında ise, önceki aşamalarda edinilen bilgi ve deneyimlerin çerçevesinde güvenliğin arttırılması ve süreçlerin iyileştirilmesi için uygulanan güvenlik uygulamaları gözden geçirilmekte ve geliştirilmektedir. Bu aşamada;

- Yazılım ve yapılandırma güncellemelerinin yapılması ve yamaların uygulanması,
- Zayıflıkların düzenli olarak izlenmesi ve giderilmesine yönelik iyileştirmelerin yapılması,
- Veri veya kayıt toplama sistemlerinin iyileştirilmesi ve güncellenmesi,
- Zafiyet tarama sistemlerinin düzenli çalıştırılması ve tespit edilen zafiyetlerin giderilmesi,
- Bağımsız kuruluşlara sızma testleri, zafiyet analizi ve güvenlik denetimlerinin yaptırılması,
- Güvenlik politikası ve yönergelerinin revize edilmesi bu aşamadaki önemli işlevler arasında bulunmaktadır.

Yeh ve Chang (2007), bilgi sistemlerinin güvenliğinin yeterliliğini değerlendirmek için yaptığı çalışmada yaygın olarak benimsenen elli temel güvenlik önlemi üzerinde durmaktadır. Bu önlemleri, genel olarak bilgi teknolojileri ile ilgili önlemler ve bilgi teknolojileri ile ilgili olmayan önlemler olarak iki ana kategoriye ayırmıştır. Her bilgi

güvenliği önlemi kategorisi beş ile sekiz önlemi içermektedir (Tablo 3.6). Çalışmada yazılım, donanım, veri ve fiziksel varlıklara daha yüksek güvenlik önlemlerinin uygulandığı, buna karşın ağ, personel ve düzenleme veya yasal varlıklar için daha düşük güvenlik önlemlerinin gerekli olduğu ortaya konulmaktadır.

Tablo 3.6: Temel güvenlik önlemleri

<table>
<tr><th>BT İle İlgili Önlemler</th><th>BT İle İlgili Olmayan Önlemler</th></tr>
<tr><td rowspan="2">Yazılım
Kullanıcı giriş günlüğü
Sistem kurtarma
Çok kullanıcılı sistem
Tarayıcı
Otomatik hata ayıklama ve test
Program kaynağına erişim kontrolü
Sistemin doğrulanması değiştirildi
Gizli kanallar ve Truva atı kodu</td><td rowspan="2">Personel
Gizlilik anlaşması
Geçersiz hesap kaldırma
Bilgi güvenliği danışmanı
Düzensiz güvenlik denetimi
Güvenlik eğitimi ve eğitimi
Operasyonel prosedürler eğitimi
Olay raporu prosedürleri</td></tr>
<tr></tr>
<tr><td>Donanım
Uzaktan yansıtma
Gözetim sistemi kullanımı
Giriş sınırlaması
Acil durum güç kaynağı (UPS)
Periyodik disk denetimi</td><td>Fiziksel tesisler ve çevre
Klima
Yanmaz kurulumlar
Su geçirmez kurulumlar
Sarsıntısız kurulumlar
Yıldırım koruyucu</td></tr>
<tr><td>Veri
Bilgi yedekleme
Veri erişim kontrolleri, kimlik doğrulama
Kullanıcı erişim hakları, yetkilendirme
Zorunlu yol
Olay günlüğü
Bilgi işleme prosedürleri
Çıkarılabilir medya yönetimi
Medyanın imha edilmesi</td><td rowspan="2">Düzenleme ve yasallık
(Risk aktarımı dâhil)
Güvenlik Politikası
Bilgi güvenliği politikası
İş sorumluluklarında güvenlik
İş sürekliliği yönetimi
Yasal gerekliliklere uygunluk
Kişisel bilgilerin gizliliği
Fikri mülkiyet hakları
Risk aktarımı
Güvenlik hizmeti sağlayıcısı
Güvenlik dış kaynak kullanımı
Birinci şahıs sigortası
Üçüncü şahıs / kamu sorumluluk sigortası</td></tr>
<tr><td>Ağ
Anti-virüs yazılımı Şifreleme
Kullanıcı doğrulama
Talimat algılama sistemleri
Güvenlik duvarları
Alternatif devre
Dijital imzalar
Bağlantı süresinin sınırlandırılması</td></tr>
</table>

3.4.1. Teknolojik Önlemler

Teknolojik bilgi güvenliği önlemleri; donanım güvenliği, yazılım güvenliği, bilgisayar güvenliği, ağ güvenliği, sunucu güvenliği, veri güvenliği ve fiziksel güvenlik teknik önlemleri kategorileri arasında incelenmektedir.

3.4.1.1. Donanım Güvenliği Önlemleri

Donanım güvenliği tehditleri, bilgi sistemlerinde kullanılan araç ve gereçlerin teknik özelliklerinden fabrikasyon aşamasına ve hatta geri dönüşüm sürecine kadar olan süreçlerde ortaya çıkabilen tehditlerdir. Bu tehditler, istenmeyen tasarım kusurları, sistem yan etkileri ve kötü niyetli tasarım değişiklikleri gibi faktörlerden kaynaklanabilir. Genellikle kriptografik işlevler, güvenlik mimarileri, fikri mülkiyet ve makine öğrenimi modelleri gibi güvenlik varlıklarını hedeflerler. Farklı donanım güvenlik tehditlerini anlamak ve bunları önlemek için etkili güvenlik araçlar tasarlamak ve önlemleri geliştirmek atılacak ilk adımlar arasında bulunmaktadır (Hu ve diğerleri, 2020).

Donanım güvenliği, bilgisayar, yazıcı, fotokopi makinası, barkod yazıcı ve okuyucu, tarayıcı ve her türlü bilgisayar çevre birimleri ile anakart, ekran kartı, işlemci, ram, kasa, harddisk, SSD, cihazlar arası bağlantılarda kullanılan dönüştürücüler, kablolar, telefon hatları, giriş veya çıkış portları, modemler, ağ kabloları ve depolama ortamı gibi çeşitli donanım ekipmanların korumasını sağlamak amacıyla oluşan yöntem ve uygulamaların bütününü kapsamaktadır. Bu ekipmanların hırsızlık, elektrik kesintileri, donanım uyumsuzlukları, dikkatsiz kullanımından kaynaklı hasar gibi her türlü tehditten korunması ve üzerlerindeki verilerin kullanılabilirliğini, gizliliğini ve bütünlüğünü sağlaması gerekmektedir (Jin, 2015).

Teknolojik gelişmeler iş istasyonlarının kullanımını arttırmaktadır. Özellikle kişisel bilgisayarların sayısı son yıllarda sürekli artmaktadır. Bilgi güvenliği farkındalığı gelişmeyen kullanıcıların, maruz kaldıkları saldırıların gün geçtikçe arttığı görülmektedir. Bilgi güvenliği ile ilgili bilinçlenmenin düşük olduğu toplumlarda gerek kişisel gerekse kurumsal işler için kullanılan bilgisayarlardaki bilgiler çalınmakta veya ifşa olmaktadır. Bu durum kişisel ve kurumsal sorunların oluşmasının yanı sıra toplumsal kargaşaya da neden olabilmektedir.

Bilgi sistemlerinin mimarisinde sunucu kullanan kuruluşlar, sunucular üzerinden oluşabilecek risklerin farkında olması ve bu doğrultuda hazırlanan bilgi güvenliği önlemlerini kullanması önem arz etmektedir. İyi bir bilgi güvenliği yönetimine sahip kuruluş, güvenli bir sunucu hizmetini de sağlayabilmektedir. Eğer ki sunucular güvenli bir veri merkezince korunamıyorsa; sunucuları kilitli tutulması, sunucu

erişimlerinin sürekli izlenmesi ve gerekirse kısıtlanması, sunucu ile ilgili günlük raporların takip edilmesi, çevre ile ilgili (sıcaklık, sel, yangın vb.) diğer risklerin değerlendirilmesi ve güç kaynağı gibi altyapı hizmetlerinin kullanması gerekmektedir (Wang, 2009).

3.4.1.2. Yazılım Güvenliği Önlemleri

Yazılım güvenliği genel olarak, yazılımların tersine mühendislik araçları ve yöntemleri kullanılarak bilgi güvenliği problemlerinin ortaya çıkarılmasını, bilginin değiştirilmesini ve çalınmasını engellemeyi amaçlayan bir dizi yöntem ve önlem olarak tanımlanmaktadır. Yazılım güvenliği, yazılım uygulamalarının saldırılara karşı korunmasını, güvenlik açıklarının tespit edilmesini ve düzeltilmesini, verilerin gizliliğini ve bütünlüğünü sağlamayı hedeflemektedir. Yazılım güvenliği, bilgi sistemlerinin güvenliğini ve bütünlüğünü sağlamak amacıyla çeşitli kontrol ve önlemleri içermektedir. Bu önlemler, yazılım geliştirme sürecinin her aşamasında dikkate alınmalıdır. Yazılım güvenliği önlemleri çeşitli şekillerde yapılmaktadır. Bunlardan bir kısmı şu şekilde örneklendirilebilir. Güvenlik testleri, yazılımın güvenlik açıklarını tespit etmek ve potansiyel saldırı noktalarını ortaya çıkarmak için yapılmaktadır. Kimlik doğrulama ve yetkilendirme süreçleri, kullanıcıların doğru bir şekilde tanımlanmasını ve yetkilendirilmesini sağlar. Veri şifreleme, hassas verilerin şifrelenerek gizliliklerinin korunmasını sağlamaktadır. Hataların düzeltilmesi sürekli izleme, güncelleme ve güvenlik yamalarının hızlıca uygulanmasını gerektirir. Saldırılara karşı koruma önlemleri ise güvenlik duvarları, saldırı tespit sistemleri ve saldırı engelleme sistemlerini içermektedir (Çakır ve diğerleri, 2014).

Donanımları işler duruma getiren yazılımlar her geçen gün gelişmekte ve güncellenmektedir. Bu gelişmeler kötü amaçlı yazılımların yenilenmesini de beraberinde getirmektedir. Bu nedenle yazılım güvenliği önlemlerinin sürekli olarak güncellenmesi de önemli bir husustur. Kötü amaçlı yazılımlardan korumayı amaçlayan yazılımların tedarik edilmesi ve kullanımına sunulması, kurumsal antivirüs yazılımlarının işler hale getirilmesi ve sürekli olarak bu yazılımların güncelleştirilmesi yazılım güvenliği açısından önemli önlem mekanizmalarının başında gelmektedir (Şahinaslan, 2010).

Kurum bilgi sistemlerine yazılımlar üzerinden saldırılar gerçekleştirmektedir. Bu saldırılar genelde şu üç nedene bağlı olarak yapılmaktadır. Birincisi, yazılımın tamamen etkisiz hale getirilerek kullanılmasını engellemektir. İkincisi, yazılımın işleyişini bozarak saldıranın hedefleri doğrultusunda çalışmasını sağlamaktır. Üçüncüsü ise, yazılımdaki güvenlik açıklarının tespit edilerek belirlenen bu zayıf noktalar üzerinden yazılımın bulunduğu sunucuya daha sonra ise tüm veri merkezlerine erişim sağlamaktır. Bu nedenlerden ötürü yazılımların planlama aşamasından kullanım aşamasına kadar tüm adımlarda uygulanması gereken birtakım sistemsel ve kullanıcı taraflı güvenlik ilkeleri bulunmaktadır. Bu güvenlik ilkeleri şu biçimde sıralanmaktadır (Whitman ve Mattord, 2018; 2019):

- **Ayrıcalıkları (yetkileri) düşük tut ilkesi**: Kullanıcıların yazılım üzerinde gerçekleştirecekleri işlemleri ihtiyaçları doğrultusunda en az işlem yetkisine sahip olacak şekilde belirlenmesidir. Kullanıcılara gereksinimleri ve iş faaliyetleri çerçevesinde yetkilendirme ve ayrıcalık verilerek yazılımlarda oluşabilecek sistemsel yavaşlıklar engellenmekte ve kullanıcının yazılım üzerinde erişebileceği alanlar kısıtlanmaktadır.
- **Tüm erişimleri kayıt altında tut ilkesi:** Yazılım ve uygulamalarda gerçekleştirilen önemli işlemlerin kayıt altında tutulması ilkesidir. Yazılımın başlatılması, kapatılması, veri eklenmesi, silinmesi, bir isteğin gerçekleşmesi ve isteğe dönen cevap gibi önemli sayılan uygulama üzerinden yapılan tüm işlemeler loglama yöntemleri ile kayıt altında tutulur. Bu sayede yazılımda gerçekleşen sorunların ve fark edilmeyen zafiyetlerin tespiti kolaylaşır.
- **Erişimleri ayrı tut ilkesi:** Yazılımda bulunan önemli bir dosyaya veya özelliğe erişilmeye çalışıldığında erişim denetiminin artırılması ilkesini kapsayan önlemlerdir. İki faktörlü doğrulama buna bir örnektir. Kullanıcı önemli bir dosyaya erişmeden önce sunucuda oturum açmalı ardından erişmek istediği yere oturum açmalıdır. Her iki doğrulama işlemi de gerçekleşirse erişim izni verilebilir, aksi durumda erişim reddedilir.
- **Varsayılanları gözden geçir ilkesi:** Uygulamalarda kullanılan tüm varsayılanların gözden geçirilmesidir. Güvenlik zafiyeti tespit edilen varsayımlar güvenli hale getirilmelidir. Kullanılan dosya ve metin belgelerinin herkese açık olması ve üzerinde düzenlemeler yapılabilmesi,

yazılımın bulunduğun dizinin kolay erişilebilir ve basit olması, erişime açık dosyalarda şifrelerin bulunması ve IP zafiyetine karşı tehdit varsayılan ayarların bulunması genel olarak yapılan hatalar arasında bulunmaktadır.

- **Ortak erişim alanlarında erişimi sınıflandırma ilkesi:** Ortak alanlara erişimlerde farklı kanallar kullanılmasıdır. Aynı kanaldan yapılan erişimlerde veri sızması ve çalışması durumu kaçınılmazdır. Bu tip durumlarda erişim kanallarını sınıflandırmak gerekir.
- **Zafiyeti tespit et ve engelle ilkesi:** Yazılımda bulunan zafiyetlerin tespit edilerek güvenlik önlemleri çerçevesinde düzenlemelerin yeniden yapılandırılmasıdır. Uygulamalara yapılan saldırılarda genellikle zafiyet oranı yüksek olan alanlar kullanılır. Güvenlik zafiyeti bulunan yazılımlar için zafiyet tarama testleri yapılarak güvenlik arttırma çalışmaları yapılmalıdır.
- **Saldırı yapılabilecek arayüz alanlarının minimuma indirilmesi ilkesi:** Uygulama ara yüzünde sunucuya bilgi gönderme veya sunucudan bilgi alma alanlarının azaltılmasıdır. Yazılım ara yüzünde bulunan iletişim alanlarının az olması yazılım güvenliğini artırır.

Yazılım saldırılarını önlemek için öncelikle yazılım güvenliği ilkelerine uygun bir yol izlenmeli ve güvenliği arttıracak tasarım yöntemleri ve uygulamaları kullanılmalıdır. Dışarıdan izinsiz veri aktarımını engellemek için form alanlarından gelen verilerin kontrol edilerek sunucuya aktarılması gerekir. Önlem almak ve güvenlik senaryolarını kafamızda kurmak, yazılımın geliştirilmesi ve bitirilmesi sonrası güvenli bir yazılım haline gelmesindeki en büyük etkendir (Özkaya ve diğerleri, 2019).

Eisenberg ve Lawthers (2005), yazılım güvenliğini korumak için aşağıdaki önlemlerin kullanılmasını önermektedir:

- Kullanıcı bilgisayarında dosyaların veya ayarların silinmesini sağlayan temizleme yazılımları,
- İş istasyonlarının belirli özelliklerini izlemek, kullanımını kısıtlamak veya devre dışı bırakmak için uygulama ve işletim düzeyinde masaüstü güvenlik yazılımları,
- Ağ üzerindeki iş istasyonlarına bir uygulama veya güncelleme yükleme sürecini otomatikleştirmek için dağıtım araçları,

- Standart Windows masaüstü arayüzlerini değiştirmek ve zaman aşımları, günlüğe kaydetme ve tarama etkinlikleri üzerinde kontrol sağlamak için menü değiştirme yazılımı,
- Bilgisayarlarda yapılan tüm değişiklikleri takip etmek, kaydetmek ve sistemin seçilen herhangi bir noktadan itibaren orijinal başlangıç noktasına geri yüklenmesini sağlayacak geri alma yazılımları kullanılmalıdır.

Yeh ve Chang (2007) ise, çalışmalarında bilgi sistemleri üzerindeki yazılımları güvence altına almak için aşağıdaki önlemleri listelenmektedir:

- Bir bilgisayarın birden çok kullanıcısı tarafından aynı anda erişime izin vermek için çok kullanıcılı işletim sistemlerinin ve uygulama yazılımlarının kullanılması,
- Yeni geliştirilen yazılım veya donanım bileşenlerindeki herhangi bir yazılım kusurunu gidermek için periyodik otomatik hata ayıklama yazılımının kullanılması,
- Saldırı veya bilinçsiz eylemler sonrası çöken bilgisayar sistemlerinin yeniden inşa etmek ve onarmak için sistem kurtarma yazılımlarının kullanılması,
- Kullanıcı giriş günlüklerini düzenli olarak kaydeden ve analiz eden yazılımların kullanılması önerilmektedir.

3.4.1.3. Ağ Güvenliği Önlemleri

Ağlar, bilgi sistemlerini birbirine bağlayarak bilgilerin çok hızlı bir biçimde aktarılmasını ve kolay erişimini sağlamaktadır. Teknolojik gelişmelere bağlı olarak ağ yapıları da gelişmekte ve kullanımı artmaktadır. Bilgilerin ve verilerin iletilmesinde önemli rol oynayan bu ağların güvenliğinin önemi gün geçtikçe artmaktadır. Bilgi işlem sistemleri üzerindeki bilgiler ağlar üzerinden gerçekleştirilen saldırılar ile çalınmakta veya ifşa edilmektedir. Bu saldırıların kurumun faaliyetlerini doğrudan etkileyen bilişim sistemlerine yönelmesi, kuruluşları bilgi, zaman, prestij ve ekonomik kayıplar açısından ciddi anlamda zor durumda bırakmaktadır (Karaarslan ve diğerleri, 2003).

Ağ güvenliği, ağlar üzerinde yer alan dijital varlıkları korumak, ağ saldırılarını takip etmek, önlemek ve bunlara karşı önleyici araçları, taktikleri ve güvenlik politikalarını tasarlamak için oluşturulmuş bir kavramdır. Ağ güvenliği, donanım ve yazılım

teknolojilerini içeren kaynaklar da dâhil olmak üzere bu kaynakları birbirine bağlayan alanları hedef alan tüm potansiyel tehditlere karşı tasarlanmış güvenlik sistemini oluşturmaktadır. Kısaca ağ güvenliği, saldırganları bilgi sistemlerindeki hassas verilerden uzak tutmak için oluşturan ağ savunmasıdır (Yavuz ve Tuna, 2019).

Ağ güvenliği stratejisi, üç temel güvenlik eylemi üzerinde odaklanmaktadır: Koruma, saldırı tespit ve saldırı engelleme. Koruma, ağa yapılacak saldırıları önlemek için tasarlanmış güvenlik politika ve araçlarını kapsamaktadır. Saldırı tespiti veya algılama, ağ trafiğine zarar verebilecek tehdit risklerinin önceden analiz edilerek bilgi sistemlerine zarar vermeden tanımlanmasını sağlayan kaynakları ifade etmektedir. Müdahale ise, tanımlanan tehditlere karşı önlemlerin en kısa sürede geliştirilmesi ve sorunları çözme yeteneği eylemlerini içermektedir (Özkaya ve diğerleri 2019).

ISO/IEC 27001 (2022) standardının referans kontroller çizelgesinde ağ güvenliği yönetimi ile ilgili kontroller verilmektedir. Bu kontroller üç başlık altında listelenmektedir:

- Ağ kontrolleri: Sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağlar yönetilmeli ve kontrol edilmelidir.
- Ağ hizmetlerinin güvenliği: Tüm ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve yönetim gereksinimleri tespit edilmeli ve hizmetler kuruluş içinden veya dış kaynak yoluyla sağlanmış olsun olmasın tüm ağ hizmetlerine ilişkin güvenlik anlaşmaları sağlanmalıdır.
- Ağlarda ayrım: Ağ kullanımları kullanım alanlarına göre genel ağ, kullanıcı ağları, misafir ağları şeklinde ayrılmalıdır.

Ağ güvenliğinde en önemli argümanların başında ağ güvenliği politikası gelmektedir. Ağ güvenliği politikası, bilgi sistemlerini birbirine bağlayan ağların güvenli kullanımı için kurum faaliyetlerine uyumlu olarak tasarlanmış belgedir. Ağ güvenlik politikası ile veri erişimi, web görüntüleme, şifre kullanımı, şifreleme ve e-posta ekleri gibi öğelerin güvenli yönetimi amaçlanmaktadır. Bu politika, bilgi güvenliği yönetim sistemine uygun ağ tasarımına yardımcı olmakta ve ağ güvenlik ilkelerini ve uygulamalarını kolaylaştırmaktadır. Kuruluşun ağ erişimi için belirlenen

güvenlik kuralları, uygulama ilkeleri ve ağ güvenlik ortamının temel mimarisi açıklanmaktadır. Politika, ayrıca kötü niyetli kullanıcıların ağ üzerinden gerçekleştireceği potansiyel riskleri de tanımlamaktadır (Whitman ve Mattord, 2018).

Ağ güvenliğini sağlamak için bir takım kontrol yöntemleri bulunmaktadır. Bunlar; güvenlik duvarı (Firewall), sanal özel ağ cihazları (VPN), antivirüs, saldırı tespit ve önleme sistemleri, web filtreleme çözümleri, güçlü tanılama yöntemleri olarak sıralanmaktadır (Çam, 2020; Aksakalli, 2019; Paşaoğlu ve diğerleri, 2019):

- Güvenlik duvarı: Yerel ağ ile dış ağlar arasındaki güvenliği sağlayan kontrol mekanizmasıdır. Bu sistemde gerçekleştirilen adımlar daha önceden belirlenen politikalara göre uygulanmaktadır. Bu kontrol mekanizması ile bilgi sistem içerisinden hangi verilerin geçeceği belirlemekte ve parola doğrulaması yapılmaktadır. Belirlenen güvenlik kuralları ile bilgi sistemlerine kimlerin erişip erişemeyeceği sağlanmaktadır.
- VPN sistemi: Farklı mekânlardaki PC ve LAN'ları internet ağı üzerinden az maliyetle daha güvenli bir şekilde birbiri ile veri alışverişini yapmasını sağlamaktadır.
- Saldırı tespit ve önleme sistemleri: Sunucu ve ağ tabanlı olmak üzere iki tip olarak karşımıza çıkmaktadır. Ağ tabanlı saldırı tespit sistemi, kurumun kullandığı ağ ya da ağlara yönlenmiş olan veri trafiğini algılayarak sorgulamakta ve herhangi bir saldırı olup olmadığına karar vererek bu saldırıları önlemektedir.
- Antivirüs yazılımları: Bilgi sistemlerine ağlar üzerinden gelebilecek virüsler bu yazılımlar ile engellenmektedir. Sunucuları üzerine kurulan antivirüs sistemleriyle dış ağlardan gelecek virüsler etkisiz hale getirilmektedir.
- Web filtreleme çözümleri: Kullanıcıların web site gezinmeleri sırasında kasıtlı veya kasıtsız yaptıkları güvenlik açıklarını engellemek için URL filtreleme denilen yazılımlar ile ağların güvenliği sağlamaktadır.
- Güçlü tanılama yöntemleri: Bilgi sistemlerine ağlar üzerinden erişenlerin kimliklerinin belirlenmesini ve tanınmasını sağlamaktadır.

3.4.1.4. Veri Güvenliği Önlemleri

Veri güvenliği endişeleri her geçen gün artmaktadır. Veri gizliliği, bütünlüğü ve kullanılabilirliğine ilişkin geleneksel gereksinimlere ek olarak, veri kalitesi, güncelliği, eksiksizliği ve kaynağı (Cui ve Widom, 2003; Missier ve diğerleri, 2003) gibi yeni gereksinimler ortaya çıkmaktadır. Özellikle verilerin tam, doğru ve dış dünya açısından güncel olması önemlidir. Artan veri kalitesi, verileri daha değerli hale getirmektedir. Son derece değerli verilerin yetkisiz erişimlere bağlı olarak kurum veya kişiler üzerinde oluşabilecek zararları artmaktadır. Dünyada üretilen veri miktarının giderek artmasından dolayı veri tabanlarının boyutunun ve sayısının da hızlı arttığı görülmektedir. Bu nedenle, verileri koruma mekanizmalarının iyi tasarlanması gerekmektedir (Agrawal ve diğerleri, 2002).

Veritabanı sistemleri, bir kuruluşun temel verilerini yönetmek ve depolamak için kullanılan kritik bileşenlerdir. Bu nedenle, veritabanı sistemlerinin güvenliği büyük önem taşımaktadır. Verilerin zarar görmesi ve kötüye kullanılması yalnızca tek bir kullanıcıyı veya uygulamayı etkilemekle kalmaz, tüm kuruluş üzerinde telafisi zor sonuçlar doğurabilmektedir. Web tabanlı uygulamaların ve bilgi sistemlerinin son zamanlarda hızla yaygınlaşması, veritabanlarının tehdit risklerine maruz kalmasını daha da arttırmaktadır. Bu nedenle veri koruma ile ilgili yapılan çalışmalar bugün her zamankinden daha önemli hale gelmiştir. Verilerin yalnızca dış tehditlerden değil, aynı zamanda içeriden gelen tehditlerden de korunması gerektiğini de bilmek önemlidir (Vural, 2018).

89 ülkeden toplanan 5.250'den fazla onaylanmış veri ihlalinden elde edilen bilgilere göre hazırlanan 2021 Veri İhlali Araştırmaları Raporu (2021 Data Breach Investigations Report)'nda en çok karşılaşılan veri ihlallerinin başında hizmet reddi, sosyal mühendislik, temel web uygumla saldırıları, kayıp ve çalınan varlıklar, sistem sızıntıları, ayrıcalıkların kötüye kullanımı ve çeşitli kullanıcı kaynaklı hatalar gelmektedir. Raporda veri ihlallerinin oluşumunda dış aktörlerin %70'in üzerinde etkisinin olduğu belirtilmektedir. Yine bu raporda veri ihlali olayları sektörlere göre incelendiğinde en başta eğlence ve halka açık sektörler gelmektedir. Daha sonra ise bilgi, eğitim, sağlık, profesyonel, bilimsel ve teknik hizmetler, yönetim, imalat, madencilik ve tarım sektörlerinin geldiği görülmektedir. Ayrıca veri ihlallerinde en çok hareketlerin ise sırasıyla dolandırıcılık, intihal, hizmet reddi, kötü amaçlı yazılım

kullanımı, bahane bulma, yanlış yapılandırma hataları, yanlış yönlendirme, kaba kuvvet, truva atı, araka kapı gibi olduğu görülmektedir (Bassett ve diğerleri, 2021).

Veriler önemli bir bilgi varlığını temsil etmektedir. Genellikle kişisel verileri toplayan ve bunları tıbbi verilerde olduğu gibi bilimsel araştırmalardan demografik eğilim analizi ve pazarlama amaçlarına kadar çeşitli amaçlarla kullanan kuruluşların sayısının giderek artmaktadır. Kuruluşlar ayrıca sahip oldukları verilere erişim sağlatmakta ve hatta bu tür verileri üçüncü taraflara verebilmektedir. Böylece artan veri setlerinin sayısı, kişi ve kuruluşların mahremiyetine yönelik ciddi tehditler oluşturmaktadır. Gizlilik önemli bir konu olduğundan, gizliliği koruyan veri yönetimi tekniklerinin geliştirilmesine yönelik çeşitli araştırma çalışmaları yapılmaktadır. Bu araştırma çalışmalarında verilerin gizliliğini koruyan üç teknik üzerinde durulmaktadır (Bertino ve Sandhu, 2005).

Bu tekniklerden ilki, verilerin üçüncü taraflara açıklanmasıyla oluşan mahremiyetin korunması ile ilgilidir. Bu durumda, veriler bir kez yayınlandıktan sonra artık onlara sahip olan kuruluşların kontrolü altında değildir. Bu nedenle, verilerin sahibi olan kuruluşlar, verilerin kullanım şeklini kontrol edememektedir. Serbest bırakılan verilerin gizliliğini ele almak için uygulanan en yaygın yaklaşım, veri öğelerini bireylerle doğrudan ilişkilendirilebilecek tüm bilgiler kaldırarak verilerin değiştirmesidir ki bu işleme veri anonimleştirme denmektedir. Serbest bırakılan verilerden adlar veya sosyal güvenlik numaraları gibi kimlik bilgileri kaldırılsa da bu yaklaşımında yeterli olmayabileceği belirtilmektedir. Yayınlanan verilerden bu tür bilgiler çıkarıldığında bile, diğer bilgi kaynaklarıyla birleşiminden kalan verilerin, bilgileri atıfta bulunduğu kişilere bağlayabildiğini göstermektedir. Bu sorunun üstesinden gelmek için, Sweeney tarafından önerilen k-anonimlik modeline dayanan mahremiyetin korunması yaklaşımları önerilmektedir (Sweeney, 2002).

İkinci teknik ise, özellikle veri madenciliği bağlamında mahremiyetin korunmasıyla ilgilidir. Veri madenciliği teknikleri günümüzde çok etkili yöntem olarak kullanılmaktadır. Bu nedenle, bir veritabanındaki özel bilgiler temizlenmiş olsa bile, veri madenciliği tekniklerinin kullanılması, kaldırılan bilgilerin kurtarılmasına izin verebilmektedir. Veri madenciliğinde birbirinden bağımsız çeşitli yaklaşımlar kullanılmaktadır. Bu yaklaşımların geneli, verileri bir şekilde değiştirmeye veya bozmaya dayanmaktadır. Bu tekniklerin çoğunda ortak olan sorun, ortaya çıkan veri

tabanının kalitesi ile ilgilidir. Veriler çok fazla değişikliğe uğrarsa, artık bu veriler yararlı olmayabilmektedir. Bu sorunları çözmek için, modifikasyonların getirdiği hataları tahmin etmek için teknikler geliştirilmiştir (Oliveira ve Zaiane, 2002; Vaidya ve Clifton, 2002).

Son teknik ise, P3P standardı kullanılarak ifade edilebilen gizlilik politikalarını desteklemek için özel olarak hazırlanmış veritabanı teknikleri üzerinde durulmaktadır. Bu teknik ile ilgili olarak Agrawal ve arkadaşları (2002) tarafından ilişkisel veri tabanı sistemlerinde mahremiyet korumasını içeren Hipokrat veritabanları tanıtılmıştır. Hipokrat veritabanı, sorgu işleme sırasında gizlilik denetimi gerçekleştirmektedir. Her sorgu veri tabanının amacına uygun olarak gönderilmektedir. Sistem önce sorguyu yapan kullanıcının gizlilik yetkileri tablosunda bu amaç için yetkili kullanıcılar grubunda olup olmadığını kontrol etmektedir. Sistem, sorgunun yalnızca gizlilik yetkileri tablosunda sorgu amacıyla açıkça listelenen alanlara erişmesini sağlamaktadır. Sorgunun çalışmasına izin verilirse, sistem, yürütme sırasında sorguya yalnızca amaç özniteliği sorgu amacını içeren kayıtların görünmesini sağlamaktadır.

Kuruluşların varlıklarını sürdürebilmeleri için hayati önem taşıyan veriler, sürekli tehdit riski altında bulunmaktadır. Veriler elektronik veya fiziksel ortamlarda kayıtlı olabilmektedir. Verilerin saklandığı manyetik veya fiziksel ortamlar zarar görebilmektedir. Bu durumda veri kısmen veya tamamen zarar görebilmekte ve okunamaz duruma gelebilmektedir. Kurumların hizmetlerine devam edebilmeleri için zarar gören verileri en kısa sürede geri kazanması gerekmektedir. Bu nedenle verilerin zarar görmesi veya tamamen yok olma risklerine karşı farklı ortamlarda yedeklenmesi gerekmektedir. Bunu da yapmanın en iyi yolu önceden yapılacak veri güvenliği planlamalarından geçmektedir.

3.4.1.5. Fiziksel ve Çevresel Güvenlik Önlemleri

Fiziksel güvenlik, bir organizasyonun kaynaklarına ve bilgi varlıklarına karşı tehditleri ve saldırıları fiziksel açıdan önlemeye yönelik tedbirleri içermektedir. Diğer bir ifadeyle, bir kurumun fiziksel kaynaklarını koruyan karşı önlemlerin tasarlanmasını, uygulanmasını ve sürdürülmesini kapsamaktadır. Bilgi güvenliğine

yönelik birçok tehdit, fiziksel güvenliğe yönelik tehditler olarak da sınıflandırılmaktadır.

ISO/IEC 27001 (2022) standardının referans kontroller çizelgesinde fiziksel ve çevresel güvenlik kontrollerini, güvenli alanlar ve teçhizat ana başlıkları altında listelenmektedir. Güvenli alanlar ile yetkisiz fiziksel erişimi, kuruluşun bilgi ve bilgi işleme olanaklarına hasar verilmemesi ve müdahale edilmemesi amaçlanmaktadır. Güvenli alanlar başlığı altında sıralanan fiziksel ve çevresel güvenlik temelleri ve kontrolleri şu biçimde listelenmektedir:

- Fiziksel güvenlik sınırı: Hassas veya kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmalı ve kullanılmalıdır.
- Fiziksel giriş kontrolleri: Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunmalıdır.
- Ofislerin, odaların ve tesislerin güvenliğinin sağlanması: Ofisler, odalar ve tesisin diğer bölümleri için fiziksel güvenlik mekanizmaları geliştirilmeli ve uygulanmalıdır.
- Dış ve çevresel tehditlere karşı koruma: Doğal felaketler, kötü niyetli saldırılar veya kazalara karşı fiziksel koruma tasarlanmalı ve uygulanmalıdır.
- Güvenli alanlarda çalışma: Güvenli alanlarda çalışma için prosedürler düzenlenmelidir.
- Teslimat ve yükleme alanları: Yetkisiz kişilerin tesise giriş yapabildiği teslimat ve yükleme alanları gibi erişim noktaları ve diğer noktalar kontrol edilmeli ve mümkünse yetkisiz erişimi engellemek için bilgi işleme olanaklarından ayrılmalıdır.

Teçhizat başlığı altında sıralanan fiziksel ve çevresel güvenlik temelleri ve kontrolleri şu biçimde listelenmektedir:

- Teçhizat yerleştirme ve koruma: Teçhizat, çevresel tehditlerden ve tehlikelerden ve yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmeli ve korunmalıdır.
- Destekleyici altyapı hizmetleri: Teçhizat destekleyici altyapı hizmetlerindeki hatalardan kaynaklanan enerji kesintileri ve diğer kesintilerden korunmalıdır.

- Kablo güvenliği: Veri veya destekleyici bilgi hizmetlerini taşıyan enerji ve telekomünikasyon kabloları, dinleme, girişim oluşturma veya hasara karşı korunmalıdır.
- Teçhizat bakımı: Teçhizatın bakımı, sürekli ve doğru şekilde yapılmalıdır.
- Varlıkların taşınması: Teçhizatlar, izinsiz kuruluş dışına çıkarılmamalıdır.
- Kuruluş dışındaki teçhizat ve varlıkların güvenliği: Kuruluş dışındaki varlıklara, kuruluş yerleşkesi dışında çalışmanın farklı riskleri de göz önünde bulundurularak güvenlik uygulanmalıdır.
- Teçhizatın güvenli yok edilmesi veya tekrar kullanımı: Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımdan önce tüm hassas verilerin ve lisanslı yazılımların kaldırılmasını veya güvenli bir şekilde üzerine yazılmasını temin etmek amacıyla doğrulanmalıdır.
- Temiz masa ve ekran politikası: Kâğıtlar ve taşınabilir depolama ortamları için temiz masa politikası, bilgi işleme olanakları için ise temiz ekran politikası benimsenmelidir.

Çakır ve arkadaşları (2014), çalışmalarında fiziksel ve çevresel güvenliğin sağlanması için sağlanacak tedbirleri şu biçimde sıralamaktadır:

- Bilgi varlıklarına yetkisiz erişimi denetlemek ve hasar risklerini azaltmak için temiz masa ve temiz ekran politikası geliştirilmelidir.
- Güvenli alanlara yetkili personelin erişimine izin veren fiziki giriş denetim sistemleri ve araçları kullanılmalıdır.
- Kartlı okuyucular, retina tarama, parmak izi gibi biyometrik ve akıllı giriş sistemleri ile kimlik kontrollerinin sağlanmalıdır.
- Hassas kaynakların veya bilgilerin bulunduğu alanlarda ziyaretçilere eşlik edilmesi, ziyaretçilerin giriş ve çıkış tarihleri not edilmeli ve gerekirse üst aramaları yapılmalıdır.
- Hassas bilgilere ve bilgi işleme araçlarına erişim denetlenmeli ve sadece yetkili kullanıcılarla sınırlanmalıdır.
- Tüm personelden, görünür biçimde kimlik kartı taşımaları istenmeli ve kimlik kartı taşımayan birine rastlandığında hemen bildirilmelidir.
- Güvenli alanlara erişim hakları düzenli aralıklarla gözden geçirilmeli ve güncellenmelidir.

- Tesisin konumu, yangın, sel, patlama, askeri saldırı ve diğer biçimdeki doğal veya insan yapımı afetlerden meydana gelebilecek hasar ihtimallerine göre seçilmelidir.
- Tesis, insanların park alanlarının ve bina girişlerinin görünürlüğünü maksimize eden mimari özellikte olmalıdır.
- Tesiste özel ve kamusal alanların birbirinden ayrılması (çitler, ağ geçitleri, peyzaj, vb.) sağlanmalıdır.
- Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmelidir.
- Tesiste yetkisiz erişimleri engellemeye yönelik mimari unsurlar (kapı kilitleri, pencere kilitleri, iç kapı menteşeleri, vb.) kullanılmalıdır.
- Tehlikeli ve patlamaya hazır maddeler, güvenli alandan uygun bir uzaklıkta güvenli bir şekilde toplanmalıdır.
- Yakın çevrede oluşan felaketler, örneğin komşu binada çıkan bir yangın, çatıdan akan veya zemin kat seviyesinden aşağıdaki katlara akan su veya caddede olan bir patlama göz önünde bulundurulmalıdır.
- Teçhizatlar, güç kaynağı bozulmalarından veya diğer olağan dışı elektriksel olaylardan korunmalıdır.
- Donanım üreticisinin belirttiği özelliklere uygun elektrik kaynağı sağlamalı,
- Veri taşıyan veya bilgi hizmetlerini destekleyen güç ve haberleşme kabloları, durdurmalardan veya hasarlardan korunmalıdır.
- Teçhizatların, elverişliliğinin ve güvenilirliğinin garanti edilmesi için doğru bir biçimde bakımı yapılmalıdır.
- Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde olmalıdır.
- Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.
- Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.
- Su bağlantısı, iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.
- Acil durumlarda iletişimin kesilmemesi için servis sağlayıcıdan iki bağımsız hat alınmış olmalıdır.

- Kurum, fiziksel güvenlik konusunda yasal yükümlülüklerini yerine getirmelidir.

3.4.2. Kurumsal (Örgütsel) Önlemler

Kurumsal bilgi güvenliği, kurumun hizmetlerinden kaynaklı bilgi varlıklarının tehlikelerden korunmasını ve gerekli önlemlerin alınmasını kapsamaktadır. Kurumun hizmetlerini ve itibarını bilgi varlıkları üzerinden olumsuz yönde etkileyecek tehdit ve tehlikelerden korunması amacıyla alınan önlemler o kurumun bilgi güvenliği yönetim çerçevesini oluşturmaktadır. Kurumsal bilgi güvenliği, birçok faktörün etkileşimine dayanan karmaşık bir süreçtir ve bu sürecin etkin bir şekilde yönetilmesi önemlidir. Bu sürecin iyi bir biçimde yönetilmesi ve yüksek seviyede bilgi güvenliğinin sağlanması için kurumsal bilgi güvenliği politikasının, kurumsal bilgi güvenliği prosedürlerinin, idari araç ve yöntemlerinin uluslararası standartlarda yapılandırılması gerekmektedir. Bu nedenle kurumlar kurumsal bilgi güvenliğini sağlayabilmesi için standartlara uygun bilgi güvenliği politikaları, prosedürleri, idari araç ve yöntemlerini oluşturması gerekir.

3.4.2.1. Bilgi Güvenliği Politikaları

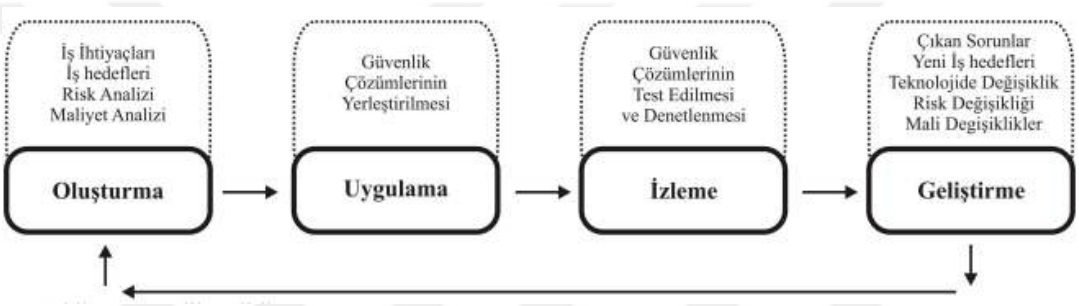
Kurumun güvenlik ihtiyaçlarını ve bu ihtiyaçları karşılama konusundaki kararlılıklarını açıklayan güvenlik politikaları, yönetimin bilgi güvenliği amaç ve hedeflerini belgelemektedir. Güvenlikle ilgili bir politikanın temel amacı saldırı riskini azaltmaktır. Bir güvenlik politikası, kurumun temel güvenlik gerçeklerini öz ve açık bir biçimde ifade etmelidir. Politikanın karmaşıklığı, yönetim ve kullanıcıların güvenlik politikasında belirlenen hususları benimsemesinde zorluk çekmelerine neden olabilmektedir. Örneğin, "Kuruluşun geleceği için güvenlik önemlidir" veya "Hizmetlerimizde güvenlik en önemli görevimizdir" gibi ifadeler, yöneticilere karar vermeleri için ihtiyaç duydukları rehberliği sağlayacaktır (Kim ve Solomon, 2018).

Bilgi güvenliği politikası, kurumların bilgi güvenliğinin sağlanmasına yönelik gerekli olan tüm önlem ve kontrollerin belirlendiği etkinlikleri kapsamaktadır. Kurumun üst düzey yönetimi tarafından desteklenen bilgi güvenlik politikaları, kurum çalışanları tarafından da benimsenmesi gerekmektedir. Bir bilgi güvenlik politikası kullanıcılar tarafından anlaşılır ve uygulanabilir; yöneticiler tarafından ise kolay yönetilebilir

olması önem arz etmektedir. Bilgi güvenliği politikaları, kurumlar arasında farklılık gösterse de genel olarak kurumun bilgi sistemlerini, bilgi varlıklarını, verilerini, çalışanlarının kişisel bilgilerini, kontrol mekanizmalarını ve diğer kritik bilgilerini maksimum derecede koruyan amaç ve hedefleri içermektedir. Politikalar, kurumların bir çeşit özel kanunları gibi düşünülen etik ve yasal değerleri içermektedir (Evrin ve Demirer, 2011).

Politikalar Şekil 3.6'da gösterildiği üzere; oluşturma, uygulama, izleme ve geliştirme süreçlerinden geçirilerek oluşturulmaktadır (Tekerek, 2008).

Şekil 3.6: Bilgi güvenliği politikası işlem süreci



Kaynak: (Tekerek, 2008)

Bir kuruluşta bilgi güvenliğinin sağlanması için öncelikli olarak hedeflerin net bir biçimde belirlenmesi gerekmektedir. Belirlenen bu hedefler doğrultusunda kurumun bilgi güvenliği politikalarını işler duruma gelmesini sağlayacak standart, rehber ve prosedür gibi diğer idari güvenlik araçlarına ihtiyacı vardır. Bütüncül bir bilgi güvenliği politikası ancak bu biçimde sağlanabilmektedir (Kara, 2018).

3.4.2.2. Bilgi Güvenliği Prosedürleri ve Kontrolleri

Bilgi güvenliği politikalarının pratik ve uygulanabilir olması için, standartlar, yönergeler ve prosedürlerle daha ayrıntılı tanımlanmaları gerekmektedir. Güvenlik politikasının belirli eylemlere ve kontrollere nasıl dönüştüğünü tanımlamak için prosedür veya kılavuz dokümanlar oluşturulmaktadır. Prosedürler, politikaların nasıl uygulanacağına dair adım adım talimatları içermektedir. Bilgi varlıklarını nasıl koruyacaklarını belirledikleri için politikalar kadar önemli dokümanlardır. Örneğin, parola oluşturma kuralları güvenlik politikası ile belirlenirken, yeni parola oluşturma, bunları dağıtma, parolaların kritik cihazlarda değiştiğinden emin olma ve parolaların

ne sıklıkla değiştirileceği ile ilgili işleyişlerin ana hatları ise prosedürler ile belirlenmektedir (Ismail, 2012).

Prosedür ve diğer kontrol belgeleri ile bilgi güvenliği faaliyetlerinin temel dayanağı olan politikaların idari ve teknik seviyesindeki işlem adımları detaylandırılmaktadır. Bu detaylandırma, planla, yap, kontrol et ve hareket et döngüsünde gerçekleştirilmektedir. Kapsamlı kurumsal bilgi güvenliği politikasında öne sürülen güvenliğe ilişkin beklentiler ve taahhüt, spesifik olarak hazırlanan kontroller, prosedürler ve ayrıntılı belgeler ile eyleme geçirilmektedir (Cosic ve Boban, 2010).

Kuruluşların özel güvenlik ilkelerini türetmeye yönelik net yöntemlerin belirlendiği prosedür ve diğer kontrol dokümanları bir güvenlik politikasının doğruluğunu, uygunluğunu ve kalitesini belirlemeleri için özel idari güvenlik mekanizmalarıdır. Bilgi güvenliği yönetiminde çok önemli bir yere sahip olan bu belgeler, bilgi güvenliği politikalarının etkinliğini sorgulamakta ve bu etkinliğe katkıda bulunan faktörleri belirlemektedir. Sonuç olarak, bir politikanın etkinliği, doğru içeriğe değil, içeriğin prosedür ve diğer kontrol belgeleri ile ele alınma ve nihai olarak kullanıcılara iletilme şekline bağlıdır (Pathari ve Sonar, 2012).

Yeterli düzeyde bilgi güvenliği için öncelikle etkili bir kontrol setinin belirlenmesi, uygulanması ve yönetilmesi; daha sonra ise bu kontrollerin bilgi sistemlerindeki etkinliğinin değerlendirmesi ve sertifikalandırılması gerekmektedir. Güvenlik kontrollerinin seçimi, iş ihtiyaçlarına ve ilgili güvenlik gereksinimlerine göre belirlenmektedir. Güvenlik gereksinimleri, bilgi güvenliği politikasında açıkça tanımlanmalı ve güvenlik politikası bu güvenlik gereksinimlerine göre gerekli korumayı sağlayacak kontrolleri içermelidir. Bu kontroller dizisinin kurumun iş ihtiyaçlarını karşıladığı değerlendirilip sertifikalandırılması, iş ihtiyaçlarını karşılayan bir dizi kontrolün belirlenmesine yönelik resmi bir yaklaşım sağlamaktadır (Barnard ve Solms, 2000).

3.4.2.3. İdari Araç ve Yöntemler

Hizmetlerin veya ürünlerin performansını desteklemek için bir takım kurumsal gereklilikler bulunmaktadır. Bilgi güvenliği yönetimi de kurumsal gerekliliğin bir parçası olarak önemlidir. Bilgi güvenliği teknik önlemlerin yanı sıra politika, rehber, standart ve prosedür gibi birtakım idari araç ve yöntemleri de kapsamaktadır.

Kurumsal faaliyetlerin performansını desteklemek için geliştirilen bu idari araç ve yöntemler, bilgi kaynaklarının yetkisiz erişime karşı korunmasını sağlamaktadır. Yönetim tarafından dokümante edilmiş ve tüm çalışan ve paydaşlara duyurulmuş bilgi güvenliği araç ve yöntemleri ile tam olarak geliştirilmiş bir bilgi güvenliği yönetim anlayışı, bilgi kaynaklarının korunmasını sağlamaya yardımcı olmak için gereken yapıyı ve rehberliği sağlamaktadır (Evrin ve Demirer, 2011).

Bilgi güvenliği için yürütülen idari araç ve yöntemler yalnızca politika ve prosedürleri içermemektedir. Öncelikle kurumun bilgi güvenliği ile ilgili mevcut risk ve tehditlerinin belirlenmesi gerekmektedir. Kurumsal ve kişisel bilgilerin güvenliğinin sağlanması için öncelikle kurum tarafından işlenen bilgi varlıklarının neler olduğu belirlenmelidir. Envanteri çıkarılan bilgi varlıklarına karşı oluşabilecek risklerin gerçekleşme olasılığının ve bu risklere karşı alınacak tedbirlerin belirlenmesi gerekmektedir. Bu risklerin tanımlanması ve alınacak tedbirlerin belirlenmesinden sonra, söz konusu risklerin en aza indirilmesi veya ortadan kaldırılmasına yönelik alternatif kontrol ve çözüm önerilerinin uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilerek gerekli idari araç ve yöntemlerin tasarlanması ve uygulanması gerekmektedir (Kim ve Solomon, 2018).

3.4.2.4. Bilgi Güvenliği Farkındalık Çalışmaları

Kurumların en değerli varlıkları arasında yer alan bilginin gizlilik, bütünlük ve kullanılabilirlik unsurlarının güvenliğinin sağlanabilmesi için birçok teknik önlem alınmaktadır. Bu teknik önlemlerin yanı sıra bilgi güvenliğinin sağlanmasında insan faktörünün daha önemli olduğu unutulmamalıdır. Fakat bilgi güvenliğinde teknik önlemlere verilen değer, insan faktörünün görmezden gelinmesine neden olmaktadır (Çek, 2017).

Kurumlar maliyetine bakmaksızın en ileri güvenlik teknolojileri ile tasarlanan güvenlik sistemleri ile bilgilerini korumaya çalışsa da, çalışanlarındaki bilgi güvenliği farkındalığını oluşturamadıkları sürece bilgi güvenliklerini tamamen sağlayamamaktadır. Bu durum bilgi güvenliği konusunda oluşabilecek sorunların sadece teknik yöntemlerle çözüme kavuşamayacağı düşüncesini oluşturmakta ve kurumları bilgi güvenliği farkındalığını arttırmaya yönelik çalışmalara yöneltmektedir (Erol, 2016).

Bilgi güvenliği bir bütün olarak sağlanabilmesi üç temel sürecin gerçekleşmesine bağlıdır. Birincisi, bilgi güvenliğinin doğru bir biçimde idare edilmesi için uygulanan politika, strateji ve planları kapsayan yönetsel süreç; ikincisi, tehdit ve saldırılara karşı teknik çözümlerin uygulandığı teknolojik önlem ve kontrol süreci; üçüncüsü ise kullanıcıların veya çalışanların bilgi güvenliği farkındalıklarının oluşması için yürütülen eğitim sürecidir. Bu üç süreç içerisinde insan faktörünün çoğunlukla ikinci plana atıldığı görülmektedir. Bu durum bilgi güvenliği faaliyetlerinin eksik tarafını oluşturmaktadır. Politika, standart, denetim, teknoloji ve altyapının yer aldığı yönetsel ve teknik sürecin başarıya ulaşmasında insan faktörü önemlidir. Çünkü insan bu iki sürecin oluşmasında rol oynamaktadır. Dolayısıyla, insan faktörü bilgi güvenliğinin ana unsuru olarak diğer süreçleri sürekli etkilemektedir. Bu nedenle bir organizasyon içerisindeki tüm insanların bilgi güvenliği farkındalığına sahip olması gerekmektedir (Gündüzalp, 2021; Aslay ve diğerleri, 2019).

Bilgi güvenliğini tehdit eden insan kaynaklı güvenlik açıkları her geçen gün artmaktadır. Teknolojik gelişmeler güvenlik önlemlerini daha da güçlendirmekte ve saldırganlar bu teknik önlemler karşısında zorlanmaktadır. Bu nedenle insan faktörlü güvenlik açıklarına yönelmektedirler. Kullanıcıların bilinçli veya bilinçsiz eylemlerinden yararlanarak bilgi sistemlerine sızmaktadırlar. Özellikle bilgi güvenliği konusunda yeterli eğitime sahip olmayan kullanıcıların bilinçsiz eylemleri, saldırganların bilgi sistemlerine erişme olasılıklarını arttırmaktadır. Bilgi güvenliği ve sistem kullanımı konularında yeterli eğitime sahip olmayan kullanıcıların farkında olmadan yaptıkları kullanımlar her ne kadar kötü niyet içermese de, saldırganlar tarafından fark edilerek birçok kötü amaçlı kullanımlara neden olmaktadır. Örneğin kötü niyetli bir yazılım içeren bir e-postanın bilinçsiz bir biçimde açılması parola, kimlik bilgisi veya benzeri verilerini çalma saldırılarına neden olmaktadır. Bu tür e-postaları açan veya cevaplayan kullanıcıların kişisel bilgileri hatta kurumsal bilgileri de çalınmaktadır (Alemdaroğlu, 2020).

Eğitim, bilgi güvenliği açısından oluşabilecek riskleri azaltmak için kullanılacak en etkili yöntemdir. Bilgi sistemlerinin bilinçli ve güvenli bir biçimde kullanmaları için kullanıcılara veya çalışanlara periyodik olarak eğitimler verilmesi gerekmektedir. Bu eğitimler ile bilgi güvenliği konusundaki bilinçsizlikler en aza indirilerek kurum açısından risk oluşturacak insan faktörlü tehditler giderilmektedir. Bu nedenle bilgi

güvenliğinin sağlanması için idari ve teknik önlemlerin yanı sıra en üst yöneticiden en alt çalışanına hatta ilişki içerisinde olduğu müşterilerine, tedarikçilerine, ziyaretçilerine kadar tüm paydaşların bilgi güvenliği farkındalık eğitimleri ile desteklenmesi gerekir. Bilgi güvenliği faaliyetlerinin benimsenmesi ve önemsenmesi kullanıcıların daha bilinçli sistem kullanımlarını desteklemektedir. Farkındalık eğitimleriyle desteklenen kullanıcılar, hangi bilgilerin korunması gerektiğini ve bu bilgilere karşı ne tür saldırıların gerçekleşebileceğini anlamakta ve nasıl önlemler alması konusunda bilinçlenmektedir (Aslay ve diğerleri, 2019).

Bilgi güvenliği farkındalık çalışmaları ile kullanıcıların bilgi güvenliği tehdit ve saldırılarından haberdar edilmesi amaçlanmaktadır. Bilgi güvenliği farkındalığının kurumsal kültür olarak geliştirilmesi, güvenlik politika ve araçlarının daha iyi bir biçimde uygulanmasını sağlayacaktır. Kullanıcıların faaliyetlerine yön veren rehber niteliğindeki bu dokümanların uygulanması, kullanıcılara verilen farkındalık eğitimleri ile daha da güçlendirilmektedir. Bu nedenle kurumların sağlam bir güvenlik politikası yürütebilmesi çalışanlarının eğitilmesi ve bilinçlendirilmesinden geçmektedir. Bilgi güvenliği farkındalığı oluşmamış personel yapısına sahip kurumlarda, değerli bilgiler yetkisiz kişilerin eline geçerek telafisi mümkün olmayan maddi ve manevi çok büyük kayıplara neden olabilmektedir.

4. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Çalışmanın bu bölümünde, bilgi güvenliği yönetim sisteminin önemi, aşamaları ve yönetim anlayışına ilişkin bilgiler sunulmaktadır. Ayrıca bilgi güvenliği yönetim sistemi (BGYS) ile PUKÖ döngüsü arasındaki ilişki incelenerek bilgi yönetim sisteminin başarı faktörlerine ilişkin bilgiler verilmektedir.

4.1. Bilgi Güvenliği Yönetim Sistemi

Yönetim, organizasyonu uygun yapılar içinde yönlendirme, kontrol etme ve sürekli iyileştirme faaliyetlerini kapsamaktadır (ISO, 2022). Yönetim, insan ilişkilerine dayalı bir süreç olup planlama, örgütleme, yürütme, koordinasyon, geliştirme ve kontrol gibi faaliyetleri içermektedir. Kurumsal ve insan kaynaklarını etkili ve verimli bir şekilde bir araya getirerek örgütün hedeflerine ulaşmasını sağlar (Çelik ve Şimşek (2013).

Sistem, basit anlamda birbiriyle ilişkili veya etkileşimli bir grup elemanın oluşturduğu bir bütün olarak tanımlanmaktadır. Sistemler; girdi, süreç, çıktı, geri bildirim ve denetim olmak üzere beş temel işleve sahiptir. Bir yönetim sistemi bu beş işlev temelinde oluşmuş bir yapıdır. Yönetim sistemi; bilgi güvenliği politikaları, süreçleri ve hedefleri oluşturmak ve bu hedeflere ulaşmak için bir organizasyon içerisinde sorumlulukları, yetkileri, ilişkileri ve kendi işlevleri olan kişi veya kişiler kümesi (ISO, 2022; 2018). Bu sistemler içerisinde yer alan yönetim bilgi sistemleri ise, yöneticilerin bilgiye erişimini kolaylaştırmakta, karar verme süreçlerini iyileştirmekte ve organizasyonun performansını artırmada önemli bir rol oynamaktadır (O'Brien ve Marakas, 2006).

Bilgi güvenliği yönetim sistemi, bir organizasyonun bilgi varlıklarını korumak için gerekli süreçleri ve politikaları içeren bir çerçeve yapıdır. Bu sistemin amacı, bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak ve organizasyonun iş hedeflerine zarar vermeden güvenlik risklerini yönetmektir. Bilgi güvenliği yönetim sistemi, aşağıdaki unsurları kapsamaktadır (Whitman ve Mattord, 2018):

- Risk değerlendirmesi: Organizasyon, potansiyel tehditleri, zayıflıkları ve riskleri belirlemek için bir risk değerlendirmesi yapar. Bu değerlendirme,

bilgi varlıklarının önemini ve korunması gereken hassas alanları belirlemek için kullanılır.

- Politikalar ve prosedürler: Bir organizasyon, bilgi güvenliği politikalarını ve prosedürlerini belirleyerek güvenlik standartlarını ve yönergelerini oluşturur. Bu politikalar ve prosedürler, çalışanların ve diğer ilgili tarafların bilgi güvenliğiyle ilgili sorumluluklarını belirler.
- Kontroller ve önlemler: Organizasyon, risklerin azaltılması ve güvenlik önlemlerinin uygulanması için gerekli kontrolleri belirler. Bu kontroller, fiziksel güvenlik önlemleri, erişim kontrolleri, şifreleme, yedekleme ve felaket kurtarma gibi çeşitli alanlarda uygulanabilir.
- İzleme ve değerlendirme: Bilgi güvenliği yönetim sistemi, sürekli izleme ve değerlendirme süreçlerini içerir. Bu süreçler, güvenlik olaylarını izlemek, güvenlik açıklarını tespit etmek ve güvenlik önlemlerinin etkinliğini değerlendirmek için kullanılır.
- İyileştirme ve sürekli gelişim: Organizasyon, bilgi güvenliği yönetim sisteminin etkinliğini sürekli olarak değerlendirir ve geliştirmek için düzeltici ve önleyici faaliyetlerde bulunur. Bu süreç, güvenlik açıklarının kapatılmasını, eğitim ve farkındalık programlarının uygulanmasını ve güvenlik politikalarının güncellenmesini içerebilir.

Bilgi güvenliği yönetim sistemi, kuruluşun bilgi varlıklarını korumak amacıyla oluşturduğu ve yönettiği politikaları, prosedürleri, kılavuzları ve ilgili dokümanları içermektedir. BGYS, kuruluşun hedeflerine ulaşabilmesi açısından oluşturduğu sistematik bir yaklaşımdır. Bu sistematik yaklaşım kuruluşun risklerini yönetebilmek ve bu riskleri etkin bir biçimde karşılayabilmek amacıyla tasarlanmış risk kabul düzeylerine dayanmaktadır. Bilgi varlıklarının korunmasına yönelik gereksinimlerin analiz edilmesi ve bu bilgi varlıklarının gerektiği şekilde korunmasını sağlamak için uygun BGYS kontrollerinin (bilgi güvenliği kurmak, uygulamak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirme) uygulanması, kuruluşun başarılı faaliyet göstermesine katkıda bulunmaktadır.(ISO, 2018; 2022).

BGYS'nin başarılı bir şekilde uygulanmasına katkı sağlayan temel ilkeler şu biçimde sıralanmaktadır (ISO, 2018) :

- Bilgi güvenliğine duyulan ihtiyaç konusundaki farkındalığın oluşmasını sağlamak,
- Bilgi güvenliği sorumluluğunu oluşturmak ve geliştirmek,
- Yönetim taahhüdünü ve paydaşların çıkarlarını sağlamak,
- Toplumsal değerlerin geliştirilmesini sağlamak,
- Kabul edilebilir risk düzeylerine ulaşmak için uygun kontrolleri belirleyen risk değerlendirmelerini yapmak,
- Güvenlik anlayışını, bilgi ağlarının ve sistemlerinin temel bir unsuru olarak işletmek,
- Bilgi güvenliğini tehdit eden olayların tespit edilmesini ve önlemesini sağlamak,
- Bilgi güvenliği yönetimine kapsamlı bir yaklaşım kazandırmak,
- Bilgi güvenliğinin sürekli olarak yeniden değerlendirilmesi ve uygun şekilde güncellenmesini sağlamak.

BGYS'nin oluşturulması ve benimsenmesi bir kuruluş için stratejik bir karar olarak beklenmektedir. Bu kararın kuruluşun ihtiyaçları doğrultusunda sorunsuz bir şekilde bütünleştirilmesi, ölçeklendirilmesi ve güncellenmesi gerekmektedir. Bir kuruluşun BGYS'nin tasarımı ve uygulanması, kuruluşun ihtiyaçları ve hedeflerinden, güvenlik gereksinimlerinden, kullanılan iş süreçlerinden, kuruluşun büyüklüğü ve yapısından etkilenmektedir.

Bilgi sistemlerinin tasarımı ve geliştirilmesinde bilgi güvenliği her zaman dikkate alınmamaktadır. Bilgi güvenliği genellikle teknik bir çözüm olarak düşünülmektedir. Fakat teknik yollarla elde edilebilecek bilgi güvenliği sınırlı olmaktadır. BGYS bağlamında oluşturulmuş uygun yönetim ve prosedürlerle desteklenmeyen bilgi güvenliği çalışmaları etkisiz kalabilmektedir. BGYS, hangi kontrollerin olması gerektiğini belirlemekte ve bilgi güvenliği planlamalarına ve detaylarına etkinlik kazandırmaktadır. BGYS, teknik (mantıksal), fiziksel, idari (yönetimsel) veya hepsinin bir arada olduğu erişim kontrolleri, kurumun bilgi güvenliği gereksinimlerine göre düzenlemektedir. BGYS'nin başarılı bir şekilde benimsenmesi, bilgi varlıklarını korunmasında organizasyona önemli olanaklar sunmaktadır (Gemici ve Yılmaz, 2019):

- Bilgi varlıklarının sürekli olarak tehditlere karşı yeterince korunduğuna dair daha fazla güvence sağlamaktadır.
- Bilgi güvenliği risklerini belirlemek, değerlendirmek, uygulanabilir kontrolleri seçmek, uygulamak, bunların etkinliğini ölçmek ve geliştirmek için yapılandırılmış kapsamlı bir çerçeve sağlamaktır.
- Kontrol ortamını sürekli iyileştirmektedir.
- Hizmetlerin yasal ve düzenleyici uyumunu sağlamaktadır.

4.2. Bilgi Güvenliği Yönetim Sistemi Süreç Aşamaları

Bilgi güvenliği yönetim sisteminin oluşturması, izlemesi, sürdürmesi ve iyileştirmesi için aşağıdaki süreçlerin takip etmesi gerekmektedir (ISO, 2018):

- Bilgi varlıklarını ve bunlarla ilişkili bilgi güvenliği gereksinimlerini tanımlamak,
- Bilgi güvenliği risklerini değerlendirmek ve uygun kontrolleri seçmek,
- Kabul edilemez riskleri yönetmek için ilgili kontrolleri seçmek ve uygulamak,
- Kuruluşun bilgi varlıklarıyla ilişkili kontrollerin etkinliğini izlemek, sürdürmek ve iyileştirmek,

4.2.1. Bilgi Güvenliği Gereksinimlerinin Belirlenmesi

Bir kuruluşun bilgi güvenliği gereksinimleri, o kuruluşun genel stratejisi, iş hedefleri, büyüklüğü ve coğrafi yayılımının yanı sıra şu üç başlık dâhilinde belirlenmektedir (ISO, 2018):

- Tanımlanmış bilgi varlıkları ve bunların değerleri,
- Bilgi işleme, depolama ve iletişim için gereksinim duyulan ihtiyaçlar (bilgi sistemleri, personel, fiziksel çevre vb.),
- Yasal, düzenleyici ve sözleşmeye dayalı gereksinimler.

4.2.2. Bilgi Güvenliği Risklerinin Değerlendirilmesi ve Düzeltilmesi

Risk değerlendirmesi, risklerin büyüklüğünü tahmin etmeye yönelik sistematik yaklaşım ve risklerin önemini belirlemek için tahmin edilen riskleri kriterlerine göre karşılaştırma süreci içermektedir. Risk değerlendirmesi, risk kabulü kriterlerine ve kuruluşla ilgili hedeflere göre tanımlamalı, ölçmeli ve öncelik vermelidir. Risk

değerlendirmesinden elde edilen sonuçlar, bilgi güvenliği risklerini yönetmek, bu risklere karşı koruma sağlamak ve seçilen kontrolleri uygulamak için uygun yönetim eylemini ve öncelikleri yönlendirmeli ve belirlemelidir (ISO, 2018).

Bilgi güvenliği risk değerlendirmesinin etkili olabilmesi için açıkça tanımlanmış bir kapsamı olması ve diğer alanlardaki risk değerlendirmeleri ile ilişkileri bulunması gerekmektedir. Bilgi güvenliği gereksinimlerinde, varlıklarda, tehditlerde ve zayıflıklarda meydana gelebilecek değişikliklere ve gelişmelere karşı periyodik olarak risk değerlendirmesi yapılmalıdır. Bu risk değerlendirmeleri, karşılaştırılabilir ve tekrarlanabilir sonuçlar üretebilen yöntemsel bir şekilde yapılmalıdır.

Kuruluşlar bir riskin ele alınmasını değerlendirmeden önce, risklerin kabul edilip edilemeyeceğini belirlemek için birtakım kriterler tanımlamalıdır. Örneğin, riskin düşük olduğu veya tedavi maliyetinin kuruluş için uygun maliyetli olmadığı değerlendirildiği durumlarda riskler kabul edilebilir olmaktadır. Bu tür kriterlerin kayıt altına alınması gerekmektedir.

Risk değerlendirmesinin ardından belirlenen risklerin her biri için bir iyileştirme kararının alınması gerekmektedir. Bilgi güvenliği risklerinin tedavisi için aşağıda sıralanan uygun kontrollerin seçilmesi ve uygulanması gerekmektedir (ISO, 2018):

- Riskleri azaltmak için uygun kontrolleri uygulamak;
- Riskleri bilerek ve nesnel olarak kabul etmek, kuruluşun risk kabul politikasını ve kriterlerini açıkça yerine getirmelerini sağlamak,
- Risklerin oluşmasına neden olacak eylemlere izin vermeyerek risklerden kaçınmak;
- Sigortacılar veya tedarikçiler gibi diğer paydaşlarla ilgili risklerin paylaşılması.

4.2.3. Bilgi Güvenliği Kontrollerin Seçilmesi ve Uygulanması

BGYS ilk iki sürecinde bilgi güvenliği gereksinimleri belirlendikten sonra tanımlanan bilgi varlıklarına yönelik bilgi güvenliği riskleri belirlenmekte ve değerlendirilmektedir. Bu değerlendirmeler sonucunda bilgi güvenliği risklerinin işlenmesine yönelik kararlar alınmaktadır. Bu adımda ise risk azaltma için kontrollerin seçimi ve uygulanması sağlanmaktadır.

Risklerin kabul edilebilir bir düzeye indirilmesi için kontrollerin seçiminde ve uygulanmasında dikkat alınması gereken hususlar şunlardır (ISO, 2018):

- Ulusal ve uluslararası mevzuat ve yönetmeliklerin gerekliliklerine ve kısıtlamalarına uygun olmalı,
- Örgütsel hedefleri sağlamalı,
- Operasyonel gereksinimleri ve kısıtlamaları içermeli,
- Azaltılan risklere ilişkin uygulama ve işletme maliyetleri ile kuruluşun gereksinim ve kısıtlamaları arasındaki orantıyı sağlanmalı,
- Kuruluşun amaçlarını desteklemek için bilgi güvenliği kontrollerinin etkinliğini ve verimliliğini izleme, değerlendirme ve iyileştirme hedeflerine ulaştırmalı,
- Kontrollerin seçimi ve uygulanması, kuruluşun gereksinimlerine uygun ve yardımcı olması için bir uygulanabilirlik beyanı ile belgelenmeli,
- Kontrollerin uygulanması ve işletilmesine yapılan yatırım ile bilgi güvenliği olaylarından kaynaklanması muhtemel kayıplar değerlendirilmelidir.

4.2.4. BGYS' nin Etkinliğinin İzlenmesi, Sürdürülmesi ve İyileştirilmesi

BGYS'nin sürekli iyileştirilmesindeki temel amaç, bilginin kullanılabilirliğinin, gizliliğin ve bütünlüğünün korunmasıyla ilgili hedeflere ulaşma olasılığını arttırmaktır. İyileştirme için fırsatlar aramak ve mevcut yönetim faaliyetlerinin yeterince iyi olmadığını varsaymak sürekli iyileştirmenin odak noktasını oluşturmaktadır (ISO, 2018).

İyileştirme eylemleri şunları içermektedir:

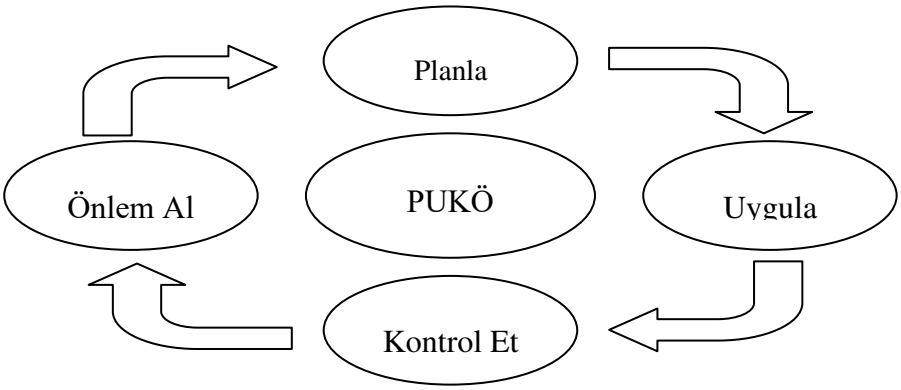
- İyileştirme alanlarını belirlemek için mevcut durumu analiz etmek ve değerlendirmek,
- İyileştirme için hedeflerin belirlenmesi,
- Hedeflere ulaşmak için olası çözümlerin araştırılması,
- Bu çözümleri değerlendirmek ve bir seçim yapmak,
- Seçilen çözümü uygulamak;
- Hedeflere ulaşıldığını belirlemek için uygulamanın sonuçlarının ölçülmesi, doğrulanması, analiz edilmesi ve değerlendirilmesi,
- Değişiklikleri resmileştirmek.

4.3. PUKÖ Döngüsü

BGYS, kuruluşların hedeflerine ulaşması, yasal uyumluluklarını sağlanması, imajlarını sürdürmesi ve geliştirmesi için bilgi varlıklarını korumak üzerine oluşturulmuş gerekli kontrol mekanizmaları ile düzeltici ve iyileştirici süreçleri içermektedir. Bu bakımdan BGYS standartlarının iş süreçleri planla, uygula, kontrol et ve önlem al aşamaları olarak bilinen PUKÖ Döngüsü yöntemine dayanmaktadır. W. Edwards Deming tarafından geliştirilmiş "Planla - Uygula - Kontrol Et - Önlem Al (PUKÖ)" metodolojisi BGYS' nin kurulması ve yönetilmesinde olduğu gibi diğer yönetim sistemlerinin de temelini oluşturmaktadır (Sanz-Calcedo ve diğerleri, 2015).

BGYS 27000 standartlar ailesinin de içinde bulunduğu tüm ISO standartlarının kurulmasında ve uygulanmasında temel yapı olarak kullanılan PUKÖ döngüsü, veri esaslı sistematik bilgi elde etme yöntemidir (Şekil 4.1). Veri ve bilgilerin dört aşamada değerlendirildiği bu yöntemde yeni bilgiler elde edildikçe yeni uygulamalar ve fikirler üretilmektedir. Bu uygulamalar ve fikirler PUKÖ döngüsü ile test edilerek sürekli iyileştirilmektedir. Planla aşamasında, amaç ve hedefler belirlenmektedir. Uygula aşamasında, belirlenen amaç ve hedeflere göre belirlenen prosedürler uygulanmaktadır. Kontrol et aşamasında, problemlere yönelik uygulanan faaliyetlerin sonuçları kontrol edilmekte ve değerlendirilmektedir. Önlem al aşamasında ise sonuçlardan elde edilen verilere ve gelecekte oluşabilecek risklere göre süreçlerin iyileştirilmesi yapılmaktadır. Bu iş süreçleri bir döngü olarak sürdürülmektedir. (Çubukçu, 2018; Akpınar ve Öğütoğulları, 2016; Sanz-Calcedo ve diğerleri, 2015; Özkılıç, 2014; Çalık, 2013).

Şekil 4.1: PUKÖ döngüsü



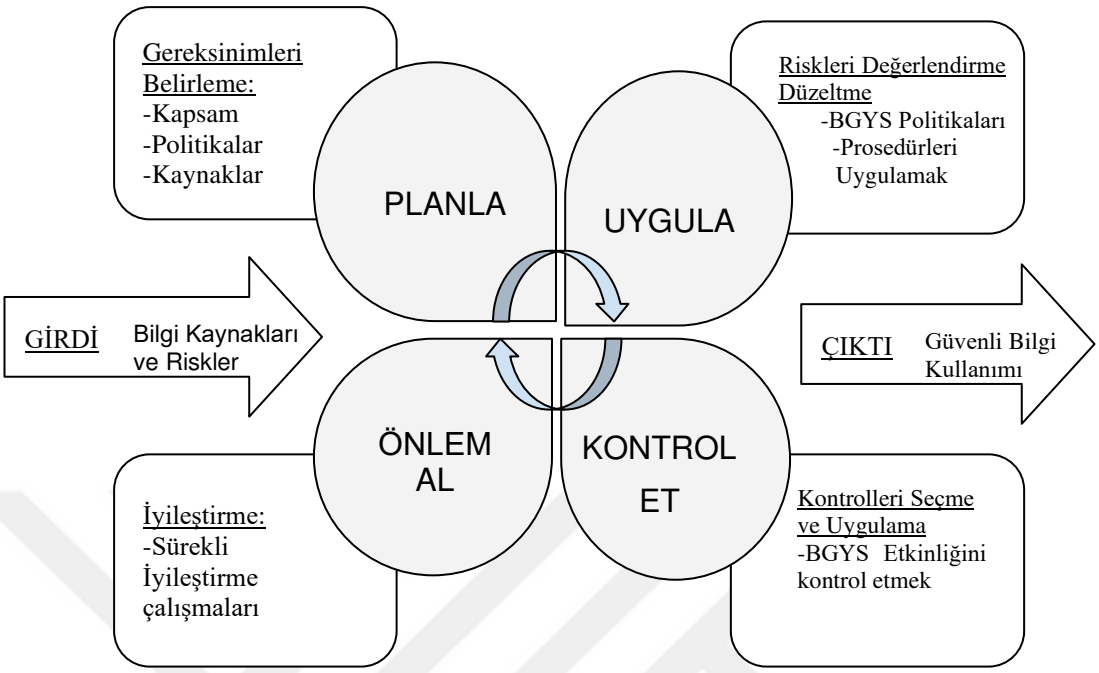
Kaynak: (Çubukçu, 2018)

PUKÖ döngüsündeki aşamalar sürdürülürken birçok dış faktörden etkilenmektedir. Bu nedenle PUKÖ döngüsüne göre planlanan faaliyetler uygulama aşamasında sürekli kontrol edilmesi gerekmektedir. Kontrollerden elde edilen olumsuz durumlar düzeltici faaliyetler ile iyileştirilmektedir. İş süreçlerinde değişen koşullar nedeniyle yapılan faaliyetler sürekli olarak tekrarlanmaktadır. Eğer PUKÖ döngüsün ilk uygulanan sürecinde sağlanan iyi sonuçlar sürekli olarak geçerli olsaydı kuruluşların yönetim sistemleri çok daha rahat işleyecekti. Fakat değişen koşullar yapılan faaliyetlerin niteliğini ve kalitesini etkilediğinden PUKÖ döngüsü sürekli olarak kullanılmaktadır (Akpınar ve Öğütoğulları, 2016).

4.4. PUKÖ Döngüsünün Aşamaları ve BGYS ile İlişkisi

BGYS' nin ana süreçleri olarak belirlenen görevler, PUKÖ döngüsüne göre düzenlenmekte ve uygulanmaktadır. PUKÖ döngüsüne göre planlanan bilgi güvenliği yönetim sistemi, girdileri işleyerek bir faydaya veya çıktıya dönüştürmektedir. Şekil 4.2'de BGYS'de işletilen süreçler ile PUKÖ döngüsü arasındaki ilişki gösterilmektedir (Çubukçu, 2018). BGYS'de yer alan her sürecin PUKÖ döngüsündeki bir aşamaya denk düştüğü görülmektedir. Bu süreç etkileşim şeması, BGYS'deki ana süreçlerin alt süreçlerle (risk yönetimi, varlık yönetimi, dokümantasyon, yönetimin gözden geçirmesi, iç tetkik, düzeltici faaliyetler, kaynak yönetimi, ihlal olayları yönetimi, iş sürekliliği yönetimi vb.) ve faaliyetlerle etkileşimini de göstermektedir.

Şekil 4.2: PUKÖ ile BGYS süreçlerinin etkileşimi



Kaynak: (Çubukçu, 2018)

PUKÖ döngüsünde yer alan her aşama bilgi güvenliği yönetim sisteminde işletilen süreçlerin temelini oluşturmaktadır. Dört ana grup altında toplanan BGYS süreçleri PUKÖ döngüsü gibi süreklilik arz etmektedir. Bu sürekliliktekı temel amaç bilgi güvenliği yönetim sisteminin kritik başarı faktörünü arttırmaktadır. Aşağıda BGYS' de yürütülen süreçler dikkate alınarak PUKÖ döngüsünde yer alan aşamalar alt başlıklar halinde ifade edilmektedir.

4.4.1. Planla

Planlama aşaması, bilgi güvenliği yönetim sisteminin amaç ve hedefleri doğrultusunda tasarımı ve kurulmasını kapsamaktadır. BGYS'nin kurulması, güvenlik politikaları ve prosedürlerin hazırlanması, üst yönetimin ve görevlerinin belirlenmesi, bilgi güvenliği personelinin atanması, gerekli yazılım ve donanımların belirlenmesi, bilgi varlıklarının envanterinin çıkarılması ve risk analizleri gibi birtakım faaliyet ve görevler yürütülmektedir. Bu aşmada bilgi güvenliği yönetim sistemine yönelik üzerinde durulan görevler şu biçimde sıralanmaktadır (Derdiyok, 2019; Çubukçu, 2018; Çalık, 2013; Ganbat, 2013; Ersoy, 2012; Aslandağ, 2010; Vural ve Sağıroğlu, 2008):

- BGYS'nin üst yönetimini belirlenmesi, desteğinin alınması ve bu yönetimin kararlar alması,
- BGYS grubunda yer alacak üyelerin seçilmesi, atanması ve görevlerinin belirlenmesi,
- Kurumun mevcut durumundaki bilgi güvenliği eksikliklerin belirlenmesi,
- BGYS hedeflerinin belirlenmesi ve dökümante edilmesi,
- BGYS kısa ve uzun süreli yatırım planlarının yapılması ve dökümante edilmesi,
- Bilgi güvenliği politikasının hazırlanması ve bir döküman olarak sunulması,
- BGYS'nin kapsamını ve bağlamını açıklayan metinlerin hazırlanması,
- BGYS kapsamı içindeki bilgi varlıklarının belirlenmesi ve varlık envanterinin oluşturulması,
- Süreçler ve bilgi varlıkları temelinde risk analizi ve değerlendirme çalışmalarının yapılması, risk metodojisi ve değerlendirme raporunun hazırlanması,
- Risklere karşı alınacak önlemler ve kontrollerin belirlenmesi, kontrol listelerinin oluşturulması,
- Uygulanabilirlik durumunun hazırlanması,
- Dokümantasyon sisteminin belirlenmesi,
- BGYS politikalarının ve prosedürlerinin hazırlanması,
- BGYS ile ilgili form, tablo, iş akışları gibi diğer dokümanların hazırlanması,
- İç ve dış birimler ile iletişim planının hazırlanması,
- İnsan kaynakları departmanına düşen görevlerin belirlenmesi ve ilgili doküman güncellemelerinin yapılması,
- Tedarikçi ve dış paydaş ilişkilerinin planlanması ve ilgili doküman güncellemelerinin yapılması.

4.4.2. Uygula

Bu aşama, önceki aşamada planlanan BGYS görevleri gerçekleştirilmektedir. Planlama aşamasında hazırlanan politika ve prosedürler uygulanmaktadır. Bu aşamada bilgi güvenliği yönetim sistemine yönelik üzerinde durulan görevler şu biçimde sıralanmaktadır (Derdiyok, 2019; Çubukçu, 2018; Çalık, 2013; Ganbat, 2013; Ersoy, 2012; Aslandağ, 2010; Vural ve Sağıroğlu, 2008):

- Seçilen kontroller ile ilgili uygulamaların yapılması,
- Düzenli yapılan işlemlerin (izleme, kapasite kontrol, bakım, arıza, vb.) kontrolü için hazırlanan kontrol listelerinin uygulanması,
- BGYS performansının izlenmesi, ölçülmesi, analiz edilmesi, uygun yöntemlerin belirlenmesi ve düzenli aralıklar ile uygulanması,
- Risklerin işlenmesi, risklere karşı uygun önlemlerin alınması ve riskleri azaltma çalışmalarının yapılması,
- Yapılan değişiklik işlemlerinin yönetilmesi,
- İş sürekliliği planlarının düzenli aralıklar ile test edilmesi,
- Yeni işe giren ve mevcut personele düzenli aralıklarla BGYS eğitimlerinin verilmesi,
- Tespit edilen risklerin gözden geçirilmesi, riskleri gidermek için tespit edilen eylemlerin değerlendirilmesi ve planlama aşamasında tamamlanan çıktıların gözden geçirilmesi için BGYS komitesinin toplanması,

4.4.3. Kontrol Et

Bu aşamada BGYS'nin izlenmesi ve gözden geçirilmesi işlemleri tamamlanmaktadır. BGYS kapsamında belirlenen faaliyetlerin performansının değerlendirilmesi ve raporlanması bu süreçte yapılmaktadır. Bu aşamada bilgi güvenliği yönetim sistemine yönelik iç tetkik, izleme, ölçme, analiz ve değerlendirme, yönetim ve dokümanların gözden geçirilmesi alt süreçleri işletilmektedir. Bu alt süreçler kapsamında yapılan görevler şu biçimde sıralanmaktadır (Derdiyok, 2019; Çubukçu, 2018; Çalık, 2013; Ganbat, 2013; Ersoy, 2012; Aslandağ, 2010; Vural ve Sağıroğlu, 2008):

- Bilgi güvenliği politikalarının, prosedürlerinin ve uygulamalarının etkinliğinin kontrol edilmesi,
- Birimler arasında bütünlüğün sağlanması ve çalışanların bilgi güvenliği farkındalığının kontrolünün yapılması,
- Belirli aralıklar ile iç tetkiklerin yapılması ve sonuçlarının üst yönetime raporlanması,
- BGYS'nin uygunluğunun, doğruluğunun ve etkinliğinin belirli aralıklar ile üst yönetim tarafından gözden geçirilmesi,

- BGYS'nin performansı uygun yöntemler belirlenerek düzenli aralıklar ile izlenmesi, ölçülmesi, analiz edilmesi,
- BGYS dokümanlarının gözden geçirilmesi ve revize edilmesi.

4.4.4. Önlem Al

Bu aşamada ise BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi işlemeleri yapılmaktadır. Üst yönetimin gözden geçirme sonuçlarına göre düzeltici ve önleyici faaliyetler sürdürülmektedir. Bu aşamada bilgi güvenliği yönetim sistemine yönelik üzerinde durulan görevler şu biçimde sıralanmaktadır (Derdiyok, 2019; Çubukçu, 2018; Çalık, 2013; Ganbat, 2013; Ersoy, 2012; Aslandağ, 2010; Vural ve Sağıroğlu, 2008):

- İç ve dış denetimler, güvenlik ihlal oylarının tespiti, açıklık testleri, değişen yasalar ve müşteri koşulları, risk kayıtları, yönetim gözden geçirme raporları ve diğer düzeltme istekleri doğrultusunda düzeltici faaliyetlerin sağlanması,
- Kontrol et aşamasında tespit edilen değişiklik ve iyileştirmelere göre güncellenen planın hayata geçirilmesi ve yapılan değişikliklerin ilgili paydaşlara duyurulması.

4.5. BGYS'nin Başarı Faktörleri ve Faydaları

Bir kuruluşun iş hedeflerine ulaşması, BGYS' nin başarılı bir şekilde uygulanmasına dayanmaktadır. Başarılı bir BGYS'nin uygulanması ise kritik öneme sahip birtakım faktörlere bağlı oluşmaktadır. BGYS, bir kuruluşun bilgi varlıklarını korumak için gereken kritik başarı faktörlerini tutarlı bir şekilde elde etme olasılığını artırmaktadır. BGYS'nin başarısını etkileyen kritik öneme sahip faktörlerin bir kısmı şunlardır (Gencer, 2015; Dister, 2013):

- Bilgi güvenliği politikasının amaçları ve hedefleri ile uyumlu faaliyetler,
- Kurum kültürüne uygun bilgi güvenliğinin tasarlanması, uygulanması, izlenmesi, sürdürülmesi ve geliştirilmesine yönelik bir yaklaşım ve çerçeve,
- Üst yönetim başta olmak üzere tüm yönetim kademelerinden görünür destek ve bağlılık,
- Bilgi güvenliği risk yönetiminin uygulanmasıyla elde edilen bilgi varlığı koruma gereksinimlerinin anlaşılması,

- Etkili bir bilgi güvenliği eğitim ve öğretim programı,
- Etkin bir bilgi güvenliği olay yönetimi süreci;
- Etkili bir iş sürekliliği yönetim yaklaşımı,
- Bilgi güvenliği yönetimindeki performansı değerlendirmek için kullanılan bir ölçüm sistemi ve iyileştirme için geri bildirim önerileri.

BGYS uygulamasının faydaları öncelikle bilgi güvenliği olaylarının neden olduğu risklerin azaltılmasına bağlı olarak sağlanmaktadır. BGYS'de benimsenen bilgi güvenliği standartları kuruluşun iş hedeflerinde sürdürülebilir başarı sağlamaktadır. BGYS'nin standartlara dayandırılması kuruluş için birçok fayda içermektedir. Bu faydalar şunlardır (Ganbat, 2013; Haklı, 2012; Bingöl, 2010):

- Kuruluşun farklı operasyon ve sahalardaki ihtiyaçlarını karşılayan kapsamlı, uygun maliyetli, değer yaratan, diğer sistemlerle entegre ve uyumlu bir BGYS sağlaması,
- Bilgi güvenliğinin bütünsel yönetimi konusunda işletme ve sistem sahiplerinin eğitilmesi,
- Kurumsal risk yönetimi bağlamında bilgi güvenliği yönetimine yönelik sorumluluklarını tutarlı bir şekilde yönetme ve işletme konusunda yardım etmesi,
- Genel kabul görmüş, iyi bilgi güvenliği uygulamalarının kuralcı olmayan bir şekilde teşvik edilmesi,
- Kuruluşlara kendi özel koşullarına uygun ilgili kontrolleri benimseme, iyileştirme ve bunları iç ve dış değişiklikler karşısında sürdürme özgürlüğü vermesi,
- Bilgi güvenliği için ortak bir dil ve kavramsal temelin sağlanması,
- Paydaşların kuruluşa duyduğu güvenin artması,
- Toplumsal ihtiyaç ve beklentilerin karşılanması,
- Bilgi güvenliği yatırımlarının daha etkin ekonomik yönetimi.

5. ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ

Çalışmanın bu bölümünde üniversite kütüphaneleri ve kütüphanelerde bilgi güvenliği yönetimi üzerinde durulmaktadır. Alanyazındaki çalışmalardan elde edilen veriler neticesinde kütüphanelerde ne tür bilgi güvenliği sorunlarının olduğu ve sorunlara karşı hangi çözüm önerilerinin getirildiği, ayrıca kütüphanelerdeki bilgi varlıklarının neleri kapsadığı üzerinde açıklamalarda bulunulmaktadır.

5.1. Üniversite Kütüphanelerinde Bilgi Güvenliğinin Önemi

İçinde bulunduğumuz çağın en değerli ürünü hiç kuşkusuz bilgidir. Bilgi çağı olarak adlandırılan bu çağın toplumuna ise bilgi toplumu denmektedir. Üniversiteler ise bu toplum yapısının gelişmesinde önderlik yapan kurumların başında gelmektedir. Bilgininin ekonomik, kültürel, sosyal ve sanatsal bir değer olarak işlendiği bu kurumlar, içinde bulunduğu toplumun bilgi seviyesine katkı sağlamaktadır. Bu nedenle bilgi ve bilgi varlıkları üniversitelerin dolayısıyla da üniversite kütüphanelerinin temel hazinesini oluşturmaktadır.

Güncel gelişmeleri takip eden iyi organize olmuş bir üniversite kütüphanesi bilim dünyası için önemli bir bilgi merkezi olarak kabul görmektedir. Bir üniversite kütüphanesinin amacı ve misyonu, üniversitenin amaç ve misyonundan ayrı düşünülemez. Bu çerçevede üniversite kütüphanelerinin görevleri şu maddelerle sıralanabilir (Çelik, 2000):

- Üniversitenin hedeflerine ulaşması için yeterli sayı ve kalitede personelin sağlanması,
- Kullanıcıların eğitim ve araştırma faaliyetleri için gerekli olan çeşitli bilgi kaynaklarını sağlamak,
- Bilgi kaynaklarının daha verimli kullanılabilmesine yönelik sağlayan danışma, ödünç verme, bibliyografik künye paylaşımı gibi hizmetler vermek,
- Farklı amaçlara hitap eden okuma ve çalışma alanları sağlamak ve düzenlemek,
- Kullanıcıların okuma ve araştırma alışkanlıklarını geliştirmelerine ve boş zamanlarını iyi değerlendirmelerine yardımcı olmak,

- Kütüphanelerin ve kütüphane kaynaklarının kullanımını artırmak için kullanıcı eğitim programlarının planlanması ve geliştirilmesini sağlamak,
- Makale, bildiri ve kitap gibi çeşitli kaynakları indekslenmek,
- Diğer kütüphaneler ve kuruluşlarla işbirliği sağlamak,
- Gelecek nesiller için koleksiyonları korumak.

Üniversite kütüphaneleri, bilimsel bilgiye erişim merkezlerinden biridir. Öğrenciler, akademisyenler ve araştırmacılar için zengin bir bilgi kaynağı sunmaktadırlar. Dijital dönüşümün hız kazandığı günümüzde, bu kütüphanelerdeki bilgilerin güvenliği büyük önem taşımaktadır. Bilgi güvenliği, kütüphane bilgi sistemlerinde işlenen ve depolanan kurumsal ve kişisel bilgilerin korunması ve veri bütünlüğünü sağlamayı amaçlayan bir disiplindir. Üniversite kütüphanelerinde iyi bir bilgi güvenliği yönetim anlayışı, akademik araştırmaların doğruluğunu ve güvenilirliğini sağlamak için kritik bir faktördür. Bu bağlamda üniversite kütüphaneleri, kullanıcılarına güvenli bir ortam sunmalı, veri güvenliği konusunda gerekli önlemleri almalı ve bilgi güvenliği politikalarını etkin bir şekilde uygulamalıdır.

Üniversite kütüphanelerindeki bilgi varlıkları, çeşitli tehditlere maruz kalabilir. Bilgi varlıklarında depolanan hassas bilgiler, öğrenci ve araştırmacıların kişisel verileri, telif haklarına tabi yayınlar ve diğer değerli bilgilerin yetkisiz kişilerin eline geçmesi, ciddi sonuçlar doğurabilir ve akademik etiği, güvenilirliği ve itibarı tehlikeye atabilir. Bu nedenle, üniversite kütüphaneleri, bilgi güvenliği politikalarını güncellemeli, güvenlik önlemlerini güçlendirmeli, personel ve kullanıcılarına bilgi güvenliği konusunda farkındalık çalışmaları yürüterek onların bilgi güvenliği farkındalık seviyelerini arttırmalıdır. Böylece, kütüphanelerdeki bilgilerin gizliliği, bütünlüğü ve erişilebilirliği korunabilir, güvenli bir öğrenme ve araştırma ortamı sağlanabilir.

Üniversite kütüphanelerinde bilgi güvenliği, bir dizi faktörü içeren geniş bir kapsama sahiptir. İlk olarak, kütüphanelerde bulunan bilgilerin gizliliği korunmalıdır. Öğrencilerin ve araştırmacıların kişisel verileri, telif haklarına tabi yayınlar ve diğer hassas bilgiler, yetkisiz erişimlere karşı korunmalıdır. Bilginin sızdırılması veya kötüye kullanılması, hem bireysel gizlilik haklarını ihlal eder hem de kütüphanelerin güvenilirliğini ve itibarını zedeler.

Bunun yanı sıra, veri bütünlüğü de büyük bir öneme sahiptir. Kütüphanelerde depolanan bilgilerin değiştirilmeden, bozulmadan veya kaybolmadan korunması gerekmektedir. Bilginin bütünlüğüne yönelik herhangi bir müdahale, araştırmaların doğruluğunu ve güvenilirliğini tehlikeye atabilir. Bu nedenle, kütüphaneler verileri yedekleme, doğrulama ve güncelleme gibi önleme mekanizmaları ile korumalıdır.

Ayrıca, erişilebilirlik de bilgi güvenliğinin bir unsuru olarak ele alınmalıdır. Kullanıcıların sorunsuz bir şekilde bilgiye erişebilmeleri sağlanmalıdır. Ancak, bu erişimin yetkilendirilmemiş kişilere engellenmesi de önemlidir. Güçlü kimlik doğrulama sistemleri, parola yönetimi ve ağ güvenliği gibi önlemler, yetkilendirilmemiş erişimleri önlemek için önemli adımlardır. Kullanıcıların verilere sadece gerekli yetki düzeyiyle erişim sağlaması, bilginin güvenliğini artırır ve yetkilendirilmemiş erişimlerin önüne geçer.

IFLA (International Federation of Library Associations)'nın yayımladığı kütüphane ortamının gizliliği bildiriminde (IFLA Statement on Privacy in the Library Environment), teknolojideki hızlı ilerlemelerin kütüphanelerin bilgi hizmetlerini ve dolayısıyla kullanıcılarının mahremiyetini etkilediği vurgulanmaktadır. Kütüphaneler, hizmetlerinde kullandığı bilgi varlıklarında çeşitli bilgi ve veriler barındırmaktadır. Bu bilgi ve verilerin içerisinde kurumsal bilgilerin yanı sıra personel, kullanıcı ve hatta diğer paydaşların bilgi ve verileri de yer almaktadır. Bu bilgi ve veriler gerek istatistik verilerin elde edilmesi için gerekse ticari amaçlar için hem kütüphaneler tarafından hem de kütüphanelerin ilişki içerilesinde olduğu ticari kurumlar tarafından kullanılabilmektedir. Ayrıca bilgi sistemlerine yapılan saldırılar veya fiziksel girişimler ile bu bilgi ve veriler ifşa edilebilmektedir. Bu itibarla IFLA, İnsan Hakları Evrensel Beyannamesine de dayanarak yayımladığı bu beyannamede, bilgiye erişim ve ifade özgürlüğünün kütüphane ve bilgi mesleği için temel kavramlar olduğunu ve gizliliğin ise bu hakları sağlamanın ayrılmaz bir parçası olduğunu belirtmektedir. IFLA, kütüphanelerde gizliliğin sağlanması için yayımladığı bu beyannamede şu önerileri sunmaktadır (IFLA, 2015):

- Kütüphane ve bilgi hizmetleri, mahremiyete hem uygulama düzeyinde hem de ilke olarak saygı göstermeli ve geliştirmelidir.
- Kütüphane ve bilgi hizmetleri, bireylerin mahremiyetini ve dijital haklarını korumak için ulusal, bölgesel ve uluslararası düzeyde savunuculuk çabalarını

desteklemeli ve kütüphane çalışanlarını bu konular üzerinde bilinçlendirmeye teşvik etmelidir.

- Kütüphane ve bilgi hizmetleri, elektronik gözetimi ve kullanıcıların kişisel verilerinin her türlü gayri meşru izlenmesini, toplanmasını veya mahremiyetlerini tehlikeye atacak ve bilgi arama, alma ve verme haklarını etkileyecek bilgi davranışlarını engelleyici önlemler almalıdır. Kurumsal ve kişisel bilgilerin toplanmasını sınırlamak için kontrol mekanizmalarını uygulamalıdır.
- Devletin, kullanıcıların verilerine erişimi ve veri gözetimi tamamen önlenemese de kütüphane ve bilgi hizmetleri, kullanıcıların bilgilerine veya iletişimlerine devlet tarafından izinsiz girilmesinin meşru ilkeler ve amaçlar çerçevesinde yapılmasını ve orantılı olmasını sağlamalıdır.
- Kütüphane ve bilgi hizmetleri, kullanıcıların mahremiyetini tehlikeye atabilecek kaynaklara, hizmetlere veya teknolojiye erişim sağladığında kullanıcıları sonuçlarından farkında olmaya teşvik etmeli, veri koruma ve mahremiyetin korunması konusunda rehberlik sağlamalıdır.
- Kütüphane ve bilgi hizmetleri, kullanıcılarının bilinçli seçimler yapma, meşru eylemlerde bulunma, iletişimlerinde ve internet üzerindeki hizmetlerin kullanımında riskleri ve faydaları bilme becerilerini desteklemelidir.
- Veri ve mahremiyetin korunması, kütüphane ve bilgi hizmeti kullanıcıları için medya ve bilgi okuryazarlığı eğitiminin bir parçası olarak dâhil edilmelidir. Kullanıcıların mahremiyetlerini korumak için kullanılacak araçlarla ilgili eğitimler düzenlenmelidir.
- Kütüphane ve bilgi uzmanlarının eğitimi, ağ ortamındaki veri ve mahremiyet koruma ilkelerini ve uygulamalarını içermelidir.

Bilgi güvenliği konusunu doğrudan ele alan bu belge dışında IFLA Etik Kuralları (2012) adıyla bilgi kullanımı konusunu kapsayan ikinci bir belge daha yayımlanıştır. Bu belgede, kütüphanecilerin ve bilgi çalışanlarının mesleki etik konularında bilinçlenmelerini ve politikalar oluşturabilmelerini sağlamak amacıyla rehberlik sağlamaktadır. Ayrıca, kütüphane çalışanlarının karşılaşabilecekleri etik ikilemleri çözebilmeleri için ilkeler sunmaktadır.

IFLA Etik Kuralları (2012), bireysel kütüphaneciler ve bilgi çalışanları yanı sıra tüm sektördeki profesyonellere de rehberlik etmektedir. Bu belgede, kütüphanecilerin etik davranış standartları ve sorumlulukları vurgulanmaktadır. Kütüphanecilerin, kullanıcılarına hizmet sunarken dürüstlük, tarafsızlık, gizlilik ve saygı gibi değerlere bağlı kalmaları teşvik edilmektedir. Ayrıca, mesleklerine yönelik öz farkındalıklarını artırmaları konusunda hedefler sunulmaktadır. Kütüphanecilerin mesleki gelişimlerini desteklemek, etiksel düşünme ve refleksif uygulama becerilerini geliştirmek için ilke ve kuralların önerildiği bu belgede, kütüphanecilerin toplumun çeşitli gruplarına hizmet sunarken kültürel ve sosyal çeşitlilik konusunda duyarlı olmaları belirtilmektedir.

IFLA Etik Kuralları (2012) belgesi özetle, kütüphanecilerin ve bilgi çalışanlarının şeffaflık ve hesap verebilirlik ilkelerine uymalarını vurgular. Kullanıcılara ve genel olarak topluma açık ve güvenilir hizmet sunma, bilgiye erişim hakkının korunması ve bilgi özgürlüğünün teşvik edilmesi gibi konular üzerinde durur. Kütüphaneciler ve diğer bilgi çalışanları için etik değerlere dayalı bir çerçeve sunar.

Bu belge, mesleki davranışın ve sorumlulukların temelini oluşturur ve kütüphanecilik mesleğinin topluma olan değerini artırmayı hedefler. Bu itibarla beş temel etik kural üzerinde durulmaktadır (IFLA, 2012):

- Bilgiye erişim,
- Bireyler ve topluma karşı sorumluluklar,
- Mahremiyet, gizlilik ve şeffaflık,
- Açık erişim ve telif hakları,
- Tarafsızlık, dürüstlük ve profesyonel beceriler,

Etik kurallarının tanımlandığı bu belgenin mahremiyet, gizlilik ve şeffaflık başlığı altında kütüphaneciler ve diğer bilgi çalışanlarının, kişisel mahremiyete ve kişisel verilerin korunmasına karşı tutumları belirtilmektedir. Kütüphaneciler ve diğer bilgi çalışanlarının kurumundaki bilgi ve bilgi varlıklarının şeffaflığını sağlamakla yükümlü olduğunu ve bu bilgi varlıklarının suiistimal, yolsuzluk ve ifşa edilmemesi konusunda kamu ve kişisel yararına göre hareket etmeleri gerektiği belirtilmektedir. Kütüphane ile kullanıcı arasındaki ilişkinin bir gizlilik ilişkisi içerisinde yürütülmesi

ve kullanıcı verilerinin kütüphane işlemlerinin ötesinde paylaşılmamasını sağlamak için uygun önlemlerin alınması gerektiği vurgulanmaktadır.

Dijital teknolojinin günlük hayatımıza sağladığı faydalar gün geçtikçe artmaktadır. Dijital teknolojinin birçok avantajını yanı sıra çevrimiçi araçlarla yaydığımız veriler mahremiyetimiz üzerinde ciddi etkiler oluşturmaktadır. Teknolojiyi kendi başına nötr olarak kabul etsek de, etkileri öyle ciddi sorunları da beraberinde getirmektedir. Bu sorunların başında ise bilgi veya veri gizliliğinin sağlanamaması gelmektedir.

Kütüphaneler mahremiyetin desteklenmesinde ve korunmasında güçlü bir rol oynamaktadır. Kütüphanelerde teknolojik ve kurumsal güvenlik önlemleri kullanılarak mahremiyet değerine sahip tüm bilgiler korunması gerekmektedir. Örneğin, kullanıcıların çevrimiçi kaynaklara erişimi sağlanırken, güvenli internet bağlantıları ve güncel güvenlik yazılımları kullanmaları sağlanmalıdır. Kullanıcıların çevrimiçi aktivitelerinin izlenmesini, takip edilmesini veya kaydedilmesini engellemek için gerekli önlemleri alması gerekir. Kütüphaneler kullanıcıların gizlilik haklarını savunmak ve toplumda bilinç oluşturmak amacıyla yasal düzenlemelere uygun hareket etmelidir. Kullanıcıların kişisel bilgilerini gizli tutma hakkında aktif bir savunuculuk rolü üstlenmelidir. Kütüphane çalışanları, kullanıcılara mahremiyetin önemi ve bilgi gizliliği konusunda farkındalık sağlamalı ve kullanıcılara gizlilik konusunda danışmanlık yapmalıdır. Sonuç olarak, kütüphaneler tüm bileşenleriyle bilgi varlıklarında barındırdığı tüm bilgilerin mahremiyetini korunma yönünde güçlü bir rol oynamalıdır (Nyst ve Falchetta, 2017).

5.2. Üniversite Kütüphanelerinde Bilgi Güvenliği Sorunları ve Önlemleri

Üniversite kütüphanelerinde bilgi güvenliğine yönelik çeşitli sorunlarla karşı karşıya kalınmaktadır. Bu sorunlar, gelişen teknolojiler, artan dijital kaynak kullanımı ve kullanıcıların çeşitli ihtiyaçlarından kaynaklanabilir. Özellikle, kütüphanelerde depolanan ve kullanıcılara sunulan dijital veriler, siber saldırganların hedefi olabilir. Bu nedenle, kütüphaneler, güçlü bir güvenlik altyapısı oluşturmalı ve siber saldırılara karşı korunma tedbirleri almalıdır.

ACRL (2016)'nin "Yükseköğretim İçin Bilgi Okuryazarlığı Çerçevesi"nde bilgi okuryazarlığının gizlilik ve kişisel bilgi güvenliği konularına dikkat etmeyi teşvik ettiğini belirtmektedir. Bilgi okuryazarlığı eğitimi, bireylerin çevrimiçi

etkileşimlerinde gizlilik ve güvenlik konularında bilinçli seçimler yapmalarına yardımcı olmayı hedefler. Bununla birlikte, bu alanda daha fazla vurgu yapılması ve bilgi okuryazarlığının bu konularda daha kapsamlı bir eğitim sunması gerektiği ifade edilmektedir. Gizlilik ve güvenliğin çevrimiçi ortamda önemli konular olduğu ve bireylerin bu konularda bilinçli olmaları, kişisel bilgilerini korumaları ve güvenli çevrimiçi davranışlar sergilemelerinin büyük önem taşıdığı belirtilmektedir. Bilgi okuryazarlığı, bireyleri bu konularda bilinçlendirmek ve onları güvenli ve sorumlu çevrimiçi kullanıcılar haline getirmek için önemli bir araç olarak kullanılması gerektiği vurgulanmaktadır.

Kütüphaneler, öncelikle bilgi güvenliğine yönelik politikaların belirlemelidir. Bu politikalar, siber saldırılara karşı alınacak teknik önlemleri, veri güvenliği ve yedekleme prosedürlerini, kullanıcı bilgilerinin gizliliğini koruma yöntemlerini ve kullanıcıların bilgi güvenliği konusunda uyulması gereken kuralları kapsar. Bu politikaların düzenli olarak gözden geçirilmesi ve güncellenmesi önemlidir, çünkü bilgi güvenliği tehditleri sürekli olarak değişmekte ve gelişmektedir.

Kütüphaneler, aynı zamanda teknolojik çözümlerle bilgi güvenliğini desteklemelidir. Güçlü güvenlik duvarları, antivirüs ve antimalware yazılımları, güvenli veri depolama sistemleri ve yetkilendirme mekanizmaları gibi teknolojiler, kütüphanelerin bilgi güvenliğini sağlamada etkili araçlardır. Ayrıca, düzenli veri yedeklemeleri ve veri kaybını önlemek için güvenilir depolama yöntemleri kullanılması da önemlidir (Şişkin, 2020).

Kullanıcı gizliliği de üniversite kütüphanelerinde büyük bir önem taşımaktadır. Kullanıcıların ödünç aldıkları materyalleri, araştırma kayıtlarını ve diğer kişisel bilgilerini gizli tutmak için gerekli önlemler alınmalıdır. Bu önlemler, gizlilik politikalarının etkin bir şekilde uygulanması, veri paylaşımının sınırlı tutulması ve kullanıcı bilgilerinin yetkisiz erişimlere karşı korunmasıyla sağlanır. Kullanıcıların güvenli ve güvenilir bir ortamda bilgiye erişebilmeleri için kütüphaneler, gizlilik konusunda titizlikle hareket etmelidir (Henkoğlu, 2015).

Teknolojideki hızlı ilerleme, kütüphanelerde bilgi hizmetleri ve kullanıcılar için gizlilik uygulamalarının artmasına neden olmuştur. Bu durum, kütüphanelerin kullanıcı bilgileri gizliliğini korumak için daha fazla dikkat etmesi gerektiği

anlamına gelir. Geleneksel olarak kütüphaneler, kullanıcıların gizliliğini ön planda tutan kuruluşlar olarak bilinirler. Ancak, dijital dönüşüm ve veri toplama teknolojilerindeki ilerlemeler, bu konuda yeni zorluklar ortaya çıkarmıştır.

Kütüphaneler, bilgi hizmetleri sunmak için internet hizmetlerini kullanmakta ve bu süreçte kullanıcılar ve davranışları hakkında kapsamlı veriler toplamaktadır. Örneğin, kullanıcıların internete erişimini sağlamak için ticari internet hizmetlerini kullanabilirler. Bu durumda kütüphaneler, kullanıcıların internet kullanımı hakkında bilgileri toplayabilir ve bu verileri hizmetlerin iyileştirilmesi veya kişiselleştirilmesi amacıyla kullanabilir. Bununla birlikte, kütüphaneler bu verileri gizli tutmalı ve kullanıcıların izni olmadan üçüncü taraflarla paylaşmamalıdır. Kullanıcılarla ilgili veriler, diğer sistemlere aktarılabilir ve farklı kurumlar arasında paylaşılabilir. Bu veri paylaşımı sürecinde kullanıcı gizliliğini korumak ve kişisel bilgilerin güvenliğini sağlamak için gerekli önlemleri almalıdır. Kullanıcı verilerini sadece hizmet sunmak veya kullanıcının taleplerini yerine getirmek amacıyla kullanmalıdır (Çelik, 2019).

Aşırı veri toplama ve kullanımı, bireysel kullanıcıların mahremiyetini tehdit etmekte ve başka sosyal ve yasal sonuçlara yol açmaktadır. İnternet kullanıcıları, büyük ölçekli veri toplama ve gözetlemenin farkında olduklarında beklenmedik sonuçlardan korktukları için davranışlarını sansürleyebilmektedir. Aşırı veri toplamanın toplum üzerinde caydırıcı bir etkisi olabilmekte ve algılanan bu tehdidin bir sonucu olarak bireyin konuşma ve ifade özgürlüğü hakkını daraltabilmektedir. İnsan Hakları Evrensel Beyannamesi'nin 19. maddesinde ifade edilen bilgiye erişim özgürlüğü ve ifade özgürlüğü, kütüphane ve bilgi mesleği için temel kavramlar olarak ifade edilmektedir. Gizlilik ise bu hakları sağlamanın ayrılmaz bir parçasıdır (IFLA, 2015).

IFLA internet bildirgesinde (IFLA ve Kuhlenkamp, 2015), kütüphane ve bilgi hizmetleri, kullanıcılarının gizliliğini ve kullandıkları kaynakların ve hizmetlerin gizli kalmasını sağlamaya çalışma sorumluluğuna sahip kurumlar olması gerektiği bildirilmektedir. Ayrıca IFLA kütüphaneciler ve diğer bilgi çalışanları için yayımladığı etik kuralları bildirgesinde (IFLA, 2012), kişisel mahremiyete saygıyı, kişisel verilerin korunmasını ve kullanıcı ile kütüphane arasındaki ilişkide gizliliği temel ilkeler olarak tanımlamaktadır.

Gizli bilgilerin yetkisiz, öngörülemeyen, kasıtlı veya kasıtsız ifşa edilmesinin etkileri ciddi sonuçlar doğurabilmektedir. Kişisel ve kurumsal bilgilerin ifşa edilmesi ile kütüphane güvenliğinin tehlikeye atılması; kütüphanelerin toplumdaki güven algısını kaybetmesine, yasal işlemlerin artmasına ve güvensiz bilgi işlem ortamı nedeniyle itibar kaybının yaşanmasına neden olabilmektedir (Stoneburner ve diğerleri, 2002).

Kütüphanelerde bilgi güvenliği planlamasında atılacak ilk adım, kütüphanenin hangi varlıkları korumaya ihtiyacı olduğunu belirlemek ve bu varlıkları korumanın neden gerekli olduğunu anlamaktır. Bu durum, bir kütüphanenin değerli varlıklarının karşı karşıya olduğu tehdit ve güvenlik açıklarının türleri hakkında bir farkındalık oluşturur.

Donanım, yazılım, fiziksel ortam, dokümantasyon ve diğer bilgi varlıkları olmak üzere tüm kütüphane bilgi sistemlerinin potansiyel tehditlerden korunması için gerekli önlemlere ihtiyaç duyulmaktadır. Kütüphanedeki bilgi varlıklarının güvenliği, kullanıcı mahremiyetinden ve yasal erişimden herhangi bir ödün verilmeksizin sağlanması gerekmektedir. Kütüphaneler, bilgi ve hizmetlerin bozulmamasını ve izinsiz değişikliklere uğramamasını garanti etmek için kütüphane sistemleri aracılığıyla depolanan, işlenen, aktarılan veya erişilen bilgilerin saldırılara karşı nasıl korunacağına karar vermesi gerekmektedir. Çünkü kütüphane bilgi sistemlerine izinsiz giriş yapan kişiler bu sistemler üzerinde yer alan kritik bilgileri çalabilmekte ve kötü amaçlarını gerçekleştirmek için kullanabilmektedir (Fox ve ElSherbiny, 2011).

Günümüzde çoğu kütüphane hizmetlerine ve bilgi kaynaklarına zaman ve yer kısıtlaması olmaksızın erişilebilmektedir. Kütüphane bilgi sistemlerin sağladığı bu erişim kolaylığı kütüphaneleri bilgi güvenliği açısından yeni risklere maruz bırakmaktadır. Çünkü kütüphane bilgi sistemlerine içeriden veya dışarıdan erişim sağlayan kötü niyetli kişiler bilgi ve kritik verileri ifşa edebilmektedir (Eisenberg ve Lawthers, 2008).

Kütüphanenin bilgi işlem ekipmanının ve ağlarının güvenliğini sağlamaktan sorumlu olan personelin, hassas veya özel bilgilerle ne zaman uğraşabileceklerini fark etme konusunda özel bir yükümlülükleri bulunmalıdır. Kurumsal ve kişisel bilgilere veya hassas bilgi içeren dosyalara erişimi olan kişilerin kütüphane etiği ve gizliliğine

ilişkin becerileri ve yetkinlikleri önemli görülmektedir. Hatta işleri doğrudan kütüphane hizmeti olmayan diğer personelin (güvenlik görevlileri, temizlik görevlileri, öğretmenler ve diğer eğitimciler vb.) de kütüphane etiği ve gizliliğine ilişkin güvenlik bilinci beklentileri bulunmaktadır. Kütüphane sistemlerinden sorumlu personel, düzenli olarak gizlilik denetimleri gerçekleştirmeli ve teknolojilerinin gizlilik standartlarını karşıladığından emin olmalıdır. Birçok endüstri veri toplamaya yönelirken, kütüphane sistemleri mümkün olan en az miktarda kullanıcı bilgisi toplayacak ve tutacak şekilde yapılandırılmalıdır. ALA kütüphanelerdeki kurumsal ve kişisel bilgilerin güvenliği için birtakım öneriler sunmaktadır. Bunlar şu şekilde sıralanmaktadır (ALA, 2006):

- Kişisel olarak tanımlanabilir bilgilerin toplanma, izlenme, ifşa edilme ve dağıtılma derecesini sınırlandırılması,
- Gereksiz kayıtlar oluşturmaktan kaçınılması,
- Kişisel olarak tanımlanabilir bilgilere erişimi, yetkili işlevleri yerine getiren personelle sınırlandırılması,
- Verilerle ilgili günlükler, dijital kayıtlar, satıcı tarafından toplanan veriler ve sistem yedeklemelerin tutulması ve kitaplığın verimliliği ve yasal işleyişi için gerekli olmadıkça kişisel olarak tanımlanabilir bilgiler içeren kütüphane kullanım kayıtlarını imha edilmesi,
- Bilgi teknolojileri birimi veya otomasyon sistemleri tarafından işlenen veya tutulan kütüphane kullanım kayıtlarının bilgi güvenliği politikalarına uygun olarak ele alınması,
- Saklanması gereken kayıtların güvenli ortamlarda muhafaza edildiğinden emin olunması,
- Kişisel olarak tanımlanabilir bilgileri kamuya açık hale getiren kütüphane uygulamalarından ve prosedürlerinden kaçınılması,
- Tedarikçi sözleşmelerinin tüm veri ve kayıtların kütüphane kontrolünü garanti etmesinin sağlanması,
- Kütüphane kullanıcıları ve çalışanları hakkındaki bilgilerin nasıl toplandığını, saklandığını, paylaşıldığını, kullanıldığını ve imha edildiğini inceleyen gizlilik denetimlerinin gerçekleştirilmesi gerekir.

5.3. Üniversite Kütüphanelerine Ait Bilgi Varlıkları

Bilgi bulunduğu ortam veya kullanıcı için bir anlam taşıyor ve fayda sağlıyor ise o zaman değerli bir varlıktır. Bu varlıklar, kütüphanelerin temel yapısını oluşturmaktadır. Cleveland (1999), bilgiyi "bir tür çevre" olarak tanımlamaktadır. Bilginin hava gibi solunduğunu ve bu süreçte bilginin değiştirildiğini belirtmektedir. Bir kitabın veya süreli yayının potansiyel kullanım amacıyla satın alındığında bilginin satın alınan birincil ürün olmadığını, satın alınan ürünün (kitap, süreli yayın, hatta videokaset, CD-Rom disk veya elektronik ortam) birden çok bilgi ögesini saklayan veya erişime sunan bir varlık olduğunu açıklamaktadır.

Üniversite kütüphaneleri, öğrenci ve akademisyenlerin araştırma, eğitim ve bilgiye erişim ihtiyaçlarını karşılamak amacıyla önemli bilgi varlıklarını barındıran kurumlardır. Bu kütüphaneler, genellikle geniş bir kitap ve dergi koleksiyonuna sahip olmanın yanı sıra dijital veritabanları, e-dergiler, e-kitaplar, tezler, araştırma makaleleri ve diğer akademik kaynaklar gibi çeşitli bilgi kaynaklarını kullanıcılarının erişimine sunmaktadır. Üniversite kütüphanelerinin bilgi güvenliği açısından değerli ve korunması gereken çeşitli bilgi varlıkları vardır. Bu varlıklar, bilgiye erişim, kullanım, paylaşım veya saklama süreçlerinde önemli bir rol oynayan her türlü bilgi veya kaynağı kapsamaktadır. Bilgi varlıkları, hem fiziksel hem de dijital ortamlarda bulunabilir.

Fiziksel bilgi varlıkları, kütüphanenin ofislerinde, kullanıcı alanlarında veya veri merkezlerinde bulunan donanım, dokümanlar, basılı materyaller ve diğer taşınabilir cihazları içerebilmektedir. Bu varlıklar, bilgisayarlar, sunucular, depolama cihazları, yazıcılar, belgeler, sözleşmeler, raporlar ve diğer fiziksel kaynaklardır. Bu tür varlıkların güvenliği, doğru bir erişim kontrolü, güvenli depolama ve koruma tedbirleri gerekir.

Dijital bilgi güvenliği varlıkları ise kütüphanenin bilgisayar sistemleri, ağları, veri tabanları, yazılımları, web siteleri, elektronik belgeler, e-posta hesapları, kullanıcı hesapları ve diğer dijital kaynakları içermektedir. Bu varlıklar, siber saldırılara, veri kaybına, yetkisiz erişime veya veri hırsızlığına karşı korunmalıdır. Bunun için güçlü parola politikaları, veri şifreleme, güvenlik duvarları, antivirüs yazılımları, güncel yazılım güvenlik yamaları ve diğer bilgi güvenlik önlemleri ile korunması gerekir.

Bilgi varlıklarının korunması, üniversite kütüphanelerinin iş sürekliliği, itibar ve rekabet avantajını sağlamak açısından kritik öneme sahiptir. Bu nedenle, kütüphaneler genellikle bilgi güvenliği politikaları, prosedürler ve teknolojik önlemler geliştirilmektedir. Bu politikalar ve önlemler, bilgiye erişimi sınırlayan, yetkilendirme ve kimlik doğrulama sistemleri, güvenlik duvarları, şifreleme teknikleri ve bilinçlendirme programları gibi çeşitli yöntemleri içerebilmektedir (Freeze ve Kulkarni, 2007).

Kütüphane ve bilgi hizmetleri hem maddi hem de maddi olmayan birçok bilgi varlığını içermektedir. Yirmi birinci yüzyılın ekonomik gerçekliğinde maddi olmayan varlıklar maddi varlıklarla birlikte, üniversite kütüphanelerinin genel değerine ve performansına kritik bir şekilde katkıda bulunmaktadır. Her iki sınıftaki bilgi varlıklarının işletilmesi ve korunması için özel yönetim faaliyetleri gerekmektedir. Maddi varlıklar, kütüphanelerin faaliyetlerini yürütebilmesi için sahip oldukları fiziksel varlıkları kapsamaktadır. Bunlar bina, tesis, envanter, demirbaş, ekipman, insan kaynağı ve fiziksel diğer ürünlerdir. Maddi olmayan varlık ise, maddi bir değeri olmayan fakat maddi varlıklar gibi bulunduğu ortama değer kazandıran varlık olarak yorumlanmaktadır. Maddi olmayan varlıkların başında bilgi gelmektedir. Ekonomi alanyazınında "maddi olmayan varlık" teriminin karşılığı olarak "entelektüel sermaye" terimi sıklıkla kullanılırken, yönetim bilimi alanyazınında ise "bilgi varlığı" terimi olarak kullanıldığı görülmektedir (Lev, 2001; McGinn, 2001).

Üniversite kütüphaneleri ve bilgi merkezleri, genellikle üniversite kampüslerinin merkezinde yer alan tarihi veya olması gereken albenili binalar olarak görülmektedir. Bu nedenle üniversite kütüphaneleri doğası gereği oldukça somut kurumlar olarak görülmektedir. Fakat bilgi teknolojisi ve internetin gelişmesi ve yaygınlaşmasıyla birlikte akademik kütüphaneler, bilgi teknolojilerinin doğası gereği soyut olan varlıklardan büyük ölçüde etkilenen kurum olarak bilgi hizmetleri camiasında daha rekabetçi faaliyet göstermektedir. Maddi olmayan varlıkların ekonominin tüm üretim modellerinde artan değeri, üniversite kütüphanelerini de önemli ölçüde etkilemiştir (Kostagiolas ve Asonitis, 2008). Bilgi çağına kadar daha çok bina ve derme gibi fiziksel maddi varlıkları ile değerlendirilen üniversite kütüphaneleri bilgi çağı ile birlikte bilginin manevi değeri açısından da değer kazanmıştır.

White (2007a; 2007b), çalışmalarında kütüphanelerin maddi olmayan varlıklarını insan sermayesi, kurumsal sermaye ve ilişkisel sermaye olarak üç temel grup içerisinde sınıflandırmaktadır:

- İnsan sermayesi varlıkları: Kütüphanelerin en değerli insan sermayesi varlıkları, çalışanlarıdır. Kütüphanelerdeki profesyonel personel, kütüphane hizmetlerini yönetme, kullanıcılara rehberlik etme, bilgi kaynaklarını düzenleme ve sürdürme gibi önemli rolleri üstlenir.
- Kurumsal (yapısal) sermaye varlıkları: Kütüphanelerin bilgi sistemleri, veritabanları, fiziksel altyapısı, teknolojik kaynakları ve koleksiyonları gibi unsurları içermektedir. Bu yapısal sermaye varlıkları, kütüphanelerin bilgiye erişim ve hizmet sunma yeteneklerini belirleyen önemli unsurlardır.
- İlişkisel sermaye varlıkları: Kullanıcı ilişkileri, akademisyenler ve konu uzmanları arasındaki işbirliği, personel içinde güven ve işbirliği, kullanıcı listeleri, resmi makamlarla yapılan anlaşmalar, itibar, marka adı vb. tüm bu soyut varlıklar, ilişkisel sermaye varlıklarının içerisinde değerlendirilmektedir. Kütüphaneler, ilişkisel sermaye varlıklarına da sahiptir. İlişkisel sermaye, kütüphanelerin kullanıcılar, akademisyenler, araştırmacılar ve diğer paydaşlarla kurdukları ilişkiler ve bu ilişkilerin değeridir. İlişkisel sermaye varlıkları, kütüphanelerin topluluklarla etkileşimde bulunma ve hizmet sunma yeteneklerini yansıtır.

Akademik bir kütüphanedeki soyut kaynakların miktarının artması, kütüphanenin çıktılarını çeşitlendirmekte ve bu camiadaki rekabet gücünü arttırmaktadır. Maddi olmayan varlıklara yapılan güvenlik yatırımları, üniversite kütüphanesi paydaşlarına (öğrenciler, akademisyenler, araştırmacılar vb.) ve üniversiteye değer katmaktadır. Maddi olmayan varlıklar, maddi varlıklardan yani geleneksel kütüphane kaynaklarından tamamen ayrı olarak görülmemelidir. Çünkü üniversite kütüphanelerindeki maddi olmayan varlıklar, diğer mevcut uygulamalar ve maddi varlıklar ile birlikte ele alındığında önemlidir. Aslında bu soyut varlıklar, kütüphanenin maddi olan basılı materyalleri, fiziksel ortamları ve geleneksel kaynakları içinde yer almaktadır (Epstein, Schneider, 2008; Broady-Preston ve Felice, 2006)

Kütüphane ve bilgi hizmetleri büyük ölçüde maddi olmayan varlıklara dayanmaktadır. Maddi olmayan varlıkların dinamik doğası ne kadar erken anlaşılırsa, akademik kütüphanelerin rekabet gücünün büyümesi ve artması o kadar büyük olabilir. Alanyazın incelendiğinde, yirmi birinci yüzyılın ekonomik gerçekliğinde, maddi olmayan varlıkların, maddi varlıklarla birlikte bir akademik kütüphanenin genel değerine kritik bir şekilde katkıda bulunduğu gerçeğinin farkına varılabilir. Bu nedenle, maddi olmayan duran varlıklarla ilgili özel yönetim eylemleri ve faaliyetleri gereklidir. Maddi olmayan duran varlıkların tanımlanması, geliştirilmesi ve değerlemesi ile ilgili açık ve etkin politikalar gerekli olmakla birlikte; maddi olmayan duran varlıklar, maddi duran varlıklardan ayrı görülmemelidir (Kostagiolas ve Asonitis, 2009).

Kütüphane ve bilgi hizmetleri büyük ölçüde maddi olmayan varlıklara dayanmaktadır. Maddi olmayan varlıkların dinamik doğası ne kadar erken anlaşılırsa, üniversite kütüphanelerinin rekabet gücünün büyümesi ve değerinin artması o kadar büyük olabilir. Yirmi birinci yüzyılın ekonomik gerçekliğinde, maddi olmayan varlıkların maddi varlıklarla birlikte üniversite kütüphanelerinin genel değerine kritik bir şekilde katkıda bulunmaktadır. Bu nedenle, maddi bilgi varlıklarının yönetimi ve güvenliği için gösterilen özenin maddi olmayan duran varlıklara da sağlanması önemlidir. Maddi olmayan bilgi varlıklarının tanımlanması, hizmete sunulması ve güvenliğini sağlanması ile ilgili açık ve etkin güvenlik ve yönetim politikalarının gerekliği ile birlikte; maddi olmayan bilgi varlıkların maddi bilgi varlıklardan ayrı görülmemesi gerekir (Fister, 2010).

Kütüphane hizmetleri, çeşitli formatlarda sunulan birçok bilgi öğesini barındırmaktadır (Öztemiz ve Yılmaz, 2013):

- Kütüphane hizmetlerinin yönetimi ile ilgili bilgi varlıkları: Kurumsal veriler, sözleşmeler, insan kaynakları verileri, mali veriler, bilgi yönetimi ile ilgili dokümanlar, kullanıcı hizmetleri verileri, güvenlik veriler, bina ve bakım-onarım verileri vb.
- Kütüphane koleksiyonları ile ilgili bilgi varlıkları: Basılı koleksiyondaki tüm materyaller, dijital materyaller, katalog bilgileri ve meta verileri vb.

- Teknolojik bilgi varlıkları: Bilgisayarlar, sunucular, yazıcılar, bellek aygıtları, mobil aygıtlar, telefonlar ve diğer iletişim araçları gibi donanımlar; uygulama, sistem ve gibi yazılımlar; ağlar, veri tabanları vb.
- Fiziksel ve çevresel bilgi varlıkları: Sistem odası, bilgi işlem ofisleri, arşiv odalar, ısıtma, aydınlatma, elektrik, klimalar gibi sistemler, danışmanlık hizmetleri, teknik destek hizmetleri, kiralık servisler, bina ve çevre güvenlik sistemleri vb.
- Kişisel bilgi varlıkları: Personel ve kullanıcıya ait kişisel bilgilerden oluşmaktadır.

Kişisel bilgi varlıkları üniversite kütüphanesi kullanıcıları ağırlıklı olarak barındığı bilgi varlıkları arasında yer almaktadır. Kullanıcı kayıt bilgileri temel olarak kullanıcı kimliği ve kullanıcı arka plan bilgilerini içermektedir. Kişisel kimlik bilgileri temel olarak kullanıcı adı, yaş, cinsiyet, irtibat telefonu, e-posta, adres gibi bilgilerden oluşmaktadır. Bu bilgilerin kütüphane ve kullanıcıları arasında gizli kalması ve kütüphaneler tarafından kullanıcıların meşru haklarının ve çıkarlarının korunması ve güvenini kazanması önemlidir (Gao, 2016).

5.4. Üniversite Kütüphanelerinde Bilgi Sistemlerinin İşlevi ve Güvenliği

Bilgi sistemleri, kütüphanelerde kullanılan yazılım, donanım ve ağ altyapılarından oluşmaktadır. Bu sistemler aracılığıyla kütüphane hizmetlerinin yönetimini desteklemekte, kaynaklar organize edilmekte, kullanıcıların bilgiye erişimi kolaylaştırılmakta ve diğer kütüphane süreçleri etkinleştirilmektedir. İşlevsel olarak, üniversite kütüphanelerindeki bilgi sistemlerinin temel görevleri şu şekilde sıralanmaktadır (Kazandır, 2011; Keskinkılıç, 2011; Tamdoğan, 2009; Güveli, 2006;Anameriç, 2005; 2003).

- Kataloglama ve üst veri yönetimi: Kütüphane koleksiyonlarının kataloglanması ve metaveri yönetimi için çeşitli otomasyon sistemleri kullanılmaktadır. Bu sistemler, kitaplar, dergiler, elektronik kaynaklar gibi materyallerin tanımlanması, sınıflandırılması ve etiketlenmesini sağlamaktadır. Kullanıcılar, bu sistemler aracılığıyla kütüphanedeki kaynaklara kolaylıkla erişebilmektedirler.

- Ödünç verme ve iade işlemleri: Ödünç verme ve iade işlemlerinin yönetiminde kullanılan sistemler aracılığıyla kullanıcılar, kütüphane sistemine kaydolarak kaynakları ödünç alabilmekte ve iade edebilmektedir. Sistem üzerinden kullanıcıların ödünç aldıkları kaynaklar takip edilebilmektedir.
- Elektronik kaynak yönetimi: Üniversite kütüphanelerinde elektronik kaynaklar, önemli bir yer tutmaktadır. Bilgi sistemleri, elektronik kaynakların yönetimini kolaylaştırmaktadır. Kullanıcılar, bu sistemler aracılığıyla elektronik dergi, veritabanı veya diğer çevrimiçi kaynaklara erişebilmektedirler. Ayrıca bu sistemler, lisanslama, erişim kontrolü ve kullanım istatistikleri gibi elektronik kaynak yönetimi süreçlerini de desteklemektedir.
- Kullanıcı hesap yönetimi: Kütüphane kullanıcılarının hesaplarının yönetildiği sistemler ile kullanıcılar, kütüphane sistemlerine kaydolabilmektedirler. Bu hesaplar, kullanıcıların kişisel bilgilerini, ödünç alma geçmişini ve diğer kütüphane hizmetlerini takip etmek için kullanılmaktadır.
- Veri analizi ve raporlama: Kütüphane verilerinin analiz edilmesi ve raporlanması için kullanılır. Kullanım istatistikleri, koleksiyon performansı, kullanıcı talepleri gibi veriler, sistem tarafından toplanır ve raporlar oluşturulur. Bu raporlar, kütüphane yöneticilerine stratejik kararlar almak ve hizmetlerini iyileştirmek için değerlendirme sağlar.
- Kütüphane yönetim sistemi: Bu sistemler, kütüphane işlemlerinin otomasyonunu sağlar. Koleksiyon yönetimi, satın alma süreçleri, envanter kontrolü, etkinlik planlama, personel yönetimi gibi kütüphane işlemleri, bilgi sistemleri üzerinden yürütülür.
- İnternet ve web hizmetleri: Üniversite kütüphanelerinin web siteleri ve diğer çevrimiçi hizmetleri de bilgi sistemleri tarafından desteklenmektedir. Kullanıcılar, kataloglara, dijital koleksiyonlara, elektronik kaynaklara ve diğer kütüphane hizmetlerine erişmek için web tabanlı arayüzleri kullanır. Bu hizmetler, bilgi sistemleri tarafından sağlanır ve güncellenir.
- Veri güvenliği ve yedekleme: Kütüphane verilerinin güvenliğinin ve yedeklemesinin sağlandığı sistemlerdir. Kullanıcı bilgileri, koleksiyon verileri

ve diğer kritik bilgiler bu sistemler tarafından korunur ve düzenli yedeklemeleri yapılır. Veri kaybı veya güvenlik ihlalleri durumunda, bu sistemlere yedeklenen bilgilerden geri yükleme yapılabilmektedir.

Üniversite kütüphanelerindeki bilgi sistemleri, kütüphane hizmetlerinin etkin ve verimli bir şekilde yürütülmesine yardımcı olmaktadır. Bu sistemler, kaynakların yönetimi, kullanıcı hizmetleri, veri analizi, otomasyon ve güvenlik gibi çeşitli işlevleri yerine getirerek kütüphanelerin bilgi kaynaklarını en iyi şekilde kullanmalarını sağlamaktadır. Bu sistemler üzerinde kayıtlı bilgiler üniversite kütüphaneleri için çok değerlidir. Bu nedenle üniversite kütüphanelerindeki bilgi sistemlerinin güvenliği büyük önem taşmaktadır. Çünkü bu sistemlerde yer alan bilgiler, kullanıcıların kişisel verileri, kütüphane koleksiyonlarına ilişkin bilgiler, finansal veriler ve diğer hassas bilgileri içerebilmektedir. Bu nedenle, kütüphaneler bilgi güvenliği önlemleri alarak bu bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumaya özen göstermek durumundadırlar.

Üniversitelerin gelişen akademik ve araştırma ortamına ayak uydurmak için üniversite kütüphaneleri, üretilen araştırma tezleri, akademik personel tarafından tamamlanan araştırma projeleri ve üniversite bünyesinde üretilen raporlar gibi birçok fikri varlığını dijital ortamlara aktararak ve bu ortamlardan erişime sunarak hizmet vermektedir. Dijital kaynaklar, geleneksel kütüphane materyallerine göre çeşitli avantajlara sahiptir; ancak, dijital kaynaklar güvenlik, mahremiyet ve uzun vadeli erişilebilirlik gibi konularda daha fazla dikkat gerektirmektedir. Kullanıcı bilgilerini ve kurumun fikri mülkiyetini (örneğin, araştırma raporları, tezler, doktora tezleri vb.) güvence altına almak amacıyla, üniversite kütüphanelerinin sınırlı veri ve bilgi güvenliği önlemlerini iyileştirmesi ve geliştirmesi gerekmektedir (Khan ve diğerleri, 2021).

Üniversite kütüphaneleri, teknoloji, bütçe, altyapı gibi birçok zorlukla karşı karşıya kalmaktadır ve aynı zamanda kullanıcılarına en iyi hizmeti sunmaya çalışırken bilgi güvenliği tehditleriyle de uğraşmaktadır. Fikri mülkiyetin bütünlüğünün korunması, veri hırsızlığı ve bozulmasının önlenmesi, özellikle gizlilik ve güvenlik konularının korunması, gelişen teknoloji ve bilgi güvenliği gereksinimlerinin yeni yönleri nedeniyle daha da önemli hale gelmektedir. Bu sorunlar, teknoloji kullanımının hızla arttığı ancak sağlam altyapı gelişiminin henüz başlangıç aşamasında olduğu

gelişmekte olan ülkelerde daha ciddi bir sorun olarak ortaya çıkmaktadır. (Nicolas-Rocca ve Burkhard, 2019).

Donanım, yazılım ve veriler, üniversite kütüphanelerinde kullanılan sistemlerin temelini oluşturmaktadır. Bu sistemler üzerinde meydana gelebilecek herhangi bir hata veya kusur, kullanıcı bilgi verilerinin silinmesine, değiştirilmesine veya açığa çıkmasına yol açabilmektedir. Bu nedenle, kullanıcı bilgilerinin gizliliği, kütüphane sistemlerinin güvenliğinin tam olarak sağlanmasına dayanmaktadır. Kapsamlı güvenlik, çok katmanlı bir koruma mimarisi ile sağlanabilir. Üniversite kütüphane sistemleri, fiziksel sistemler, yazılım sistemleri, ağ sistemleri ve yönetim sistemleri gibi çok katmanlı bir mimariye sahiptir (Pattanaik ve Viswakarma, 2014; Ismail, 2012).

Fiziksel sistem; sel, deprem, yangın, elektromanyetizma, hırsızlık gibi fiziksel tehditlere karşı üniversite kütüphanesinin temel tesislerini, işletim ekipmanlarını, bilgi sistemlerini ve diğer bilgi varlıklarını ifade etmektedir. Fiziksel sistem, kütüphane sisteminin normal çalışmasını ve kullanıcıların bilgi güvenliğinin sağlandığı donanım temelli çalışan sistemdir.

Yazılım sistemi, dijital kütüphane sistemindeki sunucu, istemci ve diğer bilgisayar ekipmanı üzerinde çalışan işletim sistemi, veri tabanı sistemi, sayısal bilgi sistemi ve diğer sistem yazılımlarını ifade etmektedir. Yazılım sistemi, üniversite kütüphanesi veri tabanı kaynaklarını ve dijital bilgi kaynaklarını koordine eden, yöneten ve çeşitli kaynakların performansına tam yetki veren kullanıcı bilgilerinin korunması temelli bir sitemdir.

Ağ sistemi, üniversite kütüphane sistemi için açık ağ ortamında etkin hizmetler sağlamaktadır. Ağ sistemi, üniversite kütüphane sisteminin güvenli çalışmasını ve etkili bilgi hizmetleri sağlamaktadır. Bu hizmetleri sağlarken bir taraftan da ağ üzerinden iletilen kullanıcı verilerinin ve bilgilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamakla yükümlüdür.

Yönetim sistemi ise üniversite kütüphane sisteminin günlük yönetim hizmetlerini, kütüphane operasyonlarını ve teknoloji biriminin temel işlevlerini kapsamaktadır. Bu sistem, tüm hizmet seviyelerdeki faaliyetlerin yönetiminin uygun bir biçimde planlanması, bilgisayar ağ yönetimi yaklaşımları ve kullanıcı normlarının

formülasyonu dâhil olmak üzere uygun çalışma sistemi ve kurumsal normların geliştirilmesi yoluyla tüm bilgi güvenliği sisteminin garanti altına almaktadır.

Üniversite kütüphanelerinin kullandığı bilgi sistemlerindeki yazılımlar, hem üretici firmalar hem de harici firmalar tarafından erişilebilir. Bu nedenle, ilgili üniversite kütüphanesinin hizmetlerine ve personeline ait hassas bilgilerin yanı sıra kişisel bilgilerin de kaydedildiği bu yazılımlarda gizlilik önlemlerinin geliştirilmesi önemlidir. Kullanıcıların kimlik bilgileri, iletişim bilgileri, öğrenci numaraları gibi temel bilgilerin yanı sıra üyelik durumu ve diğer ikincil kullanıcı bilgileri de yazılım sistemlerinde kaydedilebilir. Bu bilgilerin güvenliğinin sağlanması ve gereksiz veri saklama sürelerinin belirlenmesi için yazılım firmalarının beyanlarının alınması önemlidir. Öğrenci ağırlıklı bir kullanıcı tabanına sahip olan üniversite kütüphaneleri, kullanıcı hareketliliğinin yüksek olması nedeniyle bilgilerin belirli bir süre saklanması ve hizmetleri kullanmayan kullanıcı bilgilerinin silinmesi gerekmektedir. Bu nedenle, kurumsal güvenlik düzenlemelerinin veya politikalarının geliştirilmesi ve uygulanması önemlidir. Bu önlemler, kullanıcı bilgilerinin güvenliğini sağlamak ve gizliliğini korumak için önemli bir adımdır.

5.5. Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi

Hizmetlerinde verimliliği ön planda tutan organizasyonlar, paylaştıkları bilgilerin değerini ve kurumsal bilgi yönetiminin önemini kabul etmektedir. Kurumsal bilgi yönetimi, bir kurumun açık ve örtük bilgisinin kullanımını tanımlamak, organize etmek ve kontrol etmek amacıyla hizmet verir. Bu nedenle, sağlam bir kurumsal bilgi yönetimi için öncelikle kurum yöneticilerinin süreci iyi bir şekilde anlamaları ve kurumun özel ihtiyaçlarına uygun bir bilgi yönetimi sistemi tanımlamaları gerekmektedir. Daha sonra, tüm personelin bu bilgi yönetimi süreçlerine uygun bir şekilde faaliyet göstermeleri sağlanmalıdır. Kurumsal bilgi yönetimi, kurumun tüm unsurlarıyla uyumlu bir şekilde yürütüldüğünde, kurumu verimli, dinamik ve kârlı bir yapıya dönüştürebilir (Odabaş, 2005; 2003).

Bilgi yönetimi, gerek kullandığı teknolojiler gerekse işlevleri bakımından diğer yönetim yaklaşımlarından farklılık gösterir. Her yönetimin kendine özgü özellikleri olduğu gibi bilgi yönetiminin de kendine özgü bazı özellikleri bulunmaktadır. Bilgi yönetimi, organizasyona ait örtük bilgi, açık bilgi, dış bilgi ve iç bilgi ile bu bilgiye

ilişkin işlemleri içeren bir kavramdır. Temel amacı, bilginin üretken bir şekilde kullanılmasını sağlayarak entelektüel sermayenin en verimli şekilde işletme içinde kullanılmasını hedeflemektedir. Bilgi yönetimi uygulamaları, bilişim teknolojisi, iletişim, yeni ekonomi, bilgi bilimi, organizasyon, finans, psikoloji, sistem analizi, sosyoloji ve mühendislik gibi disiplinlerden yararlanan bir faaliyet topluluğunu içermektedir. Bilgi yönetimi, her işletmenin ve çalışanın özel gereksinimlerine uygun olarak oluşturulur ve düzenli olarak gözden geçirilir. Bu sürekli uygulama, önemli ve kritik bilginin işletme dışına çıkmasını önleyerek bilginin açığa çıkarılmasını sağlar. Bu şekilde, işletme için önemli bilgilerin korunması ve etkin bir şekilde kullanılması sağlanır (Ardıç ve Dulkadir, 2018).

Bilgi güvenliği, risklerin varlığından kaynaklanır. Bu nedenle, gizlilik, bütünlük ve kullanılabilirlik, bilgi güvenliği temel ilkeleridir ve risklerin senteziyle ortaya çıkar. Bilgi ve belge yönetimi uygulamaları, belge yönetimi teknik ve yasal düzenlemeleri, belge oluşturma sürecinden erişim haklarının tanımlanmasına kadar tüm süreçte bu ilkeleri zorunlu kılar. Bilgi ve belgelerin gizliliği, bütünlüğü ve kullanılabilirliği açısından bilgi güvenliği yönetiminin önemi büyüktür. Bilgi güvenliği ilkeleri, kurumsal bilgi yönetimi hedeflerini somutlaştırırken, bilgi ve belge yönetimi prensipleri de bu somut hedefleri destekler (Güler ve Furat, 2022).

Diğer kurum yöneticileri gibi kütüphane yöneticileri de planlama, düzenleme, yürütme, koordinasyon, karar alma ve liderlik işlevlerini yerine getirebilmek için gerekli bilgilere ihtiyaç duymaktadır. Bu bilgiler, kendileri ve kuruluşları için önem taşımaktadır. Kurumsal bilgiler, bilgi merkezi içindeki iç ve dış kaynaklardan çeşitli bilgi sistemleri aracılığıyla toplanır, işlenir ve yöneticilere iletilir. Bu tür bilgi sistemlerinden biri de yönetim bilgi sistemidir. Yönetim bilgi sistemleri, organizasyon içindeki çeşitli yönetici düzeylerine bilgi desteği sağlamak amacıyla bilgisayar teknolojisiyle gelişmiş bilgi sistemleridir. Yönetim bilgi sistemleri, yöneticilere karar verme, planlama, koordinasyon sağlama ve denetimleri destekleme konularında kolaylık sağlar. Kütüphane yöneticilerine kitap seçimi, kataloglama, ödünç verme, elektronik kaynaklar ve bibliyografik aramalar gibi birçok konuda destek sunar. Ayrıca kütüphane yöneticilerine kütüphane verimliliği, üretkenlik, performans ve kullanıcı memnuniyeti gibi konularda bilgi sağlar. Bu sistem

sayesinde karar verme, planlama, çalışanlar ve birimler arasındaki koordinasyon ve kütüphane işlemleri ve hizmetlerinin denetimi en üst düzeyde takip edilebilir.

Kütüphanelerde, özellikle de üniversite kütüphanelerinde, bilginin yönetimi iyi bir stratejiye dayanmaktadır. Bilgi yönetimi stratejisi, kurumsal yönetim yapısının bir parçası olarak değerlendirilir. Temel amacı, kuruluşun sahip olduğu bilgi varlıklarından en yüksek değeri elde etmek ve bu varlıkların uygun maliyetle yönetilmesi ve korunmasını sağlamaktır. Bilgi yönetimi stratejisi, kuruluşun bilgiyi nasıl ve hangi amaçlarla kullanacağını belirlerken, aynı zamanda bilgilerin etkili bir şekilde yönetilmesini sağlayan uygulamaların temelini oluşturur. Bu nedenle, üniversite kütüphaneleri için bilgi güvenliği yönetim sistemi büyük önem taşır (Nicolas-Rocca ve Burkhard, 2019).

Kütüphaneler, bilgi güvenliği konusundaki farkındalığın artmasıyla birlikte bilgi güvenliğine olan ihtiyacı da hissetmektedir. Yönetimlerin bilgi güvenliği konusundaki endişelerinin değiştiği ve bu konuya yönelik hassasiyetlerinin arttığı görülmektedir. Ayrıca, bilgi güvenliği yönetiminin bir kuruluşun karşılaştığı temel sorunlar arasında önemli bir yer tuttuğu belirtilmektedir. Bu nedenle, kütüphaneler bilgi güvenliği risklerinden kaynaklanan potansiyel hasarlardan korunmak ve bu hasarları en aza indirmek için gerekli bilgi güvenliği önlemlerine ihtiyaç duyarlar. Bu ihtiyacın etkili bir şekilde karşılanabilmesi ve sorunların çözüme kavuşturulabilmesi için sağlam bir bilgi güvenliği yönetimine dayanmak gerekmektedir. Bilgi güvenliği önlemlerinin yeterince yönetilememesi birçok sorunu beraberinde getirebilir. Aşağıda bunlardan bazıları şu biçimde sıralanmaktadır (Ismail, 2012):

- Kütüphane bilgi sistemlerindeki verilerin yanlışlıkla veya kötü niyetle silinmesi ve değiştirilmesi nedeniyle veri kaybı yaşanması ve kütüphane hizmetlerinin zarar görmesi,
- Bilgi sistemlerine yetkisiz kişilerce erişilerek sistem hizmetlerinin durması veya tamamen işlem yapamaz hale gelmesi,
- Kütüphanedeki bilgi ve ağ sistemlerinin zarar görmesiyle birlikte finansal kayıp ve ekstra maliyet ihtiyacının ortaya çıkması,
- Web sayfalarının tahrif edilerek ideolojik bilgilerin sunulması, kişisel bilgilerin ifşa edilmesi ve kütüphane kayıtlarının tahrif edilmesi nedeniyle

kütüphanelere olan güvenin azalması ve kurum itibarının olumsuz etkilenmesi,

- Gizlilik veya telif haklarının ihlal edilmesi,
- Paydaş firmaların, kurumların ve diğer kütüphanelerin verilerinin ifşa edilmesi sonucunda ilişkilerin zarar görmesi,
- Kritik değere sahip bilgilerin ifşa edilmesi sonucunda yasal ve idari işlemlerin başlatılması ve cezai işlemlerin uygulanması,
- Kişisel verilerin korunmasıyla ilgili düzenleyicilerin zarar görmesi,
- Kurumsal verilerin zarar görmesi ve hizmetlerin durması olarak sıralanır.

6. TÜRKİYE'DE ÜNİVERSİTE KÜTÜPHANELERİNDE BİLGİ GÜVENLİĞİ YÖNETİMİNE İLİŞKİN BULGULAR ve TARTIŞMA

Bu kısımda katılımcılara yöneltilen ölçme aracından elde edilen veriler araştırma soruları çerçevesinde analiz edilerek çalışma kapsamında geliştirilen hipotezlerin doğruluklarını sınamaya yönelik bulgulara yer verilmiştir. Bulgular, araştırma sorularına ve hipotezlerine uygun sıra dâhilinde tablolar halinde sunulmakta ve değerlendirilmektedir.

6.1. Katılımcıların Tanımlayıcı Profillerine İlişkin Bulgular

Araştırmaya katılanların cinsiyeti, eğitim durumu, çalıştığı üniversitenin türü, üniversite kütüphanesindeki görevi ve iş tecrübesi gibi demografik bilgileri Tablo 6.1'de verilmektedir.

Tablo 6.1: Katılımcılara ait demografik bilgiler

		Devlet Üniversitesi		**Vakıf Üniversitesi**		**Toplam**	
		f	**%**	***f***	**%**	***f***	**%**
Cinsiyet	Kadın	63	50,8	54	72,0	117	58,8
	Erkek	61	49,2	21	28,0	82	41,2
Eğitim Durumunuz	Ön Lisans	0	0,0	1	1,3	1	0,5
	Lisans	79	63,7	42	56,0	121	60,8
	Lisansüstü (Yüksek Lisans/Doktora)	45	36,3	32	42,7	77	38,7
Mezuniyet Programı	Bilgi ve Belge Yönetimi vb.	106	85,5	61	81,3	167	83,9
	Bilgisayar / Bilişim / Yazılım	2	1,6	4	5,3	6	3,0
	Diğer	16	12,9	10	13,3	26	13,1
Görev	Daire Başkanı	5	4,0	15	20,0	20	10,1
	Şube Müdürü	10	8,1	2	2,7	12	6,0
	Öğretim Görevlisi	22	17,7	0	0,0	22	11,1
	Kütüphaneci	80	64,5	54	72,0	134	67,3
	Bilgisayar / Bilgi İşlem Uzmanı	4	3,2	1	1,3	5	2,5
	Diğer	3	2,4	3	4,0	6	3,0
İş Tecrübesi	1 - 5 yıl	31	25,0	40	53,3	71	35,7
	6 - 10 yıl	44	35,5	15	20,0	59	29,6
	11 - 15 yıl	29	23,4	8	10,7	37	18,6
	16 - 20 yıl	14	11,3	4	5,3	18	9,0
	21 yıl ve üzeri	6	4,8	8	10,7	14	7,0
Üniversite Türü	Devlet Üniversitesi	124	100,0	0	0,0	124	62,3
	Vakıf Üniversitesi	0	0,0	75	100,0	75	37,7
	Toplam	**124**	**100,0**	**75**	**100,0**	**199**	**100,0**

Tablo 6.1'deki veriler, her devlet ve vakıf üniversitesinden çalışmaya katılım sağlayan personelin istihdam profilleri arasında bazı farklılıkların olduğunu

göstermektedir. 199 üniversite kütüphanesinin her birinden bir personelin katılımı sağlanmıştır. Bu yönüyle katılımcılardan elde edilen tüm veriler Türkiye'de üniversite kütüphanelerinin bütününü temsil etmektedir.

Katılımcıları demografik yapısınailişkin veriler ayrı ayrı incelendiğinde, devlet üniversitesindeki katılımcıların kadın oranı %50,8 iken, Vakıf Üniversitesi'nde %72,0'dir. Genel olarak, her iki üniversitede de kadın çalışan oranı erkek çalışan oranından daha yüksektir.

Katılımcılardan lisans derecesine sahip olanlar, her iki üniversitede de en yüksek orana sahiptir. Ön lisans ve lisansüstü eğitim düzeylerinde ise küçük farklar vardır.

Katılımcıların her iki üniversite türünde de en yaygın mezuniyet programının Bilgi ve Belge Yönetimi veya benzeri programlar olduğu ve bunu Bilgisayar/Bilişim/Yazılım programlarının takip ettiği görülmektedir. Bu durum çalışmanın örneklem seçiminin amaca uygun olarak yapıldığını desteklemektedir.

Katılımcıların mezun oldukları program verilerinde "diğer" seçeneği içerisinde lisans derecesini Bilgi ve Belge Yönetimi, Kütüphanecilik, Arşivcilik ve Dokümantasyon Programlarının herhangi birinden mezun olup yüksek lisans derecelerini farklı programlarda tamamlamış kütüphaneciler ile birlikte öğretmenlik, işletme, iktisat, halkla ilişkiler ve mühendislik programlarının lisans derecesinden mezun olan katılımcılar bulunmaktadır. Kütüphanedeki görevi bakımından "diğer" seçeneğini işaretleyen katılımcıların ise şef, idari ve büro personeli olarak görev yaptıklarını belirtmişlerdir.

Katılımcılar arasında Kütüphaneci olanlar, her iki üniversitede de en yüksek görev grubunu oluştururken, daire başkanları ve şube müdürleri ikinci en yüksek grup arasında yer almıştır.

Katılımcıların çoğunlukla 6-10 yıl ve 1-5 yıl arasındaki iş tecrübesine sahip çalışanlardan oluştuğu görülmektedir. Kütüphanecilik alanında iş tecrübesi olan bu katılımcıların belirli bir yetkinliğe, eğitim ve farkındalığa sahip olabilmesi, bu çalışmanın verilerinin sağlıklı ve geçerli olması açısından yeterli bulunmaktadır.

6.2. Üniversite Kütüphanelerinde Bilgi Güvenliği Personeli ve Yönetim Aracının Varlığı

Bilginin bir sermaye gücü olarak kullanıldığı içinde bulunduğumuz çağda bilginin güvenliğine verilen değer iyi derecede olması gerekmektedir. Özellikle bilgi güvenliği konusunda eğitilmiş ve bu yetkinliklerle donatılmış personelin üniversite içerisinde görevlendirilmesi ve kurumsal bir bilgi güvenliği yönetim aracının uygulanması bilgi güvenliği yönetiminin iyi bir biçimde uygulanmasına katkı sağlamaktadır.

Bu itibarla Türkiye'de üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin ve kurumsal bilgi güvenliği yönetim aracının varlığını tespit etmeye yönelik anket katılımcılardan elde edilen verilerin frekans dağılımları Tablo 6.2'de verilmiştir.

Tablo 6.2: Üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personel

		Devlet Üniversitesi		**Vakıf Üniversitesi**		**Genel Toplam**	
		f	**%**	***f***	**%**	***f***	**%**
Bilgi güvenliğinden sorumlu personel	Var	46	37,1	26	34,7	72	36,2
	Yok	78	62,9	49	65,3	127	63,8
Bilgi güvenliği yönetim aracı	Var	68	54,8	52	69,3	120	60,3
	Yok	56	45,2	23	30,7	79	39,7
Genel Toplam		**124**	**100,0**	**75**	**100,0**	**199**	**100,0**

Tablo 6.2'ye göre, Türkiye'de devlet üniversite kütüphanelerinin %37,1'inde bilgi güvenliğinden sorumlu personel bulunurken, vakıf üniversite kütüphanelerinin %34,7'sinde bilgi güvenliğinden sorumlu personel bulunmaktadır. Genel olarak ise, üniversite kütüphanelerini %36,2'sinde bilgi güvenliğinden sorumlu personel bulunmaktadır. Ayrıca Türkiye'de devlet üniversite kütüphanelerinin %54,8'inde kurumsal bir bilgi güvenliği yönetim aracına sahipken, vakıf üniversite kütüphanelerinin ise %69,3'ünde kurumsal bir bilgi güvenliği yönetim aracının bulunduğu anlaşılmaktadır. Genel olarak ise, üniversite kütüphanelerini %60,3'ünde bilgi güvenliğinden sorumlu personel bulunmaktadır.

Bu bulgular, Türkiye'de birçok üniversite kütüphanesinde bilgi güvenliğinden sorumlu personel bulunmaması, potansiyel olarak bilgi güvenliği yönetimi zayıflıklarına yol açabilir. Bilgi güvenliği politikalarının uygulanması, risk değerlendirmeleri yapılması ve güvenlik önlemlerinin alınması gibi konularda eksiklikler olabilir. Bilgi güvenliği personeli ve yönetim aracının bulunmadığı kütüphanelerde, kullanıcı verilerinin ve diğer hassas bilgilerin korunması konusunda riskler oluşturabilir. Bilgi güvenliği personelinin ve yönetim aracının varlığı, güvenlik politikalarının uygulanması, risk değerlendirmelerinin yapılması ve güvenlik önlemlerinin alınması açısından önemlidir. Bilgi güvenliği yönetiminin güçlendirilmesi, çalışanların bilgi güvenliği konusunda farkındalığını artırırken, kütüphanelerdeki bilgi varlıklarının korunmasına ve olası güvenlik ihlallerinin önlenmesine yardımcı olabilir. Bu nedenle, üniversite kütüphaneleri yönetiminin bilgi güvenliğinden sorumlu personel istihdamına daha fazla önem vermesi, bilgi güvenliği konusunda olabildiğince çok sayıda personele hizmet içi eğitimin aldırılması ve bilgi güvenliği standartlarına uygun bir yönetim aracının tasarlanarak uygulanması gerekir.

6.3. Üniversite Kütüphanelerinde Kullanılan Bilgi Sistemleri

Teknolojik gelişmelere bağlı olarak bilgi ve iletişim sistemleri hayatın her alanında kullanılmaya başlamış ve kullanım seviyesi her geçen gün daha da artmaktadır. Günümüzde bilişim teknolojilerine bağlı sistemlere bağlılık geleneksel çalışma sistemlerini gittikçe azaltmaktadır. Özellikle bilgi ve dokümantasyon hizmeti veren kurumlar hizmetlerini zaman, mekân ve kişi olgularından bağımsız güvenli ve hızlı bir biçimde sunmak için bilgi sistemlerini kullanmaktadır. Dijital bilgi ortamlarının geliştiği ve yaygınlaştığı günümüzde kütüphane hizmetlerinin de bilgi sistemleri ile bütünleşik bir biçimde yürütülmesi yaygınlaşmaktadır.

Üniversite kütüphanelerinde bilgi kaynaklarının hizmete sunulmasında yararlanılan bilgi sistemleri, öğrencilerin, öğretim görevlilerinin ve araştırmacıların bilgi ihtiyaçlarını karşılayan önemli bilgi varlıklarıdır. Söz konusu sistemler aracılığıyla yönetilen kurumsal ve kişisel veriler bilgi güvenliği açısından önem arz etmektedir Bunlar, kullanıcıların kütüphane otomasyon sistemine kaydedilirken işlenen kişisel bilgiler, sistemlerin yürütülmesinden sorumlu personel bilgileri ve kuruma ait kritik

öneme sahip veriler gibi bir takım bilgi ve verilerden oluşabilmektedir. Bu nedenle bilgi sistemleri, bilginin gizliliği, bütünlüğü ve erişilebilirliği açısından son derece önemli bir değere sahiptir.

"Türkiye'de üniversite kütüphanelerinde kullanılan bilgi sistemleri ve bu sistemlerin bilginin kritikliği açısından korunmasının önemi nedir?" araştırma sorusuna yönelik katılımcıların görüşlerine ilişkin frekans dağılımları Tablo 6.3 ve Tablo 6.4'te verilmiştir.

Tablo 6.3: Üniversite kütüphanelerinde bilgi sistemlerinin dağılımı

	Devlet Üniversitesi		**Vakıf Üniversitesi**		**Genel Toplam**	
Bilgi Sistemleri	***f***	***%***	***f***	***%***	***f***	***%***
Kütüphane Otomasyon Sistemi	124	100,0	73	97,3	197	99,0
İntihal Yazılımları (Turnitin, Ithanticate vb.)	109	81,9	66	88,0	175	87,9
Kütüphanelerarası İş Birliği Takip Sistemi (KİTS)	114	91,9	60	80,0	174	87,4
Açık Erişim Sistemleri	110	88,7	60	80,0	170	85,4
Veri Tabanı Erişim ve İstatistik Sistemi	103	83,1	58	77,3	161	80,9
Türkiye Belge Sağlama Sistemi (TÜBESS)	94	75,8	51	68,0	145	72,9
Kütüphane Üyelik Bilgi Sistemleri	93	75,0	48	64,0	141	70,9
Ulusal Kimlik Doğrulama Sistemleri (Yetkim vb.)	35	28,2	20	26,7	55	27,6
Diğer	2	1,6	3	4,0	5	2,5
Genel Toplam	**783**		**438**		**1221**	

*Not. *Verilen cevaplar çoklu yanıt olduğundan toplam sayı, örneklem sayısını aşmaktadır.*

Tablo 6.3 incelendiğinde, Türkiye'de üniversite kütüphanelerinin %99,0 oranla tamamına yakınının kütüphane otomasyon sistemini kullandıkları görülmektedir. Daha sonra ise sırasıyla %87,9 oranla intihal yazılımları, %87,4 oranla kütüphaneler arası işbirliği takip sistemi, %85,4 oranla açık erişim sistemleri gelmektedir. Bu durum üniversite kütüphanelerinde yürütülen hizmetlerin bilgi sistemlerinde yoğun bir biçimde takip edildiğini göstermektedir. İntihal yazılımları tüm üniversite kütüphanelerine TÜBİTAK Ekual kapsamında ücretsiz sunulmasına rağmen tablodaki oranın %100 çıkmamasına, söz konusu yazılımların kütüphane dışında başka birimlerce takip ediliyor olması ya da katılımcıların bilgi eksiklikleri etki etmiş olabilir. Ancak, kullanım oranlarının düşük çıkması birkaç farklı faktöre bağlı olabilir. En az kulanım oranına (%27,6) sahip yazılım grubu olarak ise kimlik

doğrulama sistemi şeklinde kendini göstermiştir. Başta YETKİM olmak üzere bu sistemler üniversiteler tarafından son yıllarda ilgilenilen yeni nesil yazılımlardır. Ayrıca "diğer" seçeneğini işaretleyenler, oda rezervasyon sistemi, kampüs dışı erişim sistemi, web tasarım uygulamaları gibi araçlardan yararlandıklarını belirtmişlerdir.

Bu bulgular, üniversite kütüphanelerinin dijital sistemleri etkin bir şekilde kullanmaya çalıştıklarını göstermektedir. Kılıç ve Yılmaz (2017)'ın da çalışmalarında, kütüphanelerin bu sistemlerin kullanımı konusunda bilinçli oldukları ve veri güvenliği konusunda etkin bir şekilde çalıştıkları biçiminde benzer çıkarımlarda bulundukları görülmüştür. Bu sistemler, kütüphanelerin koleksiyonlarına erişimi kolaylaştırırken, kaynakların güvenliğini ve kullanıcıların da kisşisel verilerinin güvenliğini sağlamak için tasarlanmıştır. Çelik (2019) tarafından yapılan çalışmada, Türkiye'de üniversite kütüphanelerinin kişisel bilgilerin korumasına yönelik kullanılan sistemlerin yetersiz olduğu ve bu konuda daha fazla çalışmalar yapılması gerektiği belirtilmektedir.

Tablo 6.4: Bilginin kritikliği açısından bilgi sistemlerinin önemi

Bilginin kritikliği açısından bilgi sistemlerinin önemi	**Devlet Üniversitesi**		**Vakıf Üniversitesi**		**Toplam**	
	f	**%**	***f***	**%**	***f***	**%**
Çok Düşük	2	1,6	1	1,3	3	1,5
Düşük	6	4,8	6	8,0	12	6,0
Orta	32	25,8	16	21,3	48	24,1
Yüksek	57	46,0	33	44,0	90	45,2
Çok Yüksek	21	16,9	16	21,3	37	18,6
Fikrim Yok	6	4,8	3	4,0	9	4,5
Toplam	124	100,0	75	100,0	199	100,0

Tablo 6.4'teki veriler incelendiğinde, Türkiye'de üniversite kütüphanelerinde bilgi sistemlerinin kritik bilgiler taşımaları açısından kritik öneme sahip olmaları konusunda üniversite kütüphanelerinde görev yapan kullanıcıların 3 (%1,5)'ünün çok düşük, 12 (%6,0)'sinin düşük, 48 (%24,1)'inin orta, 90 (%45,2)'ının yüksek ve 37 (%18,6)'sisin çok yüksek dediği; 9 (%4,5)'unun ise konuya ilişkin fikrinin olmadığını belirttiği görülmektedir.

Bu bulgular, üniversite kütüphanelerinde bilgi sistemlerinin kritik bir öneme sahip olduğunu ve bu sistemlerin üniversite kütüphaneleri tarafından önemli bilgi bileşenleri olarak değerlendirildiğini ve kullanıldığını göstermektedir. Ayrıca bu

sistemlerin kütüphanelerin işleyişini geliştirmek, kullanıcı deneyimini artırmak ve bilgi güvenliğini sağlamak amacıyla da önemli roller üstlendiği söylenebilir.

Sonuç olarak, üniversite kütüphanelerinde bilgi sistemlerinin bilginin güvenliği, konusunda önemli olduğu düşüncesinin üniversite kütüphanelerinde görev yapanlarca yaygın olduğu anlaşılmıştır. Ancak, bu sistemlerin önemi konusunda fikir eksikliği olan veya belirsizlik yaşayan üniversite kütüphane çalışanlarının bu konuda desteklenmeye ve bilgilendirilmeye ihtiyacı bulunmaktadır.

6.4. Bilgi Varlıklarının Kritiklik Derecesinin Belirlenmesi

Bilgi varlıkları, her türlü bilgi işlem donanım ve yazılımlarından oluşan sistemler, ağlar, fiziksel mekânlar ve personel ana grupları altında toplanabilmektedir. Bu gruplar üniversite kütüphanelerinin veri işleme türüne, büyüklüğüne ve yöntemine göre değişiklik gösterebilmektedir. Üniversite kütüphanelerinin bilgi varlığı gruplarını belirlendikten sonra bu varlık gruplarının kritiklik derecesinin belirlemesi bilgi güvenliği açısından önem arz etmektedir. Kütüphaneye ait her bir bilgi varlığının kritiklik düzeyi, ayrı ayrı değerlendirilebileceği gibi tüm bilgi varlıklarının kritiklik düzeyi de bir bütün olarak belirlenebilmektedir.

Bilgi varlıklarının kritiklik derecesi, işlenen verinin bilgi güvenliği unsurları (gizlilik, bütünlük, erişilebilirlik) açısından kritikliği ve bilgi varlıklarında oluşabilecek güvenlik ihalelerinin etki alanları (kurumsal, toplumsal, sektörel ve bağımlı varlıklar) dikkate alınarak belirlenmektedir.

Bu itibarla, “Bilgi varlıklarında işlenen veya depolan kritik verilerin veya bilgilerin kritiklik derecesine etki eden faktöreler nelerdir?” araştırma sorusuna yönelik katılımcıların görüşlerine ilişkin frekans dağılımları Tablo 6.5 ve Tablo 6.6’da verilmiştir.

Tablo.6.5: Bilgi güvenliği unsurlarının bilginin kritikliğine etkisi

Bilgi güvenliği unsurları / Seçenekler		***Genel Toplam***	
		f	***%***
Bilgi varlığında işli kritik bilgilerin **"gizlilik"** unsurunun ihlal edilmesinin etkileri;	Herhangi bir zarar oluşmaz.	13	6,5
	Sadece kütüphane hizmetlerini ve çıkarlarını etkileyecek zarar verir.	48	24,1
	Üniversite çıkarlarına saygınlık derecesinde zararlar gelir fakat telafisi mümkündür.	101	50,8
	Üniversite çıkarlarına yaşamsal zararlar gelir ve telafisi mümkün değildir.	37	18,6
Bilgi varlığında işli kritik bilgilerin **"bütünlük"** unsurunun ihlal edilmesinin etkileri;	Herhangi bir zarar oluşmaz.	3	1,5
	Sadece kütüphane hizmetlerini ve çıkarlarını etkileyecek zarar verir.	57	28,6
	Üniversite çıkarlarına saygınlık derecesinde zararlar gelir fakat telafisi mümkündür.	92	46,2
	Üniversite çıkarlarına yaşamsal zararlar gelir ve telafisi mümkün değildir.	47	23,6
Bilgi varlıklarının güvenlik ihlalinde en fazla tolere edilebilecek **"erişebilirlik"** süresi;	1 saatten az süre	61	30,7
	1 saat ile 8 saatten az süre	94	47,2
	8 saat ile 24 saatten az süre	29	14,6
	24 saat ve üzeri süre	15	7,5
	Genel Toplam	**199**	**100**

Tablo 6.5'teki veriler incelendiğinde;

Bilgi varlığında işlenen kritik bilgilerin "gizlilik" unsurunun ihlal edilmesi durumunda katılımcıların 13 (%6,5)'ünün herhangi bir zarar oluşmayacağı, 48 (%24,1)'inin sadece kütüphane hizmetlerini ve çıkarlarını etkileyecek zararların oluşacağı, 101 (%50,8)'inin üniversite çıkarlarına saygınlık derecesinde zararların oluşabileceği fakat bu zararların telafisinin mümkün olduğu ve 37 (%18,6)'sinin ise üniversite çıkarlarına yaşamsal zararlar verebileceği ve bu zararların telafisinin mümkün olmadığı görüşlerine katıldıkları görülmektedir. Bu bulgular, bilgi güvenliği unsurlarından gizlilik unsurunun bilginin kritikliği üzerinde önemli düzeyde etkili olduğunu vurgulamakta ve bilgilerin gizliliği konusunda iyi seviyelerde güvenlik önlemlerinin uygulanması gerektiğini göstermektedir.

Bilgi varlığında işlenen kritik bilgilerin "bütünlük" unsurunun ihlal edilmesi durumunda katılımcıların 3 (%1,5)'ünün herhangi bir zarar oluşmayacağı, 57 (%28,6)'sinin sadece kütüphane hizmetlerini ve çıkarlarını etkileyecek zararların oluşacağı, 92 (%46,2)'sinin üniversite çıkarlarına saygınlık derecesinde zararların oluşabileceği fakat bu zararların telafisinin mümkün olduğu ve 47 (%23,6)'sinin ise üniversite çıkarlarına yaşamsal zararlar verebileceği ve bu zararların telafisinin

mümkün olmadığı görüşlerine katıldıkları görülmektedir. Bu bulgular, bilginin doğru, eksiksiz ve güncel olarak bütünlüğünün korunmasının bilginin kritikliği bakımından büyük önem taşıdığının göstermektedir.

Bilgi varlıklarının güvenlik ihlalinde en fazla tolere edilebilecek "erişebilirlik" süresi hakkında katılımcıların 61 (%30,7)'inin 1 saatten az süre, 94 (%47,2)'ünün 1 saat ile 8 saatten az süre, 29 (%14,6)'unun 8 saat ile 24 saatten az süre ve 15 (%7,5)'inin ise 24 saat ve üzeri süre olabileceği dediği görülmektedir. Bu bulgulara göre bilgi varlıklarının erişilebilirliğini hızlı bir şekilde sağlamak ve olumsuz etkileri minimize etmek bilgi güvenliği önlemlerinin etkin bir şekilde uygulanması gerektiğini göstermektedir.

Tablo 6.5'ten elde edilen bulgulara göre, bilgi güvenliği bileşenlerinden gizlilik, bütünlük ve erişilebilirlik unsurları arasında dengeli bir yaklaşımın benimsenmesinin bilginin kritikliği açısından önemli olduğu söylenebilir. Gizlilik, bütünlük ve erişilebilirlik ihlallerinin kütüphaneleri ve bağlı olduğu üniversiteleri genel olarak olumsuz yönde etkileyebileceği ve üniversite çıkarlarına zarar verebileceği görüşünün hâkim olduğu görülmüştür. Bu da, katılımcıların bilgi güvenliği yönetimini ne derecede önemli bulduğunu göstermektedir. Bu nedenle, bilgi güvenliği önlemlerinin tüm bu unsurları kapsayacak bir şekilde planlanması ve etkin bir biçimde yürütülmesi üniversite kütüphaneleri açısından önemlidir.

Tablo 6.6: Bilgi güvenliği ihlallerinin etki alanları üzerindeki durumu

Bilgi varlığı üzerinde oluşabilecek güvenlik ihlallerinin		***Çok Düşük***	***Düşük***	***Orta***	***Yüksek***	***Çok Yüksek***	***Fikrim Yok***
Kurumsal alana etkisi	*f*	2	20	51	77	35	14
	%	1,0	10,1	25,6	38,7	17,6	7,0
Toplumsal alana etkisi	*f*	12	37	74	46	14	16
	%	6,0	18,6	37,2	23,1	7,0	8,0
Kütüphanecilik camiasına etkisi	*f*	9	27	61	67	23	12
	%	4,5	13,6	30,7	33,7	11,6	6,0
Bağımlı dış paydaşlara etkisi	*f*	10	32	56	57	23	21
	%	5,0	16,1	28,1	28,6	11,6	10,6

Tablo 6.6'daki verilere göre, bilgi varlıklarında işlenen veya depolanan bilginin gizlilik, bütünlük ve erişebilirlik unsurlarının tamamını veya bir kısmını etkileyecek

olası en kötü senaryoya sahip bir bilgi güvenliği ihlali meydana geldiğinde söz konusu olayın;

Kurumsal yapıyı hangi seviyede etkileyeceği konusunda katılımcıların 2 (%1,0)'sinin çok düşük, 20 (%10,1)'sinin düşük, 51 (%25,6)'inin orta, 77 (%38,7)'sinin yüksek ve 35 (%17,6)'inin çok yüksek dediği; 14 (%7,0)'ünün ise ilgili etki alanı için fikrinin olmadığını belirttiği görülmektedir.

Toplumsal yapıyı hangi seviyede etkileyeceği konusunda katılımcıların 12 (%6,0)'sinin çok düşük, 37 (%18,6)'sinin düşük, 74 (%37,2)'ünün orta, 46 (%23,1)'sının yüksek ve 14 (%7,0)'ünün çok yüksek dediği; 16 (%8,0)'sının ise ilgili etki alanı için fikrinin olmadığını belirttiği görülmektedir.

Toplumsal yapıyı hangi seviyede etkileyeceği konusunda katılımcıların 9 (%4,5)'unun çok düşük, 27 (%13,6)'sinin düşük, 61 (%30,7)'inin orta, 67 (%33,7)'sinin yüksek ve 23 (%11,6)'ünün çok yüksek dediği; 12 (%6,0)'sinin ise ilgili etki alanı için fikrinin olmadığını belirttiği görülmektedir.

Tablo 6.6'dan elde edilen bulgulara göre, bilgi güvenliği ihlallerinin genellikle kurumsal alan, toplumsal alan, kütüphanecilik camiası ve bağımlı dış paydaşlar üzerinde etkili olduğu görülmektedir. Bu ihlaller, kurumsal itibarın zedelenmesine, toplumsal ilişkilerin bozulmasına, kütüphanecilik hizmetlerinin aksamasına ve dış paydaşlarla güven ilişkilerinin zedelenmesine neden olabilir. Bu nedenle, güvenlik önlemlerinin bu alanlara yönelik olarak etkili bir şekilde uygulanması önemlidir.

6.5. Üniversite Kütüphanelerinde Algılanan Bilgi Güvenliği Tehditleri

Bilgi güvenliği tehditlerine karşı güvenlik önlemlerini planlamadan önce atılması gereken ilk adım, neyi korumaya ihtiyacı olduğunun bilinmesidir. Bu nedenle üniversite kütüphaneleri bünyesindeki donanım, uygulama, veri, ağ, insan ve çevresel bilgi varlıklarının karşılaşılabileceği olası tehditleri, güvenlik açıklarını ve sorunlarını bilmesi gerekir ki, bu tehdit ve güvenlik sorunlarına karşı alınması gereken önlem mekanizmaları geliştirilir ve uygulanır. Gerek bilgi hizmetinin sunumunda gerekse kurumsal ve kişisel bilgilerin bilgi sistemlerine işlenmesi bakımından kütüphaneler üniversitelerin bilgi güvenliği tehditlerine karşı korunması gereken öncelikli birimler arasında yer almaktadır.

Bu itibarla, Türkiye'de üniversite kütüphanelerinde algılanan yaygın bilgi güvenliği tehditleri nelerdir ve bu tehditler en çok hangi unsurlardan kaynaklanmaktadır? araştırma sorusuna yönelik katılımcıların görüşlerine ilişkin frekans dağılımları Tablo 6.7 ve Tablo 6.8'de verilmiştir.

Tablo 6.7: Üniversite kütüphanelerindeki yaygın bilgi güvenliği tehditleri

	Devlet Üniversitesi		**Vakıf Üniversitesi**		**Genel Toplam**	
Bilgi Güvenliği Tehditleri	***f***	***%***	***f***	***%***	***f***	***%***
Bilgi sistemi arızası ve bakım hatası	86	11,2	35	8,9	121	10,4
E-posta saldırıları	59	7,7	34	8,7	93	8,0
Virüs, solucan, Truva atı gibi kötü yazılımlar	56	7,3	26	6,6	82	7,1
Parola saldırıları, çözümleme, çalma	42	5,5	28	7,1	70	6,0
İletişim hataları (dedikodu, dinleme, yalan vb.)	44	5,7	26	6,6	70	6,0
Doğal afetlere veya hava olaylarına bağlı tehditler	39	5,1	28	7,1	67	5,8
Yetkisiz donanım / yazılım kurulumu ve kullanımı	44	5,7	21	5,4	65	5,6
Reklam, parazit, hırsız ve casus yazılım tehditleri	42	5,5	22	5,6	64	5,5
Bilgi sistemlerini hackleme	36	4,7	26	6,6	62	5,3
Yanlış güncelleme, depolama veya yedekleme	44	5,7	18	4,6	62	5,3
Web saldırıları	38	4,9	22	5,6	60	5,2
Kasıtlı / kasıtsız personel suiistimalleri	44	5,7	16	4,1	60	5,2
Binaya izinsiz giriş ve yetkisiz erişim tehditleri	38	4,9	18	4,6	56	4,8
Kimlik hırsızlığı ve dolandırıcılığı tehditleri	32	4,2	15	3,8	47	4,1
Kimlik doğrulama saldırıları	34	4,4	13	3,3	47	4,1
Fiziksel belge / evrak / dosya hırsızlığı veya ifşası	30	3,9	14	9,6	44	3,8
Donanım hırsızlığı, sabotaj ve kasıtlı imha	32	4,2	11	2,8	43	3,7
Uzaktan yönetim aracı saldırıları	23	3,0	15	3,8	38	3,3
Fikrim / Bilgim yok	5	0,7	4	1,0	9	0,8
Toplam	**768***	**100,0**	**392**	**100,0**	**1160**	**100,0**

** Verilen cevaplar çoklu yanıt olduğundan toplam n sayısı örneklem sayısını aşmaktadır.*

Tablo 6.7'deki veriler incelendiğinde, Türkiye'de üniversite kütüphanelerinde karşılaşılan veya karşılaşması olası yaygın tehditler hakkında katılımcılardan alınan çoklu yanıtlara göre 121 katılımcının bilgi sistemi arızası ve bakım hatasını, 93 katılımcının e-posta saldırıları, 82 katılımcının virüs, solucan, Truva atı gibi kötü yazılımları, 70 katılımcının parola saldırıları, çözümleme, çalma ve iletişim hatalarını, 67 katılımcının doğal afetlere veya hava olaylarına bağlı tehditleri, 65 katılımcının yetkisiz donanım / yazılım kurulumu ve kullanımı tehditlerini, 64

katılımcının reklam, parazit, hırsız ve casus yazılım tehditlerini, 62 katılımcının bilgi sistemlerini hackleme ve yanlış güncelleme, depolama veya yedekleme tehditlerini, 60 katılımcının web saldırıları ve personel suiistimallerini, 56 katılımcının binaya izinsiz giriş ve yetkisiz erişim tehditlerini, 47 katılımcının kimlik hırsızlığı ve dolandırıcılığı tehditleri ile kimlik doğrulama saldırılarını, 44 kullanıcının fiziksel belge / evrak / dosya hırsızlığı veya ifşası tehditlerini, 43 katılımcının donanım hırsızlığı, sabotaj ve kasıtlı imha tehditlerini, 38 katılımcının uzaktan yönetim aracı saldırılarını seçtiği; 9 katılımcının ise diğer seçeneği altında lisans anlaşmalarına aykırı usulsüz kullanım, kapalı ofis olmamasından kaynaklı çevresel olumsuzluklar, veri tabanından toplu makale indirme, eski ve kullanım ömrü dolmuş teknoloji kullanımı, bütçe yetersizliğine bağlı güvenlik sorunları ve kütüphanenin yardım aldığı diğer birim kaynaklı tehditleri belirttikleri görülmektedir.

Yaygın tehditlerin görülme sıklığı üniversitelerin türüne göre incelendiğinde, ilk iki sırada yer alan "bilgi sistemi arızası ve bakım hatası" ve "e-posta saldırıları" tehditlerinin her iki üniversite türünde de aynı olduğu, daha sonrasında gelen tehditlerin ise birkaç istisna dışında hemen hemen aynı sırada yer aldığı görülmektedir.

Tablo 6.8: Üniversite kütüphanelerinde yaygın bilgi güvenliği tehdit kategorileri

	Devlet Üniversitesi		**Vakıf Üniversitesi**		**Genel Toplam**	
Bilgi Güvenliği Tehdit Kategorisi	***f***	***%***	***f***	***%***	***f***	***%***
İnsan / Diğer Tehditler	34	27,4	18	24,0	52	26,1
Ağ Tehditleri	27	21,8	13	17,3	40	20,1
Yazılım Tehditleri	22	17,7	16	21,3	38	19,1
Fiziksel / Çevresel Tehditler	13	10,5	17	22,7	30	15,1
Veri Tehditleri	18	14,5	9	12,0	27	13,6
Donanım Tehditleri	10	8,1	2	2,7	12	6,0
Genel Toplam	**124**	**100,0**	**75**	**100,0**	**199**	**100,0**

Tablo 6.8'deki veriler incelendiğinde, Türkiye'de üniversite kütüphanelerinde algılanan bilgi güvenliği tehditleri konusunda katılımcıların 52 (%26,1)'sinin çalışanların görevi kötüye kullanma veya insan hataları ile ilgili tehditleri, 40 (%20,1)'ının ağ tehditlerini, 38 (%19,1)'inin yazılım tehditlerini, 30 (%15,1)'unun fiziksel ve çevresel tehditleri, 27 (%13,6)'sinin veri tehditlerini ve 12 (%6,0)sinin ise donanım tehditlerini belirttiği görülmektedir.

Türkiye'de üniversite kütüphanelerinde algılanan en yaygın tehdit kategorisi üniversite türüne göre incelendiğinde, her iki grubun ilk sırası ile son sırasında yer alan tehdit kategorilerinin aynı olduğu gözlemlense de katılımcı oranlarının farklı olduğu görülmektedir.

Türkiye'de üniversite kütüphanelerinde en yaygın olarak algılanan tehditlerin insan ile ilgili tehditler olduğu anlaşılmaktadır. Donanım ile ilgili tehditlerin ise an az oranda algılanan tehdit grubu olduğu belirlenmiştir. İnsan ile ilgili tehdit kategorisindeki tehditlerin daha yaygın biçimde algılanmasının nedenleri arasında kütüphanelerin çok sayıda iç ve dış paydaşının olması ve bu paydaşların bilgi güvenliği konusunda eksikliklerinin olması söylenebilir.

6.6. Teknolojik Bilgi Güvenliği Önlemlerine İlişkin Bulgular

Bu başlık altında yer alan alt başlıklarda, Türkiye'de üniversite kütüphanelerinde teknolojik bilgi güvenliği önlemelerinin uygulama düzeyleri hakkında katılımcılardan elde edilen bulgular incelenmektedir. Üniversite kütüphanelerinde görev yapan katılımcılardan elde edilen veriler, istatistik testleri ile analiz edilerek Türkiye'de üniversite kütüphanelerinde hangi teknolojik bilgi güvenliği önleminin iyi, orta veya kötü düzeylerde uygulandığı ya da hangi teknolojik bilgi güvenliği önleminin ise hiç uygulanmadığına ilişkin bulgulara ulaşılmıştır. Ayrıca üniversite kütüphanelerinde teknolojik bilgi güvenliği önlemlerinin uygulama düzeyleri konusunda katılımcılardan elde edilen veriler, katılımcıların görev yaptığı üniversite türü, kütüphanede bilgi güvenliğinden sorumlu personelinin varlığı ve kurumsal bilgi güvenliği araçlarının kullanımı değişkenlerine göre analiz edilerek gruplar arasında anlamlı farklılıkların oluşup oluşturmadığına ilişkin hipotezler sınanmıştır.

Bu itibarla teknolojik bilgi güvenliği önlemlerine ilişkin katılımcılardan 5 kategori (donanım, yazılım, ağ, veri, fiziksel çevre) altında toplam 59 madden oluşan önlemin görev yaptığı üniversite kütüphanesinde uygulanma düzeyine uygun seçeneğin işaretlenmesi istenmiştir. Ayrı ayrı maddelerde belirtilen güvenlik önlemlerinin uygulanıp uygulanmadığı, uygulanıyorsa hangi düzeylerde uygulanmakta olduğuna ilişkin uygun sınıflama seçenekleri kullanılmıştır. Bu seçenekler arasında güvenlik önlemi uygulanmıyorsa "hiç"; uygulanmıyor ise "çok kötü", "kötü", "orta", "iyi" ve "çok iyi" seçenekleri bulunmaktadır.

Katılımcıların bir teknoloji güvenliği önleminin uygulama düzeyine ilişkin "çok kötü" ve "kötü" seçimi, o güvenlik önleminin "kötü düzeyde uygulandığını"; "orta" seçimi, o güvenlik önleminin "orta düzeyde uygulandığını"; "iyi" ve "çok iyi" seçimi, o güvenlik önleminin "iyi düzeyde uygulandığını"; "hiç" seçimi ise o güvenlik önleminin "hiç uygulanmadığını" göstermektedir.

Ayrıca teknolojik güvenlik önlemlerine ilişkin herhangi bir bilgisi olmayan ya da çalıştığı kütüphanede varlığı veya uygulanmasına ilişkin tereddüt yaşayan katılımcıların cevabının diğer katılımcıların cevaplarındaki niteliği etkilememesi veya o maddeyi boş bırakmaması için her maddeye "fikrim yok" seçeneği de eklenmiştir.

Bu kapsamda aşağıdaki araştırma soruları, katılımcılardan elde edilen verilere ve yukarıda açıklanan değerlendirme kriterlerine göre incelenmiştir.

- Bilgi güvenliği tehditlerine karşı alınan teknolojik bilgi güvenliği önlemlerinin Türkiye'de üniversite kütüphanelerinde uygulanma düzeyleri nedir?
- Teknolojik bilgi güvenliği önlemlerinin uygulanma düzeylerinde üniversitenin türüne, bilgi güvenliğinden sorumlu personelin varlığına ve kurumsal bilgi güvenliği yönetim aracının kullanımına bağlı olarak farklılıklar oluşmakta mıdır?

6.6.1. Teknolojik Bilgi Güvenliği Önlemlerinin Genel Uygulanma Düzeyleri

Bu başlık altında, üniversite kütüphanelerinde teknolojik bilgi güvenliği önlemlerinden donanım, yazılım, ağ, ver, güvenliği ve fiziksel-çevresel güvenlik kategorilerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin her önlem maddesinin frekans dağılımları verilmiştir.

Tablo 6.9'da teknolojik bilgi güvenliği önlemlerinden donanım önlemlerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.9: Donanım güvenliği önlemlerinin uygulama düzeyleri

	Donanım Güvenliği Önlemleri Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	***Kötü***	***Orta***	***İyi***	
1	Veri işleme, depolama ve iletme yeteneğine sahip tüm donanımların güncel envanteri tutulmakta ve kullanım tahsisleri yapılmaktadır.	*f*	2	5	43	138	11
		%	1,0	2,5	21,6	69,3	5,5
2	Kütüphane envanterindeki tüm cihaz ve taşınabilir ortamlar, kaybolma veya çalınma riskine karşı şifrelenmektedir.	*f*	3	21	55	108	12
		%	1,5	10,6	27,6	54,3	6,0
3	Kritik bilgi içeren taşınabilir cihaz ve ortamlar güvenli şekilde saklanmakta ve kurum dışına çıkarılmasına izin verilmemektedir.	*f*	1	9	33	147	9
		%	0,5	4,5	16,6	73,9	4,5
4	Kütüphane envanterinden çıkarılan donanımların veri depolama ünitelerindeki veri ve bilgiler geri getirilmeyecek şekilde silinmektedir	*f*	6	7	41	90	55
		%	3,0	3,5	20,6	45,2	27,6
5	Kullanım ömrünü tamamlamış veri depolama üniteleri (HDD, SSD, harici bellek, USB, disk vb.) güvenli bir biçimde imha edilmektedir.	*f*	11	15	31	85	57
		%	5,5	7,5	15,6	42,7	28,6
6	Yeni tedarik edilen sabit diskler veri kurtarmaya imkân sağlamayacak bir şekilde biçimlendirilerek sisteme dâhil edilmektedir	*f*	10	15	36	70	68
		%	5,0	7,5	18,1	35,2	34,2
7	Bilgi içeren tüm cihaz ve ortamların ısı, nem ve elektromanyetik gibi tehditlere maruz kalamaması için çevresel önlemler alınmaktadır.	*f*	9	17	53	101	19
		%	4,5	8,5	26,6	50,8	9,5
8	Onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihaz ve ortamlardaki kritik bilgiler geri getirilmeyecek şekilde silinmektedir.	*f*	12	14	36	74	63
		%	6,0	7,0	18,1	37,2	31,7
9	Nesnelerin interneti (IoT cihazları) ile ilgili kurulum, imha ve yeniden kullanıma alma gibi işlemler yetkili personelce yapılmaktadır.	*f*	5	9	31	117	37
		%	2,5	4,5	15,6	58,8	18,6

Tablo 6.9'daki donanım güvenliğine ilişkin veriler incelendiğinde;

"Veri işleme, depolama ve iletme yeteneğine sahip tüm donanımların güncel envanteri tutulmakta ve kullanım tahsisleri yapılmaktadır" maddesinin uygulanması konusunda katılımcıların 2 (%1,0)'sinin hiç; 5 (%2,5)'inin kötü, 43 (%21,6)'ünün orta, 138 (%69,3)'inin iyi dediği; 11 (%5,5)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kütüphane envanterindeki tüm cihaz ve taşınabilir ortamlar, kaybolma veya çalınma riskine karşı şifrelenmektedir" maddesinin uygulanması konusunda katılımcıların 3 (%1,5)'ünün hiç, 21 (%10,6)'inin kötü, 55 (%27,6)'inin orta, 108 (%54,3)'inin iyi dediği; 12 (%6,0)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kritik bilgi içeren taşınabilir cihaz ve ortamlar güvenli şekilde saklanmakta ve kurum dışına çıkarılmasına izin verilmemektedir" maddesinin uygulanması

konusunda katılımcıların 1 (%0,5)'inin hiç, 9 (%4,5)'unun kötü, 33 (%16,6)'ünün orta, 147 (%73,9)'sinin iyi dediği; 9 (%4,5)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kütüphane envanterinden çıkarılan donanımların veri depolama ünitelerindeki veri ve bilgiler geri getirilmeyecek şekilde silinmektedir." maddesinin uygulanması konusunda katılımcıların 6 (%3,0)'sının hiç, 7 (%13,50,6)'sinin kötü, 41 (%20,6)'inin orta, 90 (%45,2)'ının iyi dediği; 55 (%27,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kullanım ömrünü tamamlamış veri depolama üniteleri güvenli bir biçimde imha edilmektedir" maddesinin uygulanması konusunda katılımcıların 11 (%5,5)'inin hiç, 15 (%7,5)'inin kötü, 31 (%15,6)'inin orta, 85 (%42,7)'inin iyi dediği; 57 (%26,6)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Yeni tedarik edilen sabit diskler veri kurtarmaya imkân sağlamayacak bir şekilde biçimlendirilerek sisteme dâhil edilmektedir" maddesinin uygulanması konusunda katılımcıların 10 (%5,0)'unun hiç, 15 (%7,5)'inin kötü, 36 (%18,1)'sının orta, 70 (%35,2)'inin iyi dediği; 68 (%34,2)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi içeren tüm cihaz ve ortamların ısı, nem ve elektromanyetik gibi tehditlere maruz kalamaması için çevresel önlemler alınmaktadır." maddesinin uygulanması konusunda katılımcıların 9 (%4,5)'unun hiç, 17 (%8,5)'sinin kötü, 53 (%26,6)'ünün orta, 101 (%50,8)'inin iyi dediği; 19 (%9,5)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihaz ve ortamlardaki kritik bilgiler geri getirilmeyecek şekilde silinmektedir" maddesinin uygulanması konusunda katılımcıların 12 (%6,0)'sinin hiç, 14 (%7,0)'ünün kötü, 36 (%18,1)'sının orta, 74 (%37,2)'ünün iyi dediği; 63 (%31,7)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Nesnelerin interneti (IoT cihazları) ile ilgili kurulum, imha ve yeniden kullanıma alma gibi işlemler yetkili personelce yapılmaktadır" maddesinin uygulanması konusunda katılımcıların 5 (%2,5)'inin hiç, 9 (%4,5)'unun kötü, 31 (%15,6)'inin

orta, 117 (%58,8)'sinin iyi dediği; 37 (%18,6)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu bulgulara göre; üniversite kütüphanelerindeki donanım varlılarının güvenliğine ilişkin önlemelerin çoğunluğunun (1. madde %69,3, 2. madde %54,3, 3. madde %73,9, 7. madde %50,8, 9. madde %58,8) iyi düzeylerde uygulandığı fakat önlemlerin uygulanma düzeylerine genel olarak bakıldığında yeterli seviyelerde gerçekleşmediği anlaşılmaktadır. Özellikle donanım önlemlerine ilişkin fikir sahibi olmayan kütüphane personelinin bazı donanım önlemlerinde (4. madde %27,6; 5. madde %28,6; 6. madde %34,2; 8. madde %31,7) yoğunlaştığı, bu durumun ise donanım güvenliği önlemlerine ilişkin güvenlik tehdidi risklerini arttıracağı söylenebilir.

Tablo 6.10'da teknolojik bilgi güvenliği önlemlerinden yazılım önlemlerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.10: Yazılım güvenliği önlemlerinin uygulanma düzeyleri

	Yazılım Güvenliği Önlemleri Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	***Kötü***	***Orta***	***İyi***	
10	Yazılımların adı, sürümü, yayımcısı, sözleşme, lisans ve edinim tarihi gibi bilgilerden oluşan detaylı yazılım envanteri tutulmaktadır.	*f*	2	6	32	137	22
		%	1,0	3,0	16,1	68,8	11,1
11	Yazılım ve uygulamaların kurulumu, yapılandırılması ve güncellemesi yetkili personel tarafından yapılacak şekilde kısıtlanmaktadır.	*f*	1	6	39	140	13
		%	0,5	3,0	19,6	70,4	6,5
12	Yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması gibi kontroller kullanılmaktadır.	*f*	7	13	35	67	77
		%	3,5	6,5	17,6	33,7	38,7
13	Bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması gibi kontroller uygulanmaktadır.	*f*	7	9	32	93	58
		%	3,5	4,5	16,1	46,7	29,1
14	Bilgisayarların ve bilişim sistemlerinin korunması ve taranması için zararlı yazılım tespit uygulamaları (Norton, Mcafee, Bitdefender vb. kullanılmaktadır.	*f*	2	8	28	140	21
		%	1,0	4,0	14,1	70,4	10,6
15	Zararlı yazılım ve saldırı tespit gibi koruma uygulamaları, kullanıcılar tarafından devre dışı bırakılmayacak şekilde yapılandırılmaktadır.	*f*	2	9	39	106	43
		%	1,0	4,5	19,6	53,3	21,6
16	Kritik veri işleyen sistem yazılımları, onaylanmamış dosya yüklemelerine ve yetkisiz değişikliklere karşı düzenli olarak gözden geçirilmektedir.	*f*	5	13	30	99	52
		%	2,5	6,5	15,1	49,7	26,1
17	Felaket, saldırı, sistem arızası ve kullanıcı hatası kaynaklı veri / bilgi kayıplarına karşı yazılım ve uygulama yedeklemeleri yapılmaktadır.	*f*	5	6	33	122	33
		%	2,5	3,0	16,6	61,3	16,6
18	Olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemleri düzenli olarak gözden geçirilmektedir.	*f*	6	6	35	102	50
		%	3,0	3,0	17,6	51,3	25,1
19	Bilgi sistemlerinde tespit edilen zararlı yazılımlar ve saldırılar üst yönetime ve bilgi işlem birimine iletilmektedir.	*f*	2	6	28	137	26
		%	1,0	3,0	14,1	68,8	13,1
20	Bilgisayarlar, taşınabilir ortamları zararlı yazılım taramasından otomatik olarak geçirilecek ve otomatik olarak çalıştırılmasına izin vermeyecek şekilde yapılandırılmaktadır.	*f*	4	5	40	105	45
		%	2,0	2,5	20,1	52,8	22,6
21	Kurumsal ve kişisel bilgi içeren uygulamalara ve yazılımlara, kişisel cihaz ve ortamların bağlanmasına izin verilmemektedir.	*f*	7	16	49	100	27
		%	3,5	8,0	24,6	50,3	13,6

Tablo 6.10'daki yazılım güvenliğine ilişkin veriler incelendiğinde;

"Yazılımların adı, sürümü, yayımcısı, sözleşme, lisans ve edinim tarihi gibi bilgilerden oluşan detaylı yazılım envanteri tutulmaktadır" maddesinin uygulanması konusunda katılımcıların 2 (%1,0)'sinin hiç, 6 (%3,0)'sının kötü, 32 (%16,1)'sinin orta, 137 (%68,8)'sinin iyi dediği; 22 (%11,1)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Yazılım ve uygulamaların kurulumu, yapılandırılması ve güncellemesi yetkili personel tarafından yapılacak şekilde kısıtlanmaktadır” maddesinin uygulanması konusunda katılımcıların 1 (%0,5)’inin hiç, 6 (%3,0)’sının kötü, 39 (%19,6)’unun orta, 140 (%70,4)’ının iyi dediği; 13 (%6,5)’ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması gibi kontroller kullanılmaktadır” maddesinin uygulanması konusunda katılımcıların 7 (%3,5)’sinin hiç, 9 (%4,5)’unun kötü, 32 (%16,1)’sinin orta, 93 (%46,7)’ünün iyi dediği; 58 (%29,1)’inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması gibi kontroller uygulanmaktadır” maddesinin uygulanması konusunda katılımcıların 7 (%3,5)’sinin hiç, 9 (%4,5)’unun kötü, 32 (%16,1)’sinin orta, 93 (%46,7)’ünün iyi dediği; 58 (%29,1)’sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Bilgisayarların ve bilişim sistemlerinin korunması ve taranması için zararlı yazılım tespit uygulamaları (Norton, Mcafee, Bitdefender vb. kullanılmaktadır” maddesinin uygulanması konusunda katılımcıların 2 (%1,0)’sinin hiç, 8 (%4,0)’inin kötü, 28 (%14,1)’inin orta, 140 (%70,4)’ının iyi dediği; 21 (%10,6)’inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Zararlı yazılım ve saldırı tespit gibi koruma uygulamaları, kullanıcılar tarafından devre dışı bırakılmayacak şekilde yapılandırılmaktadır” maddesinin uygulanması konusunda katılımcıların 2 (%1,0)’sinin hiç, 9 (%4,5)’unun kötü, 39 (%19,6)’unun orta, 106 (%53,3)’sının iyi dediği; 43 (%21,6)’ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Kritik veri işleyen sistem yazılımları, onaylanmamış dosya yüklemelerine ve yetkisiz değişikliklere karşı düzenli olarak gözden geçirilmektedir” maddesinin uygulanması konusunda katılımcıların 5 (%2,5)’inin hiç, 13 (%6,5)’ünün kötü, 30 (%15,1’unun orta, 99 (%49,7)’unun iyi dediği; 52 (%26,1)’sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Felaket, saldırı, sistem arızası ve kullanıcı hatası kaynaklı veri / bilgi kayıplarına karşı

yazılım ve uygulama yedeklemeleri yapılmaktadır" maddesinin uygulanması konusunda katılımcıların 5 (%2,5)'inin hiç, 6 (%3,0)'sının kötü, 33 (%16,6)'ünün orta, 122 (%61,3)'sinin iyi dediği; 33 (%16,6)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemleri düzenli olarak gözden geçirilmektedir" maddesinin uygulanması konusunda katılımcıların 6 (%3,0)'sının hiç, 6 (%3,0)'sının kötü, 35 (%17,6)'inin orta, 102 (%51,3)'sinin iyi dediği; 50 (%25,1)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi sistemlerinde tespit edilen zararlı yazılımlar ve saldırılar üst yönetime ve bilgi işlem birimine iletilmektedir" maddesinin uygulanması konusunda katılımcıların 2 (%1,0)'sinin hiç, 6 (%3,0)'sının kötü, 28 (%14,1)'inin orta, 137 (%68,8)'sinin iyi dediği; 26 (%13,1)'sının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgisayarlar, taşınabilir ortamları zararlı yazılım taramasından otomatik olarak geçirilecek ve otomatik olarak çalıştırılmasına izin vermeyecek şekilde yapılandırılmaktadır" maddesinin uygulanması konusunda katılımcıların 4 (%2,0)'ünün hiç, 5 (%2,5)'inin kötü, 40 (%20,1)'ının orta, 105 (%52,8)'inin iyi dediği; 45 (%22,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kurumsal ve kişisel bilgi içeren uygulamalara ve yazılımlara, kişisel cihaz ve ortamların bağlanmasına izin verilmemektedir" maddesinin uygulanması konusunda katılımcıların 7 (%3,5)'sinin hiç, 16 (%8,0)'sının kötü, 49 (%24,6)'unun orta, 100 (%50,3)'ünün iyi dediği; 27 (%13,6)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu Bulgulara göre üniversite kütüphanelerindeki yazılım varlıklarının güvenliğine ilişkin önlemelerin çoğunluğunun (10. madde %68,8; 11. madde %70,4; 14. madde %70,4; 17. madde %61,3; 19. madde %68,8) iyi düzeylerde uygulandığı görülmektedir. Fakat birçok yazılım önleminde (12. madde %38,7; 13. madde %29,1; 15. madde %21,6; 16. madde %26,1; 18. madde %25,1; 20. madde %22,6) yüksek oranlarda katılımcının fikir sahibi olmadığı, bu nedenle donanım güvenliği önlemlerine ilişkin uygulamaların tam anlamıyla bilinmediği ve eksikliklerin olduğu söylenebilir.

Tablo 6.11'de teknolojik bilgi güvenliği önlemlerinden ağ önlemlerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.11: Ağ güvenliği önlemlerinin uygulanma düzeyleri

	Ağ Güvenliği Önlemleri Maddeleri		***Uygulanma Düzeyi***				***Yorum***
			Hiç	***Kötü***	***Orta***	***İyi***	
22	Ağ hizmetlerinin güvenliği için kullanıcı kimlik doğrulama ve şifreleme gibi ağ bağlantısı kontrolleri uygulanmaktadır.	*f*	1	3	23	162	10
		%	0,5	1,5	11,6	81,4	5,0
23	Ağlar; personel, öğrenci gibi kullanıcı seviyelerine ve bilgi sistemlerine göre birbirinden ayrılmaktadır. (Personel / öğrenci ağı, sunucu / istemci ağı vb.)	*f*	4	6	24	154	11
		%	2,0	3,0	12,1	77,4	5,5
24	Misafir cihazlarının yalnızca misafir ağına erişimlerinin olduğu genel ağdan izole edilmiş ayrı bir ağ kullanılmaktadır.	*f*	10	11	29	120	29
		%	5,0	5,5	14,6	60,3	14,6
25	Bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemleri kullanılmaktadır.	*f*	3	3	26	107	60
		%	1,5	1,5	13,1	53,8	30,2
26	Onaylanmayan ve erişimi yasak olan web sitelerinin bağlantısını engellemek için ağ tabanlı URL filtrelemesi uygulanmaktadır.	*f*	1	5	26	129	38
		%	0,5	2,5	13,1	64,8	19,1
27	Ağlar arasında iletişim güvenliğini sağlamak ve uzak kullanıcıları kurum ağlarına güvenli şekilde bağlamak için güvenlik duvarı gibi güvenli ağ geçitleri kullanılmaktadır.	*f*	2	4	30	141	22
		%	1,0	2,0	15,1	70,9	11,1
28	Kritik bilgi işleyen bilgisayar ve diğer sistemlerin wifi, bluetooth, 3G gibi kablosuz ve kablolu ağ bağlantıları sınırlandırılmakta veya engellenmektedir.	*f*	10	8	24	94	63
		%	5,0	4,0	12,1	47,2	31,7
29	Elektronik bilgi iletiminde, elektronik haberleşme ile ilgili iş süreçleri, yasal ve güvenlik kontrol gereksinimleri dikkate alınmaktadır.	*f*	3	1	32	124	39
		%	1,5	0,5	16,1	62,3	19,6
30	Kurumun ağ yönetim sorumlularının bilgisi olmadan ağa switch, hub, modem veya access point gibi aktif cihazlar dâhil edilmemektedir.	*f*	4	3	26	125	41
		%	2,0	1,5	13,1	62,8	20,6
31	Ağ teknolojisi ile çalışan telefon, faks, fotokopi gibi cihazların kayıtları tutulmakta ve kullanıcı sorumluları belirlenmektedir.	*f*	4	4	33	121	37
		%	2,0	2,0	16,6	60,8	18,6
32	Kurum ağına bağlanan kullanıcılara ait donanımların erişimleri, port seviyesinde kontrol edilmekte ve zararlı donanımlar engellenmektedir.	*f*	2	6	24	108	59
		%	1,0	3,0	12,1	54,3	29,6

Tablo 6.11'deki ağ güvenliğine ilişkin veriler incelendiğinde;

“Ağ hizmetlerinin güvenliği için kullanıcı kimlik doğrulama ve şifreleme gibi ağ bağlantısı kontrolleri uygulanmaktadır” maddesinin uygulanması konusunda katılımcıların 1 (%0,5)’inin hiç, 3 (%1,5)’ünün kötü, 23 (%11,6)’ünün orta, 162 (%81,4)’sinin iyi dediği; 10 (%5,0)’unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Ağlar; personel, öğrenci gibi kullanıcı seviyelerine ve bilgi sistemlerine göre birbirinden ayrılmaktadır. (Personel / öğrenci ağı, sunucu / istemci ağı vb.)” maddesinin uygulanması konusunda katılımcıların 4 (%0,2)’ünün hiç, 6 (%3,0)’sının kötü, 24 (%12,1)’ünün orta, 154 (%77,4)’ünün iyi dediği; 11 (%5,5)’inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Misafir cihazlarının yalnızca misafir ağına erişimlerinin olduğu genel ağdan izole edilmiş ayrı bir ağ kullanılmaktadır” maddesinin uygulanması konusunda katılımcıların 10 (%5,0)’unun hiç, 11 (%5,5)’inin kötü, 29 (%14,6)’unun orta, 120 (%60,3)’sinin iyi dediği; 29 (%14,6)’unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemleri kullanılmaktadır” maddesinin uygulanması konusunda katılımcıların 3 (%1,5)’ünün hiç, 3 (%1,5)’ünün kötü, 26 (%13,1)’sının orta, 107 (%53,8)’sinin iyi dediği; 60 (%30,2)’ının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Onaylanmayan ve erişimi yasak olan web sitelerinin bağlantısını engellemek için ağ tabanlı URL filtrelemesi uygulanmaktadır” maddesinin uygulanması konusunda katılımcıların 1 (%0,5)’inin hiç,5 (%2,5)’inin kötü, 26 (%13,1)’sının orta, 129 (%64,8)’unun iyi dediği; 38 (%19,1)’inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Ağlar arasında iletişim güvenliğini sağlamak ve uzak kullanıcıları kurum ağlarına güvenli şekilde bağlamak için güvenlik duvarı gibi güvenli ağ geçitleri kullanılmaktadır” maddesinin uygulanması konusunda katılımcıların 2 (%1,0)’sinin hiç, 2 (%2,0)’sinin kötü, 30 (%15,1)’unun orta, 141 (%70,9)’inin iyi dediği; 22 (%11,1)’sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Kritik bilgi işleyen bilgisayar ve diğer sistemlerin wifi, bluetooth, 3G gibi kablosuz ve

kablolu ağ bağlantıları sınırlandırılmakta veya engellenmektedir" maddesinin uygulanması konusunda katılımcıların 10 (%5,0)'unun hiç, 8 (%4,0)'inin kötü, 24 (%12,1)'ünün orta, 94 (%47,2)'ünün iyi dediği; 63 (%31,7)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Elektronik bilgi iletiminde, elektronik haberleşme ile ilgili iş süreçleri, yasal ve güvenlik kontrol gereksinimleri dikkate alınmaktadır" maddesinin uygulanması konusunda katılımcıların 3 (%1,5)'ünün hiç, 1 (%0,5)'inin kötü, 32 (%16,1)'sinin orta, 124 (%62,3)'ünün iyi dediği; 39 (%19,6)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kurumun ağ yönetim sorumlularının bilgisi olmadan ağa switch, hub, modem veya access point gibi aktif cihazlar dâhil edilmemektedir" maddesinin uygulanması konusunda katılımcıların 4 (%2,0)'ünün hiç, 3 (%1,5)'ünün kötü, 26 (%13,1)'sının orta, 125 (%62,8)'inin iyi dediği; 41 (%20,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

31. maddenin uygulanması konusunda katılımcıların 4 (%2,0)'ünün hiç, 4 (%2,0)'ünün kötü, 33 (%16,6)'ünün orta, 121 (%60,8)'inin iyi dediği; 37 (%18,6)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

32. maddenin uygulanması konusunda katılımcıların 2 (%1,0)'sinin hiç, 6 (%3,0)'sının kötü, 24 (%12,1)'ünün orta, 108 (%54,3)'inin iyi dediği; 59 (%29,6)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu bulgulara göre, üniversite kütüphanelerindeki ağ varlıklarının güvenliğine ilişkin önlemelerden 28. maddedeki (%47,2) önlem dışında diğer önlemlerin %53,3 ile %81,4 oranları arasında iyi düzeylerde uygulandığı sonucuna ulaşılmıştır. 28. maddedeki önleme ilişkin %31,7 oranında katılımcının fikir sahibi olmadığını belirtmesi, bu maddedeki önlemin diğerlerine göre iyi oranlarda çıkmamasına sebep olduğu söylenebilir. Ayrıca 25. maddedeki önleme %30,2 ve 32. maddedeki önleme ise %29,6 oranında kullanıcının fikir sunmadığı, bu nedenle bu maddelerdeki uygulama düzeyinin de iyi olduğu görülse de diğer iyi seviyedeki uygulamalara göre düşük oranda olduğu görülmektedir. Ağ güvenliği önlemleri uygulamalarının hiç uygulanmaması ise %0,5 ile %5,0 arasında düşük oranlarda gerçekleştiği görülmektedir.

Tablo 6.12'de teknolojik bilgi güvenliği önlemlerinden veri önlemlerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.12: Veri güvenliği önlemlerinin uygulanma düzeyleri

	Veri Güvenliği Önlemleri Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	*Kötü*	*Orta*	*İyi*	
33	Bilgi yaşam döngüsü içerisinde işlenen, depolanan, iletilen ve imha edilen kritik bilgiler belirlenmekte ve kayıtları tutulmaktadır.	*f*	4	8	42	105	40
		%	2,0	4,0	21,1	52,8	20,1
34	Bilgiler; değeri, kritikliği ve gizliliği gibi hassasiyetlere göre sınıflandırılmakta ve uygun sınıflandırma etiketi verilmektedir.	*f*	5	10	39	104	41
		%	2,5	5,0	19,6	52,3	20,6
35	Bilgisayar ve taşınabilir ortamlarda (HDD, SSD, harici bellek vb.) muhafaza edilen kritik bilgiler şifrelenmektedir.	*f*	7	9	47	92	44
		%	3,5	4,5	23,6	46,2	22,1
36	Kritik ve değerli bilgiler, depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmekte ve saklanmaktadır.	*f*	4	7	39	118	31
		%	2,0	3,5	19,6	59,3	15,6
37	Kullanım dışı kalan bilgisayar ve depolama ortamlarındaki kritik bilgiler, yetkili personelce güvenli şekilde silinmektedir.	*f*	4	6	41	109	39
		%	2,0	3,0	20,6	54,8	19,6
38	Kritik bilgiye ve bilgi işleme sistemlerine erişimler, en az ayrıcalık ilkesine göre yetkilendirilen personelle kısıtlanmaktadır.	*f*	2	6	38	115	38
		%	1,0	3,0	19,1	57,8	19,1
39	Kişisel bilgilerin erişim yetkilendirmeleri önceden belirlenmiş ilke ve yöntemlere göre verilmektedir.	*f*	0	10	35	120	34
		%	0,0	5,0	17,6	60,3	17,1
40	Bilgi sistemlerindeki kullanıcı bilgilerinin tedarikçilerce ihlal edilmemesi karşılıklı sözleşme ile koruma altına alınmaktadır.	*f*	3	6	35	103	52
		%	1,5	3,0	17,6	51,8	26,1
41	Personel, tedarikçi ve kullanıcıların bilgi sistemlerindeki bilgilere erişim yetkileri, düzenli aralıklarla gözden geçirilmekte ve ilişkileri sone erdiğinde kaldırılmaktadır.	*f*	2	9	30	121	37
		%	1,0	4,5	15,1	60,8	18,6
42	Bilgi sistemi ve hizmetlerinden yararlanacak her kullanıcı için ayrı bir hesap tanımlanmakta ve ortak hesap kullanımına izin verilmemektedir.	*f*	1	6	30	139	23
		%	0,5	3,0	15,1	69,8	11,6
43	Kullanıcılardan kişisel bilgilerin sistemler arasında veya gerekli hallerde kurum içinde kullanılacağı ile ilgili açık rıza onayı alınmaktadır.	*f*	7	10	37	110	35
		%	3,5	5,0	18,6	55,3	17,6
44	Bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin (T.C. numarası, doğum tarihi vb. üyelik numarası ve şifre olarak kullanılmamaktadır.	*f*	8	23	40	99	29
		%	4,0	11,6	20,1	49,7	14,6
45	Bilgi sistemlerine varsayılan kullanıcı hesap parolalarıyla giriş izni verilmemekte, güçlü parola kullanımı uygulanmaktadır.	*f*	7	20	37	111	24
		%	3,5	10,1	18,6	55,8	12,1
46	Kritik bilgilerin kurum dışına aktarımı sadece yetkili kullanıcı hesaplarıyla yapılmaktadır.	*f*	3	5	31	122	38
		%	1,5	2,5	15,6	61,3	19,1
47	Veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi kimlik doğrulama sistemleri kullanılmaktadır.	*f*	11	10	29	89	60
		%	5,5	5,0	14,6	44,7	30,2

Tablo 6.12'deki veri güvenliğine ilişkin veriler incelendiğinde;

"Bilgi yaşam döngüsü içerisinde işlenen, depolanan, iletilen ve imha edilen kritik bilgiler belirlenmekte ve kayıtları tutulmaktadır" maddesinin uygulanması konusunda katılımcıların 4 (%2,0)'ünün hiç, 8 (%4,0)'inin kötü, 42 (%21,1)'sinin orta, 105 (%52,8)'inin iyi dediği; 40 (%20,1)'ının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgiler; değeri, kritikliği ve gizliliği gibi hassasiyetlere göre sınıflandırılmakta ve uygun sınıflandırma etiketi verilmektedir." maddesinin uygulanması konusunda katılımcıların 5 (%2,5)'inin hiç, 10 (%5,0)'unun kötü, 39 (%19,6)'unun orta, 104 (%52,3)'ünün iyi dediği; 41 (%20,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgisayar ve taşınabilir ortamlarda (HDD, SSD, harici bellek vb.) muhafaza edilen kritik bilgiler şifrelenmektedir" maddesinin uygulanması konusunda katılımcıların 7 (%3,5)'sinin hiç, 9 (%4,5)'unun kötü, 47 (%23,6)'sinin orta, 92 (%46,2)'sinin iyi dediği; 44 (%22,1)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kritik ve değerli bilgiler, depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmekte ve saklanmaktadır" maddesinin uygulanması konusunda katılımcıların 4 (%2,0)'ünün hiç, 7 (%3,5)'sinin kötü, 39 (%19,6)'unun orta, 118 (%59,3)'inin iyi dediği; 31 (%15,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kullanım dışı kalan bilgisayar ve depolama ortamlarındaki kritik bilgiler, yetkili personelce güvenli şekilde silinmektedir" maddesinin uygulanması konusunda katılımcıların 4 (%2,0)'ünün hiç, 6 (%3,0)'sının kötü, 38 (%19,1)'inin orta, 109 (%54,8)'unun iyi dediği; 39 (%19,6)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kritik bilgiye ve bilgi işleme sistemlerine erişimler, en az ayrıcalık ilkesine göre yetkilendirilen personelle kısıtlanmaktadır" maddesinin uygulanması konusunda katılımcıların 2 (%1,0)'sinin hiç, 6 (%3,0)'sının kötü, 38 (%19,1)'inin orta, 115 (%57,8)'inin iyi dediği; 38 (%19,1)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Kişisel bilgilerin erişim yetkilendirmeleri önceden belirlenmiş ilke ve yöntemlere göre verilmektedir” maddesinin uygulanması konusunda katılımcıların 10 (%5,0)’unun kötü, 35 (%17,6)’inin orta, 120 (%60,3)’sinin iyi dediği; 34 (%17,1)’ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Bilgi sistemlerindeki kullanıcı bilgilerinin tedarikçilerce ihlal edilmemesi karşılıklı sözleşme ile koruma altına alınmaktadır” maddesinin uygulanması konusunda katılımcıların 3 (%1,5)’ünün hiç, 6 (%3,0)’sının kötü, 35 (%17,6)’inin orta, 103 (%51,8)’ünün iyi dediği; 52 (%26,1)’sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Personel, tedarikçi ve kullanıcıların bilgi sistemlerindeki bilgilere erişim yetkileri, düzenli aralıklarla gözden geçirilmekte ve ilişkileri sone erdiğinde kaldırılmaktadır” maddesinin uygulanması konusunda katılımcıların 2 (%1,0)’sinin hiç, 9 (%4,5)’unun kötü, 30 (%15,1)’unun orta, 121 (%60,8)’inin iyi dediği; 37 (%18,6)’sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Bilgi sistemi ve hizmetlerinden yararlanacak her kullanıcı için ayrı bir hesap tanımlanmakta ve ortak hesap kullanımına izin verilmemektedir” maddesinin uygulanması konusunda katılımcıların 1 (%0,5)’inin hiç, 6 (%3,0)’sının kötü, 30 (%15,1)’unun orta, 139 (%69,8)’unun iyi dediği; 23 (%11,6)’ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Kullanıcılardan kişisel bilgilerin sistemler arasında veya gerekli hallerde kurum içinde açık rıza onayı alınmaktadır” maddesinin uygulanması konusunda katılımcıların 7 (%3,5)’sinin hiç, 10 (%5,0)’unun kötü, 37 (%18,6)’sinin orta, 110 (%55,3)’unun iyi dediği; 35 (%17,6)’inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin (T.C. numarası, doğum tarihi vb. üyelik numarası ve şifre olarak kullanılmamaktadır” maddesinin uygulanması konusunda katılımcıların 8 (%4,0)’inin hiç, 23 (%11,6)’ünün kötü, 40 (%20,1)’ının orta, 99 (%49,7)’unun iyi dediği; 29 (%14,6)’unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Bilgi sistemlerine varsayılan kullanıcı hesap parolalarıyla giriş izni verilmemekte, güçlü parola kullanımı uygulanmaktadır” maddesinin uygulanması konusunda

katılımcıların 7 (%3,5)'sinin hiç, 20 (%10,1)'sinin kötü, 37 (%18,6)'sinin orta, 111 (%55,8)'inin iyi dediği; 24 (%12,1)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kritik bilgilerin kurum dışına aktarımı sadece yetkili kullanıcı hesaplarıyla yapılmaktadır" maddesinin uygulanması konusunda katılımcıların 3 (%1,5)'ünün hiç, 5 (%2,5)'inin kötü, 31 (%15,6)'inin orta, 122 (%11,3)'sinin iyi dediği; 38 (%19,1)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi kimlik doğrulama sistemleri kullanılmaktadır" maddesinin uygulanması konusunda katılımcıların 11 (%5,5)'inin hiç, 10 (%5,0)'unun kötü, 29 (%14,6)'unun orta, 89 (%44,7)'unun iyi dediği; 60 (%30,2)'ının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu bulgulara göre, üniversite kütüphanelerindeki veri varlıklarının güvenliğine ilişkin önlemelerden 35. madde (%46,2), 44. madde (%49,7) ve 47. madde (%44,7), önlemleri dışındaki çoğu önlemin %51,8 ile %69,8 oranları arasında iyi düzeylerde uygulandığı sonucuna ulaşılmıştır. Ayrıca %11,6 ile %30,2 oranları arasında katılımcının bu gruptaki önlemler hakkında fikir sunmadıkları görülmüştür. Veri güvenliği önlemlerine bu oranlarda fikir sunmayan katılımcının olması, bu gruptaki önlemlerin uygulanması konusunda risk oluşturduğu söylenebilir.

Tablo 6.13'te teknolojik bilgi güvenliği önlemlerinden donanım önlemlerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.13: Fiziksel ve çevresel güvenlik önlemlerinin uygulanma düzeyleri

	Fiziki ve Çevresel Güvenlik Önlemleri Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	*Kötü*	*Orta*	*İyi*	
48	Kütüphanenin ana giriş ve çıkış kapıları güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile denetlenmektedir.	*f*	14	9	22	154	0
		%	7,0	4,5	11,1	77,4	0,0
49	Kritik bilgi barındıran alanların fiziksel güvenlik sınırları belirlenmekte ve kapı, pencere gibi kısımlar güvenlik mekanizmaları ile korunmaktadır.	*f*	8	20	40	126	5
		%	4,0	10,1	20,1	63,3	2,5
50	Kütüphanede güvenlik kontrollerini sağlayacak yetkinliğe sahip yeterli sayıda güvenlik personeli çalıştırılmaktadır.	*f*	30	41	44	83	1
		%	15,1	20,6	22,1	41,7	0,5
51	Kütüphanenin iç ve dış alanları güvenlik kameraları ile takip edilmektedir.	*f*	5	15	36	141	2
		%	2,5	7,5	18,1	70,9	1,0
52	Ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb. giriş ve çıkışları kayıt altına alınmakta ve sadece ilgili amaçları için erişim izni verilmektedir.	*f*	22	28	38	108	3
		%	11,1	14,1	19,1	54,3	1,5
53	Ziyaretçilerin kabul edileceği alanlar personel ve kullanıcı çalışma alanlarından ayrı bir bölgede konumlandırılmaktadır.	*f*	37	38	42	82	0
		%	18,6	19,1	21,1	41,2	0,0
54	Refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğu uygulanmaktadır.	*f*	68	44	30	53	4
		%	34,2	22,1	15,1	26,6	2,0
55	Kritik bilgilerin işlendiği veya saklandığı alanlara erişim, uygun kontroller (kartlı / şifreli erişim vb.) uygulanarak yetkili kişiler ile sınırlandırılmaktadır.	*f*	13	22	35	120	9
		%	6,5	11,1	17,6	60,3	4,5
56	Kütüphane binasına ait pencereler, kapılar ve bahçe alanları, demir parmaklık, çit, kilit, tel örgü gibi dış güvenlik unsurlarıyla kontrol edilmektedir.	*f*	26	31	46	95	1
		%	13,1	15,6	23,1	47,7	0,5
57	Bilgi sistemlerinin enerji ve iletişim hizmetlerini taşıyan kablolar, dinleme ve hasara karşı kablo kanalı ve izolasyon malzemeleriyle korunmaktadır.	*f*	7	12	39	102	39
		%	3,5	6,0	19,6	51,3	19,6
58	Doğal afetler, kötü niyetli saldırılar ve kazaklara karşı fiziksel koruma önlemleri büyük oranda alınmakta ve personel bilgilendirilmektedir.	*f*	9	27	52	103	8
		%	4,5	13,6	26,1	51,8	4,0
59	Elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarları kullanılmaktadır.	*f*	10	19	40	76	54
		%	5,0	9,5	20,1	38,2	27,1

Tablo 6.13'teki fiziksel ve çevresel güvenliğe ilişkin veriler incelendiğinde;

"Kütüphanenin ana giriş ve çıkış kapıları güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile denetlenmektedir" maddesinin uygulanması konusunda katılımcıların 14 (%7,0)'ünün hiç, 9 (%4,5)'unun kötü, 22 (%11,1)'sinin orta, 154 (%77,4)'ünün iyi dediği görülmektedir.

“Kritik bilgi barındıran alanların fiziksel güvenlik sınırları belirlenmekte ve kapı, pencere gibi kısımlar güvenlik mekanizmaları ile korunmaktadır” maddesinin uygulanması konusunda katılımcıların 8 (%4,0)’inin hiç, 20 (%10,1)’sinin kötü, 40 (%20,1)’ının orta, 126 (%63,3)’sının iyi dediği; 5 (%2,5)’inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Kütüphanede güvenlik kontrollerini sağlayacak yetkinliğe sahip yeterli sayıda güvenlik personeli çalıştırılmaktadır” maddesinin uygulanması konusunda katılımcıların 30 (%15,1)’unun hiç, 41 (%20,6)’inin kötü, 44 (%22,1)’ünün orta, 83 (%41,7)’ünün iyi dediği; 1 (%0,5)’inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Kütüphanenin iç ve dış alanları güvenlik kameraları ile takip edilmektedir” maddesinin uygulanması konusunda katılımcıların 5 (%2,5)’inin hiç, 15 (%7,5)’inin kötü, 36 (%18,1)’sının orta, 141 (%70,9)’inin iyi dediği; 2 (%1,0)’sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb. giriş ve çıkışları kayıt altına alınmakta ve sadece ilgili amaçları için erişim izni verilmektedir” maddesinin uygulanması konusunda katılımcıların 22 (%11,1)’sinin hiç, 28 (%14,1)’inin kötü, 38 (%19,1)’inin orta, 108 (%54,3)’inin iyi dediği; 3 (%1,5)’ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Ziyaretçilerin kabul edileceği alanlar personel ve kullanıcı çalışma alanlarından ayrı bir bölgede konumlandırılmaktadır” maddesinin uygulanması konusunda katılımcıların 37 (%18,6)’sinin hiç, 38 (%19,1)’inin kötü, 42 (%21,1)’sinin orta, 82 (%41,2)’sinin iyi dediği görülmektedir.

“Refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğu uygulanmaktadır” maddesinin uygulanması konusunda katılımcıların 68 (%34,2)’inin hiç, 44 (%22,1)’ünün kötü, 30 (%15,1)’unun orta, 53 (%26,6)’ünün iyi dediği; 4 (%2,0)’ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Kritik bilgilerin işlendiği veya saklandığı alanlara erişim, uygun kontroller (kartlı / şifreli erişim vb.) uygulanarak yetkili kişiler ile sınırlandırılmaktadır” maddesinin uygulanması konusunda katılımcıların 13 (%6,5)’ünün hiç, 22 (%11,1)’sinin kötü, 35

(%17,6)'inin orta, 120 (%60,3)'sinin iyi dediği; 9 (%4,5)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kütüphane binasına ait pencereler, kapılar ve bahçe alanları, demir parmaklık, çit, kilit, tel örgü gibi dış güvenlik unsurlarıyla kontrol edilmektedir" maddesinin uygulanması konusunda katılımcıların 26 (%13,1)'sının hiç, 31 (%15,6)'inin kötü, 46 (%23,1)'sının orta, 95 (%47,7)'inin iyi dediği; 1 (%1,5)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi sistemlerinin enerji ve iletişim hizmetlerini taşıyan kablolar, dinleme ve hasara karşı kablo kanalı ve izolasyon malzemeleriyle korunmaktadır" maddesinin uygulanması konusunda katılımcıların 7 (%3,5)'sinin hiç, 12 (%6,0)'sinin kötü, 39 (%19,6)'unun orta, 102 (%51,3)'sinin iyi dediği; 39 (%19,6)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Doğal afetler, kötü niyetli saldırılar ve kazaklara karşı fiziksel koruma önlemleri büyük oranda alınmakta ve personel bilgilendirilmektedir" maddesinin uygulanması konusunda katılımcıların 9 (%4,5)'unun hiç, 27 (%13,6)'sinin kötü, 52 (%26,1)'sinin orta, 103 (%51,8)'ünün iyi dediği; 8 (%4,0)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarları kullanılmaktadır" maddesinin uygulanması konusunda katılımcıların 10 (%5,0)'unun hiç, 19 (%9,5)'unun kötü, 40 (%20,1)'ının orta, 76 (%38,2)'sının iyi dediği; 54 (%27,1)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu bulgulara göre, üniversite kütüphanelerindeki fiziksel ce çevresel varlıklarının güvenliğine ilişkin önlemelerden 48. madde (%77,4), 49. madde (%63,3), 51. madde (%70,9) ve 55. maddedeki (%60,3) önlemlerin iyi oranlarda uygulandığı görülmektedir. 54. maddedeki önlemin bu grup altında en az oranda uygulandığı hatta hiç uygulanmama oranın (%34,2) en yüksek olduğu uygulama olduğu belirlenmiştir. Bu kategori altında yer alan önlemelere ilişkin katılımcıların fikir sahip olama oranı yüksek oranlarda olduğu görülmektedir. Sadece 57. madde (%19,6) ve 59. maddedeki (%27,1) önlemlere ilişkin fikir sahibi olmama oranın yüksek olması katılımcıların kütüphanelerindeki altyapı hizmetlerine ilişkin bilgilerinin olmaması söylenebilir.

6.6.2. Üniversite Türü Değişkenine Göre Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri

Bu başlık altında, katılımcıların görev yaptıkları üniversitelerin türüne göre teknolojik bilgi güvenliği önlemlerinden donanım güvenliği, yazılım güvenliği, ağ güvenliği, veri güvenliği ve fiziksel/çevresel güvenlik kategorilerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin ilişkin frekans dağılımları ve ki kare istatistikleri verilmiştir.

Tablo 6.14'te görev yapılan üniversitelerin türüne göre, teknolojik bilgi güvenliği önlemlerinden donanım önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.14: Katılımcıların görev yaptıkları üniversitelerin türüne göre donanım önlemlerinin uygulanma düzeyleri

	Donanım Güvenliği *Önlemleri Maddeleri*	Üniversite Türü		Uygulanma düzeyi Hiç	Kötü	Orta	İyi	X^2
1	Veri işleme, depolama ve iletme yeteneğine sahip tüm donanımların envanteri tutulmakta ve kullanım tahsisleri yapılmaktadır.	Devlet	*f*	2	4	29	80	X^2=2,747 p>,05
			%	1,7	3,5	25,2	69,6	
		Vakıf	*f*	0	1	14	58	
			%	0,0	1,4	19,2	79,5	
2	Kütüphane envanterindeki tüm cihaz ve taşınabilir ortamlar, kaybolma veya çalınma riskine karşı şifrelenmektedir.	Devlet	*f*	3	16	37	58	X^2=6,691 p>,05
			%	2,6	14,0	32,5	50,9	
		Vakıf	*f*	0	5	18	50	
			%	0,0	6,8	24,7	68,5	
3	Kritik bilgi içeren taşınabilir cihaz ve ortamlar güvenli şekilde saklanmakta ve kurum dışına çıkarılmasına izin verilmemektedir.	Devlet	*f*	1	6	18	91	X^2=1,377 p>,05
			%	0,9	5,2	15,5	78,4	
		Vakıf	*f*	0	3	15	56	
			%	0,0	4,1	20,3	75,7	
4	Kütüphane envanterinden çıkarılan donanımların veri depolama ünitelerindeki veri ve bilgiler geri getirilmeyecek şekilde silinmektedir	Devlet	*f*	4	7	23	55	X^2=5,132 p>,05
			%	4,5	7,9	25,8	61,8	
		Vakıf	*f*	2	0	18	35	
			%	3,6	0,0	32,7	63,6	
5	Kullanım ömrünü tamamlamış veri depolama üniteleri (HDD, SSD, harici bellek vb.) güvenli bir biçimde imha edilmektedir.	Devlet	*f*	7	12	14	54	X^2=5,816 p>,05
			%	8,0	13,8	16,1	62,1	
		Vakıf	*f*	4	3	17	31	
			%	7,3	5,5	30,9	56,4	
6	Yeni tedarik edilen sabit diskler veri kurtarmaya imkân sağlamayacak bir şekilde biçimlendirilerek sisteme dâhil edilmektedir	Devlet	*f*	4	10	24	39	X^2=3,036 p>,05
			%	5,2	13,0	31,2	50,6	
		Vakıf	*f*	6	5	12	31	
			%	11,1	9,3	22,2	57,4	
7	Bilgi içeren tüm cihaz ve ortamların ısı, nem gibi tehditlere maruz kalamaması için çevresel önlemler alınmaktadır.	Devlet	*f*	7	11	35	59	X^2=1,922 p>,05
			%	6,3	9,8	31,3	52,7	
		Vakıf	*f*	2	6	18	42	
			%	2,9	8,8	26,5	61,8	
8	Onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihaz ve ortamlardaki kritik bilgiler geri getirilmeyecek şekilde silinmektedir.	Devlet	*f*	7	11	22	46	X^2=1,647 p>,05
			%	8,1	12,8	25,6	53,5	
		Vakıf	*f*	5	3	14	28	
			%	10,0	6,0	28,0	56,0	
9	Nesnelerin interneti (IoT cihazları) ile ilgili kurulum, imha ve yeniden kullanıma alma gibi işlemler yetkili personelce yapılmaktadır.	Devlet	*f*	4	7	18	70	X^2=1,761 p>,05
			%	4,0	7,1	18,2	70,7	
		Vakıf	*f*	1	2	13	47	
			%	1,6	3,2	20,6	74,6	

Tablo 6.14'teki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden donanım kategorisinde yer alan önlemlerin uygulanma düzeyleri hakkında

katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olmadığı görülmektedir.

Tablo 6.15'te görev yapılan üniversitelerin türüne göre, teknolojik bilgi güvenliği önlemlerinden yazılım önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.15: Katılımcıların görev yaptıkları üniversitelerin türüne göre yazılım önlemlerinin uygulanma düzeyleri

	Yazılım Güvenliği Önlemleri Maddeleri	Üniversite Türü		Uygulanma düzeyi				X^2
				Hiç	Kötü	Orta	İyi	
10	Yazılımların adı, sürümü, yayımcısı, sözleşme, lisans ve edinim tarihi gibi bilgilerden oluşan detaylı yazılım envanteri tutulmaktadır.	Devlet	*f*	1	5	18	82	
			%	0,9	4,7	17,0	77,4	X^2=1,744
		Vakıf	*f*	1	1	14	55	p>,05
			%	1,4	1,4	19,7	77,5	
11	Yazılım ve uygulamaların kurulumu, yapılandırılması ve güncellemesi yetkili personel tarafından yapılacak şekilde kısıtlanmaktadır.	Devlet	*f*	1	5	24	84	
			%	0,9	4,4	21,1	73,7	X^2=1,722
		Vakıf	*f*	0	1	15	56	p>,05
			%	0,0	1,4	20,8	77,8	
12	Yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması gibi kontroller kullanılmaktadır.	Devlet	*f*	7	12	17	36	
			%	9,7	16,7	23,6	50,0	**X^2=13,738**
		Vakıf	*f*	0	1	18	31	**p<,05**
			%	0,0	2,0	36,0	62,0	
13	Bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması gibi kontroller uygulanmaktadır.	Devlet	*f*	7	7	18	52	
			%	8,3	8,3	21,4	61,9	X^2=6,708
		Vakıf	*f*	0	2	14	41	p>,05
			%	0,0	3,5	24,6	71,9	
14	Bilgisayarların ve bilişim sistemlerinin korunması ve taranması için zararlı yazılım tespit uygulamaları (Norton, Mcafee, Bitdefender vb. kullanılmaktadır.	Devlet	*f*	2	6	15	86	
			%	1,8	5,5	13,8	78,9	X^2=2,146
		Vakıf	*f*	0	2	13	54	p>,05
			%	0,0	2,9	18,8	78,3	
15	Zararlı yazılım ve saldırı tespit gibi koruma uygulamaları, kullanıcılar tarafından devre dışı bırakılmayacak şekilde yapılandırılmaktadır.	Devlet	*f*	2	6	24	63	
			%	2,1	6,3	25,3	66,3	X^2=1,135
		Vakıf	*f*	0	3	15	43	p>,05
			%	0,0	4,9	24,6	70,5	
16	Kritik veri işleyen sistem yazılımları, onaylanmamış dosya yüklemelerine ve yetkisiz değişikliklere karşı düzenli olarak gözden geçirilmektedir.	Devlet	*f*	5	10	19	56	
			%	5,6	11,1	21,1	62,2	X^2=5,099
		Vakıf	*f*	0	3	11	43	p>,05
			%	0,0	5,3	19,3	75,4	
17	Felaket, saldırı, sistem arızası ve kullanıcı hatası kaynaklı veri / bilgi kayıplarına karşı yazılım ve uygulama yedeklemeleri yapılmaktadır.	Devlet	*f*	5	4	20	75	
			%	4,8	3,8	19,2	72,1	X^2=1,647
		Vakıf	*f*	0	2	13	47	p>,05
			%	0,0	3,2	21,0	75,8	
18	Olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemleri düzenli olarak gözden geçirilmektedir.	Devlet	*f*	6	6	19	61	
			%	6,5	6,5	20,7	66,3	**X^2=8,251**
		Vakıf	*f*	0	0	16	41	**p<,05**
			%	0,0	0,0	28,1	71,9	
19	Bilgi sistemlerinde tespit edilen zararlı yazılımlar ve saldırılar üst yönetime ve bilgi işlem birimine iletilmektedir.	Devlet	*f*	2	5	12	87	
			%	1,9	4,7	11,3	82,1	X^2=3,036
		Vakıf	*f*	0	1	16	50	p>,05
			%	0,0	1,5	23,9	74,6	
20	Bilgisayarlar, taşınabilir ortamları zararlı yazılım taramasından otomatik olarak geçirilecek ve otomatik olarak çalıştırılmasına izin vermeyecek şekilde yapılandırılmaktadır	Devlet	*f*	4	4	24	61	
			%	4,3	4,3	25,8	65,6	X^2=3,160
		Vakıf	*f*	0	1	16	44	p>,05
			%	0,0	1,6	26,2	72,1	
21	Kurumsal ve kişisel bilgi içeren uygulamalara ve yazılımlara, kişisel cihaz ve ortamların bağlanmasına izin verilmemektedir.	Devlet	*f*	5	11	31	57	
			%	4,8	10,6	29,8	54,8	X^2=1,376
		Vakıf	*f*	2	5	18	43	p>,05
			%	2,9	7,4	26,5	63,2	

Tablo 6.15'teki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden yazılım kategorisindeki 12.ve 18. maddede yer alan önlemlerin uygulanmasında

katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olduğu görülmektedir (p<0,05). Bu bulgulardan hareketle devlet üniversitesi kütüphanelerinde bu iki yazılım güvenliği önleminin uygulanma düzeyinin vakıf üniversitesi kütüphanelerinden daha düşük olduğu söylenebilir.

Tablo 6.16'da görev yapılan üniversitelerin türüne göre, teknolojik bilgi güvenliği önlemlerinden ağ önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.16: Katılımcıların görev yaptıkları üniversitelerin türüne göre ağ önlemlerinin uygulanma düzeyleri

	Ağ Güvenliği Önlemleri Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
22	Ağ hizmetlerinin güvenliği için kullanıcı kimlik doğrulama ve şifreleme gibi ağ bağlantısı kontrolleri uygulanmaktadır.	Devlet	*f*	0	2	14	100	X^2=1,701 p>,05
			%	0,0	1,7	12,1	86,2	
		Vakıf	*f*	1	1	9	62	
			%	1,4	1,4	12,3	84,9	
23	Ağlar; personel, öğrenci gibi kullanıcı seviyelerine ve bilgi sistemlerine göre birbirinden ayrılmaktadır.	Devlet	*f*	4	5	15	90	X^2=3,664 p>,05
			%	3,5	4,4	13,2	78,9	
		Vakıf	*f*	0	1	9	64	
			%	0,0	1,4	12,2	86,5	
24	Misafir cihazlarının yalnızca misafir ağına erişimlerinin olduğu genel ağdan izole edilmiş ayrı bir ağ kullanılmaktadır.	Devlet	*f*	4	8	20	68	X^2=3,674 p>,05
			%	4,0	8,0	20,0	68,0	
		Vakıf	*f*	6	3	9	52	
			%	8,6	4,3	12,9	74,3	
25	Bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemleri kullanılmaktadır.	Devlet	*f*	3	3	14	63	X^2=3,621 p>,05
			%	3,6	3,6	16,9	75,9	
		Vakıf	*f*	0	0	12	44	
			%	0,0	0,0	21,4	78,6	
26	Onaylanmayan ve erişimi yasak olan web sitelerinin bağlantısını engellemek için ağ tabanlı URL filtrelemesi uygulanmaktadır.	Devlet	*f*	1	4	14	80	X^2=1,856 p>,05
			%	1,0	4,0	14,1	80,8	
		Vakıf	*f*	0	1	12	49	
			%	0,0	1,6	19,4	79,0	
27	Ağlar arasında iletişim güvenliğini sağlamak ve uzak kullanıcıları kurum ağlarına güvenli şekilde bağlamak için güvenlik duvarı gibi güvenli ağ geçitleri kullanılmaktadır	Devlet	*f*	2	3	20	84	X^2=1,664 p>,05
			%	1,8	2,8	18,3	77,1	
		Vakıf	*f*	0	1	10	57	
			%	0,0	1,5	14,7	83,8	
28	Kritik bilgi işleyen bilgisayar ve diğer sistemlerin wifi, bluetooth, 3G gibi kablosuz ve kablolu ağ bağlantıları sınırlandırılmakta veya engellenmektedir.	Devlet	*f*	6	3	16	58	X^2=5,099 p>,05
			%	7,2	3,6	19,3	69,9	
		Vakıf	*f*	4	5	8	36	
			%	7,5	9,4	15,1	67,9	
29	Elektronik bilgi iletiminde, elektronik haberleşme ile ilgili iş süreçleri, yasal ve güvenlik kontrol gereksinimleri dikkate alınmaktadır.	Devlet	*f*	3	1	16	75	X^2=2,218 p>,05
			%	3,2	1,1	16,8	78,9	
		Vakıf	*f*	0	0	16	49	
			%	0,0	0,0	24,6	75,4	
30	Kurumun ağ yönetim sorumlularının bilgisi olmadan ağa switch, hub, modem veya access point gibi aktif cihazlar dâhil edilmemektedir.	Devlet	*f*	3	2	17	73	X^2=0,929 p>,05
			%	3,2	2,1	17,9	76,8	
		Vakıf	*f*	1	1	9	52	
			%	1,6	1,6	14,3	82,5	
31	Ağ teknolojisi ile çalışan telefon, faks, fotokopi gibi cihazların kayıtları tutulmakta ve kullanıcı sorumluları belirlenmektedir.	Devlet	*f*	3	4	20	74	X^2=2,406 p>,05
			%	3,0	4,0	19,8	73,3	
		Vakıf	*f*	1	0	13	47	
			%	1,6	0,0	21,3	77,0	
32	Kurum ağına bağlanan kullanıcılara ait donanımların erişimleri, port seviyesinde kontrol edilmekte ve zarlı donanımlar engellenmektedir.	Devlet	*f*	1	5	13	62	X^2=1,900 p>,05
			%	1,2	6,2	16,0	76,5	
		Vakıf	*f*	1	1	11	46	
			%	1,7	1,7	18,6	78,0	

Tablo 6.16'daki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden ağ

kategorisinde yer alan önlemlerin uygulanma düzeyleri hakkında katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olmadığı görülmektedir.

Tablo 6.17'de görev yapılan üniversitelerin türüne göre, teknolojik bilgi güvenliği önlemlerinden veri önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.17: Katılımcıların görev yaptıkları üniversitelerin türüne göre veri önlemlerinin uygulanma düzeyleri

	Veri Güvenliği Önlemleri Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
33	Bilgi yaşam döngüsü içerisinde işlenen, depolanan, iletilen ve imha edilen kritik bilgiler belirlenmekte ve kayıtları tutulmaktadır.	Devlet	*f*	4	5	25	63	X^2=2,345 p>,05
			%	4,1	5,2	25,8	64,9	
		Vakıf	*f*	0	3	17	42	
			%	0,0	4,8	27,4	67,7	
34	Bilgiler; değeri, kritikliği ve gizliliği gibi hassasiyetlere göre sınıflandırılmakta ve uygun sınıflandırma etiketi verilmektedir.	Devlet	*f*	5	6	23	62	X^2=3,179 p>,05
			%	5,2	6,3	24,0	64,6	
		Vakıf	*f*	0	4	16	42	
			%	0,0	6,5	25,8	67,7	
35	Bilgisayar ve taşınabilir ortamlarda (HDD, SSD, harici bellek vb.) muhafaza edilen kritik bilgiler şifrelenmektedir.	Devlet	*f*	4	7	31	52	X^2=2,294p >,05
			%	4,3	7,4	33,0	55,3	
		Vakıf	*f*	3	2	16	40	
			%	4,9	3,3	26,2	65,6	
36	Kritik ve değerli bilgiler, depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmekte ve saklanmaktadır.	Devlet	*f*	4	7	24	66	**X^2=7,956 p<,05**
			%	4,0	6,9	23,8	65,3	
		Vakıf	*f*	0	0	15	52	
			%	0,0	0,0	22,4	77,6	
37	Kullanım dışı kalan bilgisayar ve depolama ortamlarındaki kritik bilgiler, yetkili personelce güvenli şekilde silinmektedir.	Devlet	*f*	4	3	27	63	X^2=3,436 p>,05
			%	4,1	3,1	27,8	64,9	
		Vakıf	*f*	0	3	14	46	
			%	0,0	4,8	22,2	73,0	
38	Kritik bilgiye ve bilgi işleme sistemlerine erişimler, en az ayrıcalık ilkesine göre yetkilendirilen personelle kısıtlanmaktadır.	Devlet	*f*	2	5	22	69	X^2=2,174 p>,05
			%	2,0	5,1	22,4	70,4	
		Vakıf	*f*	0	1	16	46	
			%	0,0	1,6	25,4	73,0	
39	Kişisel bilgilerin erişim yetkilendirmeleri önceden belirlenmiş ilke ve yöntemlere göre verilmektedir.	Devlet	*f*	8	20	73	8	X^2=1,624 p>,05
			%	7,9	19,8	72,3	7,9	
		Vakıf	*f*	2	15	47	2	
			%	3,1	23,4	73,4	3,1	
40	Bilgi sistemlerindeki kullanıcı bilgilerinin tedarikçilerce ihlal edilmemesi karşılıklı sözleşme ile koruma altına alınmaktadır.	Devlet	*f*	3	6	20	61	X^2=5,621 p>,05
			%	3,3	6,7	22,2	67,8	
		Vakıf	*f*	0	0	15	42	
			%	0,0	0,0	26,3	73,7	
41	Personel, tedarikçi ve kullanıcıların bilgi sistemlerindeki bilgilere erişim yetkileri, düzenli aralıklarla gözden geçirilmekte ve ilişkileri sone erdiğinde kaldırılmaktadır.	Devlet	*f*	2	7	17	71	X^2=2,253 p>,05
			%	2,1	7,2	17,5	73,2	
		Vakıf	*f*	0	2	13	50	
			%	0,0	3,1	20,0	76,9	
42	Bilgi sistemi ve hizmetlerinden yararlanacak her kullanıcı için ayrı bir hesap tanımlanmakta ve ortak hesap kullanımına izin verilmemektedir.	Devlet	*f*	1	5	17	89	X^2=2,020 p>,05
			%	0,9	4,5	15,2	79,5	
		Vakıf	*f*	0	1	13	50	
			%	0,0	1,6	20,3	78,1	
43	Kullanıcılardan kişisel bilgilerin sistemler arasında veya gerekli hallerde kurum içinde kullanılacağı ile ilgili açık rıza onayı alınmaktadır.	Devlet	*f*	4	8	21	65	X^2=1,860 p>,05
			%	4,1	8,2	21,4	66,3	
		Vakıf	*f*	3	2	16	45	
			%	4,5	3,0	24,2	68,2	

Tablo 6.17'nin Devamı

	Veri Güvenliği Önlemleri Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	***Kötü***	***Orta***	***İyi***	
44	Bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin (T.C. numarası, doğum tarihi vb.) üyelik numarası ve şifre olarak kullanılmamaktadır.	Devlet	*f*	7	20	24	54	**X^2=10,863**
			%	6,7	19,0	22,9	51,4	**p<,05**
		Vakıf	*f*	1	3	16	45	
			%	1,5	4,6	24,6	69,2	
45	Bilgi sistemlerine varsayılan kullanıcı hesap parolalarıyla giriş izni verilmemekte, güçlü parola kullanımı uygulanmaktadır.	Devlet	*f*	4	15	25	65	
			%	3,7	13,8	22,9	59,6	X^2=2,542
		Vakıf	*f*	3	5	12	46	p>,05
			%	4,5	7,6	18,2	69,7	
46	Kritik bilgilerin kurum dışına aktarımı sadece yetkili kullanıcı hesaplarıyla yapılmaktadır.	Devlet	*f*	1	4	20	72	
			%	1,0	4,1	20,6	74,2	X^2=1,960
		Vakıf	*f*	2	1	11	50	p>,05
			%	3,1	1,6	17,2	78,1	
47	Veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi kimlik doğrulama sistemleri kullanılmaktadır.	Devlet	*f*	7	7	16	54	
			%	8,3	8,3	19,0	64,3	X^2=0,779
		Vakıf	*f*	4	3	13	35	p>,05
			%	7,3	5,5	23,6	63,6	

Tablo 6.17'deki eriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden veri kategorisindeki 36. ve 44. maddede yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$). Bu bulgular, devlet üniversitesi kütüphanelerinde bazı yazılım önlemlerinin uygulanma düzeyinin vakıf üniversitesi kütüphanelerinden daha düşük olduğunu göstermektedir. Bu bulgulardan hareketle devlet üniversitesi kütüphanelerinde bu iki maddede yer alan kritik bilgilerin hasarı ve kaybı riskine karşı farklı bir güvenli ortamda yedeklenmesi ve kullanıcıların kişisel bilgilerinin üyelik bilgileri olarak kullanılmaması önlemlerinin uygulanma düzeyinin vakıf üniversitesi kütüphanelerinden daha düşük olduğu söylenebilir

Tablo 6.18'de görev yapılan üniversitelerin türüne göre, teknolojik bilgi güvenliği önlemlerinden fiziksel ve çevresel önlemlerin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.18: Katılımcıların görev yaptıkları üniversitelerin türüne göre fiziksel ve çevresel önlemlerin uygulanma düzeyleri

	Fiziksel ve Çevresel Güvenlik Önlemleri Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
48	Kütüphanenin ana giriş ve çıkış kapıları güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile denetlenmektedir.	Devlet	*f*	4	4	13	103	**X^2=9,478 p<,05**
			%	3,2	3,2	10,5	83,1	
		Vakıf	*f*	10	5	9	51	
			%	13,3	6,7	12,0	68,0	
49	Kritik bilgi barındıran alanların fiziksel güvenlik sınırları belirlenmekte ve kapı, pencere gibi kısımlar güvenlik mekanizmaları ile korunmaktadır.	Devlet	*f*	5	13	20	82	X^2=3,050 p>,05
			%	4,2	10,8	16,7	68,3	
		Vakıf	*f*	3	7	20	44	
			%	4,1	9,5	27,0	59,5	
50	Kütüphanede güvenlik kontrollerini sağlayacak yetkinliğe sahip yeterli sayıda güvenlik personeli çalıştırılmaktadır.	Devlet	*f*	19	25	28	52	X^2=0,73 p<,05
			%	15,3	20,2	22,6	41,9	
		Vakıf	*f*	11	16	16	31	
			%	14,9	21,6	21,6	41,9	
51	Kütüphanenin iç ve dış alanları güvenlik kameraları ile takip edilmektedir.	Devlet	*f*	5	8	24	86	X^2=3,704 p>,05
			%	4,1	6,5	19,5	69,9	
		Vakıf	*f*	0	7	12	55	
			%	0,0	9,5	16,2	74,3	
52	Ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb.) giriş ve çıkışları kayıt altına alınmakta ve sadece ilgili amaçları için erişim izni verilmektedir.	Devlet	*f*	19	19	28	55	**X^2=13,732 p<,05**
			%	15,7	15,7	23,1	45,5	
		Vakıf	*f*	3	9	10	53	
			%	4,0	12,0	13,3	70,7	
53	Ziyaretçilerin kabul edileceği alanlar personel ve kullanıcı çalışma alanlarından ayrı bir bölgede konumlandırılmaktadır.	Devlet	*f*	28	25	22	49	X^2=5,001 p>,05
			%	22,6	20,2	17,7	39,5	
		Vakıf	*f*	9	13	20	33	
			%	12,0	17,3	26,7	44,0	
54	Refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğu uygulanmaktadır.	Devlet	*f*	52	27	15	27	**X^2=10,640 p<,05**
			%	43,0	22,3	12,4	22,3	
		Vakıf	*f*	16	17	15	26	
			%	21,6	23,0	20,3	35,1	
55	Kritik bilgilerin işlendiği veya saklandığı alanlara erişim, uygun kontroller (kartlı / şifreli erişim vb.) uygulanarak yetkili kişiler ile sınırlandırılmaktadır.	Devlet	*f*	8	14	24	72	X^2=0,871 p>,05
			%	6,8	11,9	20,3	61,0	
		Vakıf	*f*	5	8	11	48	
			%	6,9	11,1	15,3	66,7	
56	Kütüphane binasına ait pencereler, kapılar ve bahçe alanları, demir parmaklık, çit, kilit, tel örgü gibi dış güvenlik unsurlarıyla kontrol edilmektedir.	Devlet	*f*	22	20	26	56	**X^2=6,700 p<,05**
			%	17,7	16,1	21,0	45,2	
		Vakıf	*f*	4	11	20	39	
			%	5,4	14,9	27,0	52,7	
57	Bilgi sistemlerinin enerji ve iletişim hizmetlerini taşıyan kablolar, dinleme ve hasara karşı kablo kanalı ve izolasyon malzemeleriyle korunmaktadır.	Devlet	*f*	6	8	22	59	X^2=2,326 p>,05
			%	6,3	8,4	23,2	62,1	
		Vakıf	*f*	1	4	17	43	
			%	1,5	6,2	26,2	66,2	
58	Doğal afetler, kötü niyetli saldırılar ve kazaklara karşı fiziksel koruma önlemleri büyük oranda alınmakta ve personel bilgilendirilmektedir.	Devlet	*f*	8	20	28	64	X^2=5,897 p>,05
			%	6,7	16,7	23,3	53,3	
		Vakıf	*f*	1	7	24	39	
			%	1,4	9,9	33,8	54,9	
59	Elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarları kullanılmaktadır.	Devlet	*f*	7	11	23	43	X^2=0,658 p>,05
			%	8,3	13,1	27,4	51,2	
		Vakıf	*f*	3	8	17	33	
			%	4,9	13,1	27,9	54,1	

Tablo 6.18'deki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden fiziksel ve çevresel önlemler kategorisindeki 48, 52, 54 ve 56. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$). Bu bulgulardan hareketle devlet üniversitesi kütüphanelerinde ana giriş ve çıkış kapıları güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile

denetlenmesi önlemlerinin uygulanma düzeyinin vakıf üniversitesi kütüphanelerinden daha yüksek olduğu söylenebilir. Fakat ziyaretçilerin giriş ve çıkışlarını kayıt altına alınması, refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartının takma zorunluluğu uygulanması ve kütüphane binasına ait pencereler, kapılar ve bahçe alanlarının dış güvenlik unsurlarıyla kontrol edilmesi önlemlerinin vakıf üniversitesi kütüphanelerinden daha yüksek düzeylerde uygulandığı söylenebilir.

6.6.3. Bilgi Güvenliği Personeli Değişkenine Göre Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri

Bu başlık altında, üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre teknolojik bilgi güvenliği önlemlerinden donanım güvenliği, yazılım güvenliği, ağ güvenliği, veri güvenliği ve fiziksel/çevresel güvenlik kategorilerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin ilişkin frekans dağılımları ve ki kare istatistikleri verilmiştir.

Tablo 6.19'da üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre, teknolojik bilgi güvenliği önlemlerinden donanım önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.19: Bilgi güvenliğinden sorumlu personelin varlığına göre donanım önlemlerinin uygulanma düzeyleri

	Donanım Güvenliği *Önlemleri Maddeleri*	Bilgi Güvenliği Personeli		Uygulanma düzeyi Hiç	Kötü	Orta	İyi	X^2
01	Veri işleme, depolama ve iletme yeteneğine sahip tüm donanımların güncel envanteri tutulmakta ve kullanım tahsisleri yapılmaktadır.	Var	*f*	0	0	20	50	X^2=5,115 p>,05
			%	0,0	0,0	28,6	71,4	
		Yok	*f*	2	5	23	88	
			%	1,7	4,2	19,5	74,6	
2	Kütüphane envanterindeki tüm cihaz ve taşınabilir ortamlar, kaybolma veya çalınma riskine karşı şifrelenmektedir.	Var	*f*	0	2	19	49	**X^2=12,023 p<,05**
			%	0,0	2,9	27,1	70,0	
		Yok	*f*	3	19	36	59	
			%	2,6	16,2	30,8	50,4	
3	Kritik bilgi içeren taşınabilir cihaz ve ortamlar güvenli şekilde saklanmakta ve kurum dışına çıkarılmasına izin verilmemektedir.	Var	*f*	0	0	11	60	**X^2=7,359 p<,05**
			%	0,0	0,0	15,5	84,5	
		Yok	*f*	1	9	22	87	
			%	0,8	7,6	18,5	73,1	
4	Kütüphane envanterinden çıkarılan donanımların veri depolama ünitelerindeki veri / bilgi geri getirilmeyecek şekilde silinmektedir	Var	*f*	0	1	16	35	X^2=4,940 p>,05
			%	0,0	1,9	30,8	67,3	
		Yok	*f*	6	6	25	55	
			%	6,5	6,5	27,2	59,8	
5	Kullanım ömrünü tamamlamış veri depolama üniteleri (HDD, SSD, harici bellek, USB, disk vb.) güvenli bir biçimde imha edilmektedir.	Var	*f*	1	2	12	41	**X^2=11,282 p<,05**
			%	1,8	3,6	21,4	73,2	
		Yok	*f*	10	13	19	44	
			%	11,6	15,1	22,1	51,2	
6	Yeni tedarik edilen sabit diskler veri kurtarmaya imkân sağlamayacak bir şekilde biçimlendirilerek sisteme dâhil edilmektedir	Var	*f*	2	3	13	36	**X^2=8,045 p<,05**
			%	3,7	5,6	24,1	66,7	
		Yok	*f*	8	12	23	34	
			%	10,4	15,6	29,9	44,2	
7	Bilgi içeren tüm cihaz ve ortamların ısı, nem ve elektromanyetik zararlara maruz kalamaması için çevresel önlemleri alınmaktadır.	Var	*f*	1	2	19	44	**X^2=9,155 p<,05**
			%	1,5	3,0	28,8	66,7	
		Yok	*f*	8	15	34	57	
			%	7,0	13,2	29,8	50,0	
8	Onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihaz ve ortamlardaki kritik bilgiler geri getirilmeyecek şekilde silinmektedir.	Var	*f*	1	2	15	36	**X^2=11,242 p<,05**
			%	1,9	3,7	27,8	66,7	
		Yok	*f*	11	12	21	38	
			%	13,4	14,6	25,6	46,3	
9	Nesnelerin interneti (IoT cihazları) ile ilgili kurulum, imha ve yeniden kullanıma alma gibi işlemler yetkili personelce yapılmaktadır.	Var	*f*	0	3	10	49	X^2=4,014 p>,05
			%	0,0	4,8	16,1	79,0	
		Yok	*f*	5	6	21	68	
			%	5,0	6,0	21,0	68,0	

Tablo 6.19'daki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden donanım kategorisindeki 2, 3. 5, 6, 7 ve 8. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.20'de üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre, teknolojik bilgi güvenliği önlemlerinden yazılım önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki

kare istatistiği verilmiştir.

Tablo 6.20: Bilgi güvenliğinden sorumlu personelin varlığına göre yazılım önlemlerinin uygulanma düzeyleri

	Yazılım Güvenliği Önlemleri Maddeleri	**Bilgi Güvenliği Personeli**		*Uygulanma düzeyi*				X^2
					Kötü	***Orta***	***İyi***	
10	Yazılımların adı, sürümü, yayımcısı, sözleşme, lisans ve edinim tarihi gibi bilgilerden oluşan detaylı yazılım envanteri tutulmaktadır.	Var	*f*	0	2	11	55	X^2=0,815 p>,05
			%	0,0	2,9	16,2	80,9	
		Yok	*f*	2	4	21	82	
			%	1,8	3,7	19,3	75,2	
11	Yazılım ve uygulamaların kurulumu, yapılandırılması ve güncellemesi yetkili personel tarafından yapılacak şekilde kısıtlanmaktadır.	Var	*f*	0	2	12	56	X^2=1,725 p>,05
			%	0,0	2,9	17,1	80,0	
		Yok	*f*	1	4	27	84	
			%	0,9	3,4	23,3	72,4	
12	Yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması gibi kontroller kullanılmaktadır.	Var	*f*	1	3	15	33	X^2=5,259 p>,05
			%	1,9	5,8	28,8	63,5	
		Yok	*f*	6	10	20	34	
			%	8,6	14,3	28,6	48,6	
13	Bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması gibi kontroller uygulanmaktadır.	Var	*f*	0	0	14	42	**X^2=12,666 p<,05**
			%	0,0	0,0	25,0	75,0	
		Yok	*f*	7	9	18	51	
			%	8,2	10,6	21,2	60,0	
14	Bilgisayarların ve bilişim sistemlerinin korunması ve taranması için zararlı yazılım tespit uygulamaları (Norton, Mcafee, Bitdefender vb. kullanılmaktadır.	Var	*f*	0	2	10	55	X^2=1,470 p>,05
			%	0,0	3,0	14,9	82,1	
		Yok	*f*	2	6	18	85	
			%	1,8	5,4	16,2	76,6	
15	Zararlı yazılım ve saldırı tespit gibi koruma uygulamaları, kullanıcılar tarafından devre dışı bırakılmayacak şekilde yapılandırılmaktadır.	Var	*f*	0	3	14	46	X^2=1,854 p>,05
			%	0,0	4,8	22,2	73,0	
		Yok	*f*	2	6	25	60	
			%	2,2	6,5	26,9	64,5	
16	Kritik veri işleyen sistem yazılımları, onaylanmamış dosya yüklemelerine ve yetkisiz değişikliklere karşı düzenli olarak gözden geçirilmektedir.	Var	*f*	0	2	13	45	**X^2=7,659 p<,05**
			%	0,0	3,3	21,7	75,0	
		Yok	*f*	5	11	17	54	
			%	5,7	12,6	19,5	62,1	
17	Felaket, saldırı, sistem arızası ve kullanıcı hatası kaynaklı veri / bilgi kayıplarına karşı yazılım ve uygulama yedeklemeleri yapılmaktadır.	Var	*f*	0	1	10	53	X^2=6,001 p>,05
			%	0,0	1,6	15,6	82,8	
		Yok	*f*	5	5	23	69	
			%	4,9	4,9	22,5	67,6	
18	Olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemleri düzenli olarak gözden geçirilmektedir.	Var	*f*	0	1	12	50	**X^2=8,566 p<,05**
			%	0,0	1,6	19,0	79,4	
		Yok	*f*	6	5	23	52	
			%	7,0	5,8	26,7	60,5	
19	Bilgi sistemlerinde tespit edilen zararlı yazılımlar ve saldırılar üst yönetime ve bilgi işlem birimine iletilmektedir.	Var	*f*	0	1	12	55	X^2=2,220 p>,05
			%	0,0	1,5	17,6	80,9	
		Yok	*f*	2	5	16	82	
			%	1,9	4,8	15,2	78,1	
20	Bilgisayarlar, taşınabilir ortamları zararlı yazılım taramasından otomatik olarak geçirilecek ve otomatik olarak çalıştırılmasına izin vermeyecek şekilde yapılandırılmaktadır	Var	*f*	0	2	14	47	X^2=3,708 p>,05
			%	0,0	3,2	22,2	74,6	
		Yok	*f*	4	3	26	58	
			%	4,4	3,3	28,6	63,7	
21	Kurumsal ve kişisel bilgi içeren uygulamalara ve yazılımlara, kişisel cihaz ve ortamların bağlanmasına izin verilmemektedir.	Var	*f*	1	2	19	45	**X^2=7,975 p<,05**
			%	1,5	3,0	28,4	67,2	
		Yok	*f*	6	14	30	55	
			%	5,7	13,3	28,6	52,4	

Tablo 6.20'deki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden yazılım kategorisindeki 13, 16, 18ve 21. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu

görülmektedir (p<0,05) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.21'de üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre, teknolojik bilgi güvenliği önlemlerinden ağ önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.21: Bilgi güvenliğinden sorumlu personelin varlığına göre ağ önlemlerinin uygulanma düzeyleri

	Ağ Güvenliği Önlemleri Maddeleri	**Bilgi Güvenliği Personeli**		*Uygulanma düzeyi*				X^2
				Hiç	***Kötü***	***Orta***	***İyi***	
22	Ağ hizmetlerinin güvenliği için kullanıcı kimlik doğrulama ve şifreleme gibi ağ bağlantısı kontrolleri uygulanmaktadır.	Var	*f*	0	0	11	60	X^2=2,996 p>,05
			%	0,0	0,0	15,5	84,5	
		Yok	*f*	1	3	12	102	
			%	0,8	2,5	10,2	86,4	
23	Ağlar; personel, öğrenci gibi kullanıcı seviyelerine ve bilgi sistemlerine göre birbirinden ayrılmaktadır.	Var	*f*	1	0	11	60	X^2=4,541 p>,05
			%	1,4	0,0	15,3	83,3	
		Yok	*f*	3	6	13	94	
			%	2,6	5,2	11,2	81,0	
24	Misafir cihazlarının yalnızca misafir ağına erişimlerinin olduğu genel ağdan izole edilmiş ayrı bir ağ kullanılmaktadır.	Var	*f*	4	3	9	52	X^2=2,187 p>,05
			%	5,9	4,4	13,2	76,5	
		Yok	*f*	6	8	20	68	
			%	5,9	7,8	19,6	66,7	
25	Bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemleri kullanılmaktadır.	Var	*f*	0	0	12	44	X^2=3,621 p>,05
			%	0,0	0,0	21,4	78,6	
		Yok	*f*	3	3	14	63	
			%	3,6	3,6	16,9	75,9	
26	Onaylanmayan ve erişimi yasak olan web sitelerinin bağlantısını engellemek için ağ tabanlı URL filtrelemesi uygulanmaktadır.	Var	*f*	0	0	10	53	X^2=3,783 p>,05
			%	0,0	0,0	15,9	84,1	
		Yok	*f*	1	5	16	76	
			%	1,0	5,1	16,3	77,6	
27	Ağlar arasında iletişim güvenliğini sağlamak ve uzak kullanıcıları kurum ağlarına güvenli şekilde bağlamak için güvenlik duvarı gibi güvenli ağ geçitleri kullanılmaktadır	Var	*f*	0	1	10	57	X^2=1,664 p>,05
			%	0,0	1,5	14,7	83,8	
		Yok	*f*	2	3	20	84	
			%	1,8	2,8	18,3	77,1	
28	Kritik bilgi işleyen bilgisayar ve diğer sistemlerin wifi, bluetooth, 3G gibi kablosuz ve kablolu ağ bağlantıları sınırlandırılmakta veya engellenmektedir.	Var	*f*	0	3	9	46	**X^2=10,271 p<,05**
			%	0,0	5,2	15,5	79,3	
		Yok	*f*	10	5	15	48	
			%	12,8	6,4	19,2	61,5	
29	Elektronik bilgi iletiminde, elektronik haberleşme ile ilgili iş süreçleri, yasal ve güvenlik kontrol gereksinimleri dikkate alınmaktadır.	Var	*f*	0	0	13	54	X^2=2,573 p>,05
			%	0,0	0,0	19,4	80,6	
		Yok	*f*	3	1	19	70	
			%	3,2	1,1	20,4	75,3	
30	Kurumun ağ yönetim sorumlularının bilgisi olmadan ağa switch, hub, modem veya access point gibi aktif cihazlar dâhil edilmemektedir.	Var	*f*	1	0	11	51	X^2=2,021 p>,05
			%	1,6	0,0	17,5	81,0	
		Yok	*f*	3	3	15	74	
			%	3,2	3,2	15,8	77,9	
31	Ağ teknolojisi ile çalışan telefon, faks, fotokopi gibi cihazların kayıtları tutulmakta ve kullanıcı sorumluları belirlenmektedir.	Var	*f*	0	0	11	55	X^2=6,598 p>,05
			%	0,0	0,0	16,7	83,3	
		Yok	*f*	4	4	22	66	
			%	4,2	4,2	22,9	68,8	
32	Kurum ağına bağlanan kullanıcılara ait donanımların erişimleri, port seviyesinde kontrol edilmekte ve zararlı donanımlar engellenmektedir.	Var	*f*	0	0	8	53	**X^2=8,111 p<,05**
			%	0,0	0,0	13,1	86,9	
		Yok	*f*	2	6	16	55	
			%	2,5	7,6	20,3	69,6	

Tablo 6.21'deki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden ağ kategorisindeki 28 ve 32. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.22'de üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre, teknolojik bilgi güvenliği önlemlerinden veri önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.22: Bilgi güvenliğinden sorumlu personelin varlığına göre veri önlemlerinin uygulanma düzeyleri

	Veri Güvenliği Önlemleri Maddeleri	**Bilgi Güvenliği Personeli**		***Uygulanma düzeyi***				***X²***
				Hiç	***Kötü***	***Orta***	***İyi***	
33	Bilgi yaşam döngüsü içerisinde işlenen, depolanan, iletilen ve imha edilen kritik bilgiler belirlenmekte ve kayıtları tutulmaktadır.	Var	*f*	0	1	14	47	
			%	0,0	1,6	22,6	75,8	X^2=6,337
		Yok	*f*	4	7	28	58	p>,05
			%	4,1	7,2	28,9	59,8	
34	Bilgiler; değeri, kritikliği ve gizliliği gibi hassasiyetlere göre sınıflandırılmakta ve uygun sınıflanma etiketi taşımaktadır.	Var	*f*	0	0	13	47	
			%	0,0	0,0	21,7	78,3	**X^2=12,258**
		Yok	*f*	5	10	26	57	**p<,05**
			%	5,1	10,2	26,5	58,2	
35	Bilgisayar ve taşınabilir ortamlarda (HDD, SSD, harici bellek vb.) muhafaza edilen kritik bilgiler şifrelenmektedir.	Var	*f*	0	0	15	44	
			%	0,0	0,0	25,4	74,6	**X^2=14,788**
		Yok	*f*	7	9	32	48	**p< ,05**
			%	7,3	9,4	33,3	50,0	
36	Kritik ve değerli bilgiler, depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmekte ve saklanmaktadır.	Var	*f*	0	0	14	51	
			%	0,0	0,0	21,5	78,5	**X^2=7,789**
		Yok	*f*	4	7	25	67	**p<,05**
			%	3,9	6,8	24,3	65,0	
37	Kullanım dışı kalan bilgisayar ve depolama ortamlarındaki kritik bilgiler, yetkili personelce güvenli şekilde silinmektedir.	Var	*f*	0	0	19	44	
			%	0,0	0,0	30,2	69,8	X^2=6,948
		Yok	*f*	4	6	22	65	p>,05
			%	4,1	6,2	22,7	67,0	
38	Kritik bilgiye ve bilgi işleme sistemlerine erişimler, en az ayrıcalık ilkesine göre yetkilendirilen personelle kısıtlanmaktadır.	Var	*f*	0	0	14	52	
			%	0,0	0,0	21,2	78,8	X^2=6,233
		Yok	*f*	2	6	24	63	p>,05
			%	2,1	6,3	25,3	66,3	
39	Kişisel bilgilerin erişim yetkilendirmeleri önceden belirlenmiş ilke ve yöntemlere göre verilmektedir.	Var	*f*	0	14	51	0	
			%	0,0	21,5	78,5	0,0	**X^2=6,990**
		Yok	*f*	10	21	69	10	**p<,05**
			%	10,0	21,0	69,0	10,0	
40	Bilgi sistemlerindeki kullanıcı bilgilerinin tedarikçilerce ihlal edilmemesi karşılıklı sözleşme ile koruma altına alınmaktadır.	Var	*f*	0	0	15	47	
			%	0,0	0,0	24,2	75,8	X^2=6,661
		Yok	*f*	3	6	20	56	p>,05
			%	3,5	7,1	23,5	65,9	
41	Personel, tedarikçi ve kullanıcıların bilgi sistemlerindeki bilgilere erişim yetkileri, düzenli aralıklarla gözden geçirilmekte ve ilişkileri sone erdiğinde kaldırılmaktadır.	Var	*f*	0	0	10	52	
			%	0,0	0,0	16,1	83,9	**X^2=8,362**
		Yok	*f*	2	9	20	69	**p<,05**
			%	2,0	9,0	20,0	69,0	

Tablo 6.22'nin Devamı

	Veri Güvenliği Önlemleri Maddeleri	**Bilgi Güvenliği Personeli**		*Uygulanma düzeyi*				X^2
				Hiç	***Kötü***	***Orta***	***İyi***	
42	Bilgi sistemi ve hizmetlerinden yararlanacak her kullanıcı için ayrı bir hesap tanımlanmakta ve ortak hesap kullanımına izin verilmemektedir.	Var	*f*	0	0	12	55	
			%	0,0	0,0	17,9	82,1	X^2=4,360
		Yok	*f*	1	6	18	84	p>,05
			%	0,9	5,5	16,5	77,1	
43	Kullanıcılardan kişisel bilgilerin sistemler arasında veya gerekli hallerde kurum içinde kullanılacağı ile ilgili açık rıza onayı alınmaktadır	Var	*f*	0	1	16	47	
			%	0,0	1,6	25,0	73,4	**X^2=9,029p**
		Yok	*f*	7	9	21	63	**<,05**
			%	7,0	9,0	21,0	63,0	
44	Bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin (T.C. numarası, doğum tarihi vb. üyelik numarası ve şifre olarak kullanılmamaktadır.	Var	*f*	1	3	14	41	
			%	1,7	5,1	23,7	69,5	**X^2=8,471**
		Yok	*f*	7	20	26	58	**p<,05**
			%	6,3	18,0	23,4	52,3	
45	Bilgi sistemlerine varsayılan kullanıcı hesap parolalarıyla giriş izni verilmemekte, güçlü parola kullanımı uygulanmaktadır.	Var	*f*	1	6	11	46	
			%	1,6	9,4	17,2	71,9	X^2=3,421
		Yok	*f*	6	14	26	65	p>,05
			%	5,4	12,6	23,4	58,6	
46	Kritik bilgilerin kurum dışına aktarımı sadece yetkili kullanıcı hesaplarıyla yapılmaktadır.	Var	*f*	0	1	11	51	
			%	0,0	1,6	17,5	81,0	X^2=2,632
		Yok	*f*	3	4	20	71	p>,05
			%	3,1	4,1	20,4	72,4	
47	Veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi kimlik doğrulama sistemleri kullanılmaktadır.	Var	*f*	3	1	12	38	
			%	5,6	1,9	22,2	70,4	X^2=4,664
		Yok	*f*	8	9	17	51	p>,05
			%	9,4	10,6	20,0	60,0	

Tablo 6.22'deki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden veri kategorisindeki 34, 35, 36, 39, 41, 43 ve 44. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.23'te üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre, teknolojik bilgi güvenliği önlemlerinden fiziksel ve çevresel önlemlerin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.23: Bilgi güvenliğinden sorumlu personelin varlığına göre fiziksel ve çevresel önlemlerin uygulanma düzeyleri

	Fiziksel ve Çevresel Güvenlik Önlemleri Maddeleri	**Bilgi Güvenliği Personeli**		*Uygulanma düzeyi* *Hiç*	*Kötü*	*Orta*	*İyi*	X^2
48	Kütüphanenin ana giriş ve çıkış kapıları güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile denetlenmektedir.	Var	*f*	4	2	9	57	X^2=1,370 p>,05
			%	5,6	2,8	12,5	79,2	
		Yok	*f*	10	7	13	97	
			%	7,9	5,5	10,2	76,4	
49	Kritik bilgi barındıran alanların fiziksel güvenlik sınırları belirlenmekte ve kapı, pencere gibi kısımlar güvenlik mekanizmaları ile korunmaktadır.	Var	*f*	1	4	11	56	**X^2=9,072 p<,05**
			%	1,4	5,6	15,3	77,8	
		Yok	*f*	7	16	29	70	
			%	5,7	13,1	23,8	57,4	
50	Kütüphanede güvenlik kontrollerini sağlayacak yetkinliğe sahip yeterli sayıda güvenlik personeli çalıştırılmaktadır.	Var	*f*	5	10	15	41	**X^2=13,823 p<,05**
			%	7,0	14,1	21,1	57,7	
		Yok	*f*	25	31	29	42	
			%	19,7	24,4	22,8	33,1	
51	Kütüphanenin iç ve dış alanları güvenlik kameraları ile takip edilmektedir.	Var	*f*	2	4	7	57	X^2=6,244 p>,05
			%	2,9	5,7	10,0	81,4	
		Yok	*f*	3	11	29	84	
			%	2,4	8,7	22,8	66,1	
52	Ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb. giriş ve çıkışları kayıt altına alınmakta ve sadece ilgili amaçları için erişim izni verilmektedir.	Var	*f*	2	8	13	48	**X^2=10,946 p<,05**
			%	2,8	11,3	18,3	67,6	
		Yok	*f*	20	20	25	60	
			%	16,0	16,0	20,0	48,0	
53	Ziyaretçilerin kabul edileceği alanlar personel ve kullanıcı çalışma alanlarından ayrı bir bölgede konumlandırılmaktadır.	Var	*f*	8	9	16	39	**X^2=10,632 p>,05**
			%	11,1	12,5	22,2	54,2	
		Yok	*f*	29	29	26	43	
			%	22,8	22,8	20,5	33,9	
54	Refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğu uygulanmaktadır.	Var	*f*	19	12	13	27	**X^2=9,149p <,05**
			%	26,8	16,9	18,3	38,0	
		Yok	*f*	49	32	17	26	
			%	39,5	25,8	13,7	21,0	
55	Kritik bilgilerin işlendiği veya saklandığı alanlara erişim, uygun kontroller (kartlı / şifreli erişim vb.) uygulanarak yetkili kişiler ile sınırlandırılmaktadır.	Var	*f*	4	3	9	55	**X^2=11,241 p<,05**
			%	5,6	4,2	12,7	77,5	
		Yok	*f*	9	19	26	65	
			%	7,6	16,0	21,8	54,6	
56	Kütüphane binasına ait pencereler, kapılar ve bahçe alanları, demir parmaklık, çit, kilit, tel örgü gibi dış güvenlik unsurlarıyla kontrol edilmektedir.	Var	*f*	7	6	18	41	X^2=1,379 p>,05
			%	9,7	8,3	25,0	56,9	
		Yok	*f*	19	25	28	54	
			%	15,1	19,8	22,2	42,9	
57	Bilgi sistemlerinin enerji ve iletişim hizmetlerini taşıyan kablolar, dinleme ve hasara karşı kablo kanalı ve izolasyon malzemeleriyle korunmaktadır.	Var	*f*	3	3	15	43	X^2=2,326 p>,05
			%	4,7	4,7	23,4	67,2	
		Yok	*f*	4	9	24	59	
			%	4,2	9,4	25,0	61,5	
58	Doğal afetler, kötü niyetli saldırılar ve kazaklara karşı fiziksel koruma önlemleri büyük oranda alınmakta ve personel bilgilendirilmektedir.	Var	*f*	3	5	17	46	X^2=6,999 p>,05
			%	4,2	7,0	23,9	64,8	
		Yok	*f*	6	22	35	57	
			%	5,0	18,3	29,2	47,5	
59	Elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarları kullanılmaktadır.	Var	*f*	2	3	16	39	**X^2=10,138 p<,05**
			%	3,3	5,0	26,7	65,0	
		Yok	*f*	8	16	24	37	
			%	9,4	18,8	28,2	43,5	

Tablo 6.23'teki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden fiziksel ve çevresel kategorisindeki 49, 50, 52, 53, 54, 55, ve 59. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip

olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

6.6.4. Bilgi Güvenliği Yönetim Aracı Değişkenine Göre Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri

Bu başlık altında, üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre teknolojik bilgi güvenliği önlemlerinden donanım güvenliği, yazılım güvenliği, ağ güvenliği, veri güvenliği ve fiziksel/çevresel güvenlik kategorilerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin ilişkin frekans dağılımları ve ki kare istatistikleri verilmiştir.

Tablo 6.24'te üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre, teknolojik bilgi güvenliği önlemlerinden donanım önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.24: Bilgi güvenliği yönetim aracının kullanımına göre donanım önlemlerinin uygulanma düzeyleri

	Donanım Güvenliği *Önlemleri Maddeleri*	Bilgi Güvenliği Yönetim Aracı		Uygulanma düzeyi Hiç	Kötü	Orta	İyi	X^2
01	Veri işleme, depolama ve iletme yeteneğine sahip tüm donanımların güncel envanteri tutulmakta ve kullanım tahsisleri yapılmaktadır.	Var	*f*	0	1	25	91	**X^2=7,457 p<,05**
			%	0,0	0,9	21,4	77,8	
		Yok	*f*	2	4	18	47	
			%	2,8	5,6	25,4	66,2	
2	Kütüphane envanterindeki tüm cihaz ve taşınabilir ortamlar, kaybolma veya çalınma riskine karşı şifrelenmektedir.	Var	*f*	1	8	27	80	**X^2=16,757 p<,05**
			%	0,9	6,9	23,3	69,0	
		Yok	*f*	2	13	28	28	
			%	2,8	18,3	39,4	39,4	
3	Kritik bilgi içeren taşınabilir cihaz ve ortamlar güvenli şekilde saklanmakta ve kurum dışına çıkarılmasına izin verilmemektedir.	Var	*f*	0	3	15	99	**X^2=10,059 p<,05**
			%	0,0	2,6	12,8	84,6	
		Yok	*f*	1	6	18	48	
			%	1,4	8,2	24,7	65,8	
4	Kütüphane envanterinden çıkarılan donanımların veri depolama ünitelerindeki veri ve bilgiler geri getirilmeyecek şekilde silinmektedir	Var	*f*	3	1	24	60	**X^2=7,792 p<,05**
			%	3,4	1,1	27,3	68,2	
		Yok	*f*	3	6	17	30	
			%	5,4	10,7	30,4	53,6	
5	Kullanım ömrünü tamamlamış veri depolama üniteleri (HDD, SSD, harici bellek, USB, disk vb.) güvenli bir biçimde imha edilmektedir.	Var	*f*	6	5	18	63	**X^2=10,869 p<,05**
			%	6,5	5,4	19,6	68,5	
		Yok	*f*	5	10	13	22	
			%	10,0	20,0	26,0	44,0	
6	Yeni tedarik edilen sabit diskler veri kurtarmaya imkân sağlamayacak bir şekilde biçimlendirilerek sisteme dâhil edilmektedir	Var	*f*	7	7	21	53	X^2=6,476 p>,05
			%	8,0	8,0	23,9	60,2	
		Yok	*f*	3	8	15	17	
			%	7,0	18,6	34,9	39,5	
7	Bilgi içeren tüm cihaz ve ortamların ısı, nem ve elektromanyetik gibi tehditlere maruz kalamaması için çevresel önlemler alınmaktadır.	Var	*f*	3	8	26	74	**X^2=13,906 p<,05**
			%	2,7	7,2	23,4	66,7	
		Yok	*f*	6	9	27	27	
			%	8,7	13,0	39,1	39,1	
8	Onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihaz ve ortamlardaki kritik bilgiler geri getirilmeyecek şekilde silinmektedir.	Var	*f*	6	8	23	55	X^2=4,329 p>,05
			%	6,5	8,7	25,0	59,8	
		Yok	*f*	6	6	13	19	
			%	13,6	13,6	29,5	43,2	
9	Nesnelerin interneti (IoT cihazları) ile ilgili kurulum, imha ve yeniden kullanıma alma gibi işlemler yetkili personelce yapılmaktadır.	Var	*f*	1	6	19	77	X^2=4,182 p>,05
			%	1,0	5,8	18,4	74,8	
		Yok	*f*	4	3	12	40	
			%	6,8	5,1	20,3	67,8	

Tablo 6.24'teki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden donanım kategorisindeki 1, 2, 3, 4, 5, ve 7. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.25'te üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre, teknolojik bilgi güvenliği önlemlerinden yazılım önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.25: Bilgi güvenliği yönetim aracının kullanımına göre yazılım önlemlerinin uygulanma düzeyleri

	Yazılım Güvenliği Önlemleri Maddeleri	**Bilgi Güvenliği Yönetim Aracı**		***Uygulanma düzeyi***			X^2
				Kötü	***Orta***	***İyi***	
10	Yazılımların adı, sürümü, yayımcısı, sözleşme, lisans ve edinim tarihi gibi bilgilerden oluşan detaylı yazılım envanteri tutulmaktadır.	Var	*f*	1	2	17	90	X^2=4,353 p>,05
			%	0,9	1,8	15,5	81,8	
		Yok	*f*	1	4	15	47	
			%	1,5	6,0	22,4	70,1	
11	Yazılım ve uygulamaların kurulumu, yapılandırılması ve güncellemesi yetkili personel tarafından yapılacak şekilde kısıtlanmaktadır.	Var	*f*	0	2	21	92	X^2=5,516 p>,05
			%	0,0	1,7	18,3	80,0	
		Yok	*f*	1	4	18	48	
			%	1,4	5,6	25,4	67,6	
12	Yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması gibi kontroller kullanılmaktadır.	Var	*f*	3	6	24	51	X^2=6,863 p>,05
			%	3,6	7,1	28,6	60,7	
		Yok	*f*	4	7	11	16	
			%	10,5	18,4	28,9	42,1	
13	Bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması gibi kontroller uygulanmaktadır.	Var	*f*	2	3	18	71	**X^2=14,033 p<,05**
			%	2,1	3,2	19,1	75,5	
		Yok	*f*	5	6	14	22	
			%	10,6	12,8	29,8	46,8	
14	Bilgisayarların ve bilişim sistemlerinin korunması ve taranması için zararlı yazılım tespit uygulamaları (Norton, Mcafee, Bitdefender vb. kullanılmaktadır.	Var	*f*	1	4	17	87	X^2=0,993 p>,05
			%	0,9	3,7	15,6	79,8	
		Yok	*f*	1	4	11	53	
			%	1,4	5,8	15,9	76,8	
15	Zararlı yazılım ve saldırı tespit gibi koruma uygulamaları, kullanıcılar tarafından devre dışı bırakılmayacak şekilde yapılandırılmaktadır.	Var	*f*	1	4	23	71	X^2=2,846 p>,05
			%	1,0	4,0	23,2	71,7	
		Yok	*f*	1	5	16	35	
			%	1,8	8,8	28,1	61,4	
16	Kritik veri işleyen sistem yazılımları, onaylanmamış dosya yüklemelerine ve yetkisiz değişikliklere karşı düzenli olarak gözden geçirilmektedir.	Var	*f*	1	6	20	68	X^2=6,676 p>,05
			%	1,1	6,3	21,1	71,6	
		Yok	*f*	4	7	10	31	
			%	7,7	13,5	19,2	59,6	
17	Felaket, saldırı, sistem arızası ve kullanıcı hatası kaynaklı veri / bilgi kayıplarına karşı yazılım ve uygulama yedeklemeleri yapılmaktadır.	Var	*f*	2	2	15	83	**X^2=8,737 p<,05**
			%	2,0	2,0	14,7	81,4	
		Yok	*f*	3	4	18	39	
			%	4,7	6,3	28,1	60,9	
18	Olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemleri düzenli olarak gözden geçirilmektedir.	Var	*f*	1	4	20	73	**X^2=8,612 p<,05**
			%	1,0	4,1	20,4	74,5	
		Yok	*f*	5	2	15	29	
			%	9,8	3,9	29,4	56,9	
19	Bilgi sistemlerinde tespit edilen zararlı yazılımlar ve saldırılar üst yönetime ve bilgi işlem birimine iletilmektedir.	Var	*f*	1	2	19	89	X^2=3,068 p>,05
			%	0,9	1,8	17,1	80,2	
		Yok	*f*	1	4	9	48	
			%	1,6	6,5	14,5	77,4	
20	Bilgisayarlar, taşınabilir ortamları zararlı yazılım taramasından otomatik olarak geçirilecek ve otomatik olarak çalıştırılmasına izin vermeyecek şekilde yapılandırılmaktadır	Var	*f*	1	2	23	76	**X^2=7,590 p<,05**
			%	1,0	2,0	22,5	74,5	
		Yok	*f*	3	3	17	29	
			%	5,8	5,8	32,7	55,8	
21	Kurumsal ve kişisel bilgi içeren uygulamalara ve yazılımlara, kişisel cihaz ve ortamların bağlanmasına izin verilmemektedir.	Var	*f*	3	9	26	72	X^2=7,229 p>,05
			%	2,7	8,2	23,6	65,5	
		Yok	*f*	4	7	23	28	
			%	6,5	11,3	37,1	45,2	

Tablo 6.25'teki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden yazılım kategorisindeki 13, 17, 18 ve 20. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma

düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.26'da üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre, teknolojik bilgi güvenliği önlemlerinden ağ önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.26: Bilgi güvenliği yönetim aracının kullanımına göre ağ önlemlerinin uygulanma düzeyleri

	Ağ Güvenliği Önlemleri Maddeleri	**Bilgi Güvenliği Yönetim Aracı**		*Uygulanma düzeyi*				X^2
				Hiç	***Kötü***	***Orta***	***İyi***	
22	Ağ hizmetlerinin güvenliği için kullanıcı kimlik doğrulama ve şifreleme gibi ağ bağlantısı kontrolleri uygulanmaktadır.	Var	*f*	0	0	16	99	X^2=6,266 p>,05
			%	0,0	0,0	13,9	86,1	
		Yok	*f*	1	3	7	63	
			%	1,4	4,1	9,5	85,1	
23	Ağlar; personel, öğrenci gibi kullanıcı seviyelerine ve bilgi sistemlerine göre birbirinden ayrılmaktadır.	Var	*f*	1	3	15	98	X^2=2,893 p>,05
			%	0,9	2,6	12,8	83,8	
		Yok	*f*	3	3	9	56	
			%	4,2	4,2	12,7	78,9	
24	Misafir cihazlarının yalnızca misafir ağına erişimlerinin olduğu genel ağdan izole edilmiş ayrı bir ağ kullanılmaktadır.	Var	*f*	8	5	16	80	X^2=4,011 p>,05
			%	7,3	4,6	14,7	73,4	
		Yok	*f*	2	6	13	40	
			%	3,3	9,8	21,3	65,6	
25	Bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemleri kullanılmaktadır.	Var	*f*	0	0	16	73	**X^2=10,225 p<,05**
			%	0,0	0,0	18,0	82,0	
		Yok	*f*	3	3	10	34	
			%	6,0	6,0	20,0	68,0	
26	Onaylanmayan ve erişimi yasak olan web sitelerinin bağlantısını engellemek için ağ tabanlı URL filtrelemesi uygulanmaktadır.	Var	*f*	0	2	12	86	**X^2=6,562 p<,05**
			%	0,0	2,0	12,0	86,0	
		Yok	*f*	1	3	14	43	
			%	1,6	4,9	23,0	70,5	
27	Ağlar arasında iletişim güvenliğini sağlamak ve uzak kullanıcıları kurum ağlarına güvenli şekilde bağlamak için güvenlik duvarı gibi güvenli ağ geçitleri kullanılmaktadır	Var	*f*	1	3	13	94	X^2=6,264 p>,05
			%	0,9	2,7	11,7	84,7	
		Yok	*f*	1	1	17	47	
			%	1,5	1,5	25,8	71,2	
28	Kritik bilgi işleyen bilgisayar ve diğer sistemlerin wifi, bluetooth, 3G gibi kablosuz ve kablolu ağ bağlantıları sınırlandırılmakta veya engellenmektedir.	Var	*f*	6	6	15	63	X^2=,725 p>,05
			%	6,7	6,7	16,7	70,0	
		Yok	*f*	4	2	9	31	
			%	8,7	4,3	19,6	67,4	
29	Elektronik bilgi iletiminde, elektronik haberleşme ile ilgili iş süreçleri, yasal ve güvenlik kontrol gereksinimleri dikkate alınmaktadır.	Var	*f*	0	0	18	88	**X^2=9,584 p<,05**
			%	0,0	0,0	17,0	83,0	
		Yok	*f*	3	1	14	36	
			%	5,6	1,9	25,9	66,7	
30	Kurumun ağ yönetim sorumlularının bilgisi olmadan ağa switch, hub, modem veya access point gibi aktif cihazlar dâhil edilmemektedir.	Var	*f*	2	1	14	80	X^2=2,453 p>,05
			%	2,1	1,0	14,4	82,5	
		Yok	*f*	2	2	12	45	
			%	3,3	3,3	19,7	73,8	
31	Ağ teknolojisi ile çalışan telefon, faks, fotokopi gibi cihazların kayıtları tutulmakta ve kullanıcı sorumluları belirlenmektedir.	Var	*f*	0	1	16	86	**X^2=14,880 p<,05**
			%	0,0	1,0	15,5	83,5	
		Yok	*f*	4	3	17	35	
			%	6,8	5,1	28,8	59,3	
32	Kurum ağına bağlanan kullanıcılara ait donanımların erişimleri, port seviyesinde kontrol edilmekte ve zararlı donanımlar engellenmektedir.	Var	*f*	0	1	12	82	**X^2=16,620 p<,05**
			%	0,0	1,1	12,6	86,3	
		Yok	*f*	2	5	12	26	
			%	4,4	11,1	26,7	57,8	

Tablo 6.26'daki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden ağ kategorisindeki 25, 26, 29, 31 ve 32. maddelerde yer alan önlemlerin uygulanması

hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.27'de üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre, teknolojik bilgi güvenliği önlemlerinden veri önlemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.27 :Bilgi güvenliği yönetim aracının kullanımına göre veri önlemlerinin uygulanma düzeyleri

	Veri Güvenliği Önlemleri Maddeleri	**Bilgi Güvenliği Yönetim Aracı**		***Uygulanma düzeyi***				***X²***
				Hiç	***Kötü***	***Orta***	***İyi***	
33	Bilgi yaşam döngüsü içerisinde işlenen, depolanan, iletilen ve imha edilen kritik bilgiler belirlenmekte ve kayıtları tutulmaktadır.	Var	*f*	0	6	23	72	**X²=9,208 p<,05**
			%	0,0	5,9	22,8	71,3	
		Yok	*f*	4	2	19	33	
			%	6,9	3,4	32,8	56,9	
34	Bilgiler; değeri, kritikliği ve gizliliği gibi hassasiyetlere göre sınıflandırılmakta ve uygun sınıflandırma etiketi verilmektedir.	Var	*f*	0	4	21	76	**X²=16,209 p<,05**
			%	0,0	4,0	20,8	75,2	
		Yok	*f*	5	6	18	28	
			%	8,8	10,5	31,6	49,1	
35	Bilgisayar ve taşınabilir ortamlarda (HDD, SSD, harici bellek vb.) muhafaza edilen kritik bilgiler şifrelenmektedir.	Var	*f*	3	5	23	68	**X²=10,290 p<,05**
			%	3,0	5,1	23,2	68,7	
		Yok	*f*	4	4	24	24	
			%	7,1	7,1	42,9	42,9	
36	Kritik ve değerli bilgiler, depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmekte ve saklanmaktadır.	Var	*f*	0	1	21	85	**X²=18,422 p<,05**
			%	0,0	0,9	19,6	79,4	
		Yok	*f*	4	6	18	33	
			%	6,6	9,8	29,5	54,1	
37	Kullanım dışı kalan bilgisayar ve depolama ortamlarındaki kritik bilgiler, yetkili personelce güvenli şekilde silinmektedir.	Var	*f*	1	4	25	71	X²=2,734 p>,05
			%	1,0	4,0	24,8	70,3	
		Yok	*f*	3	2	16	38	
			%	5,1	3,4	27,1	64,4	
38	Kritik bilgiye ve bilgi işleme sistemlerine erişimler, en az ayrıcalık ilkesine göre yetkilendirilen personelle kısıtlanmaktadır.	Var	*f*	1	4	19	79	X²=4,818 p>,05
			%	1,0	3,9	18,4	76,7	
		Yok	*f*	1	2	19	36	
			%	1,7	3,4	32,8	62,1	
39	Kişisel bilgilerin erişim yetkilendirmeleri önceden belirlenmiş ilke ve yöntemlere göre verilmektedir.	Var	*f*	5	20	84	5	X²=3,333 p>,05
			%	4,6	18,3	77,1	4,6	
		Yok	*f*	5	15	36	5	
			%	8,9	26,8	64,3	8,9	
40	Bilgi sistemlerindeki kullanıcı bilgilerinin tedarikçilerce ihlal edilmemesi karşılıklı sözleşme ile koruma altına alınmaktadır.	Var	*f*	1	0	23	76	**X²=14,953 p<,05**
			%	1,0	0,0	23,0	76,0	
		Yok	*f*	2	6	12	27	
			%	4,3	12,8	25,5	57,4	
41	Personel, tedarikçi ve kullanıcıların bilgi sistemlerindeki bilgilere erişim yetkileri, düzenli aralıklarla gözden geçirilmekte ve ilişkileri sone erdiğinde kaldırılmaktadır.	Var	*f*	0	2	16	86	**X²=13,516 p<,05**
			%	0,0	1,9	15,4	82,7	
		Yok	*f*	2	7	14	35	
			%	3,4	12,1	24,1	60,3	
42	Bilgi sistemi ve hizmetlerinden yararlanacak her kullanıcı için ayrı bir hesap tanımlanmakta ve ortak hesap kullanımına izin verilmemektedir.	Var	*f*	0	3	16	92	X²=4,007 p>,05
			%	0,0	2,7	14,4	82,9	
		Yok	*f*	1	3	14	47	
			%	1,5	4,6	21,5	72,3	
43	Kullanıcılardan kişisel bilgilerin sistemler arasında veya gerekli hallerde kurum içinde kullanılacağı ile ilgili açık rıza onayı alınmaktadır	Var	*f*	4	2	22	77	**X²=10,182 p<,05**
			%	3,8	1,9	21,0	73,3	
		Yok	*f*	3	8	15	33	
			%	5,1	13,6	25,4	55,9	
44	Bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin (T.C. numarası, doğum tarihi vb. üyelik numarası ve şifre olarak kullanılmamaktadır.	Var	*f*	3	6	24	72	**X²=19,069 p<,05**
			%	2,9	5,7	22,9	68,6	
		Yok	*f*	5	17	16	27	
			%	7,7	26,2	24,6	41,5	
45	Bilgi sistemlerine varsayılan kullanıcı hesap parolalarıyla giriş izni verilmemekte, güçlü parola kullanımı uygulanmaktadır.	Var	*f*	5	10	20	73	X²=3,147 p>,05
			%	4,6	9,3	18,5	67,6	
		Yok	*f*	2	10	17	38	
			%	3,0	14,9	25,4	56,7	
46	Kritik bilgilerin kurum dışına aktarımı sadece yetkili kullanıcı hesaplarıyla yapılmaktadır.	Var	*f*	1	1	18	83	X²=6,536 p>,05
			%	1,0	1,0	17,5	80,6	
		Yok	*f*	2	4	13	39	
			%	3,4	6,9	22,4	67,2	
47	Veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi kimlik doğrulama sistemleri kullanılmaktadır.	Var	*f*	9	2	18	60	**X²=9,684 p<,05**
			%	10,1	2,2	20,2	67,4	
		Yok	*f*	2	8	11	29	
			%	4,0	16,0	22,0	58,0	

Tablo 6.27'deki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden veri kategorisindeki 33, 34, 35, 36, 40, 41, 43, 44 ve 47. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.28'de üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre, teknolojik bilgi güvenliği önlemlerinden fiziksel ve çevresel önlemlerin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.28: Bilgi güvenliği yönetim aracının kullanımına göre fiziksel ve çevresel önlemlerin uygulanma düzeyleri

	Fiziksel ve Çevresel Güvenlik Önlemleri Maddeleri	**Bilgi Güvenliği Yönetim Aracı**		*Uygulanma düzeyi* *Hiç*	*Kötü*	*Orta*	*İyi*	X^2
48	Kütüphanenin ana giriş ve çıkış kapıları güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile denetlenmektedir.	Var	*f*	9	5	14	92	X^2=,300 p>,05
			%	7,5	4,2	11,7	76,7	
		Yok	*f*	5	4	8	62	
			%	6,3	5,1	10,1	78,5	
49	Kritik bilgi barındıran alanların fiziksel güvenlik sınırları belirlenmekte ve kapı, pencere gibi kısımlar güvenlik mekanizmaları ile korunmaktadır.	Var	*f*	4	9	23	82	X^2=3,745 p>,05
			%	3,4	7,6	19,5	69,5	
		Yok	*f*	4	11	17	44	
			%	5,3	14,5	22,4	57,9	
50	Kütüphanede güvenlik kontrollerini sağlayacak yetkinliğe sahip yeterli sayıda güvenlik personeli çalıştırılmaktadır.	Var	*f*	17	18	27	57	X^2=7,207 p>,05
			%	14,3	15,1	22,7	47,9	
		Yok	*f*	13	23	17	26	
			%	16,5	29,1	21,5	32,9	
51	Kütüphanenin iç ve dış alanları güvenlik kameraları ile takip edilmektedir.	Var	*f*	3	4	22	90	**X^2=7,651 p<,05**
			%	2,5	3,4	18,5	75,6	
		Yok	*f*	2	11	14	51	
			%	2,6	14,1	17,9	65,4	
52	Ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb. giriş ve çıkışları kayıt altına alınmakta ve sadece ilgili amaçları için erişim izni verilmektedir.	Var	*f*	8	14	24	72	**X^2=8,457 p<,05**
			%	6,8	11,9	20,3	61,0	
		Yok	*f*	14	14	14	36	
			%	17,9	17,9	17,9	46,2	
53	Ziyaretçilerin kabul edileceği alanlar personel ve kullanıcı çalışma alanlarından ayrı bir bölgede konumlandırılmaktadır.	Var	*f*	19	19	28	54	X^2=4,689 p>,05
			%	15,8	15,8	23,3	45,0	
		Yok	*f*	18	19	14	28	
			%	22,8	24,1	17,7	35,4	
54	Refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğu uygulanmaktadır.	Var	*f*	37	24	20	37	X^2=4,108 p>,05
			%	31,4	20,3	16,9	31,4	
		Yok	*f*	31	20	10	16	
			%	40,3	26,0	13,0	20,8	
55	Kritik bilgilerin işlendiği veya saklandığı alanlara erişim, uygun kontroller (kartlı / şifreli erişim vb.) uygulanarak yetkili kişiler ile sınırlandırılmaktadır.	Var	*f*	9	9	18	81	X^2=7,597 p>,05
			%	7,7	7,7	15,4	69,2	
		Yok	*f*	4	13	17	39	
			%	5,5	17,8	23,3	53,4	
56	Kütüphane binasına ait pencereler, kapılar ve bahçe alanları, demir parmaklık, çit, kilit, tel örgü gibi dış güvenlik unsurlarıyla kontrol edilmektedir.	Var	*f*	15	14	29	62	X^2=4,167 p>,05
			%	12,5	11,7	24,2	51,7	
		Yok	*f*	11	17	17	33	
			%	14,1	21,8	21,8	42,3	
57	Bilgi sistemlerinin enerji ve iletişim hizmetlerini taşıyan kablolar, dinleme ve hasara karşı kablo kanalı ve izolasyon malzemeleriyle korunmaktadır.	Var	*f*	4	6	22	71	X^2=3,759 p>,05
			%	3,9	5,8	21,4	68,9	
		Yok	*f*	3	6	17	31	
			%	5,3	10,5	29,8	54,4	
58	Doğal afetler, kötü niyetli saldırılar ve kazaklara karşı fiziksel koruma önlemleri büyük oranda alınmakta ve personel bilgilendirilmektedir.	Var	*f*	3	15	31	69	X^2=4,815 p>,05
			%	2,5	12,7	26,3	58,5	
		Yok	*f*	6	12	21	34	
			%	8,2	16,4	28,8	46,6	
59	Elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarları kullanılmaktadır.	Var	*f*	5	9	21	58	**X^2=10,447 p<,05**
			%	5,4	9,7	22,6	62,4	
		Yok	*f*	5	10	19	18	
			%	9,6	19,2	36,5	34,6	

Tablo 6.20'deki veriler incelendiğinde, teknolojik bilgi güvenliği önlemlerinden fiziksel ve çevresel kategorisindeki 51, 52 ve 59. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma

düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

6.7. Kurumsal Bilgi Güvenliği Önlemlerine İlişkin Bulgular

Kurumsal önlemler, teknolojik önlemler gibi bilgi güvenliği için önemli bir süreci kapsamaktadır. Bilgi güvenliği programının başarılı bir biçimde yönetilmesi için gerekli olan tüm politikaları, prosedürleri, yönergeleri, standartları, idari araçları ve bilgi güvenliği farkındalık çalışmalarını içermektedir. Bu önlemler, kurum ve kuruluşların bilgi varlıklarının bilgi güvenliği tehditlerden korunması için yapılması gereken işlemleri düzenlemektedir. Ayrıca çalışanların bilgi güvenliği hakkında bilinçlenmelerine yardımcı olmakta ve kuruluşun tüm seviyelerinde bilgi güvenliği kültürünü desteklemektedir. Bilgi güvenliği eğitimleri ve farkındalık programları gibi faaliyetlerle çalışanların, bilgi güvenliği risklerini tanımlamalarına ve önlem almalarına yardımcı olmaktadır. Böylelikle, bu belgeler kurum ve kuruluşların bilgi güvenliği risklerini belirlemelerine ve en iyi bir biçimde yönetmelerine yardımcı olmaktadır.

Sağlam bilgi güvenliği yönetimi oluşturmak için teknolojik güvenlik önlemlerine kurumsal güvenlik önlemlerinin entegre edilmesi gerekir. Bilgi güvenliğinin genellikle kurumsal, personel, fiziksel ve prosedürel kontroller gibi idari önlemler yoluyla sağlanabileceği veya bu önlemlerle desteklenebileceği kabul edilmektedir. Bu nedenle üniversite kütüphaneleri bilgi güvenliği önlemlerini değerlendirmede, yönetim ve kurumsal güvenlik önlemlerini de dikkate alması önem arz etmektedir.

Bu başlık altında yer alan alt başlıklarda, Türkiye'de üniversite kütüphanelerinde kurumsal bilgi güvenliği önlemelerinin uygulama düzeyleri hakkında katılımcılardan elde edilen bulgular incelenmektedir. Üniversite kütüphanelerinde görev yapan katılımcılardan elde edilen veriler, istatistik testleri ile analiz edilerek Türkiye'de üniversite kütüphanelerinde hangi kurumsal bilgi güvenliği önleminin iyi, orta veya kötü düzeylerde uygulandığı ya da hangi teknolojik bilgi güvenliği önleminin ise hiç uygulanmadığına ilişkin bulgulara ulaşılmıştır. Ayrıca üniversite kütüphanelerinde kurumsal bilgi güvenliği önlemlerinin uygulama düzeyleri konusunda katılımcılardan elde edilen veriler, katılımcıların görev yaptığı üniversite türü, kütüphanede bilgi güvenliğinden sorumlu personelinin varlığı ve kurumsal bilgi güvenliği araçlarının

kullanımı değişkenlerine göre analiz edilerek gruplar arasında anlamlı farklılıkların oluşup oluşturmadığına ilişkin hipotezler sınanmıştır.

Bu itibarla kurumsal bilgi güvenliği önlemelerine ilişkin katılımcılardan 4 kategori (güvenlik politikası, prosedürü, idari araçları ve farkındalık çalışmaları) altında toplam 45 madden oluşan önlemin görev yaptığı üniversite kütüphanesinde uygulanma düzeyine uygun seçeneğin işaretlenmesi istenmiştir. Ayrı ayrı maddelerde belirtilen güvenlik önlemlerinin uygulanıp uygulanmadığı, uygulanıyorsa hangi düzeylerde uygulanmakta olduğuna ilişkin uygun sınıflama seçenekleri kullanılmıştır. Bu seçenekler arasında güvenlik önlemi uygulanmıyorsa "hiç"; uygulanmıyor ise "çok kötü", "kötü", "orta", "iyi" ve "çok iyi" seçenekleri bulunmaktadır.

Katılımcıların bir kurumsal güvenliği önleminin uygulama düzeyine ilişkin "çok kötü" ve "kötü" seçimi, o güvenlik önleminin "kötü düzeyde uygulandığını"; "orta" seçimi, o güvenlik önleminin "orta düzeyde uygulandığını"; "iyi" ve "çok iyi" seçimi, o güvenlik önleminin "iyi düzeyde uygulandığını"; "hiç" seçimi ise o güvenlik önleminin "hiç uygulanmadığını" göstermektedir.

Ayrıca kurumsal güvenlik önlemlerine ilişkin herhangi bir bilgisi olmayan ya da çalıştığı kütüphanede varlığı veya uygulanmasına ilişkin tereddüt yaşayan katılımcıların cevabının diğer katılımcıların cevaplarındaki niteliği etkilememesi veya o maddeyi boş bırakmaması için her maddeye "fikrim yok" seçeneği de eklenmiştir.

Bu kapsamda aşağıdaki araştırma soruları, katılımcılardan elde edilen verilere ve yukarıda açıklanan değerlendirme kriterlerine göre incelenmiştir.

- Bilgi güvenliği tehditlerine karşı alınan kurumsal bilgi güvenliği önlemlerinin Türkiye'de üniversite kütüphanelerinde uygulanma düzeyleri nedir?
- Kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinde üniversitenin türüne, bilgi güvenliğinden sorumlu personelin varlığına ve kurumsal bilgi güvenliği yönetim aracının kullanımına bağlı olarak farklılıklar oluşmakta mıdır?

6.7.1. Kurumsal Bilgi Güvenliği Önlemelerinin Genel Uygulanma Düzeyleri

Bu başlık altında, üniversite kütüphanelerinde kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikaları, prosedürleri, idari araç ve yöntemleri ve farkındalık çalışmaları kategorilerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin her önlem maddesinin frekans dağılımları verilmiştir.

Tablo 6.29'da kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikalarının uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.29: Bilgi güvenliği politikalarının uygulanma düzeyleri

	Bilgi Güvenliği Politikaları Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	***Kötü***	***Orta***	***İyi***	
1	Personel, kullanıcı ve tedarikçilerin bilgi sistemleri ve varlıklarındaki bilgilerin kabul edilebilir kullanımlarını tanımlayan ilkeler	*N*	8	13	53	102	23
		%	4,0	6,5	26,6	51,3	11,6
2	Kâğıt veya elektronik ortamda bulunan kritik bilgilere yetkisiz erişim, bunların hasar görmesi ve kaybolması risklerini azaltan temiz masa / ekran ilke ve yöntemleri	*N*	10	11	49	98	31
		%	5,0	5,5	24,6	49,2	15,6
3	Kritik bilgi, evrak, yazılım ve diğer bilgi varlıklarının kurum dışına çıkarılması ya da başka ortamlara aktarılması ile ilgili bilgi transferi ilke ve yöntemleri	*N*	10	15	39	107	28
		%	5,0	7,5	19,6	53,8	14,1
4	Taşınabilir cihazların kullanılmasıyla ortaya çıkan risklerin yönetilmesini ve üzerlerindeki kayıtlı bilgilerin güvenliğini temin eden ilkeler	*N*	10	17	48	94	30
		%	5,0	8,5	24,1	47,2	15,1
5	Uzak çalışma alanlarından kurumun bilgi sistemlerinde işlenen ve depolanan bilgiyi koruma amacı güden uzaktan çalışma ilkeler	*N*	6	11	49	106	27
		%	3,0	5,5	24,6	53,3	13,6
6	Bilgi sistemlerine kaynağı belirli, kişisel ve kötü niyet şüphesi olmayan hangi tür yazılımların kurulabileceğini tanımlayan ilke ve yöntemler	*N*	9	13	41	97	39
		%	4,5	6,5	20,6	48,7	19,6
7	Bilgi sistemleri ve varlıklarına erişim sağlayan kullanıcı ve tedarikçilerin haklarını, kısıtlamalarını ve sınırlığını belirleyen erişim kontrol ilke ve yöntemleri	*N*	8	14	41	110	26
		%	4,0	7,0	20,6	55,3	13,1
8	Bilginin değeri, kritikliği ve ifşa edilme hassasiyetine uygun seviyelerde korunmasını teminen bilgi sınıflandırma ve etiketleme ilkeleri	*N*	8	18	44	101	28
		%	4,0	9,0	22,1	50,8	14,1
9	Kritik bilgi barındıran alan ve sistemlerin korunmasını ve kütüphanenin güvenlik sınırlarını ve önlemlerini tanımlayan fiziksel ve çevresel güvenlik ilke ve yöntemleri	*N*	9	21	49	100	20
		%	4,5	10,6	24,6	50,3	10,1
10	Olası bir felaket ve ortam hatasından kaynaklanan veri kaybına karşı kritik bilgi, yazılım ve sistemlerin korunmasını amaçlayan bilgi yedekleme ilke ve yöntemleri	*N*	10	10	38	111	30
		%	5,0	5,0	19,1	55,8	15,1
11	Bilgi sistemlerinin zararlı yazılım saldırılarından korumak için tespit etme, engelleme ve kurtarma kontrollerini içeren zararlı yazılımlara karşı ilke ve yöntemler	*N*	9	7	43	109	31
		%	4,5	3,5	21,6	54,8	15,6
12	Bilgilerin gizliliğinin ve bütünlüğünün korunması için şifreleme kontrollerinin doğru ve etkin kullanımını temin eden ilke ve yöntemler	*N*	8	9	44	110	28
		%	4,0	4,5	22,1	55,3	14,1
13	Ağa bağlı sistem ve uygulamalardaki verilerin ve ağ alt yapısının güvenliğini ve yetkisiz erişimlerden korunmasını temin eden ağ yönetimi ilke ve yöntemleri	*N*	8	7	37	113	34
		%	4,0	3,5	18,6	56,8	17,1
14	Kişisel kimlik bilgilerinin gizliliğini ve korunmasını temin eden kişisel bilgilerin mahremiyeti ve koruması ilke ve yöntemleri	*N*	8	10	39	125	17
		%	4,0	5,0	19,6	62,8	8,5
15	Patentli yazılım ve bilgi varlıklarının yasal kullanım haklarının ilgili yasa ve anlaşmalar çerçevesinde korunmasını temin eden fikri mülkiyet ilke ve yöntemleri	*N*	8	7	39	112	33
		%	4,0	3,5	19,6	56,3	16,6
16	Tedarikçilerin kullanıcı ve kurumsal bilgi varlıklarına erişimi ile ilgili risklerin azaltılmasını ve kritik bilgilerin korunmasını temin eden tedarikçi ilişkileri yöntemleri	*N*	7	9	42	103	38
		%	3,5	4,5	21,1	51,8	19,1

Tablo 6.29'daki bilgi güvenliği politikalarına ilişkin veriler incelendiğinde;

"Personel, kullanıcı ve tedarikçilerin bilgi sistemleri ve varlıklarındaki bilgilerin kabul edilebilir kullanımlarını tanımlayan ilkeler" maddesinin uygulanması konusunda

katılımcıların 8 (%4,0)'inin hiç, 13 (%6,5)'ünün kötü, 53 (%26,6)'ünün orta, 102 (%51,3)'sinin iyi dediği; 23 (%11,6)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kâğıt veya elektronik ortamda bulunan kritik bilgilere yetkisiz erişim, bunların hasar görmesi ve kaybolması risklerini azaltan temiz masa / ekran ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 10 (%5,0)'unun hiç, 11 (%5,5)'inin kötü, 49 (%24,6)'unun orta, 98 (%49,2)'inin iyi dediği; 31 (%15,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kritik bilgi, evrak, yazılım ve diğer bilgi varlıklarının kurum dışına çıkarılması ya da başka ortamlara aktarılması ile ilgili bilgi transferi ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 10 (%5,0)'unun hiç, 15 (%7,5)'inin kötü, 39 (%19,6)'unun orta, 107 (%53,8)'sinin iyi dediği; 28 (%14,1)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Taşınabilir cihazların kullanılmasıyla ortaya çıkan risklerin yönetilmesini ve üzerlerindeki kayıtlı bilgilerin güvenliğini temin eden ilkeler" maddesinin uygulanması konusunda katılımcıların 10 (%5,0)'unun hiç, 17 (%8,5)'sinin kötü, 48 (%24,1)'inin orta, 94 (%47,2)'ünün iyi dediği; 30 (%15,1)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Uzak çalışma alanlarından kurumun bilgi sistemlerinde işlenen ve depolanan bilgiyi koruma amacı güden uzaktan çalışma ilkeler" maddesinin uygulanması konusunda katılımcıların 6 (%3,0)'sının hiç, 11 (%5,5)'inin kötü, 49 (%24,6)'unun orta, 106 (%53,3)'sının iyi dediği; 27 (%13,6)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi sistemlerine kaynağı belirli, kişisel ve kötü niyet şüphesi olmayan hangi tür yazılımların kurulabileceğini tanımlayan ilke ve yöntemler" maddesinin uygulanması konusunda katılımcıların 9 (%4,5)'unun hiç, 13 (%6,5)'ünün kötü, 41 (%20,6)'inin orta, 97 (%48,7)'sinin iyi dediği; 39 (%19,6)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi sistemleri ve varlıklarına erişim sağlayan kullanıcı ve tedarikçilerin haklarını, kısıtlamalarını ve sınırlığını belirleyen erişim kontrol ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 8 (%4,0)'inin hiç, 14 (%7,0)'ünün kötü, 41

(%20,6)'inin orta, 110 (%55,3)'unun iyi dediği; 26 (%13,1)'sının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilginin değeri, kritikliği ve ifşa edilme hassasiyetine uygun seviyelerde korunmasını teminen bilgi sınıflandırma ve etiketleme ilkeleri" maddesinin uygulanması konusunda katılımcıların 8 (%4,0)'inin hiç, 18 (%9,0)'inin kötü, 44 (%22,1)'ünün orta, 101 (%50,8)'inin iyi dediği; 28 (%14,1)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kritik bilgi barındıran alan ve sistemlerin korunmasını ve kütüphanenin güvenlik sınırlarını ve önlemlerini tanımlayan fiziksel ve çevresel güvenlik ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 9 (%4,5)'unun hiç, 21 (%10,6)'inin kötü, 49 (%24,6)'unun orta, 100 (%50,3)'ünün iyi dediği; 20 (%10,1)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Olası bir felaket ve ortam hatasından kaynaklanan veri kaybına karşı kritik bilgi, yazılım ve sistemlerin korunmasını amaçlayan bilgi yedekleme ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 10 (%5,0)'unun hiç, 10 (%5,0)'unun kötü, 38 (%19,1)'inin orta, 111 (%55,8)'inin iyi dediği; 30 (%15,1)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi sistemlerinin zararlı yazılım saldırılarından korumak için tespit etme, engelleme ve kurtarma kontrollerini içeren zararlı yazılımlara karşı ilke ve yöntemler" maddesinin uygulanması konusunda katılımcıların 9 (%4,5)'unun hiç, 7 (%635)'sinin kötü, 43 (%21,6)'ünün orta, 109 (%54,8)'unun iyi dediği; 31 (%15,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgilerin gizliliğinin ve bütünlüğünün korunması için şifreleme kontrollerinin doğru ve etkin kullanımını temin eden ilke ve yöntemler" maddesinin uygulanması konusunda katılımcıların 8 (%4,0)'inin hiç, 9 (%4,5)'unun kötü, 44 (%22,1)'ünün orta, 110 (%55,3)'unun iyi dediği; 28 (%14,1)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Ağa bağlı sistem ve uygulamalardaki verilerin ve ağ alt yapısının güvenliğini ve yetkisiz erişimlerden korunmasını temin eden ağ yönetimi ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 8 (%4,0)'inin hiç, 7 (%3,5)'sinin kötü, 37 (%18,6)'sinin orta, 113 (%56,8)'ünün iyi dediği; 34 (%17,1)'ünün ise ilgili

madde için fikrinin olmadığını belirttiği görülmektedir.

“Kişisel kimlik bilgilerinin gizliliğini ve korunmasını temin eden kişisel bilgilerin mahremiyeti ve koruması ilke ve yöntemleri” maddesinin uygulanması konusunda katılımcıların 8 (%4,0)’inin hiç, 10 (%5,0)’unun kötü, 39 (%19,6)’unun orta, 125 (%62,8)’inin iyi dediği; 17 (%8,5)’sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Patentli yazılım ve bilgi varlıklarının yasal kullanım haklarının ilgili yasa ve anlaşmalar çerçevesinde korunmasını temin eden fikri mülkiyet ilke ve yöntemleri” maddesinin uygulanması konusunda katılımcıların 8 (%4,0)’inin hiç, 7 (%3,5)’sinin kötü, 39 (%19,6)’unun orta, 112 (%56,3)’sinin iyi dediği; 33 (%16,6)’ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

“Tedarikçilerin kullanıcı ve kurumsal bilgi varlıklarına erişimi ile ilgili risklerin azaltılmasını ve kritik bilgilerin korunmasını temin eden tedarikçi ilişkileri yöntemleri” maddesinin uygulanması konusunda katılımcıların 7 (%3,5)’sinin hiç, 9 (%4,5)’unun kötü, 42 (%21,1)’sinin orta, 103 (%51,8)’ünün iyi dediği; 38 (%19,1)’inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu bulgulara göre, üniversite kütüphanelerinde bilgi güvenliği politikalarına ilişkin uygulamaların iyi seviyelerde olduğu görülmektedir. Bilgi güvenliği politikalarının hiç olmadığına ilişkin görüşlerin en yüksek %5,0 oranında olduğu ve bu düzeyin kurumsal bilgi güvenliğinin temel uygulamaları açısından gayet iyi olduğu söylenebilir. Bilgi güvenliği politikalarına ilişkin fikri olmayan katılımcıların aranın ise %8,5 ile %19,6 oranları arasında olması ise katılımcıların kurumsal güvenlik politikalarından haberdar olmaması veya politikaların duyurulması konusunda eksikliklerin olduğu düşüncesine varılabilir.

Tablo 6.30’da kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği prosedürleri uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.30: Bilgi güvenliği prosedürlerinin uygulama düzeyleri

	Bilgi Güvenliği Prosedürleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	***Kötü***	***Orta***	***İyi***	
17	Kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması, taşınması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ilke ve yöntemler	*f*	9	8	43	97	42
		%	4,5	4,0	21,6	48,7	21,1
18	Sistem ve hizmetlere güvenli erişimi temin etmek için kullanıcı kaydetme, kayıt silme, erişim izni verme, kimlik doğrulama gibi faaliyetlerin belirlendiği kullanıcı erişim ilke ve yöntemleri	*f*	9	5	38	121	26
		%	4,5	2,5	19,1	60,8	13,1
19	Sistem ve uygulamalara yetkisiz erişimi engellemek için faaliyetlerin belirlendiği güvenli oturum açma ilke ve yöntemleri	*f*	6	7	39	120	27
		%	3,0	3,5	19,6	60,3	13,6
20	Güvenli alanlara sadece yetkili personele erişim izni vermek için uygun giriş kontrollerinin ve faaliyetlerinin belirlendiği fiziksel giriş ilke ve yöntemleri	*f*	11	9	39	114	26
		%	5,5	4,5	19,6	57,3	13,1
21	Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir şekilde müdahale edilmesini amaçlayan faaliyetlerin ve yönetim sorumluluklarının belirlendiği ilke ve yöntemler	*f*	12	13	40	94	40
		%	6,0	6,5	20,1	47,2	20,1
22	Yıkıcı bir olayı yönetmek ve mevcut durumu korumak veya en az zararla atlatabilme için gereksinim duyulan planlama ve faaliyetlerin belirlendiği iş sürekliliği ve felaket kurtarma ilke ve yöntemleri	*f*	14	15	40	96	34
		%	7,0	7,5	20,1	48,2	17,1
23	Kütüphane sistemleri, internet ağı, elektronik posta ve diğer erişimler için güçlü parola kullanımı ve yönetme standartları düzenleyen parola işleme ve kullanımı ilke ve yöntemleri	*f*	7	9	39	120	24
		%	3,5	4,5	19,6	60,3	12,1
24	Bilgi varlıklarının kapasitelerinin planlanması ve kapasite kullanımlarının belli sınırlar içinde tutulması faaliyetlerini düzenleyen kapasite yönetimi ilke ve yöntemleri	*f*	12	6	45	105	31
		%	6,0	3,0	22,6	52,8	15,6
25	Kullanıcıların doğru ve güvenli e-posta kullanımına yönelik kişisel ve kurumsal faaliyetleri düzenleyen elektronik posta ilke ve yöntemleri	*f*	8	10	37	116	28
		%	4,0	5,0	18,6	58,3	14,1
26	Ziyaretçilerin kabulü, dolaşımları ve kütüphaneden ayrılmalarıyla ilgili faaliyetleri düzenleyen ziyaretçi kabul ilke ve yöntemleri	*f*	17	16	48	97	21
		%	8,5	8,0	24,1	48,7	10,6

Tablo 6.30'daki bilgi güvenliği prosedürlerine ilişkin veriler incelendiğinde;

"Kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması, taşınması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ilke ve yöntemler" maddesinin uygulanması konusunda katılımcıların 9 (%4,5)'unun hiç, 8 (%4,0)'inin kötü, 43 (%21,6)'ünün orta, 97 (%48,7)'sinin iyi dediği; 42 (%21,1)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Sistem ve hizmetlere güvenli erişimi temin etmek için kullanıcı kaydetme, kayıt silme, erişim izni verme, kimlik doğrulama gibi faaliyetlerin belirlendiği kullanıcı erişim ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 9

(%4,5)'unun hiç, 5 (%2,5)'inin kötü, 38 (%19,1)'inin orta, 121 (%60,8)'inin iyi dediği; 26 (%13,1)sının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Sistem ve uygulamalara yetkisiz erişimi engellemek için faaliyetlerin belirlendiği güvenli oturum açma ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 6 (%3,0)'sının hiç, 7 (%3,5)'sinin kötü, 39 (%19,6)'unun orta, 120 (%60,3)'sinin iyi dediği; 27 (%13,6)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Güvenli alanlara sadece yetkili personele erişim izni vermek için uygun giriş kontrollerinin ve faaliyetlerinin belirlendiği fiziksel giriş ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 11 (%5,5)'inin hiç, 9 (%4,5)'unun kötü, 39 (%19,6)'unun orta, 114 (%57,3)'ünün iyi dediği; 26 (%13,1)'sının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir şekilde müdahale edilmesini amaçlayan faaliyetlerin ve yönetim sorumluluklarının belirlendiği ilke ve yöntemler" maddesinin uygulanması konusunda katılımcıların 12 (%6,0)'sinin hiç, 13 (%6,5)'ünün kötü, 40 (%20,1)'ının orta, 94 (%47,2)'ünün iyi dediği; 40 (%20,1)'ının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Yıkıcı bir olayı yönetmek ve mevcut durumu korumak veya en az zararla atlatabilme için gereksinim duyulan planlama ve faaliyetlerin belirlendiği iş sürekliliği ve felaket kurtarma ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 14 (%7,0)'ünün hiç, 15 (%7,5)'inin kötü, 40 (%20,1)'ının orta, 96 (%48,2)'sının iyi dediği; 34 (%171)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kütüphane sistemleri, internet ağı, elektronik posta ve diğer erişimler için güçlü parola kullanımı ve yönetme standartları düzenleyen parola işleme ve kullanımı ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 7 (%3,5)'sinin hiç, 9 (%4,5)'unun kötü, 39 (%19,6)'unun orta, 120 (%60,3)'sinin iyi dediği; 24 (%12,1)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi varlıklarının kapasitelerinin planlanması ve kapasite kullanımlarının belli sınırlar içinde tutulması faaliyetlerini düzenleyen kapasite yönetimi ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 12 (%6,0)'sinin hiç, 6 (%3,0)'sının

kötü, 45 (%22,6)'inin orta, 105 (%52,8)'inin iyi dediği; 31 (%15,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kullanıcıların doğru ve güvenli e-posta kullanımına yönelik kişisel ve kurumsal faaliyetleri düzenleyen elektronik posta ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 8 (%4,0)'inin hiç, 10 (%5,0)'unun kötü, 37 (%18,6)'sinin orta, 116 (%58,3)'sının iyi dediği; 28 (%14,1)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Ziyaretçilerin kabulü, dolaşımları ve kütüphaneden ayrılmalarıyla ilgili faaliyetleri düzenleyen ziyaretçi kabul ilke ve yöntemleri" maddesinin uygulanması konusunda katılımcıların 17 (%8,5)'sinin hiç, 16 (%8,0)'sının kötü, 48 (%24,1)'inin orta, 97 (%48,7)'sinin iyi dediği; 21 (%10,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu bulgulara göre, üniversite kütüphanelerinde bilgi güvenliği prosedürlerine ilişkin uygulamaların iyi seviyelere yakın uygulandığı örülmektedir. Bilgi güvenliği prosedürlerinin hiç olmadığına ilişkin görüşlerin en yüksek %8,5 oranında olduğu ve bu düzeyin kurumsal bilgi güvenliği politikalarına göre artmasının sebebi olarak prosedürlerin politikalara göre düzenlenmesi söylenebilir. Bu nedenle bilgi güvenliği prosedürlerinin politikalara göre daha iyi uygulanamaması kütüphane yönetimlerinin kurumsal güvenlik araçlarını iyi seviyelerde planlayamadıkları görüşünü öncelikli olarak düşündürmektedir. Bilgi güvenliği prosedürlerinin varlığına ilişkin fikri olmayan katılımcıların oranın ise %10,6 ile %21,1 oranları arasında olması da bu düşünceyi desteklemektedir. Çünkü bilgi güvenliği prosedürlerinin iyi bir biçimde planlanmaması ve uygulanmaması kütüphane personelinde de bilgi eksikliklerini arttırdığı anlaşılmaktadır.

Tablo 6.31'de kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği idari araç ve yöntemlerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.31: Bilgi güvenliği idari araç ve yöntemlerinin uygulama düzeyleri

	Bilgi Güvenliği İdari Araç ve Yöntemleri Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	*Kötü*	*Orta*	*İyi*	
27	Bilgi güvenliği politika ve prosedürleri ihlallerinin raporlanması ve ilgili birimlere bildirilmesini düzenleyen kılavuz ve talimatlar	*f*	18	19	46	86	30
		%	9,0	9,5	23,1	43,2	15,1
28	Bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi bir disiplin mekanizması	*f*	12	16	41	87	43
		%	6,0	8,0	20,6	43,7	21,6
29	Yeni istihdam edilen personele bilgi güvenliği sorumluluklarını ve görevi son bulan personele ise istihdamın sona ermesinden sonra devam ettirmesi gereken bilgi güvenliği sorumluluklarını bildiren talimat ve uygulamalar	*f*	16	22	46	89	26
		%	8,0	11,1	23,1	44,7	13,1
30	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenmeden önce ilgili kullanıcının bilgilendirilmesini amaçlayan aydınlatma metni uygulamaları	*f*	14	12	47	102	24
		%	7,0	6,0	23,6	51,3	12,1
31	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenme amacının ilgilisine açıkça ifade edilmesini amaçlayan açık rıza yönetimi uygulamaları	*f*	17	12	47	99	24
		%	8,5	6,0	23,6	49,7	12,1
32	Bilgi güvenliği tehditlerinden korumaya yönelik ilgili aksiyon planlarını kapsayan risk analizi tabanlı idari araçlar ve uygulamalar (varlık performans analizi, tehdit analizi, risk analizi vb.)	*f*	12	15	41	87	44
		%	6,0	7,5	20,6	43,7	22,1
33	Bilgi güvenliği yönetim sisteminin etkin, güncel, izlenebilir ve gelişime açık yapıda olmasını amaçlayan iç denetim ilke ve uygulamaları	*f*	10	14	42	98	35
		%	5,0	7,0	21,1	49,2	17,6
34	Üçüncü taraf tedarikçi firma ve kurumlar ile yapılacak bilgi alışverişinin güvenliğini sağlamaya yönelik yapılan sözleşmelere ilişkin idari ilke ve yöntemler	*f*	8	9	38	104	40
		%	4,0	4,5	19,1	52,3	20,1

Tablo 6.31'deki bilgi güvenliği idari araç ve yöntemlerine ilişkin veriler incelendiğinde;

"Bilgi güvenliği politika ve prosedürleri ihlallerinin raporlanması ve ilgili birimlere bildirilmesini düzenleyen kılavuz ve talimatlar" maddesinin uygulanması konusunda katılımcıların 18 (%9,0)'inin hiç, 19 (%9,5)'unun kötü, 46 (%23,1)'sının orta, 86 (%43,2)'sının iyi dediği; 30 (%15,1)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi bir disiplin mekanizması" maddesinin uygulanması konusunda katılımcıların 12 (%6,0)'sinin hiç, 16 (%8,0)'sının kötü, 41 (%20,6)'inin orta, 87 (%43,7)'sinin iyi dediği; 43 (%21,6)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Yeni istihdam edilen personele bilgi güvenliği sorumluluklarını ve görevi son bulan personele ise istihdamın sona ermesinden sonra devam ettirmesi gereken bilgi güvenliği sorumluluklarını bildiren talimat ve uygulamalar" maddesinin uygulanması

konusunda katılımcıların 16 (%8,0)'sının hiç, 22 (%11,1)'sinin kötü, 46 (%23,1)'sının orta, 89 (%44,7)'unun iyi dediği; 26 (%13,1)'sının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kişisel bilgilerin kütüphane bilgi sistemlerine işlenmeden önce ilgili kullanıcının bilgilendirilmesini amaçlayan aydınlatma metni uygulamaları" maddesinin uygulanması konusunda katılımcıların 14 (%7,0)'ünün hiç, 12 (%6,0)'sinin kötü, 47 (%23,6)'sinin orta,102 (%51,3)'sinin iyi dediği; 24 (%12,1)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kişisel bilgilerin kütüphane bilgi sistemlerine işlenme amacının ilgilisine açıkça ifade edilmesini amaçlayan açık rıza yönetimi uygulamaları" maddesinin uygulanması konusunda katılımcıların 17 (%8,5)'sinin hiç, 12 (%6,0)'sinin kötü, 47 (%23,6)'sinin orta, 99 (%49,7)'unun iyi dediği; 24 (%12,1)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi güvenliği tehditlerinden korumaya yönelik ilgili aksiyon planlarını kapsayan risk analizi tabanlı idari araçlar ve uygulamalar (varlık performans analizi, tehdit analizi, risk analizi vb.)" maddesinin uygulanması konusunda katılımcıların 12 (%6,0)'sinin hiç, 15 (%7,5)'inin kötü, 41 (%20,6)'inin orta, 87 (%43,7)'sinin iyi dediği; 44 (%22,1)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi güvenliği yönetim sisteminin etkin, güncel, izlenebilir ve gelişime açık yapıda olmasını amaçlayan iç denetim ilke ve uygulamaları" maddesinin uygulanması konusunda katılımcıların 10 (%5,0)'unun hiç, 14 (%7,0)'ünün kötü, 42 (%21,1)'sinin orta, 98 (%49,2)'inin iyi dediği; 35 (%17,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Üçüncü taraf tedarikçi firma ve kurumlar ile yapılacak bilgi alışverişinin güvenliğini sağlamaya yönelik yapılan sözleşmelere ilişkin idari ilke ve yöntemler" maddesinin uygulanması konusunda katılımcıların 8 (%4,0)'inin hiç, 9 (%4,5)'unun kötü, 38 (%19,1)'inin orta, 104 (%52,3)'ünün iyi dediği; 40 (%20,1)'ının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu bulgulara göre, üniversite kütüphanelerinde bilgi güvenliği idari araç ve yöntemlere ilişkin uygulamaların iyi seviyelere yakın uygulandığı fakat bunun yeterli seviyede

olmadığı görülmektedir. Bu kategoride yer alan önlemlerin uygulanmasında katılımcıların kötü ve orta düzeyde de belirgin oranlarda görüş bildirdiği anlaşılmaktadır. Bilgi güvenliği idari araç ve yöntemlerinin varlığına ilişkin fikri olmayan katılımcıların oranın ise %12,1 ile %22,1 oranları arasında olduğu görülmektedir. Bu durumun da bu kategorideki uygulama düzeylerinin diğer kurumsal önlemlere göre düşük oranlara sahip olmasını desteklemektedir. Kurumsal bilgi güvenliği önlenmeleri bir bütün olarak düşünüldüğünde idari araç ve yöntemlerinin politika ve prosedürlerden sonra önemli kurumsal araçlar olduğu fakat üniversite kütüphanelerinde bu önlemlere ilişkin üst seviyelerde planlama ve uygulamaların olmadığı anlaşılmaktadır.

Tablo 6.32'de kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği farkındalık çalışmaları uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 6.32: Bilgi güvenliği farkındalık çalışmalarının uygulama düzeyleri

	Bilgi Güvenliği Farkındalık Çalışmaları		***Uygulanma Düzeyi***				***Fikrim yok***
			Hiç	***Kötü***	***Orta***	***İyi***	
35	Personelin ve kullanıcıların bilgi güvenliği sorumluluklarını farkında olmalarını ve yerine getirmelerini amaçlayan bilgi güvenliği farkındalık eğitimi çalışmaları	*f*	21	26	54	86	12
		%	10,6	13,1	27,1	43,2	6,0
36	Bilgi güvenliği eğitim faaliyetlerinin kapsamının belirlendiği ve ihtiyaçların netleştirildiği eğitim planlama rehberleri	*f*	27	30	52	74	16
		%	13,6	15,1	26,1	37,2	8,0
37	Bilgi güvenliği alanında görevlendirilen personelin yetenek ihtiyaç analizinin yapılması ve sonuçlarına göre hizmetçi eğitim uygulamaları	*f*	26	28	50	75	20
		%	13,1	14,1	25,1	37,7	10,1
38	Kütüphanenin bilgi güvenliği çerçevesini oluşturan politika, prosedür ve idari yöntemler hakkında tedarikçilerin farkındalığını geliştirme çalışmaları	*f*	26	22	51	79	21
		%	13,1	11,1	25,6	39,7	10,6
39	Personel ve kullanıcıların bilgi güvenliği farkındalığını arttırıcı interaktif eğitim çalışmaları	*f*	32	25	52	77	13
		%	16,1	12,6	26,1	38,7	6,5
40	Bilgi güvenliği ile ilgili broşür, poster ve kitapçık gibi bilgilendirici doküman çalışmaları	*f*	39	31	52	63	14
		%	19,6	15,6	26,1	31,7	7,0
41	Kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması	*f*	47	36	48	55	13
		%	23,6	18,1	24,1	27,6	6,5
42	Kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları, fare altlığı, not kâğıtları gibi farkındalık arttırıcı faaliyetler	*f*	42	38	47	60	12
		%	21,1	19,1	23,6	30,2	6,0
43	Personele ve kullanıcılara bilgi güvenliği ile ilgili mail ve SMS yoluyla bilgilendirme mesajlarının gönderilmesi	*f*	28	28	52	78	19
		%	14,1	14,1	26,1	39,2	6,5
44	Personel ve kullanıcıların bilgi güvenliği hassasiyetlerinin ödüllendirilme çalışmaları	*f*	55	36	42	45	21
		%	27,6	18,1	21,1	22,6	10,6
45	Kütüphanenizin bilgi güvenliği politika, prosedür ve idari yöntemleri ile ilgili yapılan güncellemelerin kullanıcılara zamanında bildirilme	*f*	27	24	49	84	15
		%	13,6	12,1	24,2	42,2	7,5

Tablo 6.32'deki bilgi güvenliği farkındalık çalışmalarına ilişkin veriler incelendiğinde;

"Personelin ve kullanıcıların bilgi güvenliği sorumluluklarını farkında olmalarını ve yerine getirmelerini amaçlayan bilgi güvenliği farkındalık eğitimi çalışmaları" maddesinin uygulanması konusunda katılımcıların 21 (%10,6)'inin hiç, 26 (%13,1)'sının kötü, 54 (%27,1)'ünün orta, 86 (%43,2)'sının iyi dediği; 12 (%6,0)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi güvenliği eğitim faaliyetlerinin kapsamının belirlendiği ve ihtiyaçların netleştirildiği eğitim planlama rehberleri" maddesinin uygulanması konusunda katılımcıların 27 (%13,6)'sinin hiç, 30 (%15,1)'unun kötü, 52 (%26,1)'sinin orta, 74 (%37,2)'ünün iyi dediği; 16 (%8,1)'sının ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi güvenliği alanında görevlendirilen personelin yetenek ihtiyaç analizinin yapılması ve sonuçlarına göre hizmetçi eğitim uygulamaları" maddesinin uygulanması konusunda katılımcıların 26 (%13,1)'sının hiç, 28 (%14,1)'inin kötü, 50 (%25,1)'sinin orta, 75 (%37,7)'inin iyi dediği; 20 (%10,1)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kütüphanenin bilgi güvenliği çerçevesini oluşturan politika, prosedür ve idari yöntemler hakkında tedarikçilerin farkındalığını geliştirme çalışmaları" maddesinin uygulanması konusunda katılımcıların 26 (%13,1)'sının hiç, 22 (%11,1)'sinin kötü, 51 (%25,6)'inin orta, 79 (%39,7)'unun iyi dediği; 21 (%10,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Personel ve kullanıcıların bilgi güvenliği farkındalığını arttırıcı interaktif eğitim çalışmaları" maddesinin uygulanması konusunda katılımcıların 32 (%16,1)'sinin hiç, 25 (%12,6)'inin kötü, 52 (%26,1)'sinin orta, 77 (%38,7)'sinin iyi dediği; 13 (%6,5)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Bilgi güvenliği ile ilgili broşür, poster ve kitapçık gibi bilgilendirici doküman çalışmaları" maddesinin uygulanması konusunda katılımcıların 39 (%19,6)'unun hiç, 31 (%15,6)'inin kötü, 52 (%26,1)'sinin orta, 63 (%31,7)'ünün iyi dediği; 14 (%7,0)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini

arttırmaya yönelik film gibi görsellerin sunulması" maddesinin uygulanması konusunda katılımcıların 47 (%23,6)'sinin hiç, 36 (%18,1)'sının kötü, 48 (%24,1)'inin orta, 55 (%27,6)'inin iyi dediği; 13 (%6,5)'ünün ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları, fare altlığı, not kâğıtları gibi farkındalık arttırıcı faaliyetler" maddesinin uygulanması konusunda katılımcıların 42 (%21,1)'sinin hiç, 38 (%19,1)'inin kötü, 47 (%23,6)'sinin orta, 60 (%30,2)'ının iyi dediği; 12 (%6,0)'sinin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Personele ve kullanıcılara bilgi güvenliği ile ilgili mail ve sms yoluyla bilgilendirme mesajlarının gönderilmesi" maddesinin uygulanması konusunda katılımcıların 28 (%14,1)'inin hiç, 28 (%14,1)'inin kötü, 52 (%26,1)'sinin orta, 78 (%39,2)'inin iyi dediği; 19 (%6,5)'unun ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Personel ve kullanıcıların bilgi güvenliği hassasiyetlerinin ödüllendirilme çalışmaları" maddesinin uygulanması konusunda katılımcıların 55 (%27,6)'inin hiç, 36 (%18,1)'sının kötü, 42 (%21,1)'sinin orta, 45 (%22,6)'inin iyi dediği; 21 (%10,6)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

"Kütüphanenizin bilgi güvenliği politika, prosedür ve idari yöntemleri ile ilgili yapılan güncellemelerin kullanıcılara zamanında bildirilme" maddesinin uygulanması konusunda katılımcıların 27 (%13,6)'sinin hiç, 24 (%12,1)'ünün kötü, 49 (%24,2)'unun orta, 84 (%42,2)'ünün iyi dediği; 15 (%7,5)'inin ise ilgili madde için fikrinin olmadığını belirttiği görülmektedir.

Bu bulgulara göre, üniversite kütüphanelerinde bilgi güvenliği farkındalık çalışmalarına ilişkin uygulamaların iyi seviyelerde olmadığı görülmektedir. Bu kategoride yer alan maddelere verilen "hiç uygulanmakta", "kötü" ve "orta" düzeyde uygulanmakta görüşlerinin tüm kategoriler içerisinde daha yüksek oranlara sahip olduğu görülmektedir. Bu kategorideki maddelere ilişkin katılımcıların bilgi sahibi olmama durumlarının diğer kategorilerdeki maddelere kıyasla daha düşük düzeylerde olduğu da gözlemlenmektedir.

6.7.2. Üniversite Türü Değişkenine Göre Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri

Bu başlık altında, katılımcıların görev yaptıkları üniversitelerin türüne göre kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikaları, bilgi güvenliği prosedürleri, bilgi güvenliği idari araç ve yöntemleri ve bilgi güvenliği farkındalık araçları kategorilerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin ilişkin frekans dağılımları ve ki kare istatistikleri verilmiştir.

Tablo 6.33'te görev yapılan üniversitelerin türüne göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikalarının uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.33: Katılımcıların görev yaptıkları üniversitelerin türüne göre bilgi güvenliği politikalarının uygulanma düzeyleri

	Bilgi Güvenliği Politikaları Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
1	Personel, kullanıcı ve tedarikçilerin bilgi sistemleri ve varlıklarındaki bilgilerin kabul edilebilir kullanımlarını tanımlayan ilkeler	Devlet	*f*	6	11	33	57	X^2=4,681 p>,05
			%	5,6	10,3	30,8	53,3	
		Vakıf	*f*	2	2	20	45	
			%	2,9	2,9	29,0	65,2	
2	Kâğıt veya elektronik ortamda bulunan kritik bilgilere yetkisiz erişim, bunların hasar görmesi ve kaybolması risklerini azaltan temiz masa / ekran ilke ve yöntemleri	Devlet	*f*	8	10	31	50	**X^2=9,314 p<,05**
			%	8,1	10,1	31,3	50,5	
		Vakıf	*f*	2	1	18	48	
			%	2,9	1,4	26,1	69,6	
3	Kritik bilgi, evrak, yazılım ve diğer bilgi varlıklarının kurum dışına çıkarılması ya da başka ortamlara aktarılması ile ilgili bilgi transferi ilke ve yöntemleri	Devlet	*f*	8	10	24	58	X^2=3,277p >,05
			%	8,0	10,0	24,0	58,0	
		Vakıf	*f*	2	5	15	49	
			%	2,8	7,0	21,1	69,0	
4	Taşınabilir cihazların kullanılmasıyla ortaya çıkan risklerin yönetilmesini ve üzerlerindeki kayıtlı bilgilerin güvenliğini temin eden ilkeler	Devlet	*f*	8	13	27	53	X^2=4,369 p>,05
			%	7,9	12,9	26,7	52,5	
		Vakıf	*f*	2	4	21	41	
			%	2,9	5,9	30,9	60,3	
5	Uzak çalışma alanlarından kurumun bilgi sistemlerinde işlenen ve depolanan bilgiyi koruma amacı güden uzaktan çalışma ilkeler	Devlet	*f*	5	7	32	59	X^2=2,616 p>,05
			%	4,9	6,8	31,1	57,3	
		Vakıf	*f*	1	4	17	47	
			%	1,4	5,8	24,6	68,1	
6	Bilgi sistemlerine kaynağı belirli, kişisel ve kötü niyet şüphesi olmayan hangi tür yazılımların kurulabileceğini tanımlayan ilke ve yöntemler	Devlet	*f*	7	11	25	51	X^2=6,542 p>,05
			%	7,4	11,7	26,6	54,3	
		Vakıf	*f*	2	2	16	46	
			%	3,0	3,0	24,2	69,7	
7	Bilgi sistemleri ve varlıklarına erişim sağlayan kullanıcı ve tedarikçilerin haklarını, kısıtlamalarını ve sınırlığını belirleyen erişim kontrol ilke ve yöntemleri	Devlet	*f*	6	9	27	63	X^2=1,639 p>,05
			%	5,7	8,6	25,7	60,0	
		Vakıf	*f*	2	5	14	47	
			%	2,9	7,4	20,6	69,1	
8	Bilginin değeri, kritikliği ve ifşa edilme hassasiyetine uygun seviyelerde korunmasını temin eden bilgi sınıflandırma ve etiketleme ilkeleri	Devlet	*f*	6	11	24	62	X^2=1,327 p>,05
			%	5,8	10,7	23,3	60,2	
		Vakıf	*f*	2	7	20	39	
			%	2,9	10,3	29,4	57,4	
9	Kritik bilgi barındıran alan ve sistemlerin korunmasını ve kütüphanenin güvenlik sınırlarını ve önlemlerini tanımlayan fiziksel ve çevresel güvenlik ilke ve yöntemleri	Devlet	*f*	6	14	30	59	X^2=0,573 p>,05
			%	5,5	12,8	27,5	54,1	
		Vakıf	*f*	3	7	19	41	
			%	4,3	10,0	27,1	58,6	

Tablo 6.33'ün Devamı

	Bilgi Güvenliği Politikaları Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
10	Olası bir felaket ve ortam hatasından kaynaklanan veri kaybına karşı kritik bilgi, yazılım ve sistemlerin korunmasını amaçlayan bilgi yedekleme ilke ve yöntemleri	Devlet	*f*	8	5	24	64	X^2=2,413 p>,05
			%	7,9	5,0	23,8	63,4	
		Vakıf	*f*	2	5	14	47	
			%	2,9	7,4	20,6	69,1	
11	Bilgi sistemlerinin zararlı yazılım saldırılarından korumak için tespit etme, engelleme ve kurtarma kontrollerini içeren zararlı yazılımlara karşı ilke ve yöntemler	Devlet	*f*	6	7	26	59	X^2=6,301 p>,05
			%	6,1	7,1	26,5	60,2	
		Vakıf	*f*	3	0	17	50	
			%	4,3	0,0	24,3	71,4	
12	Bilgilerin gizliliğinin ve bütünlüğünün korunması için şifreleme kontrollerinin doğru ve etkin kullanımını temin eden ilke ve yöntemler	Devlet	*f*	7	8	25	62	X^2=6,163 p>,05
			%	6,9	7,8	24,5	60,8	
		Vakıf	*f*	1	1	19	48	
			%	1,4	1,4	27,5	69,6	
13	Ağa bağlı sistem ve uygulamalardaki verilerin ve ağ alt yapısının güvenliğini ve yetkisiz erişimlerden korunmasını temin eden ağ yönetimi ilke ve yöntemleri	Devlet	*f*	6	7	19	64	X^2=6,892 p>,05
			%	6,3	7,3	19,8	66,7	
		Vakıf	*f*	2	0	18	49	
			%	2,9	0,0	26,1	71,0	
14	Kişisel kimlik bilgilerinin gizliliğini ve korunmasını temin eden kişisel bilgilerin mahremiyeti ve koruması ilke ve yöntemleri	Devlet	*f*	6	7	23	73	X^2=1,182 p>,05
			%	5,5	6,4	21,1	67,0	
		Vakıf	*f*	2	3	16	52	
			%	2,7	4,1	21,9	71,2	
15	Patentli yazılım ve bilgi varlıklarının yasal kullanım haklarının ilgili yasa ve anlaşmalar çerçevesinde korunmasını temin eden fikri mülkiyet ilke ve yöntemleri	Devlet	*f*	7	6	23	62	X^2=5,018 p>,05
			%	7,1	6,1	23,5	63,3	
		Vakıf	*f*	1	1	16	50	
			%	1,5	1,5	23,5	73,5	
16	Tedarikçilerin kullanıcı ve kurumsal bilgi varlıklarına erişimi ile ilgili risklerin azaltılmasını ve kritik bilgilerin korunmasını temin eden tedarikçi ilişkileri yöntemleri	Devlet	*f*	6	8	25	54	X^2=6,799 p>,05
			%	6,5	8,6	26,9	58,1	
		Vakıf	*f*	1	1	17	49	
			%	1,5	1,5	25,0	72,1	

Tablo 6.33'teki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden politikalar kategorisindeki 2. maddede yer alan önlemin uygulanması hakkında katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle devlet üniversitesi kütüphanelerinde bu güvenlik önleminin uygulanma düzeyinin vakıf üniversitesi kütüphanelerinden daha düşük olduğu söylenebilir.

Tablo 6.34'te görev yapılan üniversitelerin türüne göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği prosedürlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.34: Katılımcıların görev yaptıkları üniversitelerin türüne göre bilgi güvenliği prosedürlerinin uygulanma düzeyleri

	Bilgi Güvenliği Prosedürleri Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
17	Kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ilke ve yöntemler	Devlet	*f*	8	7	28	51	**X^2=7,998 p<,05**
			%	8,5	7,4	29,8	54,3	
		Vakıf	*f*	1	1	15	46	
			%	1,6	1,6	23,8	73,0	
18	Sistem ve hizmetlere güvenli erişimi temin etmek için kullanıcı kaydetme, erişim izni verme, kimlik doğrulama gibi faaliyetlerin belirlendiği kullanıcı erişim yöntemleri	Devlet	*f*	7	5	24	70	X^2=4,450 p>,05
			%	6,6	4,7	22,6	66,0	
		Vakıf	*f*	2	0	14	51	
			%	3,0	0,0	20,9	76,1	
19	Sistem ve uygulamalara yetkisiz erişimi engellemek için faaliyetlerin belirlendiği güvenli oturum açma ilke ve yöntemleri	Devlet	*f*	5	5	29	66	X^2=6,046p >,05
			%	4,8	4,8	27,6	62,9	
		Vakıf	*f*	1	2	10	54	
			%	1,5	3,0	14,9	80,6	
20	Güvenli alanlara sadece yetkili personele erişim izni vermek için uygun giriş kontrollerinin ve faaliyetlerinin belirlendiği fiziksel giriş ilke ve yöntemleri	Devlet	*f*	9	7	25	64	X^2=4,045 p>,05
			%	8,6	6,7	23,8	61,0	
		Vakıf	*f*	2	2	14	50	
			%	2,9	2,9	20,6	73,5	
21	Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir şekilde müdahale edilmesini amaçlayan faaliyetlerin belirlendiği ilke ve yöntemler	Devlet	*f*	8	7	29	53	X^2=3,508 p>,05
			%	8,2	7,2	29,9	54,6	
		Vakıf	*f*	4	6	11	41	
			%	6,5	9,7	17,7	66,1	
22	Yıkıcı bir olayı yönetmek ve mevcut durumu korumak için gereksinim duyulan planlama ve faaliyetlerin belirlendiği iş sürekliliği ve felaket kurtarma ilke ve yöntemleri	Devlet	*f*	9	11	26	53	X^2=2,553 p>,05
			%	9,1	11,1	26,3	53,5	
		Vakıf	*f*	5	4	14	43	
			%	7,6	6,1	21,2	65,2	
23	Kütüphane sistemleri, internet ağı, elektronik posta ve diğer erişimler için güçlü parola kullanımı ve yönetme standartları düzenleyen parola işleme ve kullanımı ilke ve yöntemleri	Devlet	*f*	5	4	22	75	X^2=1,830 p>,05
			%	4,7	3,8	20,8	70,8	
		Vakıf	*f*	2	5	17	45	
			%	2,9	7,2	24,6	65,2	
24	Bilgi varlıklarının kapasitelerinin planlanması ve kapasite kullanımlarının belli sınırlar içinde tutulması faaliyetlerini düzenleyen kapasite yönetimi ilke ve yöntemleri	Devlet	*f*	9	4	28	60	X^2=1,607 p>,05
			%	8,9	4,0	27,7	59,4	
		Vakıf	*f*	3	2	17	45	
			%	4,5	3,0	25,4	67,2	
25	Kullanıcıların doğru ve güvenli e-posta kullanımına yönelik kişisel ve kurumsal faaliyetleri düzenleyen elektronik posta ilke ve yöntemleri	Devlet	*f*	6	6	23	67	X^2=0,999 p>,05
			%	5,9	5,9	22,5	65,7	
		Vakıf	*f*	2	4	14	49	
			%	2,9	5,8	20,3	71,0	
26	Ziyaretçilerin kabulü, dolaşımları ve kütüphaneden ayrılmalarıyla ilgili faaliyetleri düzenleyen ziyaretçi kabul ilke ve yöntemleri	Devlet	*f*	13	13	29	52	X^2=6,592 p>,05
			%	12,1	12,1	27,1	48,6	
		Vakıf	*f*	4	3	19	45	
			%	5,6	4,2	26,8	63,4	

Tablo 6.34'teki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden prosedürler kategorisindeki 17. maddede yer alan önlemin uygulanması hakkında katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle devlet üniversitesi kütüphanelerinde bu güvenlik önleminin uygulanma düzeyinin vakıf üniversitesi kütüphanelerinden daha düşük olduğu söylenebilir.

Tablo 6.35'te görev yapılan üniversitelerin türüne göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği idari araçlarının uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.35: Katılımcıların görev yaptıkları üniversitelerin türüne göre bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeyleri

	Bilgi Güvenliği İdari Araç ve Yöntemleri Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
27	Bilgi güvenliği politika ve prosedürleri ihlallerinin raporlanması ve ilgili birimlere bildirilmesini düzenleyen kılavuz ve talimatlar	Devlet	*f*	11	14	28	48	X^2=2,126 p>,05
			%	10,9	13,9	27,7	47,5	
		Vakıf	*f*	7	5	18	38	
			%	10,3	7,4	26,5	55,9	
28	Bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi bir disiplin mekanizması	Devlet	*f*	9	11	26	50	X^2=1,939 p>,05
			%	9,4	11,5	27,1	52,1	
		Vakıf	*f*	3	5	15	37	
			%	5,0	8,3	25,0	61,7	
29	Yeni istihdam edilen ve görevi sona eren personelin bilgi güvenliği sorumluluklarını bildiren talimat ve uygulamalar	Devlet	*f*	13	15	31	48	X^2=5,889 p>,05
			%	12,1	14,0	29,0	44,9	
		Vakıf	*f*	3	7	15	41	
			%	4,5	10,6	22,7	62,1	
30	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenmeden önce ilgili kullanıcının bilgilendirilmesini amaçlayan aydınlatma metni uygulamaları	Devlet	*f*	9	9	29	60	X^2=1,265 p>,05
			%	8,4	8,4	27,1	56,1	
		Vakıf	*f*	5	3	18	42	
			%	7,4	4,4	26,5	61,8	
31	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenme amacının ilgilisine açıkça ifade edilmesini amaçlayan açık rıza yönetimi uygulamaları	Devlet	*f*	12	9	29	56	X^2=2,451 p>,05
			%	11,3	8,5	27,4	52,8	
		Vakıf	*f*	5	3	18	43	
			%	7,2	4,3	26,1	62,3	
32	Bilgi güvenliği tehditlerinden korumaya yönelik ilgili aksiyon planlarını kapsayan risk analizi tabanlı idari araçlar ve uygulamalar	Devlet	*f*	8	10	30	45	X^2=5,946 p>,05
			%	8,6	10,8	32,3	48,4	
		Vakıf	*f*	4	5	11	42	
			%	6,5	8,1	17,7	67,7	
33	Bilgi güvenliği yönetim sisteminin etkin, güncel, izlenebilir ve gelişime açık yapıda olmasını amaçlayan iç denetim ilke ve uygulamaları	Devlet	*f*	8	9	28	56	X^2=2,752 p>,05
			%	7,9	8,9	27,7	55,4	
		Vakıf	*f*	2	5	14	42	
			%	3,2	7,9	22,2	66,7	
34	Üçüncü taraf tedarikçi firma ve kurumlar ile yapılacak bilgi alışverişinin güvenliğini sağlamaya yönelik yapılan sözleşmelere ilişkin idari ilke ve yöntemler	Devlet	*f*	6	6	24	60	X^2=1,193 p>,05
			%	6,3	6,3	25,0	62,5	
		Vakıf	*f*	2	3	14	44	
			%	3,2	4,8	22,2	69,8	

Tablo 6.35'teki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden idari araç ve yöntemleri kategorisindeki önlemlerin uygulanma düzeyleri hakkında katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olmadığı görülmektedir.

Tablo 6.36'da görev yapılan üniversitelerin türüne göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği farkındalık çalışmalarının uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.36: Katılımcıların görev yaptıkları üniversitelerin türüne göre bilgi güvenliği farkındalık çalışmalarının uygulanma düzeyleri

	Bilgi Güvenliği Farkındalık Çalışmaları Maddeleri	*Üniversite Türü*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
35	Personelin ve kullanıcıların bilgi güvenliği sorumluluklarını farkında olmalarını ve yerine getirmelerini amaçlayan bilgi güvenliği farkındalık eğitimi çalışmaları	Devlet	*f*	14	17	35	48	X^2=1,795 p>,05
			%	12,3	14,9	30,7	42,1	
		Vakıf	*f*	7	9	19	38	
			%	9,6	12,3	26,0	52,1	
36	Bilgi güvenliği eğitim faaliyetlerinin kapsamının belirlendiği ve ihtiyaçların netleştirildiği eğitim planlama rehberleri	Devlet	*f*	17	21	33	40	X^2=2,681 p>,05
			%	15,3	18,9	29,7	36,0	
		Vakıf	*f*	10	9	19	34	
			%	13,9	12,5	26,4	47,2	
37	Bilgi güvenliği alanında görevlendirilen personelin yetenek ihtiyaç analizinin yapılması ve sonuçlarına göre hizmetçi eğitim uygulamaları	Devlet	*f*	17	20	32	41	X^2=2,941 p>,05
			%	15,5	18,2	29,1	37,3	
		Vakıf	*f*	9	8	18	34	
			%	13,0	11,6	26,1	49,3	
38	Kütüphanenin bilgi güvenliği çerçevesini oluşturan politika, prosedür ve idari yöntemler hakkında tedarikçilerin farkındalığını geliştirme çalışmaları	Devlet	*f*	18	15	30	44	X^2=2,177 p>,05
			%	16,8	14,0	28,0	41,1	
		Vakıf	*f*	8	7	21	35	
			%	11,3	9,9	29,6	49,3	
39	Personel ve kullanıcıların bilgi güvenliği farkındalığını arttırıcı interaktif eğitim çalışmaları	Devlet	*f*	20	16	36	42	X^2=2,955 p>,05
			%	17,5	14,0	31,6	36,8	
		Vakıf	*f*	12	9	16	35	
			%	16,7	12,5	22,2	48,6	
40	Bilgi güvenliği ile ilgili broşür, poster ve kitapçık gibi bilgilendirici doküman çalışmaları	Devlet	*f*	25	19	36	32	X^2=4,364 p>,05
			%	22,3	17,0	32,1	28,6	
		Vakıf	*f*	14	12	16	31	
			%	19,2	16,4	21,9	42,5	
41	Kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması	Devlet	*f*	31	25	33	23	**X^2=11,157 p<,05**
			%	27,7	22,3	29,5	20,5	
		Vakıf	*f*	16	11	15	32	
			%	21,6	14,9	20,3	43,2	
42	Kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları, fare altlığı, not kâğıtları gibi farkındalık arttırıcı faaliyetler	Devlet	*f*	27	30	30	26	**X^2=13,271 p<,05**
			%	23,9	26,5	26,5	23,0	
		Vakıf	*f*	15	8	17	34	
			%	20,3	10,8	23,0	45,9	
43	Personele ve kullanıcılara bilgi güvenliği ile ilgili mail ve SMS yoluyla bilgilendirme mesajlarının gönderilmesi	Devlet	*f*	20	19	35	37	**X^2=8,501 p<,05**
			%	18,0	17,1	31,5	33,3	
		Vakıf	*f*	8	9	17	41	
			%	10,7	12,0	22,7	54,7	
44	Personel ve kullanıcıların bilgi güvenliği hassasiyetlerinin ödüllendirilme çalışmaları	Devlet	*f*	36	27	25	21	X^2=7,361 p>,05
			%	33,0	24,8	22,9	19,3	
		Vakıf	*f*	19	9	17	24	
			%	27,5	13,0	24,6	34,8	
45	Kütüphanenizin bilgi güvenliği politika, prosedür ve idari yöntemleri ile ilgili yapılan güncellemelerin kullanıcılara zamanında bildirilme	Devlet	*f*	20	17	29	45	X^2=4,867 p>,05
			%	18,0	15,3	26,1	40,5	
		Vakıf	*f*	7	7	20	39	
			%	9,6	9,6	27,4	53,4	

Tablo 6.36'daki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden farkındalık çalışmaları kategorisindeki 41, 42 ve 43. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında görev yapılan üniversitelerin türüne göre anlamlı bir farklılık olduğu görülmektedir (p<0,05) Bu bulgulardan hareketle devlet üniversitesi kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeyinin vakıf üniversitesi kütüphanelerinden daha düşük olduğu söylenebilir.

6.7.3. Bilgi Güvenliği Personeli Değişkenine Göre Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri

Bu başlık altında, üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikaları, bilgi güvenliği prosedürleri, bilgi güvenliği idari araç ve yöntemleri ve bilgi güvenliği farkındalık araçları kategorilerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin ilişkin frekans dağılımları ve ki kare istatistikleri verilmiştir.

Tablo 6.37'de üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikalarının uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.37: Bilgi güvenliğinden sorumlu personelin varlığına göre bilgi güvenliği politikalarının uygulanma düzeyleri

	Bilgi Güvenliği Politikaları Maddeleri	*Bilgi Güvenliği Personeli*		*Uygulanma düzeyi* *Hiç*	*Kötü*	*Orta*	*İyi*	X^2
1	Personel, kullanıcı ve tedarikçilerin bilgi sistemleri ve varlıklarındaki bilgilerin kabul edilebilir kullanımlarını tanımlayan ilkeler	Var	*f*	0	2	18	47	**X^2=11,042**
			%	0,0	3,0	26,9	70,1	**p<,05**
		Yok	*f*	8	11	35	55	
			%	7,3	10,1	32,1	50,5	
2	Kâğıt veya elektronik ortamda bulunan kritik bilgilere yetkisiz erişim, bunların hasar görmesi ve kaybolması risklerini azaltan temiz masa / ekran ilke ve yöntemleri	Var	*f*	0	3	17	43	
			%	0,0	4,8	27,0	68,3	**X^2=8,982**
		Yok	*f*	10	8	32	55	**p<,05**
			%	9,5	7,6	30,5	52,4	
3	Kritik bilgi, evrak, yazılım ve diğer bilgi varlıklarının kurum dışına çıkarılması ya da başka ortamlara aktarılması ile ilgili bilgi transferi ilke ve yöntemleri	Var	*f*	1	2	15	48	
			%	1,5	3,0	22,7	72,7	**X^2=9,261**
		Yok	*f*	9	13	24	59	**p<,05**
			%	8,6	12,4	22,9	56,2	
4	Taşınabilir cihazların kullanılmasıyla ortaya çıkan risklerin yönetilmesini ve üzerlerindeki kayıtlı bilgilerin güvenliğini temin eden ilkeler	Var	*f*	1	4	14	44	
			%	1,6	6,3	22,2	69,8	**X^2=9,559**
		Yok	*f*	9	13	34	50	**p<,05**
			%	8,5	12,3	32,1	47,2	
5	Uzak çalışma alanlarından kurumun bilgi sistemlerinde işlenen ve depolanan bilgiyi koruma amacı güden uzaktan çalışma ilkeler	Var	*f*	0	1	16	49	
			%	0,0	1,5	24,2	74,2	**X^2=11,019**
		Yok	*f*	6	10	33	57	**p<,05**
			%	5,7	9,4	31,1	53,8	
6	Bilgi sistemlerine kaynağı belirli, kişisel ve kötü niyet şüphesi olmayan hangi tür yazılımların kurulabileceğini tanımlayan ilke ve yöntemler	Var	*f*	1	2	16	43	
			%	1,6	3,2	25,8	69,4	X^2=7,161
		Yok	*f*	8	11	25	54	p>,05
			%	8,2	11,2	25,5	55,1	
7	Bilgi sistemleri ve varlıklarına erişim sağlayan kullanıcı ve tedarikçilerin haklarını, kısıtlamalarını ve sınırlığını belirleyen erişim kontrol ilke ve yöntemleri	Var	*f*	1	4	14	47	
			%	1,5	6,1	21,2	71,2	X^2=3,740p
		Yok	*f*	7	10	27	63	>,05
			%	6,5	9,3	25,2	58,9	
8	Bilginin değeri, kritikliği ve ifşa edilme hassasiyetine uygun seviyelerde korunmasını teminen bilgi sınıflandırma ve etiketleme ilkeleri	Var	*f*	1	3	15	46	
			%	1,5	4,6	23,1	70,8	**X^2=8,149**
		Yok	*f*	7	15	29	55	**p<,05**
			%	6,6	14,2	27,4	51,9	
9	Kritik bilgi barındıran alan ve sistemlerin korunmasını ve kütüphanenin güvenlik sınırlarını ve önlemlerini tanımlayan fiziksel ve çevresel güvenlik ilke ve yöntemleri	Var	*f*	1	2	19	44	
			%	1,5	3,0	28,8	66,7	**X^2=11,573**
		Yok	*f*	8	19	30	56	**p<,05**
			%	7,1	16,8	26,5	49,6	
10	Olası bir felaket ve ortam hatasından kaynaklanan veri kaybına karşı kritik bilgi, yazılım ve sistemlerin korunmasını amaçlayan bilgi yedekleme ilke ve yöntemleri	Var	*f*	2	1	14	48	
			%	3,1	1,5	21,5	73,8	X^2=5,758
		Yok	*f*	8	9	24	63	p>,05
			%	7,7	8,7	23,1	60,6	
11	Bilgi sistemlerinin zararlı yazılım saldırılarından korumak için tespit etme, engelleme ve kurtarma kontrollerini içeren zararlı yazılımlara karşı ilke ve yöntemler	Var	*f*	2	1	16	42	
			%	3,3	1,6	26,2	68,9	X^2=2,153
		Yok	*f*	7	6	27	67	p>,05
			%	6,5	5,6	25,2	62,6	
12	Bilgilerin gizliliğinin ve bütünlüğünün korunması için şifreleme kontrollerinin doğru ve etkin kullanımını temin eden ilke ve yöntemler	Var	*f*	2	2	12	48	
			%	3,1	3,1	18,8	75,0	X^2=4,876
		Yok	*f*	6	7	32	62	p>,05
			%	5,6	6,5	29,9	57,9	
13	Ağa bağlı sistem ve uygulamalardaki verilerin ve ağ alt yapısının güvenliğini ve yetkisiz erişimlerden korunmasını temin eden ağ yönetimi ilke ve yöntemleri	Var	*f*	2	2	11	48	
			%	3,2	3,2	17,5	76,2	X^2=2,679
		Yok	*f*	6	5	26	65	p>,05
			%	5,9	4,9	25,5	63,7	
14	Kişisel kimlik bilgilerinin gizliliğini ve korunmasını temin eden kişisel bilgilerin mahremiyeti ve koruması ilke ve yöntemleri	Var	*f*	2	1	14	52	
			%	2,9	1,4	20,3	75,4	X^2=4,490
		Yok	*f*	6	9	25	73	p>,05
			%	5,3	8,0	22,1	64,6	
15	Patentli yazılım ve bilgi varlıklarının yasal kullanım haklarının ilgili yasa ve anlaşmalar çerçevesinde korunmasını temin eden fikri mülkiyet ilke ve yöntemleri	Var	*f*	2	1	16	45	
			%	3,1	1,6	25,0	70,3	X^2=2,892
		Yok	*f*	6	6	23	67	p>,05
			%	5,9	5,9	22,5	65,7	
16	Tedarikçilerin kullanıcı ve kurumsal bilgi varlıklarına erişimi ile ilgili risklerin azaltılmasını ve kritik bilgilerin korunmasını temin eden tedarikçi ilişkileri yöntemleri	Var	*f*	2	1	17	43	
			%	3,2	1,6	27,0	68,3	X^2=3,476
		Yok	*f*	5	8	25	60	p>,05
			%	5,1	8,2	25,5	61,2	

Tablo 6.37'deki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden politikalar kategorisindeki 1, 2, 3. 4, 5, 8 ve 9. maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.38'de üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği prosedürlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.38: Bilgi güvenliğinden sorumlu personelin varlığına göre bilgi güvenliği prosedürlerinin uygulanma düzeyleri

	Bilgi Güvenliği Prosedürleri Maddeleri	*Bilgi Güvenliği Personeli*		*Uygulanma düzeyi* *Hiç*	*Kötü*	*Orta*	*İyi*	X^2
17	Kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ilke ve yöntemler	Var	*f*	2	0	11	48	**X^2=14,020 p<,05**
			%	3,3	0,0	18,0	78,7	
		Yok	*f*	7	8	32	49	
			%	7,3	8,3	33,3	51,0	
18	Sistem ve hizmetlere güvenli erişimi temin etmek için kullanıcı kaydetme, erişim izni verme, kimlik doğrulama gibi faaliyetlerin belirlendiği kullanıcı erişim yöntemleri	Var	*f*	2	0	8	56	**X^2=11,797 p<,05**
			%	3,0	0,0	12,1	84,8	
		Yok	*f*	7	5	30	65	
			%	6,5	4,7	28,0	60,7	
19	Sistem ve uygulamalara yetkisiz erişimi engellemek için faaliyetlerin belirlendiği güvenli oturum açma ilke ve yöntemleri	Var	*f*	2	0	10	53	**X^2=8,885 p<,05**
			%	3,1	0,0	15,4	81,5	
		Yok	*f*	4	7	29	67	
			%	3,7	6,5	27,1	62,6	
20	Güvenli alanlara sadece yetkili personele erişim izni vermek için uygun giriş kontrollerinin ve faaliyetlerinin belirlendiği fiziksel giriş ilke ve yöntemleri	Var	*f*	2	0	12	52	**X^2=11,283 p<,05**
			%	3,0	0,0	18,2	78,8	
		Yok	*f*	9	9	27	62	
			%	8,4	8,4	25,2	57,9	
21	Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir şekilde müdahale edilmesini amaçlayan faaliyetlerin belirlendiği ilke ve yöntemler	Var	*f*	2	0	14	46	**X^2=14,998 p<,05**
			%	3,2	0,0	22,6	74,2	
		Yok	*f*	10	13	26	48	
			%	10,3	13,4	26,8	49,5	
22	Yıkıcı bir olayı yönetmek ve mevcut durumu korumak için gereksinim duyulan planlama ve faaliyetlerin belirlendiği iş sürekliliği ve felaket kurtarma ilke ve yöntemleri	Var	*f*	2	1	11	49	**X^2=18,359 p<,05**
			%	3,2	1,6	17,5	77,8	
		Yok	*f*	12	14	29	47	
			%	11,8	13,7	28,4	46,1	
23	Kütüphane sistemleri, internet ağı, elektronik posta ve diğer erişimler için güçlü parola kullanımı ve yönetme standartları düzenleyen parola işleme ve kullanımı ilke ve yöntemleri	Var	*f*	2	1	11	51	X^2=5,382 p>,05
			%	3,1	1,5	16,9	78,5	
		Yok	*f*	5	8	28	69	
			%	4,5	7,3	25,5	62,7	
24	Bilgi varlıklarının kapasitelerinin planlanması ve kapasite kullanımlarının belli sınırlar içinde tutulması faaliyetlerini düzenleyen kapasite yönetimi ilke ve yöntemleri	Var	*f*	2	0	11	50	**X^2=13,321 p<,05**
			%	3,2	0,0	17,5	79,4	
		Yok	*f*	10	6	34	55	
			%	9,5	5,7	32,4	52,4	
25	Kullanıcıların doğru ve güvenli e-posta kullanımına yönelik kişisel ve kurumsal faaliyetleri düzenleyen elektronik posta ilke ve yöntemleri	Var	*f*	1	0	10	55	**X^2=14,951 p<,05**
			%	1,5	0,0	15,2	83,3	
		Yok	*f*	7	10	27	61	
			%	6,7	9,5	25,7	58,1	
26	Ziyaretçilerin kabulü, dolaşımları ve kütüphaneden ayrılmalarıyla ilgili faaliyetleri düzenleyen ziyaretçi kabul ilke ve yöntemleri	Var	*f*	2	2	15	47	**X^2=14,891 p<,05**
			%	3,0	3,0	22,7	71,2	
		Yok	*f*	15	14	33	50	
			%	13,4	12,5	29,5	44,6	

Tablo 6.38'deki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden prosedürler kategorisindeki 23. maddedeki önlem hariç diğer tüm maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.39'da üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin

varlığına göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.39: Bilgi güvenliğinden sorumlu personelin varlığına göre bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeyleri

	Bilgi Güvenliği İdari Araç ve Yöntemleri Maddeleri	*Bilgi Güvenliği Personeli*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
27	Bilgi güvenliği politika ve prosedürleri ihlallerinin raporlanması ve ilgili birimlere bildirilmesini düzenleyen kılavuz ve talimatlar	Var	*f*	1	1	16	44	**X^2=23,418 p<,05**
			%	1,6	1,6	25,8	71,0	
		Yok	*f*	17	18	30	42	
			%	15,9	16,8	28,0	39,3	
28	Bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi bir disiplin mekanizması	Var	*f*	0	2	15	45	**X^2=18,259 p<,05**
			%	0,0	3,2	24,2	72,6	
		Yok	*f*	12	14	26	42	
			%	12,8	14,9	27,7	44,7	
29	Yeni istihdam edilen ve görevi sona eren personelin bilgi güvenliği sorumluluklarını bildiren talimat ve uygulamalar	Var	*f*	1	2	15	46	**X^2=22,458 p<,05**
			%	1,6	3,1	23,4	71,9	
		Yok	*f*	15	20	31	43	
			%	13,8	18,3	28,4	39,4	
30	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenmeden önce ilgili kullanıcının bilgilendirilmesini amaçlayan aydınlatma metni uygulamaları	Var	*f*	1	0	13	51	**X^2=21,520 p<,05**
			%	1,5	0,0	20,0	78,5	
		Yok	*f*	13	12	34	51	
			%	11,8	10,9	30,9	46,4	
31	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenme amacının ilgilisine açıkça ifade edilmesini amaçlayan açık rıza yönetimi uygulamaları	Var	*f*	2	1	14	47	**X^2=14,641 p<,05**
			%	3,1	1,6	21,9	73,4	
		Yok	*f*	15	11	33	52	
			%	13,5	9,9	29,7	46,8	
32	Bilgi güvenliği tehditlerinden korumaya yönelik ilgili aksiyon planlarını kapsayan risk analizi tabanlı idari araçlar ve uygulamalar	Var	*f*	1	1	14	44	**X^2=16,681 p<,05**
			%	1,7	1,7	23,3	73,3	
		Yok	*f*	11	14	27	43	
			%	11,6	14,7	28,4	45,3	
33	Bilgi güvenliği yönetim sisteminizin etkin, güncel, izlenebilir ve gelişime açık yapıda olmasının teminini amaçlayan iç denetim ilke ve uygulamaları	Var	*f*	1	0	11	53	**X^2=24,585 p<,05**
			%	1,5	0,0	16,9	81,5	
		Yok	*f*	9	14	31	45	
			%	9,1	14,1	31,3	45,5	
34	Üçüncü taraf tedarikçi firma ve kurumlar ile yapılacak bilgi alışverişinin güvenliğini sağlamaya yönelik yapılan sözleşmelere ilişkin idari ilke ve yöntemler	Var	*f*	1	0	12	51	**X^2=13,491 p<,05**
			%	1,6	0,0	18,8	79,7	
		Yok	*f*	7	9	26	53	
			%	7,4	9,5	27,4	55,8	

Tablo 6.39'daki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden idari araç ve yöntemler kategorisindeki tüm maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.40'da üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği farkındalık

çalışmalarının uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.40: Bilgi güvenliğinden sorumlu personelin varlığına göre bilgi güvenliği farkındalık çalışmalarının uygulanma düzeyleri

	Bilgi Güvenliği Farkındalık Çalışmaları	*Bilgi Güvenliği Personeli*		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
35	Personelin ve kullanıcıların bilgi güvenliği sorumluluklarını farkında olmalarını ve yerine getirmelerini amaçlayan bilgi güvenliği farkındalık eğitimi çalışmaları	Var	*f*	3	2	21	44	**X^2=21,594 p<,05**
			%	4,3	2,9	30,0	62,9	
		Yok	*f*	18	24	33	42	
			%	15,4	20,5	28,2	35,9	
36	Bilgi güvenliği eğitim faaliyetlerinin kapsamının belirlendiği ve ihtiyaçların netleştirildiği eğitim planlama rehberleri	Var	*f*	4	2	21	40	**X^2=27,139 p<,05**
			%	6,0	3,0	31,3	59,7	
		Yok	*f*	23	28	31	34	
			%	19,8	24,1	26,7	29,3	
37	Bilgi güvenliği alanında görevlendirilen personelin yetenek ihtiyaç analizinin yapılması ve sonuçlarına göre hizmetçi eğitim uygulamaları	Var	*f*	3	4	18	40	**X^2=22,172 p<,05**
			%	4,6	6,2	27,7	61,5	
		Yok	*f*	23	24	32	35	
			%	20,2	21,1	28,1	30,7	
38	Kütüphanenin bilgi güvenliği çerçevesini oluşturan politika, prosedür ve idari yöntemler hakkında tedarikçilerin farkındalığını geliştirme çalışmaları	Var	*f*	3	3	18	41	**X^2=20,062 p<,05**
			%	4,6	4,6	27,7	63,1	
		Yok	*f*	23	19	33	38	
			%	20,4	16,8	29,2	33,6	
39	Personel ve kullanıcıların bilgi güvenliği farkındalığını arttırıcı interaktif eğitim çalışmaları	Var	*f*	4	3	17	44	**X^2=28,889 p<,05**
			%	5,9	4,4	25,0	64,7	
		Yok	*f*	28	22	35	33	
			%	23,7	18,6	29,7	28,0	
40	Bilgi güvenliği ile ilgili broşür, poster ve kitapçık gibi bilgilendirici doküman çalışmaları	Var	*f*	5	8	18	37	**X^2=24,399 p<,05**
			%	7,4	11,8	26,5	54,4	
		Yok	*f*	34	23	34	26	
			%	29,1	19,7	29,1	22,2	
41	Kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması	Var	*f*	9	7	21	30	**X^2=19,532 p<,05**
			%	13,4	10,4	31,3	44,8	
		Yok	*f*	38	29	27	25	
			%	31,9	24,4	22,7	21,0	
42	Kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları, fare altlığı, not kâğıtları gibi farkındalık arttırıcı faaliyetler	Var	*f*	7	9	21	30	**X^2=15,988 p<,05**
			%	10,4	13,4	31,3	44,8	
		Yok	*f*	35	29	26	30	
			%	29,2	24,2	21,7	25,0	
43	Personele ve kullanıcılara bilgi güvenliği ile ilgili mail ve SMS yoluyla bilgilendirme mesajlarının gönderilmesi	Var	*f*	4	8	19	36	**X^2=9,895 p<,05**
			%	6,0	11,9	28,4	53,7	
		Yok	*f*	24	20	33	42	
			%	20,2	16,8	27,7	35,3	
44	Personel ve kullanıcıların bilgi güvenliği hassasiyetlerinin ödüllendirilme çalışmaları	Var	*f*	11	9	19	25	**X^2=17,036 p<,05**
			%	17,2	14,1	29,7	39,1	
		Yok	*f*	44	27	23	20	
			%	38,6	23,7	20,2	17,5	
45	Kütüphanenizin bilgi güvenliği politika, prosedür ve idari yöntemleri ile ilgili yapılan güncellemelerin kullanıcılara zamanında bildirilme	Var	*f*	3	4	19	44	**X^2=20,299 p<,05**
			%	4,3	5,7	27,1	62,9	
		Yok	*f*	24	20	30	40	
			%	21,1	17,5	26,3	35,1	

Tablo 6.40'taki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden farkındalık çalışmaları kategorisindeki tüm maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin

uygulanma düzeylerinin bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

6.7.4. Bilgi Güvenliği Yönetim Aracı Değişkenine Göre Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri

Bu başlık altında, üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikaları, bilgi güvenliği prosedürleri, bilgi güvenliği idari araç ve yöntemleri ve bilgi güvenliği farkındalık araçları kategorilerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin ilişkin frekans dağılımları ve ki kare istatistikleri verilmiştir.

Tablo 6.41'de üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikalarının uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.41: Bilgi güvenliği yönetim aracının kullanımına göre bilgi güvenliği politikalarının uygulanma düzeyleri

	Bilgi Güvenliği Politikaları Maddeleri	**Bilgi Güvenliği Yönetim Aracı**		***Uygulanma düzeyi***				***X²***
				Hiç	***Kötü***	***Orta***	***İyi***	
1	Personel, kullanıcı ve tedarikçilerin bilgi sistemleri ve varlıklarındaki bilgilerin kabul edilebilir kullanımlarını tanımlayan ilkeler	Var	*f*	1	4	27	81	**X²=29,482**
			%	0,9	3,5	23,9	71,7	**p<,05**
		Yok	*f*	7	9	26	21	
			%	11,1	14,3	41,3	33,3	
2	Kâğıt veya elektronik ortamda bulunan kritik bilgilere yetkisiz erişim, bunların hasar görmesi ve kaybolması risklerini azaltan temiz masa / ekran ilke ve yöntemleri	Var	*f*	2	5	27	72	**X²=14,979**
			%	1,9	4,7	25,5	67,9	**p<,05**
		Yok	*f*	8	6	22	26	
			%	12,9	9,7	35,5	41,9	
3	Kritik bilgi, evrak, yazılım ve diğer bilgi varlıklarının kurum dışına çıkarılması ya da başka ortamlara aktarılması ile ilgili bilgi transferi ilke ve yöntemleri	Var	*f*	2	6	19	82	**X²=23,443**
			%	1,8	5,5	17,4	75,2	**p<,05**
		Yok	*f*	8	9	20	25	
			%	12,9	14,5	32,3	40,3	
4	Taşınabilir cihazların kullanılmasıyla ortaya çıkan risklerin yönetilmesini ve üzerlerindeki kayıtlı bilgilerin güvenliğini temin eden ilkeler	Var	*f*	2	8	23	74	**X²=24,520**
			%	1,9	7,5	21,5	69,2	**p<,05**
		Yok	*f*	8	9	25	20	
			%	12,9	14,5	40,3	32,3	
5	Uzak çalışma alanlarından kurumun bilgi sistemlerinde işlenen ve depolanan bilgiyi koruma amacı güden uzaktan çalışma ilkeler	Var	*f*	1	6	27	77	**X²=11,058**
			%	0,9	5,4	24,3	69,4	**p<,05**
		Yok	*f*	5	5	22	29	
			%	8,2	8,2	36,1	47,5	
6	Bilgi sistemlerine kaynağı belirli, kişisel ve kötü niyet şüphesi olmayan hangi tür yazılımların kurulabileceğini tanımlayan ilke ve yöntemler	Var	*f*	1	6	24	72	**X²=17,155**
			%	1,0	5,8	23,3	69,9	**p<,05**
		Yok	*f*	8	7	17	25	
			%	14,0	12,3	29,8	43,9	
7	Bilgi sistemleri ve varlıklarına erişim sağlayan kullanıcı ve tedarikçilerin haklarını, kısıtlamalarını ve sınırlığını belirleyen erişim kontrol ilke ve yöntemleri	Var	*f*	1	5	23	80	**X²=18,528**
			%	0,9	4,6	21,1	73,4	**p<,05**
		Yok	*f*	7	9	18	30	
			%	10,9	14,1	28,1	46,9	
8	Bilginin değeri, kritikliği ve ifşa edilme hassasiyetine uygun seviyelerde korunmasını teminen bilgi sınıflandırma ve etiketleme ilkeleri	Var	*f*	1	8	22	75	**X²=19,501**
			%	0,9	7,5	20,8	70,8	**p<,05**
		Yok	*f*	7	10	22	26	
			%	10,8	15,4	33,8	40,0	
9	Kritik bilgi barındıran alan ve sistemlerin korunmasını ve kütüphanenin güvenlik sınırlarını ve önlemlerini tanımlayan fiziksel ve çevresel güvenlik ilke ve yöntemleri	Var	*f*	2	7	31	72	**X²=17,728**
			%	1,8	6,3	27,7	64,3	**p<,05**
		Yok	*f*	7	14	18	28	
			%	10,4	20,9	26,9	41,8	
10	Olası bir felaket ve ortam hatasından kaynaklanan veri kaybına karşı kritik bilgi, yazılım ve sistemlerin korunmasını amaçlayan bilgi yedekleme ilke ve yöntemleri	Var	*f*	3	4	23	77	**X²=8,721**
			%	2,8	3,7	21,5	72,0	**p<,05**
		Yok	*f*	7	6	15	34	
			%	11,3	9,7	24,2	54,8	
11	Bilgi sistemlerinin zararlı yazılım saldırılarından korumak için tespit etme, engelleme ve kurtarma kontrollerini içeren zararlı yazılımlara karşı ilke ve yöntemler	Var	*f*	3	4	23	77	**X²=7,894**
			%	2,8	3,7	21,5	72,0	**p<,05**
		Yok	*f*	6	3	20	32	
			%	9,8	4,9	32,8	52,5	
12	Bilgilerin gizliliğinin ve bütünlüğünün korunması için şifreleme kontrollerinin doğru ve etkin kullanımını temin eden ilke ve yöntemler	Var	*f*	2	3	22	81	**X²=16,518**
			%	1,9	2,8	20,4	75,0	**p<,05**
		Yok	*f*	6	6	22	29	
			%	9,5	9,5	34,9	46,0	
13	Ağa bağlı sistem ve uygulamalardaki verilerin ve ağ alt yapısının güvenliğini ve yetkisiz erişimlerden korunmasını temin eden ağ yönetimi ilke ve yöntemleri	Var	*f*	2	4	19	82	**X²=11,665**
			%	1,9	3,7	17,8	76,6	**p<,05**
		Yok	*f*	6	3	18	31	
			%	10,3	5,2	31,0	53,4	
14	Kişisel kimlik bilgilerinin gizliliğini ve korunmasını temin eden kişisel bilgilerin mahremiyeti ve koruması ilke ve yöntemleri	Var	*f*	2	4	23	87	**X²=9,521**
			%	1,7	3,4	19,8	75,0	**p<,05**
		Yok	*f*	6	6	16	38	
			%	9,1	9,1	24,2	57,6	
15	Patentli yazılım ve bilgi varlıklarının yasal kullanım haklarının ilgili yasa ve anlaşmalar çerçevesinde korunmasını temin eden fikri mülkiyet ilke ve yöntemleri	Var	*f*	3	2	24	78	**X²=7,645**
			%	2,8	1,9	22,4	72,9	**p<,05**
		Yok	*f*	5	5	15	34	
			%	8,5	8,5	25,4	57,6	
16	Tedarikçilerin kullanıcı ve kurumsal bilgi varlıklarına erişimi ile ilgili risklerin azaltılmasını ve kritik bilgilerin korunmasını temin eden tedarikçi ilişkileri yöntemleri	Var	*f*	2	2	27	73	**X²=12,042**
			%	1,9	1,9	26,0	70,2	**p<,05**
		Yok	*f*	5	7	15	30	
			%	8,8	12,3	26,3	52,6	

Tablo 6.41'deki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden politikalar kategorisindeki tüm maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.42'de üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği prosedürlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.42: Bilgi güvenliği yönetim aracının kullanımına göre bilgi güvenliği prosedürlerinin uygulanma düzeyleri

	Bilgi Güvenliği Prosedürleri Maddeleri	**Bilgi Güvenliği Yönetim Aracı**		***Uygulanma düzeyi***				***X²***
				Hiç	***Kötü***	***Orta***	***İyi***	
17	Kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ilke ve yöntemler	Var	*f*	3	4	19	77	**X²=21,801 p<,05**
			%	2,9	3,9	18,4	74,8	
		Yok	*f*	6	4	24	20	
			%	11,1	7,4	44,4	37,0	
18	Sistem ve hizmetlere güvenli erişimi temin etmek için kullanıcı kaydetme, erişim izni verme, kimlik doğrulama gibi faaliyetlerin belirlendiği kullanıcı erişim yöntemleri	Var	*f*	2	3	15	89	**X²=20,727 p<,05**
			%	1,8	2,8	13,8	81,7	
		Yok	*f*	7	2	23	32	
			%	10,9	3,1	35,9	50,0	
19	Sistem ve uygulamalara yetkisiz erişimi engellemek için faaliyetlerin belirlendiği güvenli oturum açma ilke ve yöntemleri	Var	*f*	2	3	18	86	**X²=12,028 p<,05**
			%	1,8	2,8	16,5	78,9	
		Yok	*f*	4	4	21	34	
			%	6,3	6,3	33,3	54,0	
20	Güvenli alanlara sadece yetkili personele erişim izni vermek için uygun giriş kontrollerinin ve faaliyetlerinin belirlendiği fiziksel giriş ilke ve yöntemleri	Var	*f*	2	5	18	84	**X²=19,600 p<,05**
			%	1,8	4,6	16,5	77,1	
		Yok	*f*	9	4	21	30	
			%	14,1	6,3	32,8	46,9	
21	Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir şekilde müdahale edilmesini amaçlayan faaliyetlerin belirlendiği ilke ve yöntemler	Var	*f*	4	6	20	73	**X²=17,764 p<,05**
			%	3,9	5,8	19,4	70,9	
		Yok	*f*	8	7	20	21	
			%	14,3	12,5	35,7	37,5	
22	Yıkıcı bir olayı yönetmek ve mevcut durumu korumak için gereksinim duyulan planlama ve faaliyetlerin belirlendiği iş sürekliliği ve felaket kurtarma ilke ve yöntemleri	Var	*f*	4	9	19	74	**X²=19,366 p<,05**
			%	3,8	8,5	17,9	69,8	
		Yok	*f*	10	6	21	22	
			%	16,9	10,2	35,6	37,3	
23	Kütüphane sistemleri, internet ağı, elektronik posta ve diğer erişimler için güçlü parola kullanımı ve yönetme standartları düzenleyen parola işleme ve kullanımı ilke ve yöntemleri	Var	*f*	3	5	18	84	**X²=8,736 p<,05**
			%	2,7	4,5	16,4	76,4	
		Yok	*f*	4	4	21	36	
			%	6,2	6,2	32,3	55,4	
24	Bilgi varlıklarının kapasitelerinin planlanması ve kapasite kullanımlarının belli sınırlar içinde tutulması faaliyetlerini düzenleyen kapasite yönetimi ilke ve yöntemleri	Var	*f*	4	1	23	80	**X²=20,227 p<,05**
			%	3,7	0,9	21,3	74,1	
		Yok	*f*	8	5	22	25	
			%	13,3	8,3	36,7	41,7	
25	Kullanıcıların doğru ve güvenli e-posta kullanımına yönelik kişisel ve kurumsal faaliyetleri düzenleyen elektronik posta ilke ve yöntemleri	Var	*f*	1	2	17	88	**X²=28,735 p<,05**
			%	0,9	1,9	15,7	81,5	
		Yok	*f*	7	8	20	28	
			%	11,1	12,7	31,7	44,4	
26	Ziyaretçilerin kabulü, dolaşımları ve kütüphaneden ayrılmalarıyla ilgili faaliyetleri düzenleyen ziyaretçi kabul ilke ve yöntemleri	Var	*f*	6	4	26	76	**X²=26,898 p<,05**
			%	5,4	3,6	23,2	67,9	
		Yok	*f*	11	12	22	21	
			%	16,7	18,2	33,3	31,8	

Tablo 6.42'deki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden prosedürler kategorisindeki tüm maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.43'te üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının

kullanılıp kullanılmama durumuna göre, kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.43: Bilgi güvenliği yönetim aracının kullanımına göre bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeyleri

	Bilgi Güvenliği İdari Araç ve Yöntemleri Maddeleri	**Bilgi Güvenliği Yönetim Aracı**		*Uygulanma düzeyi*				X^2
				Hiç	*Kötü*	*Orta*	*İyi*	
27	Bilgi güvenliği politika ve prosedürleri ihlallerinin raporlanması ve ilgili birimlere bildirilmesini düzenleyen kılavuz ve talimatlar	Var	*f*	5	5	27	72	**X^2=37,251 p<,05**
			%	4,6	4,6	24,8	66,1	
		Yok	*f*	13	14	19	14	
			%	21,7	23,3	31,7	23,3	
28	Bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi bir disiplin mekanizması	Var	*f*	2	5	25	69	**X^2=28,357 p<,05**
			%	2,0	5,0	24,8	68,3	
		Yok	*f*	10	11	16	18	
			%	18,2	20,0	29,1	32,7	
29	Yeni istihdam edilen ve görevi sona eren personelin bilgi güvenliği sorumluluklarını bildiren talimat ve uygulamalar	Var	*f*	2	5	29	72	**X^2=44,741 p<,05**
			%	1,9	4,6	26,9	66,7	
		Yok	*f*	14	17	17	17	
			%	21,5	26,2	26,2	26,2	
30	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenmeden önce ilgili kullanıcının bilgilendirilmesini amaçlayan aydınlatma metni uygulamaları	Var	*f*	4	3	27	76	**X^2=20,937 p<,05**
			%	3,6	2,7	24,5	69,1	
		Yok	*f*	10	9	20	26	
			%	15,4	13,8	30,8	40,0	
31	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenme amacının ilgilisine açıkça ifade edilmesini amaçlayan açık rıza yönetimi uygulamaları	Var	*f*	6	3	27	73	**X^2=18,370 p<,05**
			%	5,5	2,8	24,8	67,0	
		Yok	*f*	11	9	20	26	
			%	16,7	13,6	30,3	39,4	
32	Bilgi güvenliği tehditlerinden korumaya yönelik ilgili aksiyon planlarını kapsayan risk analizi tabanlı idari araçlar ve uygulamalar	Var	*f*	2	5	21	68	**X^2=27,348 p<,05**
			%	2,1	5,2	21,9	70,8	
		Yok	*f*	10	10	20	19	
			%	16,9	16,9	33,9	32,2	
33	Bilgi güvenliği yönetim sisteminizin etkin, güncel, izlenebilir ve gelişime açık yapıda olmasının teminini amaçlayan iç denetim ilke ve uygulamaları	Var	*f*	1	2	24	78	**X^2=38,883 p<,05**
			%	1,0	1,9	22,9	74,3	
		Yok	*f*	9	12	18	20	
			%	15,3	20,3	30,5	33,9	
34	Üçüncü taraf tedarikçi firma ve kurumlar ile yapılacak bilgi alışverişinin güvenliğini sağlamaya yönelik yapılan sözleşmelere ilişkin idari ilke ve yöntemler	Var	*f*	1	1	20	82	**X^2=32,667 p<,05**
			%	1,0	1,0	19,2	78,8	
		Yok	*f*	7	8	18	22	
			%	12,7	14,5	32,7	40,0	

Tablo 6.43'teki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden idari araç ve yöntemler kategorisindeki tüm maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

Tablo 6.44'te üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanılıp kullanılmama durumuna göre, kurumsal bilgi güvenliği önlemlerinden bilgi

güvenliği farkındalık çalışmalarının uygulanma düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımı ve ki kare istatistiği verilmiştir.

Tablo 6.44: Bilgi güvenliği yönetim aracının kullanımına göre bilgi güvenliği farkındalık çalışmalarının uygulanma düzeyleri

	Bilgi Güvenliği Farkındalık Çalışmaları	**Bilgi Güvenliği Yönetim Aracı**		***Uygulanma düzeyi***				***X²***
				Hiç	***Kötü***	***Orta***	***İyi***	
35	Personelin ve kullanıcıların bilgi güvenliği sorumluluklarını farkında olmalarını ve yerine getirmelerini amaçlayan bilgi güvenliği farkındalık eğitimi çalışmaları	Var	*f*	7	8	30	72	**X²=36,452 p<,05**
			%	6,0	6,8	25,6	61,5	
		Yok	*f*	14	18	24	14	
			%	20,0	25,7	34,3	20,0	
36	Bilgi güvenliği eğitim faaliyetlerinin kapsamının belirlendiği ve ihtiyaçların netleştirildiği eğitim planlama rehberleri	Var	*f*	10	9	34	62	**X²=35,599 p<,05**
			%	8,7	7,8	29,6	53,9	
		Yok	*f*	17	21	18	12	
			%	25,0	30,9	26,5	17,6	
37	Bilgi güvenliği alanında görevlendirilen personelin yetenek ihtiyaç analizinin yapılması ve sonuçlarına göre hizmetçi eğitim uygulamaları	Var	*f*	11	8	28	62	**X²=31,489 p<,05**
			%	10,1	7,3	25,7	56,9	
		Yok	*f*	15	20	22	13	
			%	21,4	28,6	31,4	18,6	
38	Kütüphanenin bilgi güvenliği çerçevesini oluşturan politika, prosedür ve idari yöntemler hakkında tedarikçilerin farkındalığını geliştirme çalışmaları	Var	*f*	8	8	32	64	**X²=29,255 p<,05**
			%	7,1	7,1	28,6	57,1	
		Yok	*f*	18	14	19	15	
			%	27,3	21,2	28,8	22,7	
39	Personel ve kullanıcıların bilgi güvenliği farkındalığını arttırıcı interaktif eğitim çalışmaları	Var	*f*	13	8	34	60	**X²=24,032 p<,05**
			%	11,3	7,0	29,6	52,2	
		Yok	*f*	19	17	18	17	
			%	26,8	23,9	25,4	23,9	
40	Bilgi güvenliği ile ilgili broşür, poster ve kitapçık gibi bilgilendirici doküman çalışmaları	Var	*f*	15	12	37	51	**X²=27,807 p<,05**
			%	13,0	10,4	32,2	44,3	
		Yok	*f*	24	19	15	12	
			%	34,3	27,1	21,4	17,1	
41	Kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması	Var	*f*	22	17	33	44	**X²=16,625 p<,05**
			%	19,0	14,7	28,4	37,9	
		Yok	*f*	25	19	15	11	
			%	35,7	27,1	21,4	15,7	
42	Kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları, fare altlığı, not kâğıtları gibi farkındalık arttırıcı faaliyetler	Var	*f*	21	18	29	47	**X²=12,732 p<,05**
			%	18,3	15,7	25,2	40,9	
		Yok	*f*	21	20	18	13	
			%	29,2	27,8	25,0	18,1	
43	Personele ve kullanıcılara bilgi güvenliği ile ilgili mail ve SMS yoluyla bilgilendirme mesajlarının gönderilmesi	Var	*f*	12	12	29	62	**X²=19,655 p<,05**
			%	10,4	10,4	25,2	53,9	
		Yok	*f*	16	16	23	16	
			%	22,5	22,5	32,4	22,5	
44	Personel ve kullanıcıların bilgi güvenliği hassasiyetlerinin ödüllendirilme çalışmaları	Var	*f*	26	19	30	36	**X²=14,179 p<,05**
			%	23,4	17,1	27,0	32,4	
		Yok	*f*	29	17	12	9	
			%	43,3	25,4	17,9	13,4	
45	Kütüphanenizin bilgi güvenliği politika, prosedür ve idari yöntemleri ile ilgili yapılan güncellemelerin kullanıcılara zamanında bildirilme	Var	*f*	10	5	34	67	**X²=36,540 p<,05**
			%	8,6	4,3	29,3	57,8	
		Yok	*f*	17	19	15	17	
			%	25,0	27,9	22,1	25,0	

Tablo 6.44'teki veriler incelendiğinde, kurumsal bilgi güvenliği önlemlerinden farkındalık çalışmaları kategorisindeki tüm maddelerde yer alan önlemlerin uygulanması hakkında katılımcıların görüşleri arasında üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre anlamlı bir farklılık olduğu görülmektedir ($p<0,05$) Bu bulgulardan hareketle bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde bu maddelerde belirtilen önlemlerin uygulanma

düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksek olduğu söylenebilir.

6.8. Tartışma

Bilgi güvenliği, günümüz dijital çağında büyük bir öneme sahip olan bir konudur. Özellikle kütüphaneler ve diğer bilgi merkezleri gibi bilgi kullanımı yoğunluğu yüksek ortamlar, kullanıcıların kişisel ve hassas verilerini koruma sorumluluğuyla karşı karşıyadır. Bu nedenle, bu kurumlar tarafından bilgi güvenliğiyle ilgili yapılan çalışmalar, büyük bir ilgi ve öneme sahiptir. Alanyazında bu konuda yapılan araştırmaların ve benzer tez çalışmalarının varlığı, bu konunun akademik ve profesyonel düzeyde ne kadar önemsendiğini göstermektedir.

Çalışma kapsamında elde edilen bulguların alanyazında benzer çalışmalar ile ilişkilerinin olup olmadığı konusunda değerlendirmeler yapılmasının hem mevcut bilgiye dayalı bir bakış açısı sunacağı hem de konunun gelişimi ve geleceği hakkında önemli bilgiler sağlayacağı düşünülmektedir. Bu bölümde, alanyazındaki benzer çalışmaların kapsamı, bulguları ve önerileri tartışılmakta ve bu çalışmaların kütüphaneler ve diğer kurumlar için ne tür faydalar sağlayabileceği üzerinde açıklamalarda bulunulmaktadır. Böylelikle, bilgi güvenliği alanında yapılan çalışmaların genel bir değerlendirilmesi sunularak, gelecekte yapılacak araştırmalara ve çalışmalara katkıda bulunması amaçlanlanmıştır.

6.8.1. Üniversite Kütüphanelerinde Bilgi Güvenliği Personelinin Varlığına İlişkin Tartışma

Alan araştırmasından elde edilen veriler üniversitelerde bilgi güvenliğinden sorumlu personel istihdamının yeterli olmadığını ortaya koymuştur. Ayrıca uzman bilgi güvenliği personelinin varlığı teknolojik ve kurumsal güvenlik önlemlerin etkin uygulanmasında fark yaratıcı bir durumdur.

Bu bulgular, Türkiye'de üniversite kütüphanelerinde bilgi güvenliği yönetimine verilen önemin ve bu konuda alınan önlemlerin eksikliği konusunda çeşitli düşünceleri beraberinde getirmektedir. Üniversite kütüphanelerinin önemli bir kısmında bilgi güvenliği personelinin bulunmaması, bilgi güvenliği yönetimi açısından potansiyel risklerin oluşabileceğine işaret etmektedir. Bilgi güvenliği

personelinin eksikliği, güvenlik açıklarının tespit edilmemesi veya zamanında müdahale edilememesi gibi sorunlara yol açabilir. Bu da üniversite kütüphanelerinde kişisel ve kurumsal verilerin güvenliği konusunda sorunların meydana gelebileceği söylenebilir.

Alanyazında üniversite kütüphanelerinde bilgi güvenliği personelinin varlığına ilişkin spesifik araştırma sayısı sınırlıdır (örn. Meral, 2022; Kurt, 2019; İsmail, 2012. Chang ve Wang, 2011). Ancak, bilgi güvenliği konusunun incelendiği çalışmalarda, genel olarak bilgi güvenliği konusunda uzmanlaşmış bir personelin varlığının kritik bir öneme sahip olduğu vurgulanmaktadır.

Ismail (2012)'in Malezya'da akademik kütüphanelerindeki bilgi güvenliği yönetimine ilişkin yaptığı çalışmada, akademik kütüphanelerin yarısından fazlasının (%56,4) bilgi güvenliğiyle ilgili işler için özel olarak atanan personele sahip olduğu sunucunun bu çalışmanın sonucu ile kısmen benzerlik gösterdiği söylenebilir. Ayrıca Kurt (2019)'un diğer kurumlarda yaptığı çalışmada, hastane bilgi güvenliğinden sorumlu bir uzmanın olması ile ilgili katılımcı görüşlerinin katılım oranının orta düzeyde ($\bar{x}$=3,16) olduğu; Meral (2022)'in çalışmasında, bilgi güvenliğinden sorumlu yeterli sayıda ve nitelikte personel bulunmasına ilişkin katılımcı görüşlerinin yine aynı şekilde orta düzeyde ($\bar{x}$=3,16) olduğu; Chang ve Wang (2011)'ın çalışmalarının bulgularında ise, bilgi sistemlerinin güvenliğinin iyi bir biçimde yürütülebilmesi için kurumda bilgi güvenliği yönetim bilgisine sahip bir sorumlu personelin görevlendirilmesinin kritik öneme sahip olduğu sonuçlarına ulaşılmıştır. Alanyazındaki sınırlı sayıdaki bu çalışmalara dayanarak, bilgi güvenliği personelinin varlığının kurumlardaki veri güvenliği açısından önemli bir faktör olduğu, fakat bu çalışmada ortaya konduğu gibi kurumların bu konuda yeterli düzeyde personel görevlendirmediği anlaşılmaktadır. Bu bakımdan bu çalışmanın sonuçları alanyazındaki diğer kurumlarda yapılan çalışmalar ile benzerlik göstermektedir.

Sonuç olarak, üniversite kütüphanelerinde bilgi güvenliği personelinin varlığı, veri güvenliği açısından kritik bir öneme sahiptir. Bu çalışmanın sonuçları, alanyazındaki sınırlı sayıdaki çalışmalarla desteklenmektedir. Ancak, bu konuda daha fazla araştırma yapılması ve bilgi güvenliği personelinin kütüphanelerdeki rolü ve etkisi hakkında daha fazla bilgi edinilmesi gerekmektedir.

6.8.2. Üniversite Kütüphanelerinde Kullanılan Bilgi Sistemlerinin Önemine İlişkin Tartışma

Türkiye'de üniversite kütüphanelerinde kullanılan bilgi sistemlerinin bilginin kritikliği açısından önem derecesine ilişkin yöneltilen sorudan elde edilen sonuçlara göre, verinin gizliliği, bütünlüğü ve erişilebilirliği bakımından bilgi sistemlerinin son derece önemli olduğu görüşü benimsendiği anlaşılmaktadır. Gizlilik, bütünlük ve erişebilirlik unsurları bilginin kritikliği açısından önemli güvenlik ilkeleridir. Üniversite kütüphanelerinde kullanılan bilgi sistemlerine işlenen verilerin kritik veri içermesinden ötürü bu sistemlerin bilgi güvenliği açısından önemli olduğu sonucuna ulaşılmıştır. İlgili alan yazın incelendiğinde, bu sonucu destekleyen benzer çalışmaların olduğu görülmüştür. Anameriç (2005; 2003) iki ayrı çalışmasında bu sonuca benzer çıkarımlarda bulunmaktadır. Çalışmalarda kütüphane hizmetlerinin yönetiminde kullanılan bilgi sistemlerinin kütüphane yöneticilerine ve personeline seçim ve sağlama, kataloglama ve sınıflama, ödünç verme, danışma ve bibliyografik tarama gibi birçok kütüphanecilik hizmetlerinin etkinliği, verimliliği, performansı ve kullanıcı tatmini açısından önemli olduğunu vurgulanmaktadır. Benzer biçimde, kişisel sağlık bilgi sistemlerinin etkin ve sürdürülebilir kullanımı, veri güvenliği ve mahremiyeti, standardizasyonu, entegrasyonu, erişebilirliği ve kullanılabilirliği açılarından yeni teknolojilerin kullanımında hastane bilgi sistemlerine verilen önemi vurgulayan çalışmalarda da aynı yönde sonuçlar gözlemlenmektedir (Kurt, 2019; Yıldırım, 2019; Saluvan ve Şahin 2014). Yine aynı biçimde hastane bilgi sistemlerinin önemi üzerine çalışması bulunan Onaran (2019) da bilgi sistemlerinin bilgi varlıkları için kritik öneme sahip sistemler olduğunu vurgulamaktadır. Farklı hizmet alanlarındaki çalışmalarda da bilgi sistemlerinin bilgi güvenliği açısından hayati derecede öneme sahip olduğu sonucuna ulaşılmaktadır (Aydın, 2022; Özgü, 2017). Ismail (2012)'in Malezya'daki akademik kütüphanelerdeki bilgi güvenliği yönetimi ile ilgili çalışmasında, Malezya'daki pek çok akademik kütüphanenin bilgi sistemlerinin kritik bilgi açısından çok değerli olduğunu fakat mali ve personel eksikliklerinden ötürü bu değerin yeteri düzeylerde gerçeleşediğini ifade edilmektedir. Çalışmada bilgi sistemlerine verilen önem özellikle vurgulanmakta olup bu yönüyle bu çalışmayla benzerlik gösterdiği görülmüştür.

6.8.3. Bilgi Varlıklarının Kritiklik Derecesinin Belirlenmesine İlişkin Tartışma

Bilgi varlıklarının kritiklik derecesi, işlenen verinin bilgi güvenliği unsurları (gizlilik, bütünlük, erişilebilirlik) ve bu işlenen verilere yönelik gerçekleşebilecek güvenlik ihalelerinin etki alanlarına (kurumsal, toplumsal, sektörel ve bağımlı varlıklar) göre belirlenebilmektedir. Araştırma sonuçlarına göre, Türkiye'de üniversite kütüphanelerindeki bilgi varlıklarında işlenen verinin kritiklik derecesi üzerinde gizlilik ve bütünlük unsurlarının orta, erişilebilirlik unsurunun ise yüksek derecede etkiye sahip olduğu görünüşünün hâkim olduğu belirlenmiştir. Etki alanları açsından ise kritik öneme sahip bilgilerin ihlal edilmesi kurumsal alanda yüksek; toplumsal, kütüphanecilik camiası ve kütüphanelerin dış paydaşları alanlarında ise orta düzeyde etki göstereceği sonucuna ulaşılmıştır. İlgili alan yazın incelendiğinde; Meral (2022)'in çalışmasında bilginin gizliliği, bütünlüğü ve erişebilirliği açısından benzer sonuçların çıktığı görülmektedir. Kurumun sahip olduğu verilerin kritiklik düzeyi arttıkça bilgi güvenliğinin etkinliğine o derecede ihtiyaç duyulduğu anlaşılmıştır.

Bilgi güvenliği ihlalleri, üniversite kütüphanelerinin kurumsal yapısını olumsuz etkileyerek, kütüphane yönetim sistemlerine, kataloglara ve diğer otomasyon sistemlerine sızma, yetkisiz erişim, veri kaybı veya veri bozulması gibi sorunlara neden olabilir. Bu durum, kütüphane hizmetlerinin aksamaya uğramasına, kullanıcıların bilgiye erişimini engellemesine veya kütüphane kaynaklarının yanlış yönlendirilmesine yol açabilir. Bu da üniversitedeki akademik araştırmaları, öğrenci çalışmalarını ve öğretim faaliyetlerini olumsuz etkileyebilir.

Bununla birlikte, bilgi güvenliği ihlalleri kütüphane bilgi sitemlerinde kayıtlı kullanıcı bilgilerinin gizliliği ve bütünlüğü konusunda sorunlar yaşanmasına neden olabileceğinden kütüphanecilik camiasını olumsuz etkileyecektir. İhlaller, kullanıcıların kişisel bilgilerinin ifşa olması veya yetkisiz kişiler tarafından kullanılması gibi durumlara yol açabilir. Bu da kullanıcıların güvenini sarsabilir ve kütüphanecilik camiasının itibarını zedeleyecektir.

Ayrıca, dış paydaşları arasında yer alan diğer üniversiteler, araştırma kurumları, yayınevleri ve endüstriyel ortaklar üniversite kütüphanesindeki olası bilgi güvenliği ihlallerinden etklenebilmektedir. Telif hakları, bilimsel araştırmalar ve ticari sırları

gibi dış paydaşlara ait kritik öneme sahip bilgilerin gizliliğinin ihlal edilmesi üniversite kütüphanelerinin güvenirliğini zedeleyecektir. Bu durum üniversitelerde araştırma projelerinin, yayınların ve diğer bilimsel faaliyetlerin etkilenmesine ve toplamda bilimsel ilerlemenin engellenmesine neden olabilir.

Sonuç olarak, Türkiye'deki üniversite kütüphanelerindeki bilgi güvenliği ihlallerinin, toplumsal, kurumsal, kütüphanecilik camiası ve kütüphanelere bağımlı dış paydaş alanlarını yüksek düzeyde etkilediği görülmüştür. Bu durum, bilgi güvenliği önlemlerinin öncelikli olarak üniversite kütüphanelerinin kurumsal yapısını korumaya yönelik olarak alınması gerektiğini ortaya koymaktadır. Ayrıca, kütüphanecilik camiasının bilgi güvenliği konusunda farkındalığının artırılması, güvenlik politikalarının ve prosedürlerinin güçlendirilmesi önemli adımlardır. Benzer şekilde, üniversite kütüphanelerinin dış paydaşları ile yapılan iş birliklerinde bilgi güvenliğinin gözetilmesi ve güvenli iletişim kanallarının kullanılması gerekmektedir. Bu çabalar, üniversite kütüphanelerinin toplumsal misyonunu ve rolünü güçlendirecek ve bilginin güvenli bir şekilde erişilebilir olmasını sağlayacaktır.

Bilgi ve İletişim Güvenliği Rehberi (2020)'nde kurumların varlık gruplarındaki bilgilerin kritiklik düzeylerine göre güvenlik tedbirleri ile ilgili seviyelerin belirlendiği, kritiklik düzeyi yüksek olan bilgi varlıklarında ileri seviye tedbirler uygulanması, düşük olanlar için ise düşük seviyede tedbirlerin uygulanması önerilmektedir. Bu itibarla çalışmanın sonuçlarına göre, üniversite kütüphanelerindeki bilgi varlıklarının kritiklik düzeyi arttıkça bilgi güvenliği ile ilgili tedbirlerin arttırılması gerektiği tespiti Rehber'de benimsenen yaklaşımla uyumlu olduğu değerlendirilmektedir.

6.8.4. Üniversite Kütüphanelerinde Algılanan Bilgi Güvenliği Tehditlerine İlişkin Tartışma

Türkiye'de üniversite kütüphanelerinde algılan en yaygın tehdit kaynağı insan ile ilgili tehditler olduğu görülmektedir. Bu tehdit grubunu sırasıyla ağ tehditleri, yazılım tehditleri, fiziksel ve çevresel tehditler, veri tehditleri ve donanım tehditleri izlemektedir. En yaygın algılanan tehditler ise sırasıyla; bilgi sistemi arızası ve bakım hatası, e-posta saldırıları, virüs, solucan, truva atı gibi kötü yazılımlar, parola saldırıları, iletişim hataları, doğal afetlere veya hava olaylarına bağlı tehditlerdir.

Ayrıca, yetkisiz yazılım kurulumu ve kullanımı, reklam ve casus yazılım tehditleri, bilgi sistemlerini hackleme, yanlış güncelleme, depolama veya yedekleme, web saldırıları, kasıtlı/kasıtsız personel suiistimalleri, binaya izinsiz giriş ve yetkisiz erişim tehditleri de görülmektedir.

Bu çalışma ile yöntem olarak benzerlik gösteren Ismail (2012)'in Malezya'da akademik kütüphanelerdeki çalışmasında, donanım güvenliği tehditlerinin akademik kütüphanelerde en yaygın güvenlik tehditleri olduğunu belirtlmiştir. Bu tehdit kaynağını sırasıyla; çalışanların suiistimalini veya insan hatalarını içeren insanla ilgili tehditler, fiziksel tehditler, yazılım tehditleri, ağ tehditleri ve veri tehditlerinin izlediği belirtilmiştir. Bu çalışmada donanım tehditleri içerisinde bakım hataları, ekipman arızası, hırsızlık, fiziksel sabotaj, vandalizm eylemlerinin; yazılım tehditlerinin içerisinde program veya sistem hataları, reklam ve kötü amaçlı yazılım kullanımı tehditlerinin; ağ güvenliği tehditleri içerisinde IP adresi sızdırma, yeniden yönlendirme mesajları, zayıf parola kullanımı, izinsiz giriş, iletim hataları; sosyal mühendislik ve kimlik avı tehditlerinin; fiziksel ve çevresel tehditler içerisinde kütüphane binasına izinsiz giriş, hırsızlık, sabotaj veya vandalizm, altyapı ve doğal afet tehditlerinin; insan ile ilgili tehditlerde ise veri girişi hataları, dikkatsizlik, çalışanların suiistimalleri tehditlerinin yaygın olarak görüldüğü sonucuna ulaşılmıştır.

Yine yöntem olarak bu çalışma ile benzerlik gösteren Nijerya'da üniversite kütüphanelerindeki bilgi sistemlerine yönelik bilgi güvenliği tehditlerinin değerlendirilmesine ilişkin bir çalışmada, donanım ile ilgili tehditlerde en yaygın olarak donanım arızası, yetkisiz yazılım kurulumları, bilgi işlem ekipmanlarının çalışmaması, iletişim ekipmanlarının arızası ve bakım hataları; yazılım ile ilgili tehditlerde yetkisiz yazılım ayarı değişikliği, parola saldırıları, yetkisiz yazılım veya programların yüklenmesi; ağ güvenliği ile ilgili tehditlerde iletim hatası, e-posta saldırısı ve oturum ele geçirme zayıf parola kullanımı; veri güvenliği tehditlerinde yanlış prosedürler, yetkisiz veri kopyalama, kullanıcı verilerinin/gizliliğinin kaybı, kullanıcı kimliğinin maskelenmemesi; fiziksel ve çevresel tehditlerde güç kaynağı kesintisi, yangın, sel, fırtına veya yıldırımdan kaynaklanan doğal afetler ve hırsızlık, sabotaj, vandalizm veya fiziksel izinsiz girişleri; insan kaynaklı güvenlik tehditleri

ise çalışanların suiistimali ve sadakatsiz personelin eylem tehditleri gibi tehditlerin algılandığı sonucuna ulaşılmıştır (Yusuf ve diğerleri, 2021).

Sumner (2009), kuruluşlar tarafından algılanan en önemli güvenlik tehditlerine ilişkin yaptığı çalışmada, ilk beş tehdit olarak kasıtlı yazılım saldırıları, teknik yazılım hataları, insan hatası, casusluk, sabotaj veya vandalizm eylemleri olduğu sonucunu elde etmiştir. Ernst ve Young (2002), kritik bilgi sistemlerinin kullanılamamasının en önemli iki nedeninin donanım veya yazılım arızası ve telekomünikasyon arızası olduğunu bildirmiştir. Hagg (2002) insan hatası, elektrik kesintisi, hizmet sağlayıcı arızası, iletişim arızası, doğal afet, donanım arızası ve yazılım arızasından kaynaklanan bilgi güvenliği tehditlerinin kuruluşlar tarafından en fazla algılanan tehditler olduğu sonucuna ulaşmıştır.

Çalışmada belirlenen tehditler ile alan yazındaki tehditler arasında genel anlamda benzerlik olduğu görülmektedir. Fakat bu tehditlerin daha çok hangi nedenlerden kaynaklandığına ilişkin sonuçlara bakıldığında, Malezya ve Nijerya'daki akademik kütüphanelerde yapılan çalışmalarda en yaygın tehdit kaynağını donanım ile ilgili tehditler olduğu, Türkiye'de üniversite kütüphanelerinde ise en yaygın tehdit kaynağının insan ile ilgili tehditler olduğu bulunmuştur. İnsan ile ilgili tehditlerin Malezya ve Nijerya'daki akademik kütüphanelerde ise ikinci sırada olduğu görülmektedir. Bu nedenle yaygınlık bakımından ülkeler arasındaki tehditlerin farklılık gösterebileceği fakat genel olarak aynı tür bilgi güvenliği tehditlerin tüm üniversite kütüphanelerinde görülebileceği sonucuna varılabilir.

6.8.5. Teknolojik Güvenlik Önlemlerine İlişkin Tartışma

Donanım güvenliği önlemlerinin Türkiye'de üniversite kütüphanelerinde genel olarak orta düzeyde uygulandığı görülmektedir. Fakat veri işleme, depolama ve iletim yeteneğine sahip tüm donanımların güncel envanterinin tutulması ve kullanım tahsislerinin yapılması; kritik bilgi içeren taşınabilir cihazların güvenli bir şekilde saklanması ve kurum dışına çıkarılmasına izin verilmemesi; kütüphane envanterindeki tüm cihaz ve taşınabilir ortamların kaybolma veya çalınma riskine karşı şifrelenmesi ve nesnelerin interneti (IoT cihazları) ile ilgili işlemlerin yetkili personelce yapılması önlemlerinin diğer donanım güvenliği önlemlerine göre daha iyi seviyelerde uygulandığı görülmüştür. Bu önlemlerin her ne kadar daha iyi

düzeylerde uygulandığı görülse de, daha fazla iyileştirmeye ihtiyacın olduğu da anlaşılmaktadır. Donanım güvenliğinde yer alan diğer önlemler arasında donanımların veri depolama ünitelerinde geri getirilmeyecek şekilde silinmesi, kullanım ömrünü tamamlamış veri depolama ünitelerinin güvenli bir şekilde imha edilmesi, yeni tedarik edilen sabit disklerin veri kurtarmaya imkân sağlamayacak şekilde biçimlendirilmesi gibi önlemlerin ise orta düzeylerde uygulandıkları söylenebilir. Bu bulgular, Türkiye'de donanım güvenliği önlemlerinin takip edildiğini ancak iyileştirme alanlarının bulunduğunu göstermektedir. Donanım güvenliği önlemlerinin düşük seviyede uygulanması, potansiyel güvenlik tehditlerinin artmasına ve bilgilerin gizliliği, bütünlüğü ve erişilebilirliği açısından risk oluşturmasına neden olabilir.

Donanım güvenliği konusunda benzer yöntemle yapılmış alanyazındaki çalışmalarda donanım güvenliği önlemlerinin İsmail (2012)'in Malezya'daki üniversite kütüphanelerinde gerçekleştirdiği bilgi güvenliği ile ilgili çalışmasında orta düzeyde ($\bar{x}$=3,02); Şişkin, (2020)'in Türkiye'de üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin korunması ile ilgili çalışmasında orta düzeyde ($\bar{x}$=3,80); Meral (2022)'in kamu kurumlarının bilgi işlem birimlerinde çalışan personel ile yaptığı bilgi güvenliği farkındalık araştırmasında orta düzeyde ($\bar{x}$=3,82) uygulandıklarına ilişkin bulguları bu çalışmanın bulguları arasında benzerlikler göstermektedir. Bu nedenle, üniversite kütüphanelerinin veya diğer kurumların donanım güvenliği konusunda daha fazla önlem alması ve güncel uygulamaları benimsemesi önemlidir.

Yazılım güvenliği önlemlerinin Türkiye'de üniversite kütüphanelerinde bazı alanlarda iyi seviyelerde uygulandığı ancak eksikliklerin bulunduğu görülmektedir. Yazılım envanteri tutma, yetkisiz yazılım kullanımını engelleme, zararlı web sitelerini tespit etme gibi önlemler büyük ölçüde iyi düzeyde uygulanmaktadır. Ancak, bazı önemli alanlarda (örneğin, yazılım ve uygulama yedeklemeleri, kullanıcı işlemlerinin gözden geçirilmesi) katılımcılar fikir sahibi olmadığını veya düşük düzeyde uygulandığını belirtmişlerdir. Bu bulgular, Türkiye'de üniversite kütüphanelerinde yazılım güvenliği önlemlerinin genel olarak yeterli düzeyde olmadığını göstermektedir. Eksiklikler, potansiyel güvenlik tehditlerinin ortaya çıkabileceği ve veri/bilgi kayıplarına neden olabilecek alanları kapsamaktadır. Örneğin, kullanıcıların zararlı yazılım ve saldırı tespit gibi koruma uygulamalarını

devre dışı bırakma yetkisine ilişkin önlemin çok iyi düzeyde uygulanmaması ve bilgi sistemlerindeki zararlı yazılımların düzenli olarak gözden geçirilmemesi gibi konular önemli eksikliklerdir. Bu bulgular, üniversite kütüphanelerinin yazılım güvenliği önlemlerini geliştirmeleri gerektiğini ortaya koymaktadır. Bu önlemler, güvenlik açıklarını azaltmak, verilerin korunmasını sağlamak ve potansiyel güvenlik ihlallerini tespit etmek için önemlidir. Daha iyi bir yazılım envanteri yönetimi, yetkili personel tarafından yapılandırma ve güncelleme kontrolü, zararlı yazılım tespit uygulamalarının etkin kullanımı gibi adımların atılması önemlidir. Ayrıca, katılımcıların fikir sahibi olmadığı veya düşük düzeyde uygulandığı belirtilen önlemlerin de gözden geçirilmesi ve gerekli iyileştirmelerin yapılması gerekmektedir. Katılımcıların yazılım güvenliklerine ilişkin fikir sahibi olmaması, kütüphanelerin yazılım güvenliği konusunda bilinçlenmeleri, güncel uygulamaları takip etmeleri, güvenlik açıklarını kapatmaya yönelik adımlar atmaları ve yazılım güvenliğine ilişkin farkındalık çalışmaları yapmaları gerektiği anlamına gelmektedir.

Yazılım güvenliği konusunda benzer yöntemle yapılmış alanyazındaki çalışmalarda; Ismail (2022)'in çalışmasında yazılım güvenliği önlemlerinin orta seviyenin biraz altında ($\bar{x}$=2,80) ve Şişkin (2020)'in çalışmasında ise orta seviyenin biraz üzerinde ($\bar{x}$=3,80) uygulandıklarına ilişkin bulgular ile bu çalışmanın bulguları arasında benzerlikler görülmüştür. Bu itibarla, üniversite kütüphanelerinin yazılım güvenliği önlemlerini daha da güçlendirmesi ve eksiklikleri gidermesi konusunda çalışmalarda bir fikir birliğinin olduğu görülmektedir. Bu çalışmalardan elde edilen bulgular kütüphanelerin bilgilerin gizliliği, bütünlüğü ve erişilebilirliği konusundaki çalışmalarını daha da artırmalarına yardımcı olacağı düşünülmektedir. Böylelikle kullanıcıların güvenli kütüphane ortamlarında çalışmalarının sağlanması ve olası güvenlik tehditlerinden korunmaları konusunda atılacak adımların onlarda kütüphanelere karşı olan güven duygusunu artıracaktır.

Ağ güvenliği önlemlerinin Türkiye'de üniversite kütüphanelerinde genel olarak iyi seviyelerde uygulandığı söylenebilir. Katılımcıların çoğunluğu, kullanıcı kimlik doğrulama, ağ ayrımı, misafir ağının izolasyonu gibi önlemlerin iyi düzeyde uygulandığını belirtmiştir. Bu, kullanıcıların güvenli bir ağ ortamında çalıştıklarını ve güvenlik açısından birçok riskin azaltıldığını göstermektedir. Ağ güvenliği, günümüzde herhangi bir kurum veya kuruluş için son derece önemlidir ve üniversite

kütüphaneleri de bu konuda istisna değildir. Elde edilen veriler, kütüphanelerin ağ güvenliği önlemlerini genel olarak ciddiye aldıklarını ve uygun adımlar attıklarını göstermektedir. Bu durum, kullanıcıların bilgilerinin korunması, izinsiz erişimlerin engellenmesi ve ağ altyapısının güvence altına alınması açısından olumlu bir tablo çizmektedir. Ancak, bazı önlemlerde katılımcıların fikir sunmadığı veya düşük oranda destek verdiği görülmektedir. Özellikle, elektronik bilgi iletiminde güvenlik kontrol gereksinimleri, kablosuz ve kablolu ağ bağlantılarının sınırlandırılması gibi önlemlere ilişkin fikir paylaşılmaması, bu alanlardaki uygulama düzeylerinin iyileştirilmesi gerektiğini göstermektedir. Ayrıca, bazı önlemlere ilişkin hiç uygulama olmadığına dair düşük oranlar da gözlemlenmiştir. Bu durum üniversite kütüphanelerinin bu ağ güvenliği alanlarında daha fazla çaba harcamaları ve ilgili önlemleri hayata geçirmeleri gerektiğini göstermektedir.

Ağ güvenliği konusunda benzer yöntemle yapılmış alanyazındaki çalışmalarda ağ güvenliği önlemlerinin Ismail (2022)'in çalışmasında orta düzeylerde ($\bar{x}$=3.10); Meral (2022)'in çalışmasında ise iyi düzeylerde ($\bar{x}$=4,01) uygulandıklarına ilişkin bulgular ile bu çalışmanın bulguları arasında benzerlikler görülmüştür. Sonuç olarak, üniversite kütüphanelerinde ağ güvenliği önlemlerinin çoğunlukla iyi düzeyde olduğu söylenebilir. Ancak, belirli alanlardaki uygulamaların geliştirilmesi ve eksikliklerin giderilmesi için daha fazla çalışma yapılması gerekmektedir. Kütüphanelerin ağ güvenliği konusunda daha fazla farkındalık çalışmaları yapmaları ve katılımcılarına bu konuda daha aktif bir şekilde bilgi paylaşmaları gerekir. Özellikle, elektronik bilgi iletimi ve kablosuz ağ bağlantıları gibi alanlarda yapılacak iyileştirmeler, ağ güvenliği önlemlerinin daha iyi hale gelmesini sağlayacaktır. Böylece kullanıcıların veri güvenliği ve ağ erişiminde daha yüksek bir koruma seviyesine sahip olmaları sağlanacak ve kütüphanelere olan güveni artıracaktır.

Veri güvenliği önlemlerinin Türkiye'de üniversite kütüphanelerinde çoğunlukla iyiye yakın düzeylerde uygulandığı görülmüştür. Ancak, bazı önlemler hakkında katılımcıların fikir sunmadığı veya düşük derecelendirme verdiği de gözlemlenmiştir. Özellikle bilgisayar ve taşınabilir ortamlarda muhafaza edilen kritik bilgilerin şifrelenmesi, bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin (T.C. numarası, doğum tarihi vb.) üyelik numarası ve şifre olarak kullanılması ve veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi

kimlik doğrulama sistemlerinin kullanılması konularındaki veri güvenliği önlemlerinin diğer önlemlere kıyasla daha alt düzeylerde uygulandığı sonucuna ulaşılmıştır. Bu alanlarda veri güvenliği önlemlerinin zayıf olduğu ve risklerin ortaya çıkabileceği söylenebilir. Özellikle, kritik bilgilerin aktarımı, veri tabanı yönetimi ve kullanıcı erişim yetkilendirmeleri gibi alanlarda iyileştirme gerektiren noktaların olduğu anlaşılmaktadır. Ayrıca, katılımcıların bazı önlemler hakkında fikir sunmadığı görülmüştür. Bu durum, ağ güvenliği ile ilgili önlemlerin üniversite kütüphanelerinde çalışan personel tarafından bilinirliğinin düşük olabileceğini veya katılımcıların ilgili konuları tam olarak anlamamış olabileceğini göstermektedir. Bu, veri güvenliği eğitim ve farkındalık programlarının önemini vurgulamaktadır. Üniversite kütüphanelerinde çalışan personelin bu önlemler hakkında daha fazla bilgi edinmeleri ve fikir sunmaları teşvik edilmelidir.

Veri güvenliği konusunda benzer yöntemle yapılmış alanyazındaki çalışmalarda veri güvenliği önlemlerinin Ismail (2022)'in çalışmasında orta düzeylerde ($\bar{x}$=3.10); Meral (2022)'in çalışmasında ise iyi düzeylerde ($\bar{x}$=4,01) uygulandıklarına ilişkin bulgular ile bu çalışmanın bulguları arasında benzerlikler görülmüştür. Sonuç olarak, üniversite kütüphanelerinde veri güvenliği önlemlerinin genel olarak iyi düzeyde uygulandığı, ancak bazı alanlarda geliştirme gereksinimlerinin olduğu görülmektedir. Veri güvenliği konusunda sürekli bir iyileştirme çabası ve katılımcıların bilinç düzeyinin artırılması, veri güvenliği risklerinin en aza indirilmesine ve hassas bilgilerin korunmasına yardımcı olacaktır.

Fiziksel ve çevresel güvenlik önlemlerinin Türkiye'de üniversite kütüphanelerinde genel olarak orta düzeylerde uygulandığı görülmüştür. Katılımcıların çoğunluğu, ana giriş ve çıkış kapılarının güvenlik birimi personeli veya elektronik sistemler aracılığıyla denetlendiğini belirtmiştir. Kritik bilgi barındıran alanların fiziksel güvenlik sınırlarının belirlendiği ve güvenlik mekanizmalarıyla iyi düzeylerde korunduğu ifade edilmiştir. Ancak, bazı önlemler açısından iyileştirme gereksinimlerin olduğu da görülmüştür. Örneğin, ziyaretçilerin giriş ve çıkışlarının kayıt altına alınması ve sadece ilgili amaçları için erişim izni verilmesi konusundaki uygulamalarda katılımcıların bir kısmı orta veya düşük derecelendirmelerde bulunmuştur. Ayrıca, ziyaretçilere yaka kısımlarında ziyaretçi kartı takma zorunluluğunun uygulanması ve kritik bilgilerin sadece yetkili kişilerle

sınırlandırılması gibi önlemlerin uygulanma düzeyinin oldukça düşük düzeylerde uygulandığı hatta uygulanmadığına yönelik katılımcı görüşlerinin diğer önlemlerin uygulanmasına göre daha belirgin olduğu görülmektedir. Bu önlemlere ilişkin kütüphanelerdeki uygulamaların düşük olmasının büyük risk oluşturduğu düşüncesinin katılımcılar tarafından net bir biçimde ifade edildiği anlaşılmaktadır. Elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerinin acil durum anahtarlarıyla kesilmesi konusundaki önlemin de iyi düzeylerde uygulanmadığına ilişkin bulgular, acil durum anahtarlarının kullanılmasına ilikin bazı üniversite kütüphanelerinin hala yetersiz olduğunu göstermektedir. Acil durum anahtarları, yangın, su baskını veya diğer acil durumlarda hızlı bir şekilde enerji ve diğer hizmetleri kesmeyi sağlamakta ve bu da potansiyel tehlikelerin önlenmesine yardımcı olumaktadır. Bu konuda katılımcıların bir fikir sahibi olmaması ve uygulanma düzeyinin düşük düzeylerde olması, üniversite kütüphanelerinde çalışan personelin görev yaptıkları kütüphanelerin altyapılarına ilişkin bilgi sahibi olmadıklarını göstermektedir. Bu durum, güvenlik önlemleri hakkında bilgi ve farkındalık eksikliğini bir kez daha göstermektedir. Kütüphane yönetimleri, kütüphanelerin fiziki yapıları hakkında daha fazla bilgilendirme yapmalı, çalışanlara ve kullanıcılara acil durum prosedürlerini ve önlemlerini anlatmalıdır.

Fiziksel ve çevresel bilgi güvenliği konusunda benzer yöntemle yapılmış alanyazındaki çalışmalarda fiziksel ve çevresel bilgi güvenliği önlemlerinin Ismail (2022)'in çalışmasında orta düzeyin altında ($\bar{x}$=2,92); Şişkin (2020)'in çalışmasında orta düzeylerde ($\bar{x}$=3,58) ve Meral (2022)'in çalışmasında ise iyi düzeylerde ($\bar{x}$=4,29) uygulandıklarına ilişkin bulgular ile bu çalışmanın bulguları arasında benzerlikler görülmüştür. Bu bulgulara dayanarak, üniversite kütüphanelerinin fiziksel ve çevresel güvenlik önlemlerinde bazı eksikliklerin olduğunu ve bu konuda dikkate alınması gereken noktaların bulunduğu söylenebilir. Daha fazla güvenlik personeli istihdam edilmesi, güvenlik kameralarının daha etkin bir şekilde kullanılması ve ziyaretçilerin kontrolü için daha sıkı önlemler alınması gibi adımların atılması önemlidir. Ayrıca, çalışanların ve kullanıcıların güvenlik önlemleri hakkında daha fazla bilgilendirilmesi ve farkındalığın artırılması da gerekmektedir. Bu şekilde, üniversite kütüphanelerinin güvenlik seviyesi yükseltilerek, kullanıcıların ve çalışanların güvenli bir ortamda hizmet almaları sağlanabilir.

Teknolojik güvenlik önlemlerinin etkinliğinin ölçülmesi, organizasyonların bilgi güvenliği yönetim sistemlerinin geliştirilmesi, siber saldırılara karşı savunma mekanizmalarının tasarlanması ve uygulanması gibi konularda alanyazında birçok araştırma bulunmaktadır (Amini ve diğerleri, 2021; Corrall ve Sriborisutsakul, 2010; Gürsel, 2019; Kurt, 2019; Nicolas-Rocca ve Burkhard, 2019; Onaran, 2019; Phelps, 2005; Vorakulpipat ve diğerleri, 2010). Bu çalışmalar, bilgi güvenliği alanında farkındalık yaratmak, en iyi uygulamaları belirlemek ve organizasyonların bilgi güvenliği risklerini azaltmalarına yardımcı olmak amacıyla yapılmış ve konuya ilişkin öneriler getirmiştir.

6.8.6. Kurumsal Güvenlik Önlemlerine İlişkin Tartışma

Bilgi güvenliği politikalarına ilişkin katılımcılardan elde edilen verilere göre Türkiye'de üniversite kütüphanelerinde bilgi güvenliği politikalarının uygulanması konusunda genel olarak iyi düzeylerde olunduğuna ilişkin bulgulara ulaşılmıştır. Örneğin, kişisel bilgilerin mahremiyetinin koruması; ağ yönetiminin güvenli biçimde işletilmesi ve fikri mülkiyet ile ilgili güvenliğin sağlanmasına yönelik belirlenen ilke ve yöntemlerin Türkiye'de üniversite kütüphanelerinde iyi düzeylerde gerçekleştirildiği belirlenmiştir. Bu, kurumsal bilgi güvenliğinin temel uygulamalarının bazı uygulama alnlarında iyi olduğunu göstermektedir. Ancak, bazı bilgi güvenliği ilke ve yöntemlerin de ise iyileştirmelere ihtiyaç olduğu anlaşılmaktadır. Örneğin, kritik bilgi ve bilgi varlıklarının kurum dışına çıkarılması ya da başka ortamlara aktarılması ile ilgili bilgi transferi ilke ve yöntemlerinin; bilgi sistemlerine kaynağı belirli hangi tür yazılımların kurulabileceğini tanımlayan ilke ve yöntemlerin; kâğıt veya elektronik ortamda bulunan kritik bilgilere yetkisiz erişimi ve kaybolması risklerini azaltan temiz masa/ekran ilke ve yöntemlerinin orta düzeylerde uygulandıkları belirlenmiştir. Bu bulgular, üniversite kütüphanelerinde bilgi transferi, yazılım ve temiz masa / ekran güvenlik uygulamaları konusunda daha iyi kontrollerin ve politikaların oluşturulması gerektiğini göstermektedir. Ayrıca, bazı katılımcıların ilgili maddeler hakkında fikirlerinin olmadığını belirttiği görülmüştür. Bu durum, kurumsal güvenlik politikalarının çalışanlar ve diğer ilgili taraflar arasında yeterince bilinmediği veya politikaların etkin bir şekilde

duyurulmadığı anlamına gelebilir. Bu nedenle, bilgi güvenliği politikalarının yaygın olarak paylaşılması ve çalışanlar arasında farkındalığın artırılması önemlidir.

Bilgi güvenliği politikaları konusunda benzer yöntemle yapılmış alanyazındaki çalışmalardan Ismail (2022)'in çalışmasında bilgi güvenliği politikalarına ilişkin ilke ve yöntemlerin uygulanma düzeylerinin orta düzeyde uygulandığı ($\bar{x}$=3.13) sonucu, bu çalışmanın bulguları ile benzerlik göstermektedir. Sonuç olarak, üniversite kütüphanelerinde bilgi güvenliği politikalarının genel olarak iyi bir seviyede olduğu ancak bazı alanlarda iyileştirme gerektiği sonucuna varılabilir. Üniversite kütüphane yönetimleri, bilgi güvenliği politikalarının duyurulması ve farkındalığın artırılması için daha fazla çaba sarf etmelidir. Ayrıca, politikaların etkin bir şekilde uygulanması ve çalışanların politikalara tam olarak uymaları konusunda gerekli önlemler alınmalıdır. Böylelikle, üniversite kütüphanelerindeki bilgi güvenliği politikalarına uyum artırılarak bilgi güvenliğinin heeflenen doğrultuda uygulanması sağlanacaktır.

Bilgi güvenliği prosedürlerine ilişkin katılımcılardan elde edilen verilere dayanarak, Türkiye'de üniversite kütüphanelerinde uygulamaların genel olarak orta düzeylerde uygulandığı sonucuna ulkaşılmıştır. Ancak, bazı katılımcıların bilgi güvenliği prosedürlerine ilişkin fikirlerinin olmadığını belirtmeleri ve bazı uygulamalara düşük değerlendirmelerde bulunmaları dikkat çekicidir. Bu durum, kütüphane yönetimlerinin bilgi güvenliği prosedürlerini çalışanlara etkin bir şekilde iletemediğini veya personelin bu konuda yeterince farkındalığa sahip olmadığını göstermektedir. Özellikle, kritik bilgilerin depolandığı ortamların kullanılması, taşınması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ilke ve yöntemlerin; bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir şekilde müdahale edilmesini amaçlayan ilke ve yöntemlerin; yıkıcı bir olayı yönetmek ve mevcut durumu korumak için gereksinim duyulan iş sürekliliği ve felaket kurtarma ilke ve yöntemlerin ve ziyaretçileri dolaşımlarını düzenleyen ilke ve yöntemlerin uygulanma düzeylerinin oldukça düşük olduğu görülmüştür. Bunlar, kütüphane yönetimlerinin kritik bilgilerin güvenliğini sağlamak, ziyaretçi ilke ve yöntemlerini belirlemek ve kullanıcı erişimini etkili bir şekilde yönetmek konusunda daha fazla çaba sarf etmeleri gerektiğini göstermektedir. Bilgi güvenliği prosedürleri kategorisinde değerlendirilen diğer uygulamalardan olan güvenli oturum açma, bilgi varlıklarına güvenli erişim, parola ve elektronik posta kullanımı ve kütüphanelerin fiziksel giriş

önlemlerine ilişkin ilke ve yöntemlerin daha iyi düzeylerde uygulandığı görülmüştür. Bu iyi düzeydeki uygulamalar, kütüphanelerin güvenli oturum açma mekanizmalarını etkin bir şekilde kullandığını, kullanıcıları tarafından sistem ve hizmetlere güvenli erişimlerinin sağlandığını, güçlü parola kullanımının olduğunu, personelin doğru ve güvenli e-posta kullandığını, güvenli alanlara sadece yetkili personele erişim izni vermek için uygun giriş kontrollerinin belirlendiğini ve bilgi güvenliği ihlalleri durumunda etkili bir şekilde müdahale edildiğini göstermektedir.

Bilgi güvenliği prosedürleri konusunda benzer yöntemle yapılmış alanyazındaki çalışmalardan Ismail (2022)'in çalışmasında bilgi güvenliği prosedürlerine ilişkin ilke ve yöntemlerin uygulanma düzeylerinin orta düzeyin altında uygulanması ($\bar{x}$=2,85), bu çalışmanın bulguları ile benzerlik göstermektedir. Sonuç itibarıyla, üniversite kütüphanelerinde bilgi güvenliği prosedürlerine ilişkin uygulamaların yeterli düzeylerde olmadığı söylenebilir. Özellikle bazı prosedürlerin ilke ve yöntemlerine ilişkin iyileştirmelerin yapılması gerektiği ortaya çıkmaktadır. Kritik bilgilerin güvenli bir şekilde yedeklenmesi, taşınması ve imha edilmesi ile ilgili faaliyetleri düzenlemek için daha güçlü önlemlerin alınması gerekmektedir. Kullanıcı erişimini yönetmek ve güvenli oturum açma mekanizmalarını etkin bir şekilde kullanmını sağlamak için belirlenenilke ve yöntemlerin uygulanmasına yönelik çalışmalrın artırılması önemlidir. Bu durum, kullanıcı kaydetme, kayıt silme, erişim izni verme ve kimlik doğrulama gibi faaliyetlerin belirlendiği kullanıcı erişim ilke ve yöntemlerinin daha iyi uygulanmasını sağlayacaktır. Kütüphane yönetimleri, kullanıcıların güvenli erişimini sağlamak için daha sıkı kontroller ve kimlik doğrulama mekanizmaları kullanmalıdır. Bilgi güvenliği ihlal olaylarına hızlı ve etkili biçimde müdahale etmek büyük önem taşımaktadır. Bu nedenle, ilgili ilke ve yöntemlerin daha etkin bir şekilde uygulanması ve yönetim sorumluluklarının net bir şekilde belirlenmesi gerekmektedir.

Kütüphaneler, güvenlik olaylarına müdahale süreçlerini iyileştirerek, zararın en aza indirilmesi ve sistemlerin hızlı biçimde eski haline dönmesini sağlamalıdır. İş sürekliliği ve felaket kurtarma ilke ve yöntemleri konusunda daha fazla önlem alınması gerekmektedir. Yıkıcı olayların yönetimi ve mevcut durumun korunması, bilgi güvenliği açısından kritik bir konudur. Kütüphane yönetimleri, iş sürekliliği planlamasını güçlendirmeli ve felaket durumlarında hızlı bir şekilde hareket

etmelidir. Bu, planlama ve faaliyetlerin belirlendiği iş sürekliliği ve felaket kurtarma ilke ve yöntemlerinin daha etkin bir şekilde uygulanmasını gerektirmektedir.

Kütüphane yönetimleri, kritik bilgilerin yedeklenmesi ve korunması, donanım ve yazılım yedeklemeleri, alternatif iletişim yöntemleri ve acil durum eylem planlarının oluşturulması gibi önlemleri alarak iş sürekliliğini sağlamalıdır. Güçlü parola kullanımı ve yönetimi standartlarının belirlendiği parola işleme ve kullanımı ilke ve yöntemlerine daha fazla önem vermelidir. Bilgi varlıklarının kapasite yönetimi de göz önünde bulundurulması gereken bir konudur. Kütüphane yönetimleri, kapasite kullanımlarını belirlenmiş sınırlar içinde tutarak verimli bir şekilde kaynakları yönetmeli ve aşırı yüklenmeyi önlemelidir. Kullanıcıların doğru ve güvenli e-posta kullanımına yönelik faaliyetlerin düzenlendiği elektronik posta ilke ve yöntemlerine daha fazla odaklanılmalıdır.

Kütüphane personeli ve kullanıcıları, güvenli parolalar kullanmayı ve düzenli olarak parolalarını güncellemeyi teşvik etmek için bilinçlendirilmelidir. Kullanıcılar, e-postalarını güvenli bir şekilde kullanmayı ve potansiyel tehditlere karşı dikkatli olmayı öğrenmelidir. Ziyaretçi kabul ilke ve yöntemlerinin uygulanması da önemlidir. Ziyaretçilerin kabulü, dolaşımları ve kütüphaneden ayrılmalarıyla ilgili faaliyetler düzenlemeli ve güvenliğe yönelik belirlenn ilke ve yöntemler uygulanmalıdır.

Bilgi güvenliği idari araç ve yöntemlerine ilişkin katılımcılardan elde edilen veriler, Türkiye'de üniversite kütüphanelerinde bilgi güvenliği idari araç ve yöntemlerine ilişkin uygulamaların genel olarak yetersiz olduğunu göstermiştir. Katılımcıların büyük bir kısmı, birçok idari uygulamalrın hiç uygulanmadığını veya kötü ve orta düzeyde uygulandığını belirtmiştir. Bu durum, üniversite kütüphanelerinini kendi kurumlarına özel bilgi güvenliği politika ve prosedürlerini tam olarak hayata geçirme konusunda zayıf olduklarını ortaya koymaktadır. Özellikle, bilgi güvenliği ihlallerinin raporlanması ve ilgili birimlere bildirilmesini düzenleyen kılavuz ve talimatların eksikliği ve bilgi güvenliği ihlallerine karşı resmi bir disiplin mekanizmasının olmaması endişe vericidir. Bunun yanı sıra, yeni veya işten ayrılacak personelin bilgi güvenliği sorumlulukları hakkında bilgilendirilmediğine ilişkin bulgular göze çarpmaktadır. Kişisel bilgilerin işlenmesi ve kullanımıyla ilgili önemli maddelerin uygulanmasına yönelik bulguların düşük düzeylerde olduğu

görünmektedir. Kişisel bilgilerin işlenmeden önce ilgili kullanıcının bilgilendirilmesini amaçlayan aydınlatma metinleri ve açık rıza yönetimi uygulamalarına yönelik uygulamaların katılımcılartarafından yetersiz bulunduğunu belirtilmiştir. Bu da kullanıcıların bilgi gizliliği ve güvenliği konusunda yeterince bilgilendirilmediğini göstermektedir. Ayrıca, bilgi güvenliği tehditlerinden korunmaya yönelik risk analizi tabanlı idari araç ve uygulamaların yetersiz olduğu gözlemlenmiştir. Katılımcıların birçoğu, bu konuda hiçbir önlem alınmadığını veya sadece orta düzeylerde önlemlerin uygulandığını ifade etmişlerdir. Bu da kütüphanelerin potansiyel tehditlere karşı yeterince hazırlıklı olmadığını göstermektedir. Son olarak, üçüncü taraf tedarikçilerle yapılan bilgi alışverişinin güvenliğini sağlamaya yönelik idari ilke ve yöntemlerin uygulanmasına yönelik çalışmaların da eksikliği dikkat çekmektedir. Katılımcıların bir kısmı, bu konuda uygulamanın olmadığını veya düşük düzeylerde uygulandığını belirtmiştir. Bu da kütüphanelerin dış kaynaklarla olan bilgi paylaşımında güvenlik açıklarına sahip olabileceğini göstermektedir.

Bilgi güvenliği idari araç ve yöntemlerinin uygulanması düzeyleri konusunda benzer yöntemle yapılmış alanyazındaki çalışmalardan Ismail (2022)'in çalışmasında bilgi güvenliği prosedürleri ile ilgili ilke ve uygulamaların orta düzeylerin altında $\bar{x}$=2,52 uygulandığı ve bu çalışmanın bulguları arasında benzerlik gösterdiği görülmektedir. Bul bulgulara göre, üniversite kütüphanelerinin bilgi güvenliği idari araç ve yöntemlerine yeterli önem verilmediği ve uygulamaların genellikle düşük düzeylerde uygulandığı söylenebilir. Bu durum, kütüphanelerin bilgi güvenliği konusunda potansiyel risklere karşı idari güvenlik meknizmaları olarak savunmasız olduğunu göstermektedir.

Bilgi güvenliği, günümüzde giderek artan bir öneme sahiptir. Kurumların ve özellikle kütüphanelerin, kullanıcıların kişisel bilgilerini koruma, bilgi güvenliği ihlallerini önleme ve güvenli bir ortam sağlama konusunda etkin önlemler alması gerekmektedir. Bu önlemler, politika ve prosedürlerin yanı sıra idari araç ve yöntemlerin doğru bir şekilde uygulanmasını gerektirir. Kütüphanelerde bilgi güvenliği politika ve prosedürlerine uyulmasının yanı sıra, idari araç ve yöntemlerin etkin bir şekilde kullanılması da önemlidir. Bu araçlar, bilgi güvenliği ihlallerinin raporlanması ve bildirilmesi, disiplin mekanizmaları, personel eğitimi, risk analizi,

üçüncü taraf tedarikçilerle yapılan sözleşmeler gibi alanlarda etkili olmaktadır. Bilgi güvenliği idari araç ve yöntemlerinin eksik veya düşük düzeyde uygulanması, kütüphanelerin bilgi güvenliği açısından risk altında olmasına ve kullanıcıların güvenini zedeleme potansiyeline sahip olmasına neden olabilir. Bu nedenle, üniversite kütüphanelerinin bilgi güvenliği idari araç ve yöntemlerine daha fazla önem vermeleri, bu araçları etkin bir şekilde uygulamaları ve çalışanlarını bilgi güvenliği konusunda eğitmeleri önemlidir. Ayrıca, bilgi güvenliği ile ilgili güncel gelişmeler takip edilerek en iyi uygulamaların benimsenmesine güncellemeler yapılmalıdır. Bilgi güvenliği idari araç ve yöntemlerinin etkin bir şekilde uygulanması, kütüphanelerin bilgi güvenliği konusunda daha sağlam bir temel oluşturmasına yardımcı olacaktır. Bu araçlar, bilgi güvenliği politikalarının etkili bir şekilde uygulanmasını sağlayacaktır.

Bilgi güvenliği farkındalık çalışmalarına ilişkin katılımcılardan elde edilen verilere göre, Türkiye'de üniversite kütüphanelerinde bilgi güvenliği farkındalık çalışmalarının genel olarak yetersiz olduğu söylenebilir. Katılımcıların çoğunluğu, bilgi güvenliği sorumluluklarını yerine getirmeyi amaçlayan eğitim çalışmalarının hiç uygulanmadığını veya kötü veya orta düzeylerde uygulandığını belirtmiştir. Özellikle, personel ve kullanıcıların bilgi güvenliği farkındalığını arttırıcı interaktif eğitim çalışmaları; bilgi güvenliği ile ilgili broşür, poster ve kitapçık gibi bilgilendirici doküman çalışmaları; kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması; kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları gibi farkındalık arttırıcı faaliyetlerin uygulanması ve kütüphanenin bilgi güvenliği politika, prosedür ve idari yöntemleri ile ilgili yapılan güncellemelerin kullanıcılara zamanında bildirilmesi ile ilgili farkındalık çalışmalarına ilişkin katılımcı görüşlerinin uygulanma düzeylerinin düşük düzeylerde gerçekleştiği belirlenmiştir. Bu durum, kütüphanelerde bilgi güvenliği farkındalığının düşük olduğunu ve kütüphane personelinin bilgi güvenliği farkındalıklarını arttırmaya yönelik daha fazla çaba sarf edilmesi gerektiğini göstermektedir. Eğitim faaliyetlerinin kapsamının belirlenmesi, personel ve kullanıcıların bilgi güvenliği konusunda interaktif eğitimler ve bilgilendirici dokümanlarla desteklenmesi önemlidir. Ayrıca, kütüphane içerisindeki dijital ortamların kullanımıyla ilgili farkındalığı arttırmak için görsel

materyallerin sunulması ve bilgi güvenliği politika ve prosedürlerindeki güncellemelerin zamanında bildirilmesi gerekmektedir.

Bilgi güvenliği idari araç ve yöntemlerinin uygulanması düzeyleri konusunda benzer yöntemle yapılmış alanyazındaki çalışmalardan Ismail (2022)'in çalışmasında $\bar{x}$=2,73 ortalama değer ile bilgi güvenliği farkındalık çalışmalarının orta düzeylerin altında uygulandığı bulgusu ile bu çalışmanın bulguları arasında benzerlik bulunmaktadır. Üniversite kütüphanelerinin bilgi güvenliği eğitim ve farkındalık çalışmalarına dahafazlaönem göstermesi gerekmektedir. Çalışanların ve kullanıcıların bilgi güvenliği konusunda bilinçlenmelerine yönelik çalışmalarla bilgi güvenliği yönetimi.güçlü bir biçimde sürdürülebilir.

Bu güvenlik kategorisine ilişkin alanyazında başka araştırma bulunmaktadır (örn. Meral, 2022; Polat, 2022; Oluwabunmi ve Madukoma, 2022; Jaeger ve Eckhardt, 2021; Amini ve dierleri, 2021; Şişkin, 2020; Kurt, H. Ö., 2019; Gürsel, 2019; Kurt S. G., 2019; Nicolas-Rocca ve Burkhard, 2019; Onaran, 2019; Çek, 2017; Güldüren, 2015; Keser ve Güldüren, 2015; Öztemiz ve Yılmaz, 2013; Ismail ve Zainab, 2013; Ismail, 2012; Fakeh ve diğerleri, 2012; Corrall ve Sriborisutsakul, 2010; Vorakulpipat, Siwamogsatham ve Pibulyarojana, 2010; Şahinaslan ve diğerleri, 2009, Phelps, 2005). Tüm çalışmalarda bilgi güvenliği ile ilgili farkındalık çalışmalarının bilgi güvenliği performansı üzerinde olumlu bir etkiye sahip olduğu belirtilmektedir. Fakat çıkan sonuçların tatmin edici olmadığı ve bilgi güvenliği farkındalık çalışmaları ile ilgili önerilerin sırlandığı görülmektedir. Örneğin, Kurt'un ilgili çalışmasında (2019) bilgi güvenliği konusunda farkındalığı artırmak için yapılabilecek uygulamalar arasında eğitici poster hazırlanması, SMS ile hatırlatıcı mesaj gönderilmesi, hatırlatıcı e-posta gönderilmesi ve yüz yüze veya online konferans düzenlenmesi gibi çalışmaların yürütülmesinin yararlı olacağı değerlendirilmiştir.

Üniversite kütüphanelerinin bilgi güvenliği konusunda daha fazla kaynak ve uzmana erişim sağlamaları önemlidir. Güncel bilgi güvenliği trendlerini takip etmek, en iyi uygulamaları belirlemek ve bunları kütüphane ortamına entegre etmek için uzman görüşlerine ihtiyaç vardır. Bu durum, kütüphane personelinin bilgi güvenliği konusunda güncel ve doğru bilgilere sahip olmasını sağlayacaktır. Ayrıca, bilgi güvenliği eğitimlerinin etkili bir şekilde planlanması ve uygulanması gerekmektedir.

Eğitimlerin içeriği, katılımcıların ihtiyaçlarına ve seviyelerine uygun olmalıdır. Eğitimlerin sıkıcı veya kuru olmaması, etkileşimli ve ilgi çekici unsurlar içermesi önemlidir. Örneğin, interaktif senaryolar, oyunlar veya simülasyonlar kullanılarak katılımcıların bilgi güvenliği konusunda pratiğe dökme imkânı bulması sağlanabilir. Bunun yanı sıra, kütüphaneler, bilgi güvenliği politika, prosedür ve idari yöntemlerini gözden geçirmeli ve güncellemelidir. Bu politikaların tüm personel ve kullanıcılara zamanında ve etkili bir şekilde iletilmesi sağlanmalıdır. Ayrıca, politika ve prosedürlerin uygulanması için gerekli kaynakların sağlanması ve denetim mekanizmalarının oluşturulması önemlidir. Bilgi güvenliği farkındalık çalışmalarının etkinliğini artırmak için teşvikler ve ödüllendirme programları da düşünülmelidir. Personel ve kullanıcıların bilgi güvenliği konusunda gösterdikleri hassasiyet ve uyum takdir edilmeli ve ödüllendirilmelidir. Bu, motivasyonu artırabilir ve katılımcıların daha aktif bir şekilde bilgi güvenliği politikalarına uymasını sağlayabilir. Sonuç olarak, üniversite kütüphanelerindeki bilgi güvenliği farkındalık çalışmalarının daha iyi düzeylere çıkarılması gerekmektedir. Kaynakların artırılması, etkili eğitimlerin düzenlenmesi, politika ve prosedürlerin güncellenmesi ve teşvik mekanizmalarının kullanılması, bilgi güvenliği farkındalık çalışmalarının etkinliğini artırabilir.

Kurumsal bilgi güvenliği uygulamalarına ilişkin diğer kurumlarda ve üniversite kütüphanelerinde yapılan benzer çalışmalardan Meral (2022)'in çalışmasında, kurumsal bilgi güvenliği uygulamalarının etkinliğine ilişkin sonuçların ise ortalama seviyenin üzerinde olduğu görülmektedir ($\bar{x}$=3,89). Polat (2022)'ın kurumsal bilgi güvenliğinin örgütsel iletişim, örgütsel bilgi paylaşımı ve kişisel bilgi güvenliği farkındalığı açısından değerlendirilmesi çalışmasında, kurumsal bilgi güvenliği ile ilgili sonuçların ortalama uygulama düzeyin üzerinde olduğu görülmüştür ($\bar{x}$=3,45). Şişkin (2020)'in çalışmasında ise kurumsal güvenlik önlemlerinin ortalama düzeyin üzerinde olduğu görüşülmüştür ($\bar{x}$=3,64). Adı geçen çalışmalar bu yönleri ile mevcut çalışmanın kurumsal güvenlik uygulamalarına yönelik elde edilen bulgularıyla benzerlik göstermektedir. Bu nedenle, kurumsal bilgi güvenliği çalışmalarının önemli bir konu olduğu söylenebilir.

7. ÜNİVERSİTE KÜTÜPHANELERİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) REHBER ÖNERİSİ

Çalışma sonucunda, bilgi güvenliği personelinin ve kurumsal bilgi güvenliği yönetim aracının üniversite kütüphanelerindeki varlıklarının bilgi güvenliği yönetiminde olumlu yönde etki eden faktörler olduğu sonucuna ulaşılmıştır. Bu iki faktöre sahip üniversite kütüphanelerinde bilgi güvenliği uygulamalrının daha iyi düzeylerde gerçekleştiği görülmüştür. Bu durum üniversite kütüphanelerinde iyi planlanmış bir kurumsal bilgi güvenliği aracının ve bu aracın işletilmesini sağlayacak sorumlu personelin önemini ortaya koymuştur. Bu itibarla çalışmadan elde edilen önemli sonuçların çıktı olarak alana kazandırılması adına bilgi güvenliği yönetim sistemi rehberi geliştirilmiş ve üniversite kütüphanelerinin kullanımına yönelik öneri olarak sunulmuştur.

Çalışmadan elde edilen bulgular genel olarak bilgi güvenliği önlemlerinin uygulanmasına ilişkin üniversite türü arasında anlamlı farklılıkların bulunmadığını ortaya koymuştur. Bu bakımdan çalışmada her iki üniversite türünü ayrı ayrı kapsayacak bir rehber oluşturma yoluna gidilmemiştir. Bu rehber, tüm ünivresite kütüphanelerinde bilgi güvenliği yönetiminin iyi düzeylerde uygulanmasına yönelik süreçleri ve uygulamaları tanımlamaktadır. Bu bakımdan rehber, üniversite kütüphaneleri bilgi güvenliği yönetim sistemi (BGYS)'nin süreçlerine ve ilgili dokümanların hazırlanmasına ilişkin yürütülecek çalışmaların standart yol haritasını sunmaktadır.

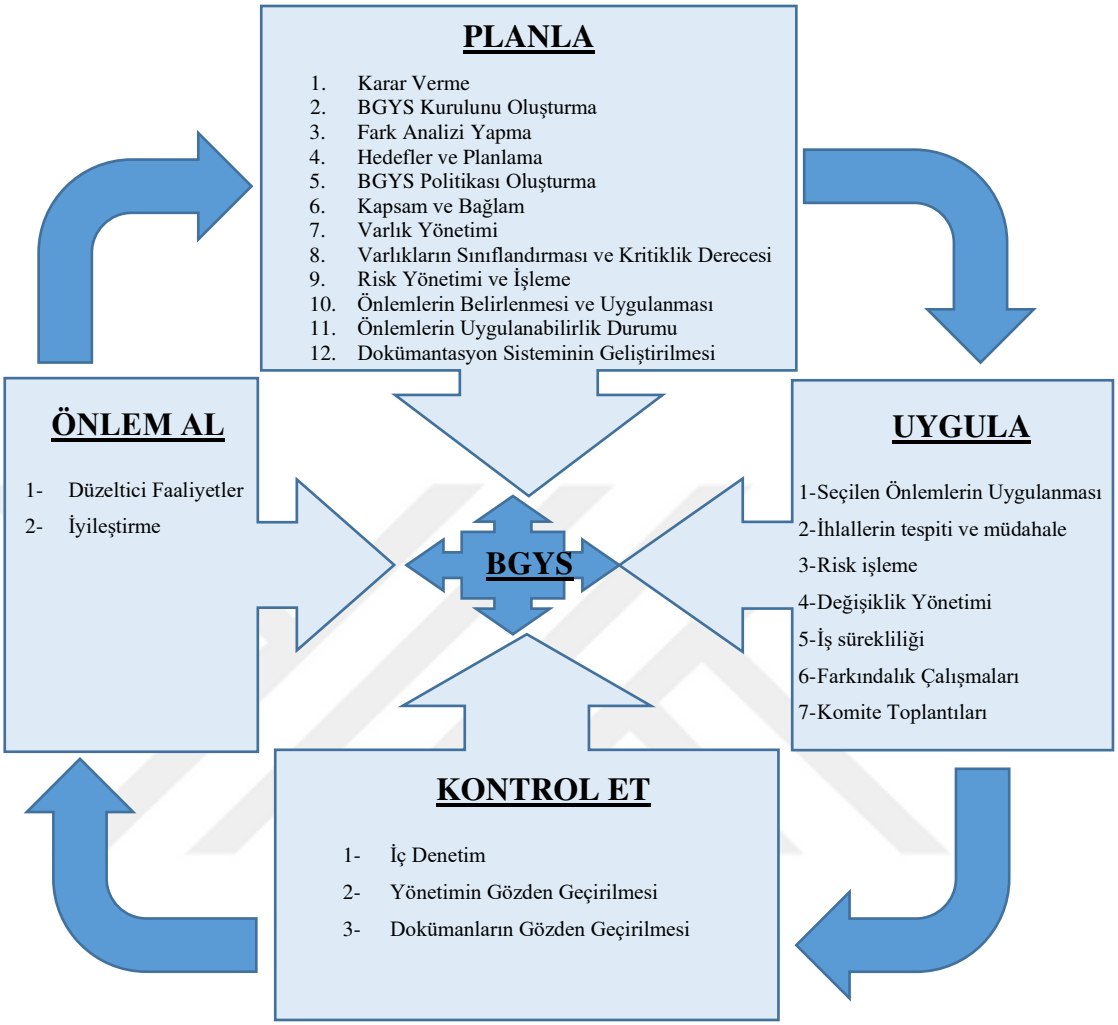
Rehber, üniversite kütüphanelerindeki bilgi güvenliği risklerinin giderilmesi, ortadan kaldırılması, azaltılması, özellikle gizliliği, bütünlüğü ve erişebilirliği ihlal edildiğinde kütüphanenin güvenliğini tehdit edebilecek veya üniversitenin kurumsal düzeninin bozulmasına neden olabilecek kritik öneme sahip bilgilerin / verilerin güvenliğinin sağlanması için minimum güvenlik önlemlerinin tanımlanması ve tanımlanan önlemlerin uygulanması için yürütülecek çalışmaların belirlenmesini amaçlamaktadır.

Bu "BGYS Rehberi" üniversite kütüphanelerine rehberlik yapması amacıyla hazırlanmış olup, rehberin uygulanması sonucu elde edilmesi beklenen birtakım hedefler şunlardır:

- Tüm üniversite kütüphanelerinde bilgi güvenliği yönetim sisteminin standartlaştırılması,
- Mükerrer çalışmalardan kaynaklanacak zaman ve maliyet kaybının önlenmesi,
- Kütüphanelerdeki varlık gruplarının belirlenerek kritiklik durumlarına göre güvenlik derecelerinin belirlenmesi ve uyumlu güvenlik önlemlerinin uygulanması,
- Güvenlik önlemleri ile ilgili süreçlere ait detayların izlenebilirliğinin sağlaması,
- Bilgi güvenliği önlemlerinin uygulanabilirliğinin denetlenmesi,
- Bilgi güvenliği önlemlerinin birbirinden bağımsız bir biçimde uygulanabilirliğini sağlayacak modüler yapının oluşturulması,
- Bilgi güvenliği önlemlerinin diğer kütüphane türlerinde de uygulanabilir yapıda olması,
- Teknik veya kurumsal gelişmelere ve ihtiyaçlara göre BGYS rehberinin sürdürülebilirliğinin sağlanması,
- BGYS rehberinin tüm iç ve dış paydaşlara hitap etmesi,
- BGYS rehber içeriğinin ulusal ve uluslararası mevzuat ve standartlara uyumlu olması,
- BGYS rehber içeriğinin, amaç ve hedefleri doğrultusunda oluşturulması,
- Kurumsal bilgi güvenliği kültürünü oluşturulması ve yaygınlaştırılması,
- Kütüphaneler arası veri paylaşımının güvenli biçimde sağlanması,
- Bilgi güvenliği sorumlularının yetkinliklerinin arttırılması,

Rehber; Planla – Uygula - Kontrol et - Önlem al (PUKÖ) ana süreçleri çerçevesinde gerçekleştirilen birtakım iş ve işlemleri kapsayan alt süreçlerden oluşmaktadır. Rehberin ana ve alt süreçlerini gösteren şema Şekil 7.1'de gösterilmektedir.

Şekil 7.1: Kütüphane bilgi güvenliği yönetim distemi PUKÖ döngüsü



7.1. Planlama Aşaması

Bu bölüm, Üniversite Kütüphaneleri BGYS'nin tasarımı ve kurulumu ile ilgili planlama sürecinde yürütülecek çalışmaları kapsamaktadır. Planlama aşaması, BGYS'nin temel bileşenlerini, prensiplerini ve çalışma şeklini ortaya koyduğundan dolayı diğer ana süreçlere daha önemlidir. Bu aşamada BGYS'nin temel omurgasını oluşturan varlık envanteri ve bilgi güvenliği risk analizi, bilgi güvenliği politikası ve uygulanabilirlik çalışmaları yapılmaktadır.

Bu ana süreç içerisinde yürütülecek çalışmalar şu biçimde sıralanmaktadır:

- BGYS'nin tasarlanmasına üst yönetim tarafından karar verilmesi,

- BGYS kurulunun oluşturulması,
- Kütüphanenin mevcut durumuna ilişkin eksiklerin belirlenmesi için fark analizinin yapılması,
- BGYS'nin hedef, planlama ve liderlik yapısının oluşturulması,
- Bilgi güvenliği politikasının yazılması,
- Kapsam ve bağlamı içeriğinin yazılması,
- BGYS kapsamı içinde değerlendirilecek bilgi varlıklarının belirlenmesi,
- Varlıkların sınıflandırılması ve kritiklik derecelerinin belirlenmesi,
- Bilgi güvenliği risklerine karşı alınacak önlem ve kontrollerin belirlenmesi,
- Uygulanabilirlik bildirgesinin hazırlanması,
- Bilgi güvenliği dokümanlarının belirlenmesi ve hazırlanması

7.1.1. Karar Verme

Kurumun üst yönetiminin ISO 27001 standartlarına uygun bir Kütüphane BGYS'nin oluşturulmasına karar ve izin verme sürecidir. Bu karar, üst yönetimin BGYS'nin kurulum sürecine gösterdiği destek açısından çok önemlidir. Üst yönetimin liderliği, BGYS çalışmalarını desteklemek ve politikalarını onaylamanın yanı sıra, BGYS'nin sürekli iyileştirilmesi ve geliştirilmesinde önemli rol oynar.

Üst yönetim, üniversitenin rektörü, rektör yardımcısı ve genel sekreteri ile üniversite senatosunda karar verme yetkisi olan kişilerdir. Üst yönetimin BGYS sürecindeki sorumlulukları şu biçimde sıralanmaktadır:

- Liderlik: BGYS sürecine dâhil ilgili tüm faaliyetlerine önderlik etmek ve süreci işlerliğini takip etmek.
- BGYS kurulunun kurulması ve desteklenmesi: Gerekli görevlendirmeler yapılır ve BGYS yöneticisi ve diğer görevlileri belirlemek.
- Dokümanların onaylanması ve yayınlanması: BGYS sürecinde belirlenen hedeflerin, planların ve bilgi güvenliği politikasının onaylanması sağlanır ve ilgili kanallarla yayımlanarak iç ve dış paydaşlara duyurmak.
- Bilgi güvenliği farkındalık çalışmalarının desteklenmesi: Kurumda bilgi güvenliği farkındalığını artırmaya yönelik çalışmalar ile tüm paydaşların bilgi güvenliği kurallarına uymasını sağlamak.

- Gerekli kaynakların sağlanması: İnsan kaynağı, finansal destek ve diğer altyapı araç ve gereçlerinin tedarikini sağlamak.
- Gözden geçirme toplantıların düzenlenmesi: BGYS süreçlerinin takip edilmesi ve başarı kriterlerinin değerlendirilmesi için periyodik olarak yönetimin gözden geçirilmesi toplantılarına liderlik yapmak.

7.1.2. BGYS Kurulunun Oluşturulması

BGYS'nin kurulması, yürütülmesi ve performansının takip edilmesi için belirli görev dağılımlarından oluşan çalışma kurulu oluşturulur. Bu kurulda görev yapacak kişilerin yetkileri ve sayıları, üniversitenin ve üniversite kütüphanesinin büyüklüğüne, yönetim sistemine, kütüphanelerin yapısına ve kütüphanelerin diğer birimler ile olan ilişkisine göre değişiklik gösterebilir.

BGYS kurulunda görev yapacak kişiler:

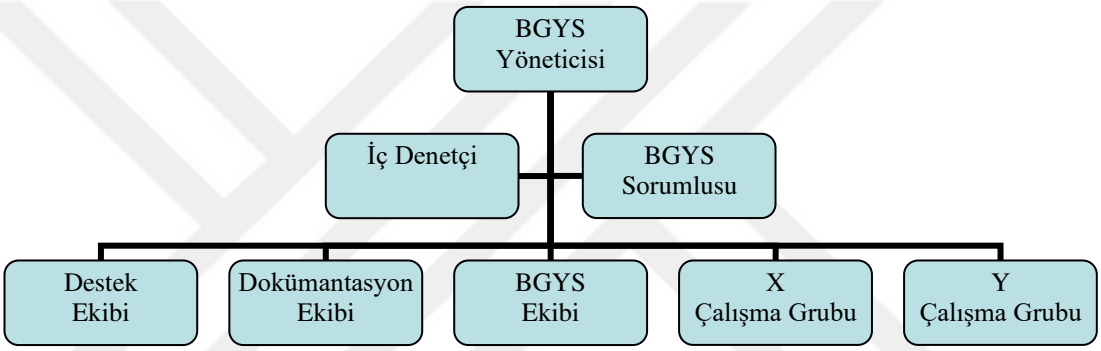
- Kütüphaneden sorumlu rektör yardımcısı
- Kütüphane biriminin en üst yetkilisi (Daire Başkanı, koordinatör vb.)
- Üniversitenin bilgi işlem biriminde yetkili bir kişi,
- Üniversitenin insan kaynakları (personel) biriminde yetkili bir kişi,
- Üniversitenin idari işleri ve strateji (personel) biriminde yetkili bir kişi,
- İş sağlığı güvenliği yetkilileri,
- Kalite biriminden yetkililer,
- Hukuk müşavirliğinden yetkili bir kişi,
- Kütüphaneciler
- Öğrenci temsilcisi
- Bilgi sistemi ve güvenliğinden sorumlu yetkililer

BGYS Kurulunun görev ve sorumlukları:

- BSYS'yi planlamak, kurmak ve işlerliğini sağlamak.
- Bilgi güvenliği kurum kültürünün oluşmasını ve gelişmesini sağlamak.
- Bilgi güvenliği risklerini belirlemek ve önlemler almak.
- Bilgi güvenliği politikalarını belirlemek ve üst yönetimin onayına sunmak.
- BGYS'nin işletimi için gerekli dokümanları hazırlamak ve güncellemeleri sağlamak.

- BGYS dokümantasyonuna uygun prosedürleri ve talimatları uygulamak.
- BGYS'nin iç denetimini yapmak ve dış denetime hazır hale getirmek.
- BGYS'yi sürekli iyileştirmek, geliştirmek ve süreçlerinin sürekliliğini sağlamak.
- Bilgi güvenliği farkındalık çalışmalarını ve eğitimlerine destek vermek.
- Bilgi güvenliği çalışma grupları ile birim sorumlularının koordinasyonu sağlamak.
- BGYS süreçlerine ilişkin diğer iş ve işlemleri yürütmek ve takip etmek.

Şekil 7.2: BGYS organizasyon şeması



7.1.3. Fark Analizi

Bu süreçte, kütüphanenin mevcut durumu itibarıyla teknolojik (donanım, yazılım, ağ, veri, fiziksel ve çevresel vb.) ve kurumsal (politikalar, prosedürler, idari araçlar, yöntemler, farkındalık çalışmaları vb.) güvenlik koşullarının, insan kaynaklarının, bilgi sitemleri, varlıkları ve dokümantasyon yönetiminin ISO/IEC 27001 bilgi güvenliği standartlarına uygun bir BGYS için yeterliliğinin ve eksiklerinin tespit edilmektedir. Bu süreç, kütüphanenin mevcut durumu ile hedeflediği bilgi güvenliği düzeyi arsındaki farkın tespiti için yapılan çalışmayı kapsamaktadır. Bu çalışma sonucunda kütüphaneye ait güvenlik eksikliklerinin değerlendirileceği bir ön rapor hazırlanır. Bu ön rapora göre Üniversite Kütüphaneleri BGYS'sini kurulması için ne kadar bir sürenin veya yatırımın yapılması ile ilgili bilgiler elde edilmiş olur. Böylelikle, BGYS'nin hedef ve planlama çalışmalarına devam edilir.

Rehber kapsamında örnek "Üniversite Kütüphaneleri Bilgi Güvenliği Fark Analizi Formu" tasarlanmış ve EK-7.28.'de verilmiştir. Bu fark analizi formu iki ana başlık

altında gruplandırılan dokuz kategoriden oluşmaktadır. Her kategori içerisinde, o kategoriye ait mevcut bilgi güvenliği yeterliliğini ölçen kontrol maddeleri bulunmaktadır.

Teknolojik güvenlik önlemeleri:

- Donanım Güvenliği Önlemleri
- Yazılım Güvenliği Önlemleri
- Ağ güvenliği Önlemeleri
- Veri Güvenliği Önlemeleri
- Fiziksel ve Çevresel Güvenlik Önlemleri

Kurumsal güvenlik önlemeleri:

- Bilgi Güvenliği Politikaları
- Bilgi Güvenliği Prosedürleri
- Bilgi Güvenliği İdari Araç ve Yöntemleri
- Bilgi Güvenliği Farkındalık Çalışmaları

Formdaki her kontrol maddesinin yeterliliğini ölçmek amacıyla "Evet", "Hayır" ve "Fikrim Yok" seçenekleri verilmektedir. Çıkan sonuçlar BGYS Kurulu tarafından değerlendirilerek çalışmanın zaman, yatırım, yöntem ve insan kaynağı gibi faktörlerine yönelik tespitler ve görüşler EK-7.31'de verilen örnek "BGYS Fark Analizi Değerlendirme Raporu"na işlenir. Bu değerlendirme raporuna göre BGYS kurma çalışmalarına devam edilir.

7.1.4. BGYS'nin Hedefleri ve Planlaması

Bu süreçte, BGYS'nin bilgi güvenliği düzeyine ve performansına yönelik hedefler belirlenir. Bu hedeflere ulaşmak için gerekli olacak kaynak ve yatırımların (donanım, yazılım, ağ ekipmanları ve diğer materyaller; insan kaynakları, dokümantasyon, eğitim, zaman ve finansal destek gibi iç kaynaklar; danışmanlar, tedarikçi hizmetleri, eğitim ve sponsorluk gibi dış kaynaklar) planlaması yapılır.

BGYS'nin temel amacı, kurumsal bilgi varlıklarının herhangi bir aksama olmadan işlerliklerinin devam ettirilmesi ve bu bilgi varlıklarına işlenen tüm bilgilerin güvenliğinin sağlanmasıdır. Bu doğrultuda BGYS'nin tipik hedefleri şu şekilde belirlenmiştir:

- Değişen teknolojilere uygun, ISO 27001'e uyumlu, ölçülebilir, raporlanabilir ve denetlenebilir bir BGYS kurmak, işletmek ve sürekli iyileştirmek
- Kurumsal itibarı ve bilgi güvenliği imajını korumak,
- Uygun iş sürekliliği planları ve sistemleri geliştirerek kritik BGYS süreçlerinin ve sistemlerinin sürekliliğini sağlamak,
- BGYS için mali ve diğer kaynakların belirlenmesini sağlamak,
- BGYS'nin zamanında tamamlanması için gerekli çalışmaları yürütmek,
- BGYS'nin teknik ve kurumsal güvenlik tedbirlerini sağlamak,
- Tüm kullanıcıları ve personelin bilgi güvenliği farkındalık seviyelerini arttırmaya yönelik eğitimler ve etkinlikler düzenlemek,
- Belirlenen kişilerin ISO/IEC 27001 bilgi güvenliği standarttı iç tetkik eğitimi almasını sağlamak,
- Başta personel bilgileri olmak üzere tüm kullanıcıların kritik bilgilerinin ihtiyaçlara uygun bir biçimde yönetilmesini ve korunmasını sağlamak,
- Üçüncü taraf olan firma ve kurumlar ile yapılan sözleşmelerde belirlenmiş bilgilerin gizliliğini ve uygunluğunu güvence altına almak,
- Yüksek kaliteli hizmet standartları için tüm bilgi sistemlerinin ve varlıklarının doğruluk/bütünlüğünü sağlamak,
- Bilgi güvenliği açıklarını ve ihlallerini etkin bir biçimde yönetmek, tekrar yaşanmaması için gerekli bilgi güvenliği aksiyonlarını geliştirmek,
- Potansiyel bilgi güvenliği tehditlerine bağlı iş kesintilerine yönelik en az bir kez tatbikat yapmak,
- Bilgi güvenliği ihlal olaylarına karşı önlemler almak ve minimum seviyeye indirmek,
- Kütüphanenin temel ve destekleyici hizmetlerini en az kesinti ile devam etmesini hatta sıfıra indirgenmesini sağlamak,
- Bilgi güvenliği risklerini minimum düzeye indirmek,
- Belirlenen hedeflerin belli bir zaman içinde yapılmasını sağlamak,

BGYS hedeflerinin nasıl başarıya ulaşılacağı ile ilgili ihtiyaçların ve yöntemin belirlendiği süreç ise zaman ve kaynak planlamasıdır. Bu süreçte şu işlemler gerçekleştirilir:

- Bilgi güvenliği ile ilgili hangi işlerin yapılacağı,

- Yapılacak her iş için hangi kaynakların gerekli olacağı,
- Kimin sorumlu olacağı,
- Ne süre zarfında tamamlanacağı ve
- Sonuçların nasıl değerlendirileceği.

Örnek "Kütüphane BGYS Planlama Çizelgesi" Tablo 7.1'de verilmiştir.

Tablo 7.1: BGYS planlama çizelgesi

BGYS Süreç Adı	Kaynak	Sorumlu	Başlangıç Tarihi	Bitiş Tarihi
Bilgisayarlara antivirüs yazılımı kurulumu	BGYS Kaynakları	Bilgi İşlem Birim Sorumlusu	…/…/202.	…/…./202.
Wireless Switch Kurulumu	BGYS Kaynakları	Bilgi İşlem Birim Sorumlusu	…/…/202.	…/…./202.
Farkındalık Eğitimi	BGYS Kaynakları		…/…/202.	…/…./202.
Kartlı/Şifrelik Kapı Kilitleri	BGYS Kaynakları	BGYS Teknik Çalışma Grubu	…/…/202.	…/…/202.
Hizmetiçi Eğitimler	BGYS Kaynakları	BGYS Eğitim Çalışma Grubu	…/…/202.	…/…/202.
BGYS Politikası Oluşturma	BGYS Kaynakları	BGYS Kurulu	…/…/202.	…/…/202.
…	…	…	…	…

7.1.5. BGYS Politikası Oluşturma

BGYS politikası, kurumların sahip olduğu kritik bilgi varlıklarının güvenliğini sağlanması ve yönetilebilmesi amacıyla ISO 9001 Kalite Yönetim Sistemi ve TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standartlarına uygun hazırlanan yazılı bir dokümandır. Bu politika, kurumun bilgi güvenliği yönetim sisteminin anayasası gibi benimsediği ve uyguladığı kurallar ve stratejik yöntemler dokümanıdır. BGYS kurulu tarafından hazırlanan bu politika, üst yönetim tarafından onaylanır.

Üst yönetimin denetimi ve onayı ile oluşturulan "Üniversite Kütüphaneleri BGYS Politikası" şu genel özellikleri mutlaka içermelidir:

- Kütüphanecinin ve üniversitenin amaçlarına uygun olmalı,
- Bilgi güvenliği hedeflerini ortaya koymalı,
- Kurum içindeki tüm çalışanlara ve kullanıcılara durdurulmalı ve iletilmeli,
- Kurum dışı ilgili taraflara duyurulmalı ve taraflarca erişilebilir olmalı,
- Sürekli iyileştirme için belirli aralıklar ile gözden geçirilmeli ve

- Yazılı bilgi olarak mevcut olmalıdır.

Rehber kapsamında örnek "Üniversite Kütüphaneleri BGYS Politikası" hazırlanmış ve EK-7.1'de verilmiştir.

7.1.6. BGYS'nin Kapsamı ve Bağlamı

Kapsam, BGYS'nin uygulama alanlarını, iş süreçlerini ve sınırlarını belirler. Bu bakımdan BGYS'nin kurlumu sürecinde en önemli süreçlerden birisi de kapsamın belirlenmesi ve yazılı bir metne dönüştürülmesidir. Kapsamın net olarak belirlenmesi, BGYS'nin denetimi açısından önem teşkil etmektedir. Çünkü denetleme bu kapsam dâhilinde gerçekleştirilmektedir.

Bağlam, BGYS'nin çerçeve yaklaşımını oluşturur. İç ve dış çevre, ekonomik koşullar, teknik ve kurumsal alt yapılar, sosyal ve diğer koşullar kurumun faaliyet gösterdiği bağlamı göstermektedir. Bağlam iç ve dış bağlam olmak üzere ikiye ayrılmaktadır. İç bağlam kurumun BGYS amaçlarını yerine getirmek üzere içinde bulunduğu ortamı, dış bağlam ise üçüncü taraflardan oluşan dış çevreyi belirtmektedir.

Rehber kapsamında, örnek BGYS kapsam ve bağlam metni hazırlanmış ve EK-7.26'da verilmiştir.

7.1.7. Varlık Yönetimi ve Envanteri

BGYS'nin temelinde bilgi varlıklarının güvenliğinin sağlanması yer almaktadır. Bilgi varlıkları; bilgi işleme ortamlarında işlenen, aktarılan ve depolanan bilgi sitemleri, bu sistemleri kullanan personel ile bilgi işleme ortamlarının barındıran fiziksel ve çevresel ortamlara ilişkin varlıkları kapsamaktadır. Rehberin düzenli planlanabilmesi ve uyunabilmesi için bu bilgi varlıklarının belirli kategoriler altında gruplandırılması ve bu kategorilerdeki bilgi varlıkları dikkate alınarak önlemlerin uygulanması gerekmektedir.

Bilgi varlığı grupları belirlenirken dikkat edilmesi gereken hususlar şunlardır:

- Tüm kütüphane bilgi varlıklarının öncelikle hangi varlık grubu ana kategorisi içerisinde yer alacağının belirlenmesi,

- Kütüphanedeki tüm bilgi varlıların mutlaka bir varlık grubu içerisinde değerlendirilmesi,
- Aynı güvenlik planlamasında değerlendirilen varlıkların mümkün olduğunca aynı bilgi varlık grubu içerisinde değerlendirilmesi,
- Farklı güvenlik seviyeleri uygulanması gereken varlıkların farklı bilgi güvenliği kategorilerinde değerlendirilecek biçimde gruplandırılması,
- Aynı güvenlik seviyesinde önlemlerin uygulanacağı değerlendirilen bilgi varlık gruplarının birleştirilerek grup sayısının mümkün olduğunca yönetilebilecek sayıda az olması.

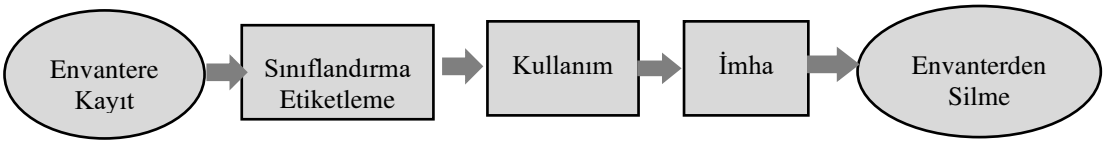
Yukarıdaki bilgilerin ışığında bu rehber kapsamında şu ana bilgi varlığı kategorileri tanımlanmıştır:

- Donanımlar
- Yazılımlar
- Ağ Ve İletişim Sistemleri
- Veri / Bilgi Ortamları
- İnsan / Personel
- Fiziksel ve Çevresel Ortamlar
- Soyut ve Kurumsal Varlıklar

Tanımlanan bu bilgi varlığı grupları içerisinde değerlendirilen bilgi varlıkları gruplarını gösteren örnek "Bilgi Varlıkları Envanter Listesi" hazırlanmış ve EK-7.32'de verilmiştir.

Varlık yönetim süreci, kütüphanenin bilgi varlıklarının belirlenip kayıt edilmesiyle başlayan bir süreçtir. Bilgi varlıklarının sınıflandırılması, etiketlenmesi ve kritiklik dereceleri belirlendikten sonra bilgi varlıklarının kullanımı sürdürülür. Belli bir zaman sonra kullanım veya ekonomik ömrünü tamamlayan bilgi varlığının imha / kullanım dışı işlemi başlatılarak o bilgi varlığının varlık yönetim süreci tamamlanmış olur. Varlık yönetiminin iş akışını gösteren süreç Şekil 7.3'te verilmiştir.

Şekil 7.3: Varlık yönetim süreci



7.1.8. Bilgi Varlıklarının Sınıflandırması ve Kritiklik Derecesinin Belirlenmesi

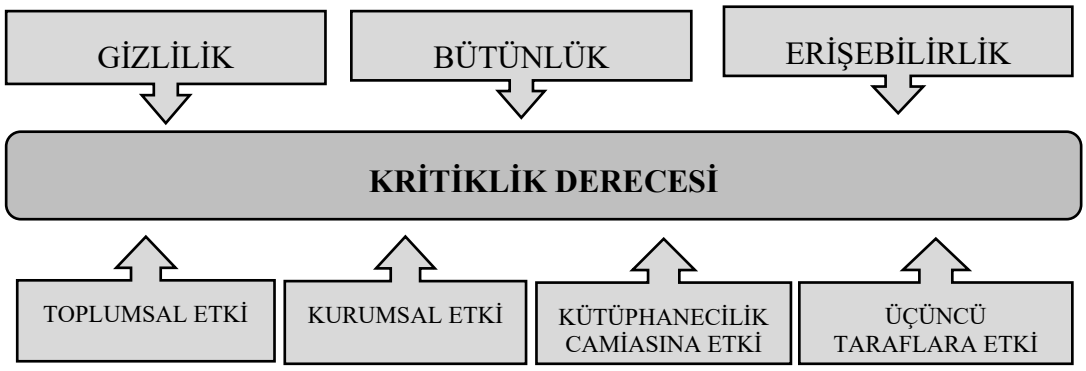
Bilgi varlıklarının envanterinin çıkarılmasından sonra bu varlıkların sınıflandırılması ve etiketlenmesi gerekmektedir. Bu süreçte bilgi varlıklarının kurumsal olarak kullanım ve kritiklik değeri ortaya konulmaktadır. Veri / bilgiler kullanım alanı hassaslığına ve kritiklik seviyesine göre sınıflandırılmaktadır. Sınıflandırma düzey sayısı ve düzeylere göre yapılacak işlemler ile verilecek izinler değişiklik gösterebilmektedir. Bilgi varlıklarının sınıflandırılmasında gizlilik belirleyici bir unsurdur. Bilgi varlıklarının gizlilik değerlerine göre sınıflandırılıp, kritiklik derecelerine göre güvenlik seviyeleri belirlenmektedir.

Bu rehber çerçevesinde kütüphane bilgi varlıkları, genel sınıflama düzeylerine göre sınıflandırılmasının uygun olacağı önerilmektedir. Bu bağlamda kütüphane bilgi varlıkları dört düzeyde sınıflandırılmaktadır: Gizli / Kritik - Hizmete Özel - Kişiye Özel - Genel.

Bilgi varlıklarının kritiklik derecesi ise, bilgi varlığına işlenen verinin gizlilik, bütünlük ve erişebilirlik unsurları bakımından değerleri ile bu bilgi varlıklarında gerçekleşebilecek güvenlik ihlallerinin etki alanları dikkate alınarak belirlenmektedir (Şekil 7.4): Düşük – Orta – Yüksek.

Rehber kapsamında bilgi varlıklarının sınıflarının ve kritiklik derecelerinin belirlendiği örnek "Bilgi Varlıklarının Sınıflandırılması ve Kritiklik Derecesi Politikası" hazırlanmış ve EK-7.2'de verilmiştir.

Şekil 7.4: Bilgi varlıklarının kritiklik derecesine etki eden unsurlar



7.1.9. Risk Yönetimi ve İşletimi

Bilgi varlıklarına karşı potansiyel bir tehlikenin varlığı veya meydana gelme olasılığı riski tanımlamaktadır. Risk yönetimi ve işleme süreci, BGYS'de önemli bir yer tutmaktadır. Bu nedenle risk yönetiminin çok iyi tanımlanması ve uygulanması gerekir. Varlık envanteri ve risk analizi çalışmaları tamamlandığında BGYS'nin önemli ilk çalışma süreçleri tamamlanmış olur.

Riskin temel bileşenleri şunlardır: Tehlike, tehdit, açıklık, zayıflık, olasılık, olumsuz etki (zarar), fırsat, etki, kontrol.

Risk yönetimi sayesinde kütüphane, sahip olduğu bilgi varlıklarına karşı olası tehlikeleri ve sonucunda oluşabilecek zararları erken aşamalarda görebilmekte ve bunlara karşı kontrol mekanizmalarımı geliştirir ve uygular.

Risk yönetimi ile;

- Hedeflerin gerçekleşme ihtimali artar.
- Proaktif bir yönetim anlayışı gelişir.
- Fırsatlar ve tehlikelerin belirlenmesi ve iyileştirilmesi sağlanır.
- İlgi yasa, mevzuat ve standartların şartlarına ve uluslararası normlara uyum sağlanır.
- Kurumsal yönetim iyileşir.
- Paydaş ve üçüncü taraf güveni ve itimadı güçlenir.
- Karar verme ve planlama ile ilgili güvenilir bir temel oluşur.
- Denetim ve kontroller iyileşir.
- Kaynakların etkili ve verimli bir biçimde kullanımını sağlanır.
- Operasyonel iş etkinliği ve verimliliği artar.
- Bilgi güvenliği performansı, motivasyonu ve aynı zamanda çevresel koruma gelişir.
- Zararın önlenmesi ve kaza yönetimi iyileşir.
- Kayıplar minimum seviyelere indirilir.
- Kurumsal bilgi güvenliği farkındalığı ve kültürü güçlenir.
- Esnek iş planlama ve organizasyonu sağlanır.

Bilgi güvenliği risk yönetiminin adımları:

- Risk belirleme: İş süreçleri ve bilgi varlıklarına ilişkin tehditler tanımlanır.
- Risk analizi (Değerlendirme): Riskler belirli bir sınıflamaya veya düşük, orta, yüksek gibi derecelendirmeye tabi tutulur.
- Risk işleme: Riskleri azaltmak, transfer etmek, kaçınmak ya da kabul etmek gibi teknik işlemler yürütülür.
- Riskleri raporlama: Yapılan risk değerlendirme çalışmasının sonuçlarının yönetime ve BGYS kuruluna sunulmasıdır. Böylelikle risklere karşı alınacak önlemler belirlenir.
- Riskleri izleme: Bilgi varlıklarının risklerinin işlenmesine ilişkin çalışmaların sürekli yapılmasını sağlanır.

Risk belirleme işlemi, bilgi güvenliği yönetim sistemine ilişkin iş süreçleri ve bilgi varlıklarının risklerini tanımlamak için yapılan çalışmayı kapsar. Bu süreçte riskleri belirlemek için bir takım teknikler kullanılır. Risklerin belirlenesinde, görüşmeler, olay envanteri, eski veriler, kütüphanecilik camiasına ait veriler ve anketler kullanılabilir. Rehber kapsamında, kütüphanelerdeki bilgi varlıklarına karşı oluşabilecek risklerin belirlenmesine yönelik örnek "Risk Belirleme Formu" hazırlanmış ve EK-7.29'da verilmiştir.

Risklerin kaydı yapıldıktan analiz edilmesi, değerlendirilmesi ve sonuç olarak risk için hangi kabul edilebilir önlemlerin alınacağı belirlenmesi işlemine geçilir. Üniversite kütüphanelerindeki bilgi varlıklarına karşı oluşabilecek tehditlerin olasılık değerlerini belirleyen model hazırlanmış ve Tablo 7.2'de verilmiştir.

Tablo 7.2: Tehdit olasılık değerleri

Risk Olasılığı	Etki Değeri	Anlamı	Sıklık
Çok Küçük	1	Risk olasılığı var fakat olay gerçekleşmez. Zararsız (etkisiz)	Hemen hemen hiç
Düşük	2	Risk olayının gerçekleşmesi çok düşük. Hafif hasar (az etkili).	Yılda bir kez
Orta	3	Risk olayı geçmişte gerçekleşmiş ve gerçekleşme ihtimali yine var. Orta dereceli zarar (hasar).	Yılda birkaç kez
Yüksek	4	Risk olayının gerçekleşme olasılığı bir ok kez gerçekleşmiş ve sıklıkla meydana gelebilir. Ciddi zararlar gelebilir.	Ayda bir kez
Çok Yüksek	5	Risk olayının gerçekleşme olasılığı çok yüksek ve neredeyse her gün gerçekleşebilir. Çok ciddi zararlar verebilir.	Her hafta / Her gün

Toplam risk değeri, bilgi varlıklarına karşı oluşabilecek tehditlerin olasılık değeri ile bilgi varlığının kritiklik derecesinin birbiri ile olan ilişki ile bulunmaktadır. Bu anlamda kullanılan tipik toplam risk formülü şu şekildedir:

Risk: "Bilgi varlığına karşı tehdidin gerçekleşme olasılığı" X "Bilgi varlığının kritiklik derecesi"

Üniversite kütüphanelerinde bir bilgi arlığına ait toplam risk değerinin belirlenmesi amacıyla rehber kapsamında hazırlanan örnek "Üniversite Kütüphanelerinde Bilgi Güvenliği Risk Matrisi" Tablo 7.3'te ve hesaplanan risk değerlerinin dereceleri ise Tablo 7.4'te verilmiştir.

Tablo 7.3: Toplam risk değerleri

Bilgi varlığı	**Tehdidin**		**Kritiklik dereceleri**				
Bilgi varlığı	**Adı**	**Olasılığı**	**Gizlilik**	**Bütünlük**	**Erişebilirlik**	**Hesaplama**	**Toplam Risk**
X donanımı	Arıza	2	3	2	1	(2*3)+(2*2)+(2*1)	12
X yazılımı	Saldırı	4	3	3	2	(4*3)+(4*3)+(3*2)	32
X verisi	Çalınma	5	3	3	3	(5*3)+(5*3)+(5*3)	75
…	…	…	…	…	…	…	…

Tablo 7.4: Risk dereceleri

Risk Değeri	**Derece**	**Eylem**	**Açıklama**
3 – 23 arası	Düşük	Kabul edilebilir risk	Aksiyon gerekmez
24- 44 arası	Orta	Dikkate değer risk	İzlenmeli ve orta vadede aksiyon alınmalı
45 – 75 arası	Yüksek	Kabul edilemez risk	Hemen aksiyon gerekir.

Tablo 7.4'tekiş bilgilere göre, "düşük" düzeydeki riskler kabul edilebilir riskler olarak kabul edilmekte olup bu düzeydeki risklerin kütüphaneye zarar vermeyeceği düşünülmektedir. "Orta" düzeydeki riskler dikkate değer riskler olup önlem alınması gerekir. "Yüksek" düzeydeki riskler ise kabul edilemez riskler olup acil önlem alınması gerekir.

Risk işleme, risklere karşı uygun önlemlerin belirlenerek risklerin azaltılması için yapılan çalışma sürecidir.

Risk işleme sürecinde şu kararlar alınabilir:

- Kabul: Riskleri farkına varıp kabul etmek.
- Azaltma: Önlemler alınarak riskleri azaltmak.
- Kaçınma: Riskli olacağı düşüncesiyle önlemi almamak veya o işi ortadan kaldırarak riskten kaçınmak.
- Transfer: Riskleri başka birimlere veya kişilere sevk etmek.

Risk işleme sürecinin iyi yönetilebilmesi için bir risk işleme planı oluşturulur. Bu risk işleme planı ile riske karşı alınacak aksiyonların nasıl ve ne zaman yapılacağı ile ilgili planlamalar yapılır. Bu rehber kapsamında hazırlanan örnek "Risk İşleme Planı" Tablo 7.24'te verilmiştir.

Tablo 7.5: Risk işleme planı

Risk	Riskin mevcut değeri	Risk İşleme metodu	Yapılacak İşlem	Sorumlu	Tarih	Hedeflenen Risk değeri
X donanımı arızası	12	KABUL	Sürecin takip edilmesi	Birim Sorumlusu	../../202.	3
X yazılım saldırısı	32	AZALTMA	Önlem al	Bilgi işlem personeli	../../202.	20
X verisi çalınması	75	AZALTMA	Önlem al	Bilgi işlem personeli	../../202.	30
…	..	..	..	..	..	..

7.1.10. Önlemlerin Belirlenmesi ve Uygulanması

Yapılan risk değerlendirmesi çalışmaları sonucunda bilgi güvenliği risklerinin azaltılması veya ortadan kaldırılması için önlemler belirlenmeli ve uygulanmalıdır. Bu rehber kapsamında hazırlanan önlemler iki ana başlı ve dokuz alt kategori altında belirlenmiştir. Bunlar:

- Teknolojik güvenlik önlemleri:
  - Donanım güvenliği önlemleri
  - Yazılım güvenliği önlemleri
  - Ağ güvenliği önlemleri
  - Veri güvenliği önlemleri

    - Fiziksel ve Çevresel güvenlik önlemleri
- Kurumsal güvenlik önlemleri:
    - Bilgi güvenliği politikaları
    - Bilgi güvenliği prosedürleri
    - Bilgi güvenliği idari araç ve mekanizmaları
    - Bilgi güvenliği farkındalık çalışmaları

Teknolojik önlemler, risk önlemede oldukça etkili önlemlerdir. Bu önlemler destekleyici, önleyici, tespit edici ve düzeltici olmak üzere çeşitli yapılarda sınıflandırılabilir:

- Destekleyici önlemler: Önlemlerin uygulanmasını sağlayan temel teknolojik sistem ve araçlardır. Örneğin kimlik tanımlama sistemleri ve yazılım güvenliği önlemleridir.
- Önleyici önlemler: Bilgi güvenliği ihlal olaylarının gerçekleşmesini önleyici önlemlerdir. Örneğin, parola, akıllı kart ve diğer erişim önlemleridir.
- Tespit edici önlemler: Bilgi güvenliği ihlal olaylarından sonra neyin, nasıl, ne zaman ve kimin tarafından yapıldığını bulmak için kullanılır.
- Düzeltici önlemler: Bilgi güvenliği sorunları tespitinden sonraki süreçte bilgi varlığını iyileştirmek için kullanılan önlemlerdir.

Kurumsal önlemler ise kurumda uygulanan politika, prosedür, standart, idari araç ve yöntemleri gibi dokümantasyon belgeleri ile düzenlenmiş kuralların uygulanmasını sağlayacak önlemlerden oluşur.

Belirlenen önleme ilişkin kontrollerin nasıl uygulanacağı, uygulama adımlarının ne olacağı ve bu önlem sürecinin ne kadar süreceğini belirleyen bir önlem uygulama planı oluşturulur. Bu uygulama planında şunlar olmalıdır:

- Belirlenen risklere karşı önlemler seçilir ve bu riskin toplam risk değerine göre önlem önerileri belirlenir.
- İhtiyaç duyulacak kaynaklar değerlendirilir.
- Önlemleri uygulamaktan sorumlu kişi veya birimler belirlenir.
- Önleme ilişkin kontrolün uygulanacağı tarih aralıkları belirlenir.

7.1.11. Önlemlerin Uygulanabilirlik Durumu

Kurumun önlem maddelerinin uygulanmasında zorunlu ve seçimli olmak üzere iki seçeneği bulunur. Zorunlu önlem maddeleri kesinlikle uygulaması gereken önlemlerdir ki bunlar ISO/IEC 27001 standartlarının ilk bölümünde yer almaktadır. Ayrıca kurumun seçimine bırakılan önlem maddeleri bulunmaktadır ki bunlar da yine aynı standardın ilgili maddelerinde belirtilmektedir. Bu nedenle kurumlar "Uygulanabilirlik Durum Çizelgesi" dokümanı kullanır ve uygulanana veya uygulanmayan önlemler / kontroller orada belirtilir. Bu belge ön denetim sırasında denetçiler tarafından istenir. Rehber kapsamında örnek bir üniversite kütüphaneleri uygulanabilirlik bildirgesi hazırlanmış olup Tablo 7.6'da verilmiştir.

Tablo 7.6: Uygulanabilirlik durum çizelgesi

BGYS Önlem Kategorisi	Önlem / Kontrol Adı	Uygulanma Durumu	Nedeni
Donanım	Donanım envanteri tutulmaktadır	Uygulanmaktadır.	BGYS için gerekli
	Kurum dışındaki teçhizat ve varlıkların güvenliği	Uygulanmamaktadır.	Kurum dışında çalışma yapılmamaktadır ve bir bilgi varlığı bulunmamaktadır.
…	…	…	…
Yazılım	Genel ağ dışında kullanıcı ağı oluşturulmuştur.	Uygulanmamaktadır.	Teknik alt yapı yetersizliği
…	…	…	…

7.1.12. BGYS Dokümantasyon Sistemi

Dokümantasyon sistemi BGYS'nin önemli bir bölümüdür. BGYS içerisinde kullanılacak dokümanlar belli bir sistematik içinde oluşturulması ve sürekli olarak güncellenmesi gerekir. Dokümantasyon belgeleri BGYS kurulunun bu konuyla ilgili olarak görevlendirdiği kişiler tarafından belirlenir ve kurumun hizmet yapısı ve bilgi varlıklarına göre hazırlanır. Dokümanlar BGYS yöneticisi tarafından kontrol edildikten sonra üst yönetimin onayına sunulur. Dokümantasyonlar sürekli olarak gözden geçirilmeli ve gerektiğinde güncellemeler yapılmalıdır. Hazırlanacak dokümanlara kılavuzluk etmek üzere özel bir prosedür olan "Doküman ve Kayıtların Kontrolü Prosedürü" oluşturulur (EK-7.16). Bu prosedürde dokümanların nasıl hazırlanacağı, yapısı ve güncelleme gibi işlemler ile dağıtımı ve saklanmasına ilişkin bütün detaylar tanımlanır.

Dokümanlar belli bir yapı ve kurullar çerçevesinde hazırlanır. Dokümanlarda genel olarak aşağıdaki bölümler yer alır:

- Amaç: Dokümanın ne amaç ile yazıldığını açıklar.
- Kapsam: Dokümandaki uygulamaların bölüm ve faaliyet alanları belirlenir.
- Sorumlular: Dokümantasyonun uygulanmasından sorumlu olanları belirtir.
- Tanımlar / Kısaltmalar: Doküman içinde kullanılan terim ve kısaltmalar hakkında bilgi verilir.
- Uygulama: Dokümana konu yapılacak iş ve işlemler belirtilir.
- İlgili dokümanlar: İşlem akışının gerçekleştirilmesinde yararlanılan ilgili dokümanlar belirtilir.
- Taahhüt/ Yürürlük: Dokümanın uygulanmasına ilişkin yönetimin taahhüttü ve onayı belirtilir.

Dokümanlar, belirli bir standart sayfa yapısı ve biçimi ile oluşturulur. Dokümanlarda olması gereken temel bilgiler şunlardır (Tablo 7.6)

- Dokümanın adı ve numarası
- Yayım tarihi
- Revizyona tarihi ve numarası
- Gizlilik Düzeyi
- Kurumun adı ve logosu
- Hazırlayan ve onaylayan bilgileri

Tablo 7.7: BGYS doküman şablonu

<table>
<tr><td rowspan="2">LOGO</td><td rowspan="2">…….. Üniversitesi
Kütüphane ve Dokümantasyon Daire Başkanlığı</td><td>Doküman No:</td><td></td></tr>
<tr><td>Yayım Tarihi</td><td></td></tr>
<tr><td rowspan="2">BGYS Dokümanı</td><td rowspan="2">…….. Politikası</td><td>Revizyon Tarihi / No:</td><td></td></tr>
<tr><td>Gizlilik Düzeyi:</td><td></td></tr>
<tr><td colspan="4">1. Amaç
2. Kapsam
3. Sorumluluklar
4. Uygulama / Politika
5. İlgili Dokümanlar
6. Yürürlük ve Onay</td></tr>
<tr><td colspan="2">Hazırlayan:</td><td colspan="2">Onaylayan</td></tr>
</table>

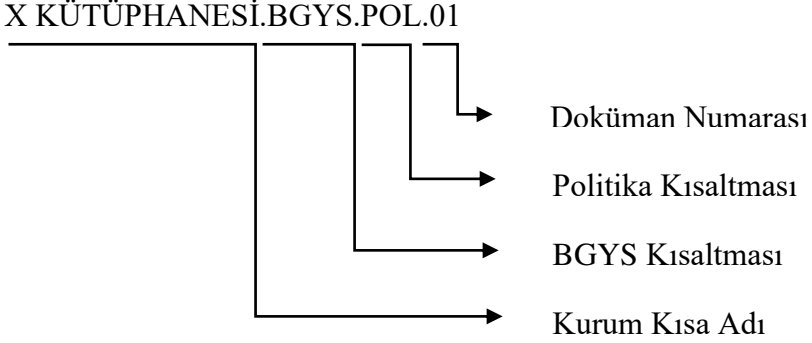
Dokümanlara ait tür kodları, doküman türünü belirten kısaltmalardır. BGYS'de standart olarak kullanılan doküman türlerinin kısaltma tür kodlarını gösteren liste Tablo 7.8'de verilmiştir.

Tablo 7.8: Doküman türlerinin kısaltılmış tür kodları listesi

Doküman Tür Kodu	Doküman adı	Doküman Tür Kodu	Doküman adı
ELK	El Kitabı	PLN	Plan
POL	Politika	ŞM	Şema
PR	Prosedür	KLZ	Kılavuz
TLM	Talimat	YNG	Yönerge
FRM	Form	YNT	Yönetmelik
PRS	Proses	SZL	Sözleşme
SRÇ	Süreç	GRV	Görev Tanımı
LST	Liste	DŞK	Dış Kaynak Dokümanı
TBL	Tablo	YD	Yardımcı Dokümanlar
ÇİZ	Çizelge	DD	Diğer Dokümanlar
RPR	Rapor	MTD	Metodoloji
KNTL	Kontrol Listesi	SNM	Sunum
KYT	Kayıt	DOK	Genel Dokümanlar
İA	İş Akışı	BEL	Genel Belgeler

Dokümantasyonlarda kullanılan numaralandırma belli bir standartta göre oluşturulur. Doküman numarasındaki alfabetik ve sayısal verilerin birer anlamı bulunur. Örnek doküman numarasına ait bilgilerin ne anlama geldiğine dair açıklamalar Şekil 7.2'de verilmiştir

Şekil 7.5: Doküman numarası örneği



Dokümanlar genellikle bilgisayar ortamındaki ofis yazılımlarının desteği ile hazırlanır. Hazırlanan dokümanlar kurum içinde üst yöneticiler tarafından

onaylandıktan sonra uygun kanallarla (kütüphane, kurum veya kalite yönetimi web sayfaları gibi) kullanıcıların erişimine sunulur. Ayrıca bu dokümanların çıktıları alınarak veya mail ortamları ile kullanıcılara iletilebilir. Bu amaçla "BGYS Doküman Dağıtım Çizelgesi (Tablo 7.9)" hazırlanabilir. Dokümanlar, kütüphanede veya kurumun arşivinde yasal süreler dâhilinde saklanır. Bu dokümanlara özel "BGYS Doküman Süreleri Çizelgesi (Tablo 7.10)" saklama sürelerini belirten listeler hazırlanabilir. Dokümanlarda yapılan değişiklikler "BGYS Dokümanları Revizyon Takip Çizelgesi (Tablo 7.11)" ile takip edilir.

Tablo 7.9: BGYS dokümanları dağıtım çizelgesi

Bölüm / Personel	**BGYS Dokümanları**				
	BGYS.POL.01	**BGYS.PRS.01**	**BGYS.FRM.01**	**BGYS.TLM.01**	**….**
Üst Yönetim	x				
BGYS Komitesi	x	x	x		x
Personel	x	x	x	x	x
Kullanıcılar	x		x	x	x
….					

Tablo 7.10: BGYS dokümanları saklama süreleri çizelgesi

Doküman No	**Doküman Adı**	**İlgili Bölüm Saklama Süresi**	**Kurum Arşiv Süresi**
BGYS.POL.01	Kütüphane BGYS Politikası	2-5 yıl	5 – 10 yıl
BGYS.DOK.01	Kütüphane BGYS Kapsam Ve Bağlam Dokümanı	2- 5 yıl	5 -10 yıl
…	…	… yıl	…yıl

Tablo 7.11: BGYS dokümanları revizyon takip çizelgesi

Doküman No	Doküman Adı	Revizyon Tarihi	Revizyon No	İşlemi yapan	Değişiklik Nedeni
BGYS.POL.01	Kütüphane BGYS Politikası	…/…/202.	01	A… K…	İlgili doküman ekleme
BGYS.DOK.01	Kütüphane BGYS Kapsam Ve Bağlam Dokümanı	…/…/202.	01	A… K…	Uygulama güncelleme
…..	…	…	…	…	…

Kütüphane BGYS'sinin düzenli ve nitelikli yürütülebilmesi için farklı amaçlarda ve yapılarda çok sayıda doküman gerekebilir. Bu rehber kapsamında genel olarak iki tür dokümantasyon yapısı kurgulanmıştır. Bunlar:

- BGYS Kurumsal Dokümanları: Bu dokümanlar bilgi güvenliğinin kurumsal yönetimine ilişkin dokümanlardır. BGYS süreçlerinin sistemli bir biçimde yürütülmesi için gerekli olan belgelerdir
- BGYS Teknik Dokümanları: Kurumun bilgi güvenliğini sağlayan teknik konuların dokümanter edildiği belgelerdir. Bilgi varlıklarının güvenliğinin sağlanmasına yönelik oluşturulan dokümanlardır.

Rehber kapsamında "BGYS Kurumsal Dokümanlar Listesi (EK-7.33)" ve "BGYS Teknik Dokümanlar Listesi (EK-7.34)" hazırlanmıştır.

7.2. Uygulama Aşaması

Bir önceki aşamada planlanan ve kurulan BGYS'nin bu aşamada gerçekleştirme sürecine geçilir. Bu aşama sırasıyla aşağıdaki işlemler işletilir:

- Seçilen Önlemlerin Uygulanması
- İhlallerin tespiti ve müdahale
- Risk işleme
- Değişiklik Yönetimi
- İş sürekliliği
- Farkındalık Çalışmaları
- Komite Toplantıları

7.2.1. Seçilen Önlemlerin Uygulanması

Bu süreçte, planlama aşmasında belirlenen önlemlerin uygulanmasına geçilir. Planlama aşmasındaki önlemlerin belirlenmesi sürecinde tanımlanan önlemlerden uygun olanlar seçilip uygulanır ya da gerekçesi gösterilerek uygulanmayabilir.

BGYS içinde gerçekleştirilen işlerin ve özellikle de bilgi teknolojileri alanında gerçekleştirilen işlemlerin bazıları veya hepsi günlük ya da belli zaman aralıkları ile kontrol edilir. Bu işlemlere ilişkin kontrol listeleri hazırlanır. Rehber kapsamında hazırlanan örnek "Önlem Kontrol Listesi" Tablo 7.0'da verilmiştir.

Tablo 7.12: Bilgi güvenliği önlem kontrol listesi

Kontrol Grubu	Kontrol zaman arlığı (gün/hafta/ay)															
Donanım Önlemleri	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	…
…	x															
…	x															

7.2.2. İhlal Olaylarının Tespiti ve Müdahale

Bilgi güvenliği ihlali bilgi varlıkları üzerinde istenmeyen ve beklenmeyen olayı ifade eder. Bir kullanıcının bilgisayarını kilitlemeden masasından ayrılması, izinsiz bir erişim ve kopyalama işlemi gibi bilgi varlıklarına veya işlenen veriye zarar veren olaylar bilgi güvenliği ihlali olarak adlandırılır.

Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir biçimde karşılık verilmesini sağlamak için iyi bir kurumsal sorumluluk yönetimi oluşturulur. İhlal olaylarına karşı gerçekleştirilecek işlemler şu aşamalar ile sağlanır:

- İhlal olaylarının tespiti ve bildirimi: Bu süreçte tespit edilen ihlal olayı ilgili birimlere (bilgi işlem vb.) veya yetkililere (birim yöneticileri, BGYS yöneticileri vb.) doğrudan ya da e-posta, telefon gibi iletişim araçları ile bildirilir. Güvenlik ihlal olayının bildiriminde "İhlal Olayı Tespit/Bildirim Formu (EK-7,35)" doldurulur
- İhlal olayının değerlendirilmesi: BGYS yöneticisi ve kurulu tarafından yapılarak ihlal olayına karşı yapılacak işlemler belirlenir.
- İhlal Olayına Müdahale: İhlal olayının kaynağının veya sorumlularının bulunması, gerekli yaptırım işlemlerinin uygulanması için olayın yasal olarak ilgili birimlere bildirilmesi ve sonuçlandırılması şeklinde gerçekleşir.

7.2.3. Risk işleme

Risk işleme, risklere karşı uygu önlemleri almak ve riskleri azaltmak için yapılır. BGYS'nin planlama aşması altında yürütülen risk yönetimi ve işletimi sürecinde takip edilen işlemler yürütülür. Bu süreçte, BGYS dokümantasyon sürecinde belirlenen risk işleme ile ilgili dokümanların kullanımı önemlidir.

7.2.4. Değişiklik Yönetimi

Değişiklik, bilgi teknolojiler üzerinde (donanı, yazılım, alt yapı vb.) yapılan ayarlamalardır. Herhangi bir bilgi sisteminde veya varlığında değişiklik işlemi gerçekleştirmeden önce bu değişiklikten etkilenecek tüm sistem, uygulamalar ve iş süreçleri belirlenir, kayıt altına alınır ve değişiklik yapacak personelin veya üçüncü

tarafın değişiklik iş yetki düzeyleri belirlenir. Tedarikçi firma tarafından yapılacak değişiklikler için test, güvenlik ve iş sürekliliği garantisi alınır.

7.2.5. İş sürekliliği

İş sürekli, BGYS içerisinde yürütülen tüm iş süreçlerinin iş sürekliliğinin sağlanması ile ilgili önlemlerin belirlendiği ve kontrol edildiği süreçtir. Bu süreçte, iş sürekliliği planları sürekli olarak kontrol edilir. Bilgi güvenliği kapsamında yürütülen tüm iş süreçleri takip edilir. İş sürekliliği politika ve prosedürlerinde belirlenen uygulamalara dikkat edilir.

7.2.6. Farkındalık Çalışmaları

BGYS, kurumda bilgi güvenliği sağlamayı amaçlar. Bunun en önemli şartı bilgi güvenliğinin bir kurum kültürü olmasının sağlanmasıdır. Bilgi güvenliğinin kurum kültürü olarak gelişmesi için BGYS içinde yapılacak önemli süreçlerden biri de çalışanlara, kullanıcılara ve üçüncü taraflara bilgi güvenliği bilincini ve farkındalığını attırıcı eğitim ve çalışmaların düzenlenmesidir. Bilgi güvenliği farkındalık çalışmalarının düzenli olarak yapılması ve bu çalışmaların etkisinin incelenmesi gerekir. Farkındalık eğitimlerinde genel olarak bilgi güvenliğinin temelleri, tehditleri ve önlemleri üzerinde durulur. Farkındalık çalışmaları ile ilgili BGYS içinde kuruma özel politikalar ve temel prosedürler tanımlanır.

7.2.7. Komite Toplantıları

BGYS kurulu, düzenli olarak toplanarak BGYS'nin işleyişi üzerinde değerlendirme toplantıları yapılır. Bu toplantılarda alınan kararlar "toplantı tutanağı" ile kayıt altına alınarak sonraki toplantılarda bu kararların gerçekleştirme durumu üzerinde değerlendirmeler yapılır ve gerekirse farklı kararlar da alınır. Böylelikle BGYS'nin düzenli olarak çalışmasının koordinesi sağlanır.

7.3. Kontrol Etme Aşaması

BGYS kurulduktan sonra işletilir ve işletilen tüm süreçlerin de düzenli olarak kontrol edilmesi gerekir. Kontrol aşamasının en temel işlemleri denetim ve izlemedir. Denetim işleminde BGYS süreçleri kontrol edilir ve değerlendirilir. İzleme süreci

ise, BGYS işlemlerinin çeşitli izleme ve değerlendirme yöntemleri ile takip edilmesidir. Bu aşamada gerçekleştirilecek temel süreçler şunlardır:

- İç Denetim
- Yönetimin Gözden Geçirilmesi
- İzleme, Ölçme, Analiz ve Değerlendirme
- Dokümanların Gözden Geçirilmesi

7.3.1. İç Denetim

BGYS'nin bilgi güvenliği politikalarının, prosedürlerinin ve uygulamalarının kontrol edildiği süreçtir. Bu süreç, bilgi güvenliği önlem ve uygulamalarının kontrol edilmesi, kurum içinde bütünlüğünün sağlanması ve tüm ilgililerinin bilgi güvenliği farkındalığının kontrolünün yapılması işlemlerini kapsar.

BGYS'nin amaç ve hedeflerine uygun olarak çalışıp çalışmadığının tarafsız yetkililer tarafından saha uygulamaları, beyanlar ve dokümanlar ile denetlenmesi sürecidir. Denetim daha önceden belirlenen iç tetkik soruları ile gerçekleşir. Bu süreçte, BGYS dokümanları ve uygulamaları incelenir, çalışanların ve kullanıcıların bilgi güvenliği farkındalıkları değerlendirilir, BGYS işlemlerinin ilgili prosedürlere uygunluğu belirlenir. İç denetim sonucunda tespit edilen uygunsuzluklar raporlanır ve bunlar düzeltilerek dış denetime hazır olunur.

- İç denetim ile ulaşılmak istenen hedefler:
- BGYS'nin ISO/IEC 27001 standartlarına uygunluğunu incelemek.
- BGYS'nin düzgün çalışıp çalışmadığını kontrol etmek.
- BGYS'nin etkinliğini değerlendirmek.
- BGYS'nin sürekli iyileştirilmesine yönelik durumları tespit etmek.
- Üst ve BGYS yönetiminin bilgilendirilmesini sağlamak.
- BGYS'nin yasal mevzuata uygunluğunu belirlemek.
- Üçüncü taraf ve kullanıcıların gereksinimlerinin yerine getirilmesini belirlemek.
- Kuruluşa özgü gereksinimlerin karşılanıp karşılanmadığını belirlemek.

İç denetim sürecinde kullanılan temel dokümanlar bulunur, bunlar Tablo 7.13'de verilmiştir.

Tablo 7.13: İç denetim dokümanları

Doküman No:	Doküman Adı
BGYS.PRS.07	İç Tetkik Prosedürü (EK-7.20)
BGYS.LST.03	İç Tetkik Soru Listesi (EK-7.30)
BGYS.PLN.01	İç Tetkik Planı
BGYS.RPR.02	İç Tetkik Raporu
BGYS.FRM.08	Uygunsuzluk Tespit/Bildirim Formu (EK-7.36)
BG.DD.11	Tetkik Açıklık Raporu
BG.DD.06	Yıllık Denetim Raporu

İç denetim soruları açık ve net olmalıdır. Mümkünse açık uçlu sorular tercih edilmeli, kapalı uçlu sorular (evet/hayır cevaplı) teyit amaçlı sorulmalıdır. İç denetim soru listeleri kuruma uygun biçimde belli alanlara (bölümlere) ayrılabilir:

- Tüm birimler için ortak soru listesi
- Teknik güvenlik önlemleri için soru listesi
- Kurumsal güvenlik önlemleri için soru listesi

İç denetim işleminin ne zaman ve hangi tetkikçi tarafından denetleneceği ile ilgili bilgileri gösteren önceden bir çizelge hazırlanıp bu çizelge denetim yapılacak ilgili birimlere veya sorumlulara bildirilir. Rehber kapsamında hazırlanan örnek "İç Denetim Planı" Tablo 7.14'te verilmiştir.

Tablo 7.14: İç denetim planı

Denetim Yapılacak Birim	Yönetici/ Birim Sorumlusu	Tarih	Saat	İç Denetimci
Açılış Toplantısı	Yöneticiler/birim sorumluları	../../202.	08.30	…
Kullanıcı Hizmetleri Birimi	…	../../202.	09.00	…
Teknik Hizmetler Birimi	…	../../202.	10.00	…
İdari Hizmetler Birimi	…	../../202.	11.00	…
…	…	…	…	…
Kapanış Toplantısı	Yöneticiler/birim sorumluları	../../202.	…	…

İç denetim işlemi, tüm denetim işlemlerinde olduğu gibi bir açılış toplantısı ile başlar. Toplantıda kurum yetkilileri, BGYS Kurulu ve denetimciler bulunur. Bu toplantıda yapılacak denetim hakkında bilgi, denetimin kapsam ve amacı, denetçiler hakkında bilgi, denetim işleminde kullanılacak yöntemler, denetimin yapılacağı alanlar, denetim sırasında personelden beklentiler ve ara verme süreleri ile kapanış zamanı belirlenir. Tüm bunlar bir tutanak ile kayıt altına alınır.

Denetim işlemi, saha denetimi, personel ile görüşme ve dokümanları inceleme yöntemleriyle yürütülür. Görüşmeler, BGYS işlemlerinden sorumlu uygun çalışanlar ile yapılır. Görüşme sırasında daha önceden hazırlanmış soru listesi kullanılır. Görüşme sırasında karşı tarafa bilgi verilerek ayrı notlar da tutulabilir. Görüşme sonunda elde edilen bulgular özetlenmeli ve görüşme yapılan kişi ile birlikte gözden geçirilmelidir. Görüşmeler sırasında "Sor-Dinle-Gör" prensibinde bir yaklaşım kullanılması uygundur. Bu yaklaşıma göre denetçi karşısındaki kişiye sorular sorar, uygun yanıtları bekler ve gerektiğinde bu yanıtını destekleyici kanıtları görmek ister. Böylelikle denetim işlemi nesnel ve objektif kanıtlar ile desteklenir. Bu nesnel kanıtlar, belgeler, dokümanlar, donanımlar, yazılımlar ve diğer teknolojik sistemler, ekran görüntüsü gibi elektronik kanıtlar ve dosyalardan oluşabilir. Dokümanların incelenmesinde ise dokümanların özellikle politika ve prosedürlere uygunlukları kontrol edilir. Görüşme ve diğer denetim yöntemleri sürecinde denetçi elde ettiği bulgulara ilişkin bir takım kısa değerlendirme notları alır bunlar şu biçimde olabilir:

- Uygulanabilir değildir
- Uygulanamamaktadır. Majör uygunsuzluk var.
- Uygun değildir. Eksiktir. Minör uygunsuzluk var.
- Uygulanmaktadır ve geliştirilmelidir. Orta düzey uygulama var.
- Uygulanmaktadır ve dokümantasyonu da yapılmıştır. İyi düzey uygulama var.

Denetim sonucunda tespit edilen uygunsuzluklar bir "İç Denetim Uygunsuzluk Tespit/Bildirim Formu" (EK-7.36) ile kayıt altına alınır ve BGYS kuruluna ve yönetime sunulur. Uygunsuzluklar belirli kriterlere göre belirlenir. Denetim sürecinde bulunan uygunsuzluklar / bulgular "majör, minör ve gözlem" olmak üzere belirtilir. Uygunsuzluk türlerine ilişkin bilgiler Tablo 7.15'te verilmiştir.

Tablo 7.15: Uygunsuzluk türleri

Uygunsuzluk Türü	Açıklama	Uygunsuzluk örneği
Majör	Büyük uygunsuzluktur. BGYS sürecinin veya işleminin herhangi bir maddesinin tamamen uygulanmadığı durumlarda oluşur. Sistematik bir eksikliği işaret eder. Sistemi doğrudan etkileyen bir uygulamanın olmaması ya da uygulanmaması anlamına gelir.	• Bilgi güvenliği politikası yok • Kullanıcı şifreleri gizli değil • Vb.
Minör	Küçük uygunsuzluktur. BGYS sürecinin veya işleminin herhangi bir maddesinin eksik uygulandığı veya yapılan uygulamaların yazılan dokümandan farklı yapılmasıdır.	• Bilgi güvenliği politikası hazırlanmış fakat duyurulmamış • Ziyaretçi ve kullanıcılar için farklı ağların kullanılmaması.
Gözlem	BGYS sürecinin veya işleminin uygulandığı ve "geliştirilmeli" şeklinde önerilerin yapıldığı gözlem notlarını belirtir.	• Bilgi güvenliği politikası hazırlanmış, duyurulmuş, uygulanmış fakat denetçi bu politikanın uygun yerlere de asılmasını öneriyor.

Denetim çalışmaları sonucunda bulgulara ilişkin bir rapor hazırlanmadan önce aynı açılış toplantısında olduğu gibi denetim ekibi yöneticilerle kapanış toplantısı yapar. Denetim sırasında sistemin çalışması ile ilgili tespit edilen uygunsuzluk tespit/bildirim formuna açıklama yapılarak işlenir ve yöneticilere verilir. Kendilerinden belli bir süre içerisinde bu uygunsuzlukların düzeltilmesi için bir "Aksiyon Planı" hazırlamalarını ve yapılan işlemlerin dokümanter edilmesi istenir.

İç denetim raporunda tetkik yapılan tarih ve birim bilgileri, açılış ve kapanış toplantısına katılların isimleri, tespit edilen uygunsuzluk sonuçları ve denetim sonucu yapılan değerlendirmelere yer verilir.

7.3.2. Yönetimin Gözden Geçirilmesi

Yönetimin gözden geçirilmesi süreci, belli dönemlerde BGYS çalışmalarının değerlendirildiği toplantılardan oluşur. Bu toplantılarda üst yönetim, BGYS kurulu, birim yöneticileri ve diğer personel yer alır. Bu toplantılar BGYS yöneticisinin sorumluluğunda gerçekleşir. Genellikle gündemdeki konular açıklanır ve katılımcıların değerlendirmeleri istenir. Belli bir gündem temelinde BGYS çalışmalarının genel olarak incelendiği ve değerlendirildiği bu toplantılarda gündem maddelerine ilişkin kararlar alınır.

Yönetimin gözden geçirme toplantılarında genellikle şu konular gözden geçirilmektedir:

- BGYS politikası
- Risk yönetim metodolojisi
- Risk işleme planları
- Değerleri düşürülen riskler
- Güncel risk raporu
- Kabul edilebilir risk düzeyleri
- Bilgi güvenliği ihlal olayları
- İş sürekliliği stratejisi
- Bilgi güvenliği farkındalık çalışmaları
- İç denetim raporları
- Varlık envanteri, varlıkların sahipliği ve varlıklara erişim hakları
- Performans izleme ve ölçme sonuçları
- Üçüncü taraf ve kullanıcı geri bildirimleri
- Donanımların kapasiteleri ve geleceğe dönük planlamaları
- Bilgi yedekleme ortamlarını ve donanımları
- Gizlilik sözleşmeleri
- Kaynaklar ve bütçe

7.3.3. Dokümanların Gözden Geçirilmesi

Dokümantasyon, BGYS için önemlidir. BGYS'nin sağlıklı ve verimli çalışabilmesi için çok sayıda doküman oluşturulur ya da iş süreçlerinin yerine getirilmesinde referans olarak kullanılır. Bu nedenle dokümanların belli süreler içerisinde gözden geçirilmesi ve günün şartlarına uygun bir biçimde güncellenmesi gerekir. Dokümanların gözden geçirilmesini gerektiren birçok durum vardır. Bunlardan bir kısmı şu şekilde sıralanmaktadır:

- Dokümanlardaki hataların bulunması ve giderilmesi
- Dokümanların yeni teknoloji ve yapılara uygun biçimde güncellenmesi
- Uygunsuzluklarının giderilmesi
- Personel, kullanıcı ve üçüncü taraflardan gelen geri bildirimlerin değerlendirilmesi

7.4. Önlem Alma Aşaması

Bu aşamada, BGYS süreçlerinde tespit edilen aksaklıklar giderilmeye ve iyileştirilmeye çalışılır. Bu süreç, BGYS rehberindeki son aşamadır. Diğer bir ifadeyle planlanan, uygulanan ve kontrol edilen BGYS'nin tüm süreçlerinde tespit edilen olumsuzlukların düzeltilmeye ve iyileştirilmeye çalışıldığı son aşamadır. Bu aşama kendi içerisinde iki alt süreçten oluşmaktadır. Bunlar; düzeltici faaliyetler ve iyileştirmedir.

7.4.1. Düzeltici Faaliyetler

Bu süreçte BGYS süreçlerinde tespit edilen olumsuzlukların giderilmesi için yapılan düzeltme çalışmalarını içerir. Düzeltici faaliyetler genelde şu iş sıralamasına göre gerçekleştirilir. Öncelikle düzeltici faaliyetin açıklaması yapılır. Daha sonra bu faaliyetin uygulanmasına geçilir. Son olarak ise düzeltici faaliyet BGYS yöneticisi tarafından kontrol edilir ve tamamlandığını teyit ettikten sonra bu faaliyete son verilir.

Düzeltici faaliyetler, BGYS süreçlerinde ISO/IEC 27001 standardına, ilgili yasalara, kullanıcı ve üçüncü taraf gereksinimlerine uygunsuzluk tespit edilmesiyle başlatılır. Tespite ilişkin öncelikle "Düzeltici Faaliyet Talep Formu" (EK-7.37) düzenlenir.

Düzeltici faaliyetlerin başlatılmasına neden olan olumsuzlukların başında şunlar gelmektedir:

- İç ve dış denetinde raporlanan uygunsuzluklar,
- Açıklık testlerinde tespit edilen bilgi güvenliği zafiyetleri ve tehditleri,
- Bilgi güvenliği ihlal olayları,
- Değişen mevzuat ve yasalara uyum sağlamak için gerekli düzeltmeler,
- Değişen kullanıcı ve üçüncü taraf gereksinimleri,
- Yönetimi gözden geçirme toplantılarında alınan karar sonuçları,
- Öneriler ve diğer istekler.

Düzeltici fatalitelerin temelinde sorunun giderilmesi bulunur. Bu nedenle sorun veya olumsuz durum ile ilgili "Kök Neden Analizi" yapılır. Kök neden analizinde soruna neden olan durumlar tespit edilir ve sorunun çözümü için yapılacak işlemler belirlenir ve düzeltme işlemi yapılır. Kök nedenlerin bulunması sorunun giderilmesi için önemlidir.

Düzeltici faaliyet tamamlandıktan sonra BGYS yöneticisi ve işin uzmanı son kontrolleri yar ve düzeltme işleminin tamamlanmasından emin olduktan sonra faaliyete son verir. Düzeltme işlemi kapatıldıktan sonra BGYS yönetici düzeltme işini talep eden birime veya ilgiliye düzeltme faaliyetinin yapıldığını bildirir.

Düzeltici faaliyetlerin yapılmasını kontrol etmek amacıyla "BGYS Düzeltici Faaliyet Prosedürü" oluşturulur (EK-7.17). Bu prosedür içerisinde, düzeltici faaliyetin

açılmasına ilişkin bilgiler (düzeltme isteyen birim veya ilgili, düzeltme işleminin adı vb.), düzeltici faaliyetin uygulanması ile ilgili bilgiler (yöntemler, çözüm vb.) ve düzeltici faaliyetin kapatılması ile ilgili işlemler yer alır.

7.4.2. İyileştirme

BGYS'nin uygunluğu, etkinliği ve doğruluğu sürekli olarak gözden geçirilerek iyileştirilmesi gerekir. Diğer bir ifadeye BGYS çalışmalarının düzgün ve nitelikli bir biçimde yürümesi için BGYS'nin sürekli iyileştirilmesi gerekir. Sürekli iyileştirme için gerçekleştirilen önemli işlemler şunlardır:

- İç ve dış denetimler
- Yönetimi gözden geçirme toplantıları
- Bilgi güvenliği açıklık / zafiyet testleri
- Ölçme, izleme ve değerlendirme çalışmaları
- Risk yönetimi çalışmaları
- İç ve dış paydaş gereksinimleri

"BGYS Rehberi"nin sağlıklı bir şekilde yürütülebilmesi amacıyla rehbere ek olarak hazırlanan dokümanlar çalışmanın "Ekler" bölümünde sunulmaktadır:

- Bilgi Güvenliği Yönetim Sistemi Politikası (EK-7.1)
- Bilgi Varlıklarının Sınıflandırılması ve Kritiklik Derecesi Politikası (EK-7.2)
- Bilgi Transferi Politikası (EK-7.3)
- Fikri Mülkiyet Politikası (EK-7.4)
- Fiziksel ve Çevresel Güvenlik Politikası (EK-7.5)
- Güvenli Sistem Mühendisliği Politikası (EK-7.6)
- İnsan Kaynakları Güvenliği Politikası (EK-7.7)
- İzleme, Ölçme, Analiz ve Değerlendirme Politikası (EK-7.8)
- Sürekli İyileştirme Politikası (EK-7.9)
- Tedarikçi ve Üçüncü Taraf Güvenliği Politikası (EK-7.10:
- Temiz Masaüstü ve Temiz Ekran Politikası (EK-7.11)
- Uyum Politikası (EK-7.12)
- Varlıkların Kabul Edilebilir Kullanımı Politikası (EK-7.13)
- Ziyaretçi Kabul Politikası (EK-7.14)
- Bilgi Sınıflandırma ve Etiketleme Prosedürü (EK-7.15)

- BGYS Doküman Kayıtların Kontrolü Prosedürü (EK-7.16)
- BGYS Düzeltici Faaliyet Prosedürü (EK-7.17)
- Eğitim / Farkındalık Eğitimi Prosedürü (EK-7.18)
- Fikri Mülkiyet Haklarının Korunması Prosedürü (EK-7.19)
- İç Denetim Prosedürü (EK-7.20)
- İhlal Olayları Yönetim Prosedürü (EK-7.21)
- İletişim Prosedürü (EK-7.22)
- İzleme, Ölçme, Analiz ve Değerlendirme Prosedürü (EK-7.23)
- Varlık Yönetimi Prosedürü (EK-7.24)
- Yönetimin Gözden Geçirme (YGG) Prosedürü (EK-7.25)
- BGYS Dokümanının Kapsam ve Bağlam Dokümanı (EK-7.26)
- Gizlilik Sözleşmesi Formu (EK-7.27)
- BGYS Fark Analizi Formu (EK-7.28)
- Bilgi Güvenliği Risk Belirleme Formu (EK-7.29)
- İç Denetim Ortak Soru Formu (EK-7.30)
- BGYS Fark Analizi Değerlendirme Raporu (EK-7.31)
- Bilgi Varlıkları Envanter Listesi (EK-7.32)
- BGYS Kurumsal Dokümanlar Listesi (EK-7.33)
- BGYS Teknik Dokümanlar Listesi (EK-7.34)
- İhlal Olayı Tespit / Bildirim Formu (EK-7.35)
- İç Denetim Uygunsuzluk Tespit / Bildirim Formu (EK-7.36)
- Düzeltici Faaliyet Talep Formu (EK-7.37)
- BGYS Risk Bildirim ve Talep Formu (EK-7.38)
- Değişiklik İzleme Formu (EK-7.39)
- Doküman Revizyon Talep Formu (EK-7.40)
- Tedarikçi Değerlendirme Formu (EK-7.41)

8. SONUÇLAR ve ÖNERİLER

Bu bölümde, çalışma kapsamında elde edilen tüm verilerin analiziyle ortaya çıkan araştırma sonuçları ve bu sonuçlar bir bütün olarak değerlendirilmiş, üniversite kütüphanelerinde bilgi güvenliği yönetimine ilişkin karşılaşılan sorunların çözümüne yönelik öneriler verilmiştir.

8.1. Sonuçlar

Çalışmanın sonuçları, çalışmanın bütünlüğü düşünülerek üç başlık altında sunulmaktadır. Öncelikle Türkiye'de üniversite kütüphanelerinde bilgi güvenliği yönetiminin altyapısına ilişkin katılımcılardan elde edilen bulgulara ilişkin sonuçlar, daha sonra ise üniversite kütüphanelerindeki mevcut teknik ve kurumsal bilgi güvenliği uygulamalarının bulgularına ilişkin sonuçlara yer verilmektedir.

8.1.1. Bilgi Güvenliği Alt Yapısına ve Tehditlerine İlişkin Sonuçlar

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği yönetim sistemin uygulanması ile ilgili personel ve teknik alt yapılarına ilişkin katılımcılardan elde edilen bulgulardan aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde yeterli düzeyde bilgi güvenliği personeli bulunduğu, devlet ve vakıf üniversitelerindeki kütüphanelerin arasında da benzer oranlarda bilgi güvenliği personeline sahip olduğu sonucuna ulaşılmıştır. Bu sonuçlar, üniversite kütüphanelerinin bilgi güvenliği yönetim sistemi açısından personel eksikliği yaşadığını göstermektedir.
- Üniversite kütüphanelerinin yoğun bir şekilde bilgi sistemlerini (kütüphane otomasyon sistemleri, intihal yazılım araçları, kütüphaneler arası iş birliği sistemleri, açık erişim sistemleri, veri tabanı erişim ve istatistik sistemleri, üyelik sistemleri ve kimlik doğrulama sistemleri gibi) kullandıkları sonucuna ulaşılmıştır.
- Türkiye'de üniversite kütüphanelerindeki bilgi varlıklarına işlenen veri / bilgilerin "gizlilik" ve "bütünlük" unsurlarının ihlal edilmesi durumunda kütüphanelerin hizmetlerini ve çıkarlarını etkileyecek olumsuzlukların

yaşanabileceği hatta kurumun genelini saygınlık derecesinde etkileyebileceği; "erişebilirlik" unsurunun zaman bakımından ihlal edilmesi durumunda ise bu ihlalin etkisinin kısa sürelerde hissedilebileceği sonucuna varılmıştır.

- Türkiye'deki üniversite kütüphanelerinde meydana gelen bilgi güvenliği ihlallerinin toplumsal, kurumsal, kütüphanecilik camiası ve kütüphanelere bağımlı dış paydaş alanlarını önemli ölçüde etkilediği gözlemlenmiştir. Olası bir bilgi güvenliği ihlalinin öncelikli olarak üniversite kütüphanelerinin kurumsal yapısını etkileyebileceği ve sırasıyla kütüphanecilik camiasını, kütüphanelerin dış paydaşlarını ve toplumsal yapıyı etkileyebileceği görülmüştür. Bu sonuçlar, bilgi güvenliği önlemlerinin göz önünde bulundurularak hangi alanların etkilenebileceğinin belirlenmesinin ve bu önlemlerin uygulanmasının önemini vurgulamaktadır.
- Türkiye'de üniversite kütüphanelerinde karşılaşılan yaygın bilgi güvenliği tehditlerinin görülme sıklığı çoktan aza doğru bilgi sistemi arızası ve bakım hatası; e-posta saldırıları; virüs, solucan, truva atı gibi kötü yazılım tehditleri; parola saldırıları; iletişim hataları; doğal afetlere ve hava olaylarına bağlı tehditler; yetkisiz donanım ve yazılım kullanımı; reklam ve casus yazılım tehditleri; bilgi sistemlerini hackleme; yanlış yazılım güncelleme hataları; web saldırıları; kasıtlı veya kasıtsız personel suiistimalleri; binaya izinsiz giriş ve yetkisiz erişim tehditleri; kimlik hırsızlığı ve dolandırıcılığı tehditleri; kimlik doğrulama saldırıları; fiziksel belge ve donanım hırsızlığı; sabotaj ve kasıtlı imha; uzaktan yönetim aracı saldırıları biçiminde sıralandığı sonucuna ulaşılmıştır.
- Türkiye'de üniversite kütüphanelerinde algılanan en yaygın bilgi güvenliği tehditlerinin insan / personel ile ilgili tehditler kategorisinde gerçekleştiği ve bu tehdit kategorisini sırasıyla ağ, yazılım, fiziksel ve çevresel, veri ve donanım tehditi kategorilerinin izlediği görülmüştür.

8.1.2. Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeylerine İlişkin Sonuçlar

Türkiye'de üniversite kütüphanelerinde donanım güvenliği önlemlerine ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde donanım güvenliği ile ilgili 9 maddedeki önlemin uygulanması konusunda %35,2 ile %73,9 arasında katılımcının iyi düzeyde, %15,6 ile %27,6 arasında katılımcının orta düzeyde, %2,5 ile %10,6 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %0 ile %6,0 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %4,5 ile %34,2 arasında katılımcının ise donanım güvenliği önlemlerinin uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir.
- Katılımcıların görev yaptıkları üniversite türlerine göre donanım kategorisinde yer alan teknolojik bilgi güvenliği önlemlerinin uygulanma düzeyleri arasında anlamlı bir farklılık olmadığı görülmektedir. Bu sonuç, donanım güvenliği önlemlerinin devlet üniversiteleri ve vakıf üniversiteleri arasında benzer şekilde uygulandığını göstermektedir.
- Üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personele sahip olmanın donanım güvenliği önlemlerinin uygulanma düzeyleri üzerinde anlamlı bir etkisi olduğu görülmüştür. Bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde, kütüphane envanterindeki cihazların şifrelenmesi, kritik bilgi içeren taşınabilir cihazların güvenli şekilde saklanması ve imha edilmesi, yeni tedarik edilen sabit disklerin veri kurtarmaya imkân vermeyecek şekilde biçimlendirilmesi, kritik bilgi içeren cihazların çevresel önlemlerinin alınması ve onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihazlardaki kritik bilgilerin geri getirilmeyecek şekilde silinmesi önlemlerinde daha yüksek uygulama düzeyi olduğu belirlenmiştir. Bu bulgular, bilgi güvenliğinden sorumlu personelin varlığının donanım güvenliği önlemlerinin etkin bir şekilde uygulanmasına katkı sağladığını göstermektedir.
- Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde görev yapan katılımcıların donanım güvenliği önlemlerinin uygulanma düzeyleri, bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinde görev yapan katılımcılara göre daha yüksektir. İlgili önlemler arasında veri işleme, depolama ve iletme yeteneğine sahip donanımların envanterinin tutulması ve kullanım tahsislerinin yapılması; kütüphane envanterindeki cihaz ve taşınabilir

ortamların şifrelenmesi; kritik bilgi içeren taşınabilir cihaz ve ortamların güvenli şekilde saklanması ve kurum dışına çıkarılmaması; kütüphane envanterinden çıkarılan donanımlardaki veri ve bilgilerin geri getirilmeyecek şekilde silinmesi; kullanım ömrünü tamamlamış veri depolama ünitelerinin güvenli bir biçimde imha edilmesi ve kritik bilgi içeren cihaz ve ortamların çevresel tehditlere karşı korunması yer almaktadır. Bu sonuçlar, bilgi güvenliği yönetim aracı kullanımının donanım güvenliği önlemlerinin etkin bir şekilde uygulanmasında olumlu bir etkisi olduğunu göstermektedir.

Türkiye'de üniversite kütüphanelerinde yazılım güvenliği önlemlerine ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde donanım güvenliği ile ilgili 12 maddedeki önlemin uygulanması konusunda %33,7 ile %70,4 arasında katılımcının iyi düzeyde, %14,1 ile %24,6 arasında katılımcının orta düzeyde, %2,5 ile %8,0 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %0,5 ile %3,5 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %6,5 ile %38,7 arasında katılımcının ise yazılım güvenliği önlemlerinin uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir.
- Katılımcıların görev yaptıkları üniversite türlerine göre yazılım kategorisinde yer alan bazı önlemlerin uygulanma düzeylerine ilişkin devlet üniversitesi ile vakıf üniversiteleri arasında anlamlı farklılıklar olduğu görülmüştür. Devlet üniversitesi kütüphanelerinde yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması gibi kontrollerin kullanılması ve olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemlerinin düzenli olarak gözden geçirilmesi önlemlerinin vakıf üniversitelerine kıyasla daha düşük düzeylerde uygulandığı belirlenmiştir. Bu sonuç, bazı yazılım güvenliği önlemlerinin devlet üniversiteleri ve vakıf üniversiteleri arasında benzer şekilde uygulanmadığını göstermektedir.
- Üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personelin varlığına bağlı olarak yazılım güvenliği önlemlerinin uygulanma düzeyleri arasında

anlamlı farklılıklar olduğu görülmüştür. Bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde, bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması gibi kontrollerin uygulanmasının; kritik veri işleyen sistem yazılımlarının düzenli olarak gözden geçirilmesinin; olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemlerinin; kurumsal ve kişisel bilgi içeren uygulama ve yazılımlara, kişisel cihaz ve ortamların bağlanmasına izin verilmemesinin uygulanma düzeyleri daha yüksek bulunmuştur. Bu bulgulara dayanarak, bilgi güvenliğinden sorumlu personelin varlığının yazılım güvenliği önlemlerinin uygulanma düzeyini olumlu yönde etkilediği söylenebilir.

- Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde yazılım güvenliği önlemlerinin uygulanma düzeyleri bilgi güvenliği yönetim aracı kullanmayan kütüphanelere kıyasla daha yüksektir. Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde kara liste uygulamaları gibi zararlı web sitelerini tespit etmeye yönelik kontrollerin; felaket, saldırı, sistem arızası ve kullanıcı hatası kaynaklı veri/bilgi kayıplarına karşı yedeklemelerin; olası güvenlik ihlallerini belirleme ve kanıt üretme amacıyla kullanıcı işlemlerinin düzenli olarak gözden geçirilmesinin; bilgisayarların zararlı yazılım taramalarından otomatik olarak geçirilmesi ve otomatik çalıştırılmamasının uygulanma düzeyi, bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerine göre daha yüksektir. Bu bulgulara dayanarak, bilgi güvenliği yönetim aracı kullanımının üniversite kütüphanelerinde yazılım güvenliği önlemlerinin uygulanmasında anlamlı bir fark oluşturduğu söylenebilir.

Türkiye'de üniversite kütüphanelerinde ağ güvenliği önlemlerine ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde ağ güvenliği ile ilgili 11 maddedeki önlemin uygulanması konusunda %47,2 ile %81,4 arasında katılımcının iyi düzeyde, %11,6 ile %16,6 arasında katılımcının orta düzeyde, %0,5 ile %5,5 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %0,5 ile %5,0 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %5,0 ile %30,2 arasında katılımcının ise ağ güvenliği

önlemlerinin uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir.

- Katılımcıların görev yaptıkları üniversite türlerine göre ağ güvenliği kategorisinde yer alan teknolojik bilgi güvenliği önlemlerinin uygulanma düzeyleri arasında anlamlı bir farklılık olmadığı görülmektedir. Bu sonuç, ağ güvenliği önlemlerinin devlet üniversiteleri ve vakıf üniversiteleri arasında benzer şekilde uygulandığını göstermektedir.
- Bilgi güvenliğinden sorumlu personel bulunan üniversite kütüphanelerinde ağ güvenliği önlemlerinin uygulanma düzeyleri, bilgi güvenliğinden sorumlu personeli olmayan üniversite kütüphanelerine göre daha yüksektir. Bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde kritik bilgi işleyen bilgisayar ve diğer sistemlerin kablosuz ve kablolu ağ bağlantılarının sınırlandırılması veya engellenmesi; kurum ağına bağlanan kullanıcılara ait donanımların erişimlerinin port seviyesinde kontrol edilmesi ve zararlı donanımların engellenmesi önlemlerinde bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek düzeylerde uygulandığı bulunmuştur. Bu bulgular ışığında, bilgi güvenliğinden sorumlu personelin varlığı, üniversite kütüphanelerinde ağ güvenliği önlemlerinin uygulanma düzeyinde anlamlı bir farklılık oluşturduğunu göstermektedir.
- Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde ağ güvenliği önlemlerinin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerine göre daha yüksek olduğu bulunmuştur. Bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemlerinin kullanılma düzeyi; onaylanmayan ve erişimi yasak olan web sitelerinin bağlantısını engellemek için ağ tabanlı URL filtrelemesinin uygulanma düzeyi; elektronik bilgi iletiminde yasal ve güvenlik kontrol gereksinimlerinin dikkate alınma düzeyi, ağ teknolojisi ile çalışan cihazların kayıtlarının tutulma ve kullanıcı sorumlularının belirlenme düzeyi; kurum ağına bağlanan kullanıcılara ait donanımların erişimlerinin kontrol edilme ve zararlı donanımların engellenme

düzeyi bilgi güvenliği yönetim aracı kullanan kütüphanelerde daha yüksek olarak gerçekleştiği görülmüştür. Sonuç olarak, bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde ağ güvenliği önlemlerinin uygulanma düzeyleri, bilgi güvenliği yönetim aracı kullanmayan kütüphanelere göre daha etkili bir şekilde gerçekleştirilmektedir.

Türkiye'de üniversite kütüphanelerinde veri güvenliği önlemlerine ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde veri güvenliği ile ilgili 15 maddedeki önlemin uygulanması konusunda %46,2 ile %61,3 arasında katılımcının iyi düzeyde, %14,6 ile %23,6 arasında katılımcının orta düzeyde, %2,5 ile %11,6 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %0 ile %5,5 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %11,6 ile %30,2 arasında katılımcının ise veri güvenliği önlemlerinin uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir.
- Katılımcıların görev yaptıkları üniversite türlerine göre ağ kategorisinde yer alan bazı önlemlerin uygulanma düzeylerine ilişkin devlet üniversitesi ile vakıf üniversiteleri arasında anlamlı farklılıklar olduğu görülmüştür. Devlet üniversitesi kütüphanelerinde kritik ve değerli bilgilerin depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmesi ve saklanması ile bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin üyelik numarası ve şifresi olarak kullanılmaması önlemlerinin vakıf üniversitelerine kıyasla daha düşük düzeylerde uygulandığı belirlenmiştir. Bu sonuç, bazı veri güvenliği önlemlerinin devlet üniversiteleri ve vakıf üniversiteleri arasında benzer şekilde uygulanmadığını göstermektedir.
- Bilgi güvenliğinden sorumlu personel bulunan üniversite kütüphanelerinde veri güvenliği önlemlerinin uygulanma düzeyleri, bilgi güvenliğinden sorumlu personeli olmayan üniversite kütüphanelerine göre daha yüksektir. Bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bilgilerin değeri, kritikliği ve gizliliği gibi hassasiyetlere göre sınıflandırılması; bilgisayar ve taşınabilir ortamlarda (HDD, SSD, harici bellek vb.) muhafaza

edilen kritik bilgilerin şifrelenmesi; kritik ve değerli bilgilerin depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmesi ve saklanması; kişisel bilgilerin erişim yetkilendirmeleri önceden belirlenmiş ilke ve yöntemlere göre verilmesi; personel, tedarikçi ve kullanıcıların kütüphane sistemlerindeki bilgilere erişim yetkilerinin düzenli aralıklarla gözden geçirilmesi ve ilişkileri sone erdiğinde kaldırılması; kullanıcılardan kişisel bilgilerinin sistemler arasında veya gerekli hallerde kurum içinde kullanılacağı ile ilgili açık rıza onayının alınması önlemlerinde bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek düzeylerde uygulandığı bulunmuştur. Bu bulgular ışığında, bilgi güvenliğinden sorumlu personelin varlığı, üniversite kütüphanelerinde veri güvenliği önlemlerinin uygulanma düzeyinde anlamlı bir farklılık oluşturduğunu göstermektedir. Bu bulgulara dayanarak, bilgi güvenliğinden sorumlu personelin varlığına bağlı olarak üniversite kütüphanelerindeki veri güvenliği önlemlerinin daha iyi uygulandığı söylenebilir. Bu durum, bilgi güvenliği personelinin önemini vurgulamakta ve bilgi güvenliği yönetimi konusunda uzman personelin etkisinin önemini ortaya koymaktadır.

- Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde veri güvenliği önlemlerinin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerine göre daha yüksek olduğu görülmüştür. Bilgi yaşam döngüsü içerisinde işlenen, depolanan, iletilen ve imha edilen kritik bilgiler belirlenmesi ve kayıtları tutulması; bilgilerin değeri, kritikliği ve gizliliği gibi hassasiyetlere göre sınıflandırılması; bilgisayar ve taşınabilir ortamlarda muhafaza edilen kritik bilgilerin şifrelenmesi; kritik ve değerli bilgilerin depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmesi ve saklanması; bilgi sistemlerindeki kullanıcı bilgilerinin tedarikçilerce ihlal edilmemesinin karşılıklı sözleşme ile koruma altına alınması; personel, tedarikçi ve kullanıcıların kütüphane sistemlerindeki bilgilere erişim yetkilerinin düzenli aralıklarla gözden geçirilmesi ve ilişkileri sone erdiğinde kaldırılması; kullanıcılardan kişisel bilgilerinin sistemler arasında veya gerekli hallerde kurum içinde kullanılacağı ile ilgili açık rıza onayının alınması; bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin

üyelik numarası ve şifresi olarak kullanılmaması; veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi kimlik doğrulama sistemlerinin kullanılması önlemlerindeki uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanan kütüphanelerde daha yüksek olarak gerçekleştiği görülmüştür. Sonuç olarak, bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde ağ güvenliği önlemlerinin uygulanma düzeyleri, bilgi güvenliği yönetim aracı kullanmayan kütüphanelere göre daha etkili bir şekilde gerçekleştirilmektedir.

Türkiye'de üniversite kütüphanelerinde fiziksel ve çevresel güvenlik önlemlerine ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde fiziksel ve çevresel güvenlik ile ilgili 12 maddedeki önlemin uygulanması konusunda %26,6 ile %77,4 arasında katılımcının iyi düzeyde, %11,1 ile %26,1 arasında katılımcının orta düzeyde, %4,5 ile %20,6 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %2,5 ile %34,2 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %0 ile %27,1 arasında katılımcının ise fiziksel ve çevresel güvenlik önlemlerinin uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir.
- Katılımcıların görev yaptıkları üniversite türlerine göre fiziksel ve çevresel güvenlik önlemlerinin uygulanma düzeyleri arasında anlamlı farklılıklar olduğu tespit edilmiştir. Devlet üniversitesi kütüphanelerinde görev yapan katılımcılar, kütüphanenin ana giriş ve çıkış kapılarının güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile denetlenmesinin uygulanması konusunda vakıf üniversitesi kütüphanelerinde görev yapan katılımcılardan daha yüksek bir uygulanma düzeyi bildirmişlerdir. Fakat ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb.) kütüphaneye giriş ve çıkışlarının kayıt altına alınması ve sadece ilgili amaçları için erişim izinlerinin verilmesi; refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğunun uygulanması; kütüphane binasına ait pencereler, kapılar ve bahçe alanlarının demir parmaklık, çit, kilit, tel örgü gibi dış güvenlik unsurlarıyla kontrol edilmesi önlemlerine ilişkin ise vakıf

üniversitelerinde üst düzeyde uygulama olduğu belirlenmiştir. Bu sonuçlar, bazı fiziksel ve çevresel güvenlik önlemlerinin üniversite türüne göre anlamlı düzeyde farklılaştığını göstermektedir.

- Üniversite kütüphanelerindeki bilgi güvenliği önlemlerinin uygulanma düzeyiyle ilgili katılımcıların görüşleri arasında, bilgi güvenliğinden sorumlu personelin varlığına göre anlamlı farklılıklar olduğu belirtilmektedir. Bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personel bulunan üniversite kütüphanelerinde fiziksel ve çevresel güvenlik önlemlerinin uygulanma düzeyleri, bilgi güvenliğinden sorumlu personeli olmayan üniversite kütüphanelerine göre daha yüksektir. Kritik bilgi barındıran alanların fiziksel güvenlik sınırları belirlenmekte ve kapı, pencere gibi kısımlar güvenlik mekanizmaları ile korunmaktadır. Kütüphanede güvenlik kontrollerini sağlayacak yetkinliğe sahip yeterli sayıda güvenlik personeli çalıştırılması; ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb.) giriş ve çıkışları kayıt altına alınması; ziyaretçilerin kabul edileceği alanların personel ve kullanıcı çalışma alanlarından ayrı bir bölgede konumlandırılması; refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğunun uygulanması; kritik bilgilerin işlendiği veya saklandığı alanlara erişimin uygun kontroller (kartlı/şifreli erişim vb.) uygulanarak yetkili kişilerle sınırlandırılması; elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarlarının kullanılması önlemlerinde bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelerinden daha yüksek düzeylerde uygulandığı bulunmuştur. Bu bulgulara dayanarak, bilgi güvenliğinden sorumlu personelin varlığına bağlı olarak üniversite kütüphanelerindeki bilgi güvenliği önlemlerinin daha iyi uygulandığı söylenebilir. Bu durum, fiziksel ve çevresel bilgi güvenliği önlemelerinin uygulanmasında bilgi güvenliği yönetimi konusunda uzman personelin etkisinin önemini ortaya koymaktadır.
- Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde fiziksel ve çevresel güvenlik önlemlerinin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerine göre daha yüksek olduğu görülmüştür. Kütüphanenin iç ve dış alanlarının güvenlik kameraları ile

takip edilmesi; ziyaretçilerin giriş ve çıkışlarının kayıt altına alınması; elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarlarının kullanılması önlemlerindeki uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanan kütüphanelerde daha yüksek olarak gerçekleştiği görülmüştür. Bu sonuçlara dayanarak, bilgi güvenliği yönetim araçlarının kullanımı üniversite kütüphanelerinde fiziksel ve çevresel bilgi güvenliği önlemlerinin uygulanma düzeyleri üzerinde olumlu yönden etkilediği görülmektedir.

8.1.3. Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Düzeylerine İlişkin Sonuçlar

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği politikalarının uygulanmasına ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde bilgi güvenliği politikaları ile ilgili 16 maddedeki önlemin uygulanması konusunda %47,2 ile %62,8 arasında katılımcının iyi düzeyde, %18,6 ile %26,6 arasında katılımcının orta düzeyde, %3,5 ile %10,6 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %3,0 ile %5,0 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %8,5 ile %19,6 arasında katılımcının ise bilgi güvenliği politikalarının uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir.
- Katılımcıların görev yaptıkları üniversite türlerine göre bilgi güvenliği politikalarının uygulanma düzeyleri arasında sadece bir uygulamada anlamlı farklılığın oluştuğu tespit edilmiştir. Devlet üniversitesi kütüphanelerinde temiz masa ve temiz ekran ilke ve yöntemlerinin uygulanma düzeyi vakıf üniversitesi kütüphanelerine göre daha düşük olduğu tespit edilmiştir. Bu sonuçlara dayanarak, devlet üniversitelerinin bilgi güvenliği politikalarını daha etkin bir şekilde uygulamaları ve özelliklede temiz masa / ekran ilke ve yöntemlerine yönelik daha fazla önlem almaları gerekmektedir.
- Bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde görev yapan katılımcıların, belirli politikaların uygulanma düzeyini daha iyi

düzeylerde değerlendirdikleri görülmektedir. Kritik bilgilere yetkisiz erişimin azaltılması, temiz masa ve temiz ekran ilke ve yöntemleri, bilgi transferi ilke ve yöntemleri, taşınabilir cihazlarla ilgili risk yönetimi, uzaktan çalışma ilkeleri, bilgi sınıflandırma ve etiketleme ilkeleri, fiziksel ve çevresel güvenlik ilkeleri gibi politikalar, bilgi güvenliğinden sorumlu personele sahip olan kütüphanelerde daha iyi düzeyde uygulanmaktadır. Bu sonuçlar, bilgi güvenliğinden sorumlu personelin varlığına göre gruplar arasında anlamlı farklılık olduğunu göstermiştir. Bu da bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerinde bilgi güvenliği politikalarının uygulanma düzeyinin, bilgi güvenliğinden sorumlu personele sahip olmayan üniversite kütüphanelere kıyasla daha yüksek olduğunu göstermektedir. Sonuç olarak, bilgi güvenliği politikalarının etkin bir şekilde uygulanması için bilgi güvenliğinden sorumlu personelin varlığı önemlidir. Bu personel, politikaların uygulanmasını yönetebilir ve bilgi güvenliği konusunda farkındalık oluşturabilir.

- Üniversite kütüphanelerinde bir bilgi güvenliği yönetim aracının kullanım durumuna göre bilgi güvenliği politikalarının uygulanma düzeylerinde gruplar arasında anlamlı farklılıkların olduğu görülmektedir. Katılımcıların görüşlerine göre, bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerindeki bilgi güvenliği politikalarının uygulanma düzeyi, bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerinden daha yüksektir. Bilgilerin kabul edilebilir kullanımlarını tanımlayan ilkelerin; temiz masa ve temiz ekran ilke ve yöntemlerinin; bilgi transferi ilke ve yöntemlerinin; taşınabilir cihazların yönetilmesini düzenleyen ilkelerin; uzaktan çalışma ilkelerinin; güvenli yazılım kurulumlarını tanımlayan ilke ve yöntemlerin; bilgi sistemleri ve varlıklarına erişim kontrol yöntemlerinin; bilgi sınıflandırma ve etiketleme ilkelerinin; kritik bilgi barındıran alan ve sistemlerin fiziksel ve çevresel güvenlik ilke ve yöntemlerinin; bilgi yedekleme ilke ve yöntemlerinin; zararlı yazılımlara karşı korunma ilke ve yöntemlerin; bilgilerin gizliliğinin ve bütünlüğünün korunması için şifreleme kontrollerinin doğru ve etkin kullanımını temin eden ilke ve yöntemlerin; ağ yönetimi ilke ve yöntemlerinin; kişisel bilgilerin mahremiyeti ve koruması ilke ve yöntemlerin; fikri mülkiyet

ilke ve yöntemlerinin; tedarikçi ilişkileri yöntemlerinin uygulanma düzeylerinin bilgi güvenliği yönetim aracı kullanan kütüphanelerde daha yüksek olarak gerçekleştiği görülmüştür.

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği prosedürlerinin uygulanmasına ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde bilgi güvenliği prosedürleri ile ilgili 10 maddedeki önlemin uygulanması konusunda %47,2 ile %60,8 arasında katılımcının iyi düzeyde, %18,6 ile %24,1 arasında katılımcının orta düzeyde, %2,5 ile %8,0 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %3,5 ile %8,5 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %10,6 ile %21,1 arasında katılımcının ise bilgi güvenliği prosedürlerinin uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir
- Katılımcıların görev yaptıkları üniversite türlerine göre bilgi güvenliği prosedürlerinin uygulanma düzeyleri arasında sadece bir uygulamada anlamlı farklılığın oluştuğu tespit edilmiştir. Devlet üniversitesi kütüphanelerinde kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ilke ve yöntemlerin uygulanma düzeyi vakıf üniversitesi kütüphanelerine göre daha düşük olduğu tespit edilmiştir. Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde, bu ilke ve yöntemlerin daha iyi uygulandığı ve katılımcıların bu konuda daha olumlu görüşlere sahip oldukları görülmektedir. Ancak, bu farklılıkların nedenleri hakkında daha fazla araştırma yapılması gerekmektedir.
- Üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personele sahip olmanın, belirli prosedürlerin uygulanma düzeyi üzerinde olumlu bir etkisi olduğu görülmektedir. Kritik bilgilerin güvenli bir şekilde kullanılması, kullanıcı erişim yöntemleri, güvenli oturum açma, fiziksel giriş kontrolü, ihlal müdahalesi, iş sürekliliği, kapasite yönetimi, elektronik posta ve ziyaretçi kabul ilke ve yöntemlerinin uygulanması açısından bilgi güvenliğinden sorumlu personele sahip kütüphanelerde daha iyi bir düzeyde gerçekleştirildiği

belirlenmiştir. Bu sonuçlar, bilgi güvenliği prosedürlerinin etkin bir şekilde uygulanması için bilgi güvenliğinden sorumlu personelin önemini vurgulamaktadır.

- Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde, kurumsal bilgi güvenliği önlemlerinin prosedürler kategorisinde yer alan önlemlerin uygulanma düzeyinin bilgi güvenliği yönetim aracı kullanmayan kütüphanelere kıyasla daha yüksek olduğu belirlenmiştir. Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması ve imha edilmesi ile ilgili faaliyetlerin; kullanıcı erişim yöntemlerinde kullanıcı kaydetme, erişim izni verme ve kimlik doğrulama gibi faaliyetlerin; güvenli oturum açma ilke ve yöntemlerin; kütüphanelere fiziksel giriş ilke ve yöntemlerin; bilgi güvenliği ihlal olaylarına müdahale edilmesini amaçlayan faaliyetlerin; iş sürekliliği ve felaket kurtarma ilke ve yöntemlerin; parola işleme ve kullanımı ilke ve yöntemlerin; bilgi varlıklarının kapasite yönetimi ilke ve yöntemlerinin; elektronik posta ilke ve yöntemlerin; ziyaretçi kabul ilke ve yöntemlerin bilgi güvenliği yönetim aracı kullanmayan kütüphanelerden daha iyi düzeyde uygulandıkları görülmüştür.

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği idari araç ve yöntemlerinin uygulanmasına ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde bilgi güvenliği idari araçları ile ilgili 8 maddedeki önlemin uygulanması konusunda %43,2 ile %52,3 arasında katılımcının iyi düzeyde, %19,1 ile %23,6 arasında katılımcının orta düzeyde, %4,5 ile %9,5 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %4,0 ile %9,0 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %13,1 ile %22,1 arasında katılımcının ise bilgi güvenliği idari araçlarının uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir.

- Katılımcıların görev yaptıkları üniversite türlerine göre bilgi güvenliği idari araç ve yöntemlerinin uygulanma düzeylerine ilişkin görüşlerinde anlamlı bir farklılık olmadığı tespit edilmiştir.
- Üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personele sahip olmanın, bilgi güvenliği idari araç ve yöntemlerinin daha iyi düzeyde uygulanması üzerinde olumlu bir etkisi olduğu görülmektedir. Bilgi güvenliğinden sorumlu personelin olduğu üniversite kütüphanelerinde bilgi güvenliği politika ve prosedürlerinin uygulanma düzeyi, ihlallerin raporlanması ve önlem alınması için disiplin mekanizmasının varlığı, yeni personelin sorumluluklarını içeren talimatlar, aydınlatma metni ve açık rıza yönetimi uygulamaları, risk analizi tabanlı idari araçlar, iç denetim ilke ve uygulamaları ile üçüncü taraf tedarikçilerle yapılan sözleşmelerin uygulama düzeylerinin bilgi güvenliğinden sorumlu personeli olmayan kütüphanelere kıyasla daha iyi olduğu belirlenmiştir. Bu bulgular, bilgi güvenliğinden sorumlu personelin varlığının üniversite kütüphanelerindeki bilgi güvenliği idari araç ve uygulamalarının etkinliği üzerinde olumlu bir etkisi olduğunu göstermektedir.
- Bilgi güvenliğinden sorumlu personele sahip olan üniversite kütüphanelerindeki katılımcılar, bilgi güvenliği idari araçlarının daha iyi bir düzeyde uygulandığını belirtmişlerdir. Eğitim planlama rehberlerinin, hizmetçi eğitim uygulamalarının, tedarikçilerin farkındalığını geliştirme çalışmalarının, interaktif eğitim çalışmalarının, bilgilendirici doküman çalışmalarının ve kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini artırmaya yönelik görsellerin sunulmasının bilgi güvenliğinden sorumlu personele sahip olan kütüphanelerde daha iyi bir düzeyde uygulanmaktadır. Bu bulgular, bilgi güvenliği önlemlerinin etkin bir şekilde uygulanması için bilgi güvenliğinden sorumlu personelin varlığının önemini vurgulamaktadır.

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği farkındalık çalışmalarının uygulanmasına ilişkin katılımcılardan elde edilen verilerden aşağıdaki sonuçlara ulaşılmıştır:

- Türkiye'de üniversite kütüphanelerinde bilgi güvenliği farkındalık çalışmaları ile ilgili 11 maddedeki önlemin uygulanması konusunda %27,6 ile %43,2

arasında katılımcının iyi düzeyde, %21,1 ile %27,1 arasında katılımcının orta düzeyde, %11,1 ile %19,1 arasında katılımcının ise kötü düzeyde uygulandığını belirttikleri tespit edilmiştir. Ayrıca, %10,6 ile %27,6 arasında katılımcının bu önlemlerin hiç uygulanmadığını ve %6,0 ile %10,1 arasında katılımcının ise bilgi güvenliği farkındalık çalışmalarının uygulanması hakkında bir fikre sahip olmadığını ifade ettiği gözlemlenmiştir.

- Katılımcıların görev yaptıkları üniversite türlerine göre bazı bilgi güvenliği farkındalık çalışmalarının uygulanma düzeyleri arasında anlamlı farklılıklar olduğu ortaya çıkmıştır. Kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması; kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları, fare altlığı, not kâğıtları gibi farkındalık arttırıcı faaliyetlerin uygulanması; personele ve kullanıcılara bilgi güvenliği ile ilgili mail ve SMS yoluyla bilgilendirme mesajlarının gönderilmesi önlemlerinin devlet üniversitesi kütüphanelerinde uygulanma düzeyinin vakıf üniversitelerine göre daha düşük olduğu görülmüştür.
- Üniversite kütüphanelerinde bilgi güvenliğinden sorumlu personele sahip olmanın, bilgi güvenliği farkındalık çalışmalarının daha iyi düzeyde uygulanmasına katkı sağladığı görülmektedir. Bilgi güvenliğinden sorumlu personelin olduğu üniversite kütüphanelerinde bilgi güvenliği politika ve prosedürlerinin uygulanma düzeyi, ihlallerin raporlanması ve önlem alınması için disiplin mekanizmasının varlığı, personelin sorumluluklarını içeren talimatların sağlanması, aydınlatma metni ve açık rıza yönetimi uygulamaları, risk analizi tabanlı idari araçlar, iç denetim ilke ve uygulamaları ile üçüncü taraf tedarikçilerle yapılan sözleşmelerin uygulama düzeylerinin bilgi güvenliğinden sorumlu personeli olmayan kütüphanelere daha iyi olduğu belirlenmiştir.
- Bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde çalışan katılımcıların bilgi güvenliği farkındalık eğitimi, eğitim planlama rehberleri, personel eğitimi, tedarikçi farkındalığı, interaktif eğitim çalışmaları ve bilgilendirici doküman çalışmaları gibi önlemlerin uygulanma düzeylerinin

bilgi güvenliği yönetim aracı kullanmayan üniversite kütüphanelerine göre daha yüksek olduğunu belirtmiştir. Bu bulgular, bilgi güvenliği yönetim aracının kullanımının üniversite kütüphanelerindeki bilgi güvenliği önlemlerinin etkinliğini artırdığını göstermektedir. Bu durum, bilgi güvenliği yönetim aracının katılımcıların bilgi güvenliği sorumluluklarını farkında olmalarını ve yerine getirmelerini amaçlayan eğitim çalışmaları düzeyini yükselttiğini göstermektedir. Sonuç olarak, bilgi güvenliği yönetim aracı kullanan üniversite kütüphanelerinde, çalışanların ve kullanıcıların bilgi güvenliği sorumluluklarını yerine getirmelerini amaçlayan önlemlerin uygulanma düzeyi, kullanmayan kütüphanelere göre daha yüksektir. Bu bulgular, bilgi güvenliği yönetim aracının üniversite kütüphanelerinde bilgi güvenliği farkındalık eğitimi çalışmalarının devamı için olumlu bir etkiye sahip olduğunu göstermektedir.

8.1.4. Hipotezlere İlişkin Sonuçlar

Sonuç olarak, güvenlik kolayca tanımlanamayan bir kavramdır. Bilgi güvenliği yönetimi, bir kuruma ait bilgi varlıklarının güvenliğinin durumunu değerlendirmek için atılan önemli kurumsal adımları kapsamaktadır. Bu çalışma, Türkiye'de üniversite kütüphanelerinde bilgi güvenliği önlemlerinin uygulama durumunun bilgi güveliğinden veya varlıklarından sorumlu personelin görüşleri aracılığıyla araştırılan konuya ilişkin bir nicel yaklaşım sunmaktadır. Bu yaklaşım, üniversite kütüphanelerinde bilgi güvenliği uygulamalarının ne ölçüde uygulandığına dair bir bakış açısı sağlayarak alana önemli bir katkı sağlamaktadır. Türkiye'de üniversite kütüphanelerinde, donanım, yazılım, ağ, veri ve fiziksel tesisler için teknolojik güvenlik önlemlerinin genel olarak uygulandığı fakat uygulama seviyelerinin orta düzeyin biraz üzerinde olduğu belirlenmiştir. Bu durum, her üniversite kütüphanesinin özelinde değişiklik gösterebilmektedir. Çünkü üniversitelerin kuruluş yılları, sahip oldukları teknolojik imkânlar ve uzman personel gibi birçok faktör üniversite kütüphanelerindeki bilgi güvenliği uygulamalarının düzeyini etkileyebilmektedir.

Teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeyleri üniversite türü, üniversite kütüphanelerinde bilgi güvenliği personelinin varlığı ve kurumsal bir

bilgi güvenliği yönetim aracının kullunım durumu değişkenlerine göre anlamlı farklılıklar gösterip göstermediğine ilişkin kurulan hipotezler çalışmadan elde edilen veriler ile sınanmıştır. Hipotezlerin imncelenmesine ilişkin sonuçlar şu biçimde sıralanmaktadır:

- "Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinde üniversite türleri arasında anlamlı farklılıklar vardır" hipotezine yönelik yapılan ki-kare testleri sonucunda üniversite türü değişkenine göre bilgi güvenliği önlemlerine ilişkin uygulamaların üniversite türü özelinde anlamlı düzeyde farklı olmadığı anlaşılmıştır. Bu nedenle bu hipotez rededilmiştir.
- "Türkiye'de üniversite kütüphanelerinde bilgi güvenliği personelinin varlığına bağlı olarak teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinde anlamlı farklılıklar vardır" hipotezini sınamaya yönelik ki-kare testleri, üniversite kütüphanelerinde bilgi güvenliği personelinin varlığının bilgi güvenliği önlemlerinin uygulanması hususunu anlamlı düzeyde farklılaştırdığı sonucunu ortaya koymaktadır. Bu nedenle bu hipotez kabul edilmiştir.
- "Türkiye'de üniversite kütüphanelerinde kurumsal bilgi güvenliği yönetim aracının varlığı ve kullanımına bağlı olarak teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinde anlamlı farklılıklar vardır" hipotezini sınamaya yönelik ki-kare testleri, üniversite kütüphanelerinde kurumsal bilgi güvenliği yönetim araçlarının varlığı ve kullanımın bilgi güvenliği önlemlerinin uygulanması hususunu anlamlı düzeyde farklılaştırdığı sonucunu ortaya koymuştur. Bu nedenle bu hipotez kabul edilmiştir.

Bilgi güvenliğinden sorumlu personelin varlığı ve kurumsal bir bilgi güvenliği yönetim aracının kullanım durumlarına göre üniversite kütüphanelerinde teknolojik ve kurumsal güvenlik önlemlerinin gruplar arasında önemli düzeyde farklılaştığını göstermiştir. Bilgi güvenliğinden sorumlu personelin varlığının ve kurumsal bir bilgi güvenliği yönetim aracının kullanımı, üniversite kütüphanelerinin bilgi güvenliği yönetim süreçlerini daha iyi düzeyde izlemelerine, yönetmelerine ve geliştirmelerine

yardımcı olduğu görülmüştür. Bu iki faktör, üniversite kütüphanelerinin iyi bir bilgi güvenliği yönetimi uygulamasında etkili olduğunu göstermektedir. Nitelikli bir bilgi güvenliği personelinin görevlendirilmesinin ve iyi planlanmış bir kurumsal bilgi güvenliği yönetim rehberinin uygulanmasının üniversite kütüphanelerinin bilgi güvenliği yönetimine büyük katkı sağladığı çalışmadan elde edilen bulgular ile desteklenmektedir. Bu itibarla çalışmadan elde edilen bu sonuçlar üniveriste türüne bakılmaksızın Türkiye'de üniversite kütüphanelerinde bilgi güvenliği yönetim sistemi rehberine ihtiyaç olduğunu göstermiştir.

8.2. Öneriler

Çalışmanın sonucunda ulaşılan bulgulara ve sonuçlara bağlı olarak kütüphanecilik camiasında ve diğer kurumlarda etkili ve verimli bir bilgi güvenliği yönetim sürecini gerçekleştirilmesi amacıyla uygulama alanlarına ve gelecekte yapılacak çalışmalara yönelik birtakım önerilerde bulunulmuştur. Bu öneriler iki başlık altında sarılanmıştır:

8.2.1. Uygulayıcılara Yönelik Öneriler

- Çalışmada sunulan rehber önerisi, üniversite kütüphanelerindeki bilgi güvenliği risklerinin giderilmesi, ortadan kaldırılması, azaltılması; bilgi varlıklarının gizliliğini, bütünlüğünü ve erişebilirliğini ihlal edebilecek bilgi güvenliği tehditlerine karşı önlemlerin geliştirilmesi ve üniversitenin kurumsal düzeninin bozulmasına neden olabilecek kritik öneme sahip verilerin güvenliğinin sağlanması için tüm üniversite kütüphanelerinde standart bir BGYS rehberi olarak kullanılabilir.
- Üniversitelerde bilgi güvenliği yönetimine ilişkin altyapı ve finansal destek sağlanmalıdır.
- Çalışanların tamamının bilgi güvenliği yönetim faaliyetlerine dâhil edilmesi ve onların görüş ve önerilerinin dikkate alınması gereklidir.
- Bilgi güvenliğinden sorumlu personelin varlığı, bilgi güvenliği önlemlerinin etkin bir şekilde uygulanmasına katkı sağlamaktadır. Bu nedenle, üniversite kütüphaneleri, bilgi güvenliğinden sorumlu personel atamalarını artırmalı ve bu kişilere gerekli eğitim ve kaynakları sağlamalıdır.

- Tüm paydaşlarda bilgi güvenliği bilinci ve farkındalığını arttırıcı faaliyet ve eğitimler düzenlenmelidir.
- Bilgi güvenliği çalışmaların sadece yasal yükümlülükler nedeniyle değil, bu çalışmaların kurumsal bir kültür olarak hizmet kalitesinin arttırılması amacıyla gerçekleştirilmelidir.
- Kurumda bilgi güvenliği kültürünün yönetim tarafından önemsendiğinin ve benimsendiğinin tüm paydaşlara hissettirilmesi için gerekli çalışmaların yapılması gerekmektedir.
- Bilgi güvenliği yönetimine ilişkin hazırlan tüm dokümantasyon belgelerinin uygulanmasına yönelik takibin yapılması ve denetim ekibinin sürece en iyi biçimde hâkim olarak bu takibi üstlenmesi sağlanmalıdır.
- BGYS rehberinin uygulanmasına yönelik plan ve programlar düzenlenmelidir.
- YÖK, ÜNAK, ANKOS, TKD ve diğer birçok kurumsal ve sivil kuruluşların önderliğinde üniversite kütüphanelerinde bilgi güvenliği yönetimine ilişkin çalışmaların yapılması sağlanmalıdır. Bu anlamda konferans, sempozyum, etkinlik ve farklı türde çalışmaların planlanmalı ve yapılmalıdır.
- Bilgi güvenliği yönetim sisteminin günün şartlarına uygun olarak sürekli olarak iyileştirilmesi ve revize edilmesi gerekmektedir.
- Bilgi güvenliği yönetimi kurumsal ve teknolojik ana kategorileri altında dengeli bir biçimde yürütülmelidir.
- Yazılım güvenliği yönetim araçlarının kullanımını teşvik etmelidir. Bu araçlar, zararlı yazılım taraması, güvenlik açıkları analizi ve güncelleme yönetimi gibi önlemlerin etkin bir şekilde uygulanmasına yardımcı olabilir. Üniversite kütüphaneleri, bu araçların kullanımını teşvik ederek yazılım güvenliğini artırabilir.
- Üniversite kütüphanesi kullanıcılarının bilgi güvenliği farkındalık düzeylerini artırmaya yönelik güvenli internet kullanımı, güçlü şifreler oluşturma ve güvenlik açıklarını rapor etme gibi konularda düzenli eğitimler planlanmalıdır.
- Üniversite kütüphaneleri için kritik bir konu olan veri güvenliği ile ilgili politikalar, prosedürler ve idari araçlar oluşturulmalıdır.

- Güvenlik açıklarını tespit etmeye ve potansiyel saldırılara karşı koruma sağlamak amacıyla düzenli aralıklarla güvenlik testleri ve denetimler gerçekleştirmelidir. Bu testlerde elde edilen sonuçlar doğrultusunda gerekli düzeltici bilgi güvenliği önlemler alınmalıdır.
- Ulusal düzeyde iyi örnek bir bilgi güvenliği yönetim sistemi geliştirilerek pilot olarak bir kurumda uygulanması ve kademeli bir şekilde tüm kurumlara yaygınlaştırılmalıdır.
- Bilgi güvenliği ile ilgi çalışmaların önemsenmesi amacıyla personelin motivasyonunu arttırıcı ödüllendirme sistemi uygulanmalıdır.
- Bilgi güvenliği yönetim çalışmaları, kütüphanenin stratejik hedeflerine uyumlu şekilde yürütülmelidir.
- Bilgi güvenliği ile ilgili tüm çalışmaların ilgililerine anında duyurulmalı ve tüm paydaşların bilgi güvenliği yönetim sürecindeki uygulamalardan haberdar edilmelidir.

8.2.2. Araştırmacılara Yönelik Öneriler

Bu çalışma gelecekte bilgi güvenliği alanında çalışacak araştırmacılar için önemli olmanın yanı sıra, kütüphanecilik camiası ile diğer bilgi merkezlerinde yapılacak bilgi güvenliği çalışmaları için de faydalı olabileceği düşünülmektedir. Gelecekteki yapılacak araştırmalara metot olarak yol gösterici bir yapıya sahip temel bir çalışma özelliğine sahiptir. Bu bakımdan araştırmacılara yönelik şu öneriler sunulabilir:

- Bilgi güvenliği yönetimi geniş kapsamlı bir konu olduğundan bu konunun sadece bir boyutu üzerinde çalışmalar gerçekleştirilebilir.
- Bu çalışma yöntem olarak nitel ve karma araştırma yöntemleriyle de gerçekleştirilerek üniversite kütüphanelerinde bilgi güvenliği yönetimine ilişkin daha ayrıntılı bulgulara ulaşılabilir ve bulgulara göre daha farklı bilgi güvenliği çözüm önerileri geliştirilebilir.
- Bu çalışma üniversite kütüphaneleri dışındaki diğer kütüphane türlerinde de gerçekleştirilebilir ve bulgularına ilişkin karşılaştırmalar yapılarak kütüphane türleri arasındaki kurumsal bilgi güvenliği çalışmaları arasındaki farklılıklar çıkarılabilir.

- Bu çalışma üniversiteleri kapsayacak biçimde gerçekleştirilerek üniversitelerin bilgi güvenliği kültürü ve bilinci ile bu kurumların içerisinde hizmet veren kütüphanelerin bilgi güvenliği kültürü ve bilinci arasındaki etkileşim incelenebilir.
- Üniversite kütüphanelerinde bilgi güvenliği yönetim bilinci ve farkındalığına ilişkin durumun tespiti için personelin dışında kullanıcıların ve dış paydaşların görüşlerine başvurularak üniversite kütüphanelerindeki bilgi güvenliği farkındalığının dışarıya yansıması incelenebilir.
- Çalışmada kullanılan anket formu daha da geliştirilerek veya bilgi güvenliği yönetiminin sadece bir boyunda oluşturularak farklı bakış açılarına sahip araştırmalar yapılabilir.
- Çalışmada sunulan BGYS rehberi, yeni çalışmalarda kullanılarak rehberin geliştirilmesi ve güncellenmesine katkı sağlanabilir.
- Gelişmiş ve gelişmekte olan ülkeler arasındaki üniversite kütüphanelerinin bilgi güvenliği uygulamalarına ilişkin farklılıkları araştırmak için karşılaştırmalı çalışmalar yapılabilir.
- Kurumlarda bilgi güvenliği yönetimine ilişkin yeterli seviyelerde alt yapı ve mali desteğin verilip verilmediği ve sonuçlarının kurumlardaki bilgi güvenliği yönetim çalışmalarını nasıl etkilediğini araştıran çalışmalar yapılabilir.
- Bilgi merkezlerini kapsayan veya bilgi merkezlerinin sadece bir türüne yönelik siber güvenlik alanında çalışmalar yürütülebilir.
- Bilgi güvenliği okuryazarlığı, bilgi güvenliği bilinci, farkındalığı ve kültürü, kişisel güvenlik uygulamaları, anlık bilgi güvenliği uygulamaları, bilgi güvenliği altyapıları ve bilgi güvenliği hazırlıkları gibi önemli konularda çalışmalar yapılabilir.

KAYNAKÇA

Aggarwal, C. C. (2015). Data Classification. C. C. Aggarwal (Ed.), Data Mining: The Textbook içinde (ss. 285-344). Cham: Springer International Publishing. doi.10.1007/978-3-319-14142-8_10

Agrawal, R., Srikant, R. and Xu, Y. (2002, January). Database technologies for electronic commerce. In *VLDB'02: Proceedings of the 28th International Conference on Very Large Databases* (ss. 1055-1058). Morgan Kaufmann.

Akdoğan, Z. (2022). *Kamu kurumlarında bilgi güvenliği yönetim sistemleri için politika geliştirme metodolojisi* [Yüksek lisans tezi, Ankara Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Akpınar, H. (2009). Enformasyon Teknolojilerinde İş Sürekliliği Yönetimi ve Felaket Planlaması. *Risk Yönetiminde Başarı Faktörü "İş Sürekliliği Yönetimi" içinde* (ss. 175 – 185). İstanbul Teknik Üniversitesi Yayını.

Akpınar, T. ve Öğütoğulları, E. (2016). Ohsas 18001 iş sağlığı ve güvenliği yönetim sistemi. *Balkan ve Yakın Doğu Sosyal Bilimler Dergisi, 2*(03), 97-104. http://ibaness.org/bnejss/2016_02_03/012_teoman_akpinar_new.pdf adresinden erişildi.

Aksakallı, İ. K. (2019). Bulut bilişimde güvenlik zafiyetleri, tehditleri ve bu tehditlere yönelik güvenlik önerileri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *5*(1), 8-34. doi.org/10.18640/ubgmd.544054

Aksu, P. K. (2014). *Hastane bilgi yönetim sisteminin bilgi güvenliği açısından değerlendirilmesi* [Yüksek lisans tezi, Marmara Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Alemdaroglu, A. (2020). Çalışanların bilgi güvenliği farkındalığına ilişkin algıları: Bankacılık sektöründe bir araştırma. (Yüksek lisans tezi). YÖK Tez Kataloğu veri tabanından erişildi.

Alımcı, E. (2022). Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi. *Ankara Barosu Dergisi, 80*(1), 47-76. doi.org/10.30915/abd.1118300

Altunışık, R., Coşkun, R., Bayraktaroğlu, S., ve Yıldırım, E. (2019). *Sosyal bilimlerde araştırma yöntemleri: SPSS uygulamalı*. Sakarya yayıncılık.

American Library Association [ALA]. (2006). Resolution on the retention of library usage records. 2006 ALA Annual Conference https://alair.ala.org/handle/11213/1594 adresinden wrişildi.

American National Standards Institute (ANSI). (2015). *Approved american national standards*. Washington, DC, USA.

Amini, M., Vakilimofrad, H. ve Saberi, M. K. (2021). Human factors affecting information security in libraries. *The Bottom Line*, *34*(1), 45-67. doi.org/10.1108/BL-04-2020-0029

Anameriç, H. (2003). *kütüphanelerde yönetim bilgi sistemleri ve bir model önerisi*. (Yüksek lisans tezi). YÖK Tez Kataloğu veri tabanından erişildi.

Anameriç, H. (2005). Bilgi merkezlerinin yönetiminde bilgi sistemlerinin rolü. *Bilgi Dünyası, 6*(1), 15-35. doi.org/10.15612/BD.2005.445

Anderson, R. J. (2008). *Security engineering: a guide to building dependable distributed systems.* John Wiley & Sons.

Andersson, D., Reimers, K. Ve Barreto, C. (2014). Post-secondary education network security: results of addressing the end user challenge. In *INTED2014 Proceedings* (pp. 6018-6027). IATED.

Ardıç, M. ve Dulkadir, B. (2018). Bilgi yönetiminin önemi ve süreçleri. In S. Nart & Y.T. Yıldırım (Eds.), In *Current debates in management & organization* (pp. 27-40) London: IJOPEC Publication Limited. doi:10.5281/zenodo.1291882

Aslandağ, K. (2010) *Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisine dair bir uygulama* [Yüksek lisans tezi, Gebze Yüksek Teknoloji Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Association of College and Research Libraries(ACRL). (2016). Framework for information literacy for higher education. Retrieved from http://www.ala.org/acrl/standards/ilframework adresinden erişildi.

Aslay, F., Çam, H. ve Özen, Ü. (2019). Yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin ölçümlenmesi. *Yönetim Bilişim Sistemleri Dergisi, 5*(2), 1-11. https://dergipark.org.tr/en/pub/ybs/issue/51328/637041 adresinden erişildi.

Avcı, Ü. ve Oruç, O. (2020). Investigation of the students' personal cyber security behaviour and ınformation security awareness. *Inonu University Journal of the Faculty of Education, 21*(1), 284-303. doi:10.17679/inuefd.526390

Aydın, Ö. (2022). *Bilgisayar sistemlerinde güvenlik ve gizlilik*. Efe Akademi Yayınları.

Barnard, L. and Von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security*, *19*(2), 185-194. doi.org/10.1016/S0167-4048(00)87829-3

Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., and Widup, S. (2021). Data breach investigations report. *Verizon DBIR Team, Tech. Rep*, 6-8.

Başdinkçi, N. (2017). *Sağlık kurumlarında bilgi güvenliği risk değerlendirilmesi ve kullanıcıların bilgi güvenliği farkındalık düzeyinin ölçülmesi* [Yüksek lisans tezi, Çukurova Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Berghel, H. (2005). The two sides of ROI: return on investment vs. risk of incarceration. *Communications of the ACM*, *48*(4), 15-20. https://dl.acm.org/doi/fullHtml/10.1145/1053291.1053305 adresinden erişildi.

Bertino, E. ve Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and secure computing*, *2*(1), 2-19. doi:10.1109/TDSC.2005.9

Bilge, L. ve Dumitras, T. (2013). Investigating zero-day attacks. *Login*, *38*(4), 6-13. https://www.usenix.org/system/files/login/articles/02_bilge_6-13_online.pdf adresinden erişildi.

Bingöl, C. (2010). *ISO 27001 Bilgi güvenliği yönetim sistemi otomasyonu.* [Yüksek lisans tezi, Sakaraya Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Bisbey, R., ve Hollingworth, D. (1978). Protection analysis: Final report ISI/SR-78-13. *USC/Information Sciences Institute*.

Bishop, M. (2002). *Computer security: Art and science.* Boston: Addison-Wesley Professional.

Bishop, M. (2005). *Introduction to computer security.* Addison-Wesley.

Blokdyk, G. (2020). *ISO IEC 27000 a complete guide* (2021 Edition). 5STARCooks.

Bond, S. ve Yuk, P. K. (2018). *Uber to pay record $148m to settle 2016 data breach claims.* Financial Times. https://www.ft.com/content/7fa7100c-c1a7-11e8 adresinden erişildi.

Broady-Preston, J. ve Felice, J. (2006). Customers, relationships and libraries: University of Matla – a case study. *Aslib Proceedings: New Information* Perspectives, 58(6), 525-36. https://www.emerald.com veritabanından erişildi.

Brooks, T. (2009). World wide web consortium (W3C). In *Encyclopedia of library and information sciences* (pp. 5695-5699). CRC Press.

Büthe, T. (2010). Engineering uncontestedness? The origins and institutional development of the International Electrotechnical Commission (IEC). *Business and Politics*, *12*(3), 1-62. doi: https://doi.org/10.2202/1469-3569.1338

Büyüköztürk Ş. (2011). *Sosyal bilimler için veri analizi el kitabı*. Pegem Akademi

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş., ve Demirel, F. (2022). *Bilimsel araştırma yöntemleri* (32. Baskı). Pegem Akademi Yayıncılık.

Calder, A. (2018). *NIST cybersecurity framework: A pocket guide*. IT Governance Publishing Ltd.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi, 9*(3), 165-174. https://dergipark.org.tr/en/pub/politeknik/issue/33021/367110 adresinden erişildi.

Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. *Kalem Uluslararası Eğitim ve İnsan Bilimleri Dergisi, 11*(2), 651-679. DOI: 10.23863/kalem.2021.219 adresinden erişildi.

CEN. (2022). European Committee for standardization. european standardization. https://www.cencenelec.eu/european-standardization/cen-and-cenelec/ adresinden erişildi.

CENELEC. (2022). European committee for electrotechnical standardization. european standardization. https://www.cencenelec.eu/european-standardization/cen-and-cenelec/ adresinden erişildi.

Ceylan, H. (2020). *Türkiye`de bilgi güvenliği algısının istatistiksel analizi.* (Yüksek lisans tezi) YÖK Tez Kataloğu veri tabanından erişildi.

Chopra, A. ve Chaudhary, M. (2020). *Implementing an ınformation security management system: security management based on ISO 27001 guidelines*. Berkeley, CA: Apress L.P. https://link.springer.com/book/10.1007/978-1-4842-5413-4 adresinden erişildi

Classified National Security Information. (2009). *U.S. department of justice, the president executive order 13526*, 29 December 2009. https://www.archives.gov/isoo/policy-documents/cnsi-eo.htm adresinden erişildi.

Cleveland Jr, A. B. (1999). Harvesting the value of information. *Journal of Management in Engineering*, *15*(4), 37-42. https://ascelibrary.org/doi/abs/10.1061/(ASCE)0742-597X(1999)15:4(37) adresinden erişildi.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). New Jersey: Rublede.

Corrall, S. ve Sriborisutsakul, S. (2010). Evaluating intellectual assets in university libraries: A multi-site case study from Thailand. *Journal of Information & Knowledge Management*, *9*(03), 277-290. doi.org/10.1142/S021964921000267X.

Cosic, Z. ve Boban, M. (2010, September). Information security management—Defining approaches to Information Security policies in ISMS. In *IEEE 8th International Symposium on Intelligent Systems and Informatics* (pp. 83-85). IEEE. doi:10.1109/SISY.2010.5647216

Coşkun, R., Altunışık, R. ve Yıldırım, E. (2019). *Sosyal bilimlerde araştırma yöntemleri: SPSS uygulamalı,* (10. baskı.). Sakarya Yayıncılık.

Crocker, S. D. (2019). The Arpanet and its impact on the state of networking. *Computer*, *52*(10), 14-23. Doi:10.1109/MC.2019.2931601

Cui, Y. ve Widom, J. (2003). Lineage tracing for general data warehouse transformations. T*he VLDB Journal*, *12*(1), 41-58. doi.org/10.1007/s00778-002-0083-8

Çakır, H., Tuğ, E. ve Adak, Ş. F. (2014). Bilişim güvenliği tedbirleri ve tkdk kurumunda uygulama örneği. *Bilgi Teknolojileri Dergisi*, *7*(1), 11-17. https://dergipark.org.tr/en/pub/gazibtd/issue/6630/88000 adresinden erişildi.

Çalık, O. (2013). *ISO 27001:2013 bilgi güvenliği yönetim sistemi standardındaki değişiklikler ve yenilikler*. http://www.bilgiguvenligi.gov.tr adresinden erişildi.

Çam, S. (2020). *Güvenlik duvarı ve sanal özel ağ çözümlerinin ağ performansına etkilerinin incelenmesi* (Yüksek lisans tezi, Trakya Üniversitesi). YÖK Tez Kataloğu veri tabanından erişildi.

Çek, E. (2017). *Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi* [Yüksek lisans tezi, İstanbul Bilgi Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Çelik, A. ve Şimşek, M. Ş. (2013). *Yönetim ve organizasyon*. Konya:Eğitim Yayınevi.

Çelik, M. (2019). Üniversite kütüphanelerinde bilgi güvenliği yönetimi: *Bir araştırma. Uluslararası Yükseköğretim Kongresi Bildiriler Kitabı* içinde (ss192-201). Ankara: YÖK.

Çelik, S. (2000). Üniversite kütüphaneleri: Amaç, görev, işlev, yönetim ve örgüt yapısı.*Doğuş Üniversitesi Dergisi*,*1*(2), 52-62. https://dergipark.org.tr/en/pub/doujournal/issue/66643/1042795 adresinden erişildi.

Çetinkaya, M. (2008). *Bilgi güvenliği yönetim sistemi altyapısının değerlendirilmesi için bir test aracı geliştirilmesi.* [Doktora tezi, İstanbul Kültür Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi..

Çınar, S. M. ve Yıldırım, A. (2020). Bir kurumsal geniş alan ağının ağ yönetim sistemiyle etkili yönetimi. *Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi, 9*(1), 9-22. doi.org/10.28948/ngumuh.611668

Çimen, Z.(2021). *Sağlık kurumlarında bilgi güvenliği ve çalışan görüşleri: Ankara ili özel hastane örneği* (Tez No: 706585) [Yüksek lisans tezi, Ankara Hacı Bayram Veli Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2018). *Sosyal bilimler için çok değişkenli istatistik: SPSS ve LISREL uygulamaları* (5. Baskı). Ankara: Pegem Akademi.

Çubukçu, F. (2018). *Bilgi güvenliği yönetim sistemi: ıso27001:2013 Uygulama kılavuzu*. İstanbul: Pusula.

Da Veiga, A. ve Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29(2),* 196-207. https://doi.org/10.1016/j.cose.2009.09.002

Deering, S. E. (1993). SIP: Simple Internet Protocol. *IEEE bassetork, 7*(3), 16-28. doi:10.1109/65.224022

Demirok, E. (2016). *Kurumsal bilgi güvenliği yönetim sistemi; vakıf üniversitesi örneği* [Yüksek lisans tezi, Okan Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Denning, D. E. (1999). *Information Warfare and Security*. Addison-Wesley.

Derdiyok, T. (2019). Üniversitelerde kalite güvence sistemi kapsamında PUKÖ yönetim döngüsü uygulamasında bir model önerisi. *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *8*(15), 173-198. https://dergipark.org.tr/en/pub/ufuksbedergi/issue/57470/815068 adresinden erişildi.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management, *Journal of Information Security, 4* (2), 92-100. https://serwiss.bib.hs-hannover.de adresinden erişildi.

Döner, S. (2022). *Üniversite öğrencilerinin bilgi güvenliği farkındalık düzeylerinin belirlenmesi: Hitit Üniversitesi örneği.* (Yüksek lisans tezi) YÖK Tez Kataloğu veri tabanından erişildi

Dursun, İ. ve Alnıaçık, Ü. (2019). Likert ölçeklerinde seçenek etiketleme kararları: kullanılan etiketler ölçüm sonuçlarını etkiler mi?. *Journal of social sciences/sosyal bilimler dergisi*, *33*. doi.org/10.14520/adyusbd.549447

Eisenberg, J. and Lawthers, C. (2008). *Library Computer and Network Security: Library Security Principles.* Infopeople Project.

Elattresh, J. A. M. (2022). *Bilgi güvenliği hizmet yönetimi: Bilgi güvenliği yönetimine bir hizmet yönetimi yaklaşımı ve bir kurumun müşterinin memnuniyeti ve güvenirliği üzerindeki etkisi* [Yüksek lisans tezi, Kastamonu Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Epstein, L. G. and Schneider, M. (2008). Ambiguity, information quality, and asset pricing. *The Journal of Finance*, *63*(1), 197-228. doi.org/10.1108/03074800110696979

Erdoğan, İ. (2012). *Pozitivist metodoloji ve ötesi: Araştırma tasarımları, niteliksel ve istatiksel yöntemler* (3. Baskı). Ankara: Erk Yayımları. http://irfanerdogan.com/kitaplar/metod2012.pdf adresinden erişildi.

Eren, A. (2021). *Bilgi güvenliği yönetim sisteminin yükseköğretim kurumlarında sürdürülebilirliğinin incelenmesi* [Yüksek lisans tezi, Ankara Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Ernst and Young, L. L. P. (2002). *Global information security survey2002* http://www.ey.com/global/download.nsf/ adresinden erişildi.

Erol, S. E. (2016). *Siber güvenlik farkındalığı için yetenek tabanlı dinamik model* (Tez No: 449489) [Yüksek lisans tezi, Gazi Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Ersoy, E. (2012). *ISO/IEC 27001 bilgi güvenliği standardı- tanımlar ve örnek uygulamalar*. ODTÜ Yayıncılık

Eşitti, B. (2018). Nicel araştırma yöntemleri: SPSS uygulamalı. D. A. Arslan (Ed), *Sosyal bilimlerde araştırma yöntem ve teknikleri* içinde(ss.307-340). Çanakkale: Paradigma Akademi Yayınları

ETSI (2022), *Search & browse standards*. European Telecommunications Standard Institute. https://www.etsi.org/standards adresinden erişildi.

Evrin, V. ve Demirer, M. (2011). Kurumsal bilgi güvenliği süreç çalışmaları: ISO/IEC-27001 örneği. *IV. Ağ ve bilgi güvenliği sempozyumu el kitabı* içinde (ss. 25-30). Ankara: TMMOB Elektrik Mühendisleri Odası Yayınları. https://elektrik.gen.tr/sites/default/files/3529111f1499a55ek.pdf#page=25 adresinden erişildi.

Fakeh, S. K. W. Zulhemay, M. N., Shahibi, M. S., Ali, J. ve Zaini, M. K. (2012). Information security awareness amongst academic librarians. *Journal of applied sciences research*, *8*(3), 1723-1735. https://www.researchgate.net adresinden erişildi..

Fidan, H. (2016). İktisadi açıdan bilgi kavramı ve bilgi kavramına yaklaşımlar üzerine bir inceleme. *Süleyman Demirel Üniversitesi Vizyoner Dergisi, 4*(9), 94-104. https://dergipark.org.tr/en/pub/vizyoner/issue/23008/246061 adresinden erişildi.

Filik, T. (2020). *Tıbbi sekreterlerde bilgi güvenliği farkındalık düzeyinin elektronik sağlık kayıtlarının güvenlik ve mahremiyet uygulamalarına etkisinin değerlendirilmesi* [Yüksek lisans tezi, Kayseri Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Filip, F. G. (2019). Management information systems: managing the digital firm eneth C. Laudon and Jane P. Laudon (Eds.). In *International Journal of Computers Communications & Control* (ss. 103-105.). Pearson

Fister, B. (2010). Critical Assets: Academic Libraries, a View from the Administration Building. *Library Journal*, *135*(8), 24-27. https://eric.ed.gov/?id=EJ930071 adresinden erişildi.

Fister, B. (2010). Critical Assets: Academic Libraries, a View from the Administration Building. *Library Journal*, *135*(8), 24-27. https://eric.ed.gov/?id=EJ930071 adresinden erişildi.

Fox, E. and ElSherbiny, N. (2011). Security and digital libraries. K. H. Huang (Ed.), *Digital Libraries-Methods and Applications* içinde (ss. 151-160). Published by im Tech.

Freeze, R. D. and Kulkarni, U. (2007). Knowledge management capability: defining knowledge assets. *Journal of Knowledge management*, 11(6), 94-109. doi/10.1108/13673270710832190

Fraenkel, J. R. and Wallen, N. E. (2006). *How to desing and evaluate research in education.* McGaw-Hill

Furnell, S. M. (2007). *Computer ınsecurity: Risking the system.* Springer Science & Business Media.

Fussell, R. S. (2005). Protecting information security availability via self-adapting intelligent agents. MILCOM 2005-2005 IEEE Military Communications Conference içinde (ss. 2977-2982). doi: 10.1109/MILCOM.2005.1606116

Gallacher, L. ve Morris, H. (2012). *ITIL foundation exam study guide*. John Wiley & Sons.

Ganbat, O. (2013). *Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması.* [Yüksek lisans tezi, Ege Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Gao, C. (2016, May). A study on strategies to improve the protection of personal information for university libraries users. In *2016 International Conference on Applied System Innovation (ICASI)* (pp. 1-3). IEEE. doi:10.1109/ICASI.2016.7539952

Gazdağı, O. ve Çetinyokuş, T. (2020). Bankacılık sektöründe bilgi güvenliği ve iş sürekliğinin sağlanması amacıyla ISO/IEC 27001 ve ISO 22301 standartlarının uygulanmasına yönelik kavramsal inceleme. *Journal of Humanities and Tourism Research*, *10*(2), 475-491. https://dergipark.org.tr/en/pub/johut/issue/55645/761090 adresinden erişildi.

Gemci, C. (2010). *Uzman sistem temelli bilgi güvenliği yönetim sistemi.* (Tez No:278481) [Doktora Tezi, Gazi Üniversitesi].YÖK Tez Kataloğu veri tabanından erişildi.

Gemici, E. ve Yılmaz, H. (2019). Güvenlik Stratejileri ve Yönetimi Açısından Havacılık Güvenliği. *Journal of aviation*, *3*(1), 15-27. doi.org/10.30518/jav.550123

Gencer, K. (2015). ISO 27001 Kapsamında kurumsal bilgi güvenliğine dinamik bir yaklaşım. [Yüksek lisans tezi, Afyon Kocatepe Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Genç, C. (2019). *Kişisel verilerin korunması kapsamında bilgi güvenliği farkındalığı analizi ve e-devlet yapısının incelenmesi* (Tez No: 584130) [Yüksek lisans tezi, İstanbul Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

George, D. and Mallery, M. (2010). *SPSS for windows step by step: a simple guide and reference, 17.0 update* (10nd ed.). Londra: Pearson Education Limited.

Gillaspy, M. L. (2005). Factors affecting the provision of consumer health ınformation in public libraries: The last five years. Mays, Tammy L. (Eds.), *In Introduction to Library Trends 53 (3) Winter 2005: Consumer Health Issues, Trends, and Research, Part 2: Applicable Research in the 21st Century* (pp. 480-495) Illinois library. https://www.ideals.illinois.edu/handle/2142/1738 adresinden erişildi.

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. (2022). *T.C. Resmi Gazete*, 31821, 26 Nisan 2022.

Grampp, F. T. ve Morris, R. H. (1984). The UNIX system: UNIX operating system security. *AT&T Bell Laboratories Technical Journal*, *63*(8), 1649-1672. doi.org/10.1002/j.1538-7305.1984.tb00058.x

Guo, L. ve Congdon, P. (2021). IEEE 802 nendica report: ıntelligent lossless data center networks. *IEEE SA Industry Connections–IEEE 802 Nendica Report: Intelligent Lossless Data Center Networks,* 1-44. https://ieeexplore.ieee.org/iel7/9457236/9457237/09457238.pdf adresinden erişildi.

Gupta, B. B. Arachchilage, N. A., and Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*, 247-267. http://hdl.handle.net/10125/41681 adresinden erişildi.

Güden, O. (2019). Küresel kuruluşların kriz yönetimi ve iletişimi süreçlerine yönelik bir değerlendirme: Facebook & Cambridge Analytica veri skandalının retoriksel arena kuramı bağlamında incelenmesi. *Galatasaray Üniversitesi İletişim Dergisi,* (31), 209-231. http://iletisimdergisi.gsu.edu.tr/en/download/article-file/905337 adresinden erilşildi

Güldüren, C. (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi* (Tez No: 396156) [Yüksek lisans tezi, İstanbul Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Güldüren, C., Çetinkaya, L. ve Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online*, *15*(2). doi.org/10.17051/io.2016.27218

Güler, C. ve Furat, F. (2022). Belge yönetimi ve arşiv uygulamalarının bilgi güvenliği ilkelerine katkısı: Kavramsal bir değerlendirme. *Türk Kütüphaneciliği, 36*(1), 74-89. doi.org/10.24146/tk.1012325

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği* [Yüksek lisans tezi, Yıldız Teknik Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Gülseçen, S. (2012). *Bilgi ve bilginin yönetimi*. Papatya Yayıncılık.

Gündüzalp, C. (2021). Üniversite Çalışanlarının Dijital Veri ve Kişisel Siber Güvenlik Farkındalıkları: Bilgi İşlem Daire Başkanlıkları Örneği. *Journal of Computer and Education Research, 9*(18), 598-625. doi.org/10.18009/jcer.907022

Güngör, M. (2015). *Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma*. [Uzmanlık tezi, T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı]. http://www.bilgitoplumu.gov.tr/ adresinden erişildi.

Güriş, S. ve Astar, M. (2014). *Bilimsel araştırmalarda SPSS ile istatistik.* İstanbul: Der yayınları. https://hdl.handle.net/11446/471 adresinden erişildi.

Gürsel, T. (2019). *Sigorta şirketlerinde bilgi güvenliği yönetim sistemi denetimi* [Yüksek lisans tezi, Marmara Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Güveli, A. (2006). İstatistik Bilgi Sistemleri ve SESRTCIC Örneği. *Bilgi Dünyası*, *7*(1), 49-62. doi.org/10.15612/BD.2006.396

Hagg, A. (2002). Benchmark report: BCP in 2002. *Contingency Planning and Management, 7 (5).*

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E. ve Tatham, R. L. (2013). *Multivariate data analysis*: Pearson Education Limited.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E. ve Tatham, R. L. (2013). *Multivariate data analysis: Pearson new ınternational edition* (7nd ed.). Pearson Education Limited.

Haklı, T. (2012). *Bilgi güvenliği standartları ve kamu kurumları bilgi güvenliği için bir model önerisi*. [Yüksek lisans tezi, Süleyman Demirel Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Haklı, T. (2012). *Bilgi güvenliği standartları ve kamu kurumları bilgi güvenliği için bir model önerisi* (Tez No: 330848) [Yüksek lisans tezi, Süleyman Demirel Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & Security, 83*, 354-366. doi.org/10.1016/j.cose.2019.02.012

Henkoğlu, T. ve Uçak, N. Ö. (2015). Üniversite kütüphanelerinde kişisel verilerin korunması. *Bilgi Dünyası, 16*(1), 45-74. doi.org/10.15612/BD.2015.472

Henkoğlu, T. (2015). *Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi* [Yüksek lisans tezi, Hacettepe Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Henkoğlu, T. (2022). Sosyal ağ platformlarının bilgi politikalarına ilişkin gizlilik algısı: kullanıcı bilgi davranışının değerlendirilmesi. *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi, 20*(02), 149-168. https://www.ceeol.com/search/article-detail?id=1082741 adresinden erişildi.

Hook, L. ve Kuchler, H. (2017). *Uber hid massive data breach from passengers and regulators.* Financial Times. https://www.ft.com/content/ed66a21a-cf0e adresinden erişildi.

Hu, W., Chang, C. H., Sengupta, A., Bhunia, S., Kastner, R. ve Li, H. (2020). An overview of hardware security and trust: Threats, countermeasures, and design tools. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *40*(6), 1010-1038. https://ieeexplore.ieee.org/abstract/document/9310331 adresinden erişildi.

IEEE. (2022). IEEE Standards Association Operations Manual. New York, ABD: Institute of Electrical and Electronics Engineers. https://standards.ieee.org/about/policies/sa-opman/ adresinden erişildi.

IFLA ve Kuhlenkamp, H. (2015*). IFLA Internet Manifest 2014*. IFLA publications.

IFLA. (2012). *IFLA code of ethics for librarians and other ınformation workers.* International Federation of Library Associations. https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment adresinden erişildi.

IFLA. (2015). *IFLA statement on privacy in the library environment.* International Federation of Library Associations. https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment/ adresinden erişildi.

Igure, V. M. ve Williams, R. D. (2008). Taxonomies of attacks and vulnerabilities in computer systems. *IEEE Communications Surveys & Tutorials*, *10*(1), 6-19. doi:10.1109/COMST.2008.4483667

International Organization for Standardization. (2015). *Quality management systems — Fundamentals and vocabulary* (ISO Standard No. 9000:2015). https://www.iso.org/standard/45481.html adresinden erişildi.

International Organization for Standardization. (2016). *Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation* (ISO Standard No. 27004:2016). https://www.iso.org/standard/64120.html adresinden erişildi.

International Organization for Standardization. (2017). *Information technology - Security techniques - Information security management systems — Guidance* (ISO Standard No. 27003:2017). https://www.iso.org/standard/63417.html adresinden erişildi.

International Organization for Standardization. (2018). *Information technology - Security techniques - Information security management systems - Overview and vocabulary* (ISO Standard No. 27000:2018). https://www.iso.org/standard/73906.html adresinden erişildi.

International Organization for Standardization. (2022a). *Information security, cybersecurity and privacy protection - Information security management systems - Requirements* (ISO Standard No. 27001:2022). https://www.iso.org/standard/27001 adresinden erişildi.

International Organization for Standardization. (2022b). *Information security, cybersecurity and privacy protection - Information security controls* (ISO Standard No. 27002:2022). https://www.iso.org/standard/75652.html adresinden erişildi.

International Organization for Standardization. (2022c). *Information security, cybersecurity and privacy protection - Guidance on managing information security risks* (ISO Standard No. 27005:2022). https://www.iso.org/standard/80585.html adresinden erişildi.

International Organization for Standardization. (2022c). *Information technology — Security techniques - Requirements for bodies providing audit and certification of information security management systems* (ISO Standard No. 27006:2015). https://www.iso.org/standard/62313.html adresinden erişildi.

International Telecommunication Union [ITU] (2020). Telecommunication standardization sector of ITU: Manual for rapporteurs and editors. Cenevre, İsviçre: International Telecommunication Union. https://www.itu.int/oth/T0A0F00002C/ adresinden erişildi.

Irmak, H. ve Baz, F. (2019). Kurumsal bilgi güvenliği tehditler ve alınması gereken önlemler üzerine bir inceleme, 2. *Uluslararası Mardin Artuklu Bilimsel Araştırmalar Kongresi, Sosyal ve Beşerî Bilimler Kitabı* içinde (ss. 333 -341).

ISACA. (2018). *COBIT 2019 Framework: Introduction and methodology*. schaumburg, USA: Isaca.

ISACA. (2019). *COBIT 5 Implementation -Supplemental Tools and Materials.* USA: ISACA.

ISACA. (2022). *IT Audit Framework (ITAF),* (4th ed.). https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko91EAC adresinden erişildi.

Ismail, R. (2012). *Assessing information security management in Malaysian academic libraries* [Doctoral dissertation, University of Malaya]. The Universiti Malaya Research Repository. http://studentsrepo.um.edu.my/5537/ adresinden erişildi.

Ismail, R. ve Zainab, A. N. (2013). Information systems security in special and public libraries: an assessment of status. *arXiv preprint arXiv:1301.5386*. doi.org/10.48550/arXiv.1301.5386

İlçin, E. T., Adak, Ş. F. ve Çakır, H. (2014). Bilişim güvenliği tedbirleri ve tkdk kurumunda uygulama örneği. *Bilgi Teknolojileri Dergisi*, *7*(1), 11-17. https://dergipark.org.tr/en/pub/gazibtd/issue/6630/88000 adresinden erişildi.

İlhan, K., Fatih, E., Orhan, Y. ve Abdülkadir, Ş. (2020). IoT ağ güvenliği için 802.1 x, DMZ ve SSL-VPN birleştirme tabanlı etkili bir güvenlik yöntemi. *Acta Infologica*, *4*(2), 65-76. doi :10.26650/acin.779547

İslamoğlu, A. H. ve Alnıaçık, Ü. (2019). *Sosyal bilimlerde araştırma yöntemleri,* (6. baskı.). İstanbul: Beta Yayıncılık.

İslamoğlu, A. H. ve Alnıaçık, Ü. (2019). *Sosyal bilimlerde araştırma yöntemleri.* (6.bs). İstanbul: Beta Yayınevi.

Jaeger, L. ve Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429-472. doi.org/10.1111/isj.12317

Jaquıer, J. J. (1990). ETSI-European telecommunications standards ınstitute-ınstitut européen de normalisation dans le domaine des télécommunications. I: Historique, mission, structure et méthodes de travail. *Technische Mitteilungen PTT*, *68*(7), 276-284.

Jin, Y. (2015). Introduction to hardware security. *Electronics, 4*(4),763-784. doi.org/10.3390/electronics4040763.

Jones, A. (2006). The ınformation security forum. *ınfosecurity today*, *3*(6), 38-40. doi.org/10.1016/S1742-6847(06)70483-9

Jones, A., and Ashenden, D. (2005). *Risk management for computer security: Protecting your network and information assets*. Elsevier.

Jouini, M., Rabai, L. B. A. ve Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496. doi.org/10.1016/j.procs.2014.05.452

Kaiser, F. M. (2008). *Protection of classified ınformation by congress: practices and proposals.* Washington DC: Library Of Congress, Congressional Research https://apps.dtic.mil/sti/citations/ADA483582 adresinden erişildi.

Kaplan, Tuncay (2013). *Kablosuz ağlarda güvenlik ve güncel güvenlik önlemleri.* [Yüksek lisans tezi, Haliç Üniversitesi]. https://acikbilim.yok.gov.tr/handle/20.500.12812/89135 adresinden erişildi.

Kara, M. (2018). *Kurumsal Bilgi Güvenliği: Teknik ve Yönetimsel Yönleriyle*. İstanbul: Papatya Yayıncılık

Karaarslan, E., Teke, A. ve Şengonca, H., (2003). Bilgisayar ağlarında güvenlik politikalarının uygulanması. *İletişim Günleri V Bildiriler Kitabı* içinde (ss. 74-81). TMMOB EMO İzmir Şubesi,

Karakaş, S. (1991). Bilim dalı olarak enformasyon. *Türk Kütüphaneciliği, 5*(1), 3-8. http://www.tk.org.tr/index.php/TK/article/view/1210 adresinden erişildi.

Karasar, N. (2019).*Bilimsel araştırma yöntemi: Kavramlar ilkeler teknikler. Ankara:* Nobel Yayınları

Karie, N. M., Sahri, N. M., Yang, W., Valli, C. ve Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, *9*, 121975-121995. doi:10.1109/ACCESS.2021.3109886

Kaur, J. ve Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781. https://www.sciencedirect.com/science/article/pii/S1319157821000203 adresinden erişildi.

Kazandır, Z. B. (2011). *Anlamsal web tabanlı kütüphane bilgi sistemi* [Yüksek lisans tezi, Gazi Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Kemiksiz, R. C. (2022) Kişisel veri güvenliği üzerine bir alan araştırması: dijital yerliler ve dijital göçmenlerin güvenlik algıları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, *9*(1), 64-91. https://dergipark.org.tr/en/pub/iled/issue/71183/1111856 adresinden erişildi.

Keser, H. ve Yayla, H. G. (2021). Fatih projesi uygulanan okullardaki öğretmenlerin bilgi güvenliği farkındalık düzeylerinin incelenmesi. *Milli Eğitim Dergisi*, *50*(229), 9-40. https://dergipark.org.tr/en/pub/milliegitim/issue/60215/874360 adresinden erişildi.

Keser, H. ve Güldüren, C. (2015). Bilgi güvenliği farkindalik ölçeği (BGFÖ) geliştirme. *Kastamonu Eğitim Dergisi*, *23*(3), 1167-1184. https://dergipark.org.tr/en/pub/kefdergi/issue/22598/241397 adresinden erişildi.

Keseroğlu, H. S. (2005). Kütüphanenin tözü: tarih öncesi dönemde bilgi. *Türk Kütüphaneciliği, 19*(3), 297-307. https://dergipark.org.tr/tr/pub/tk/issue/48945/624324 adresinden erişildi.

Keseroğlu, H. S. (2010). Bilginin bilgisi: Kütüphane ve bilgibilim kuramı sorunsalı. *Türk Kütüphaneciliği, 24*(4), 685-704. https://dergipark.org.tr/en/pub/tk/issue/48858/622486 adresinden erişildi

Keskinkılıç, A. G. M. (2011). Bilgi otomasyonu ve bir kütüphane bilgi sistemi ana modülü üzerine prototip uygulaması. S*ystem*, *2*(3). https://silo.tips/download/bilgi-otomasyonu-ve-bir-ktphane-bilgi-sistemi-ana adresinden erişildi.

Khan, A., Ibrahim, M. ve Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. *International Journal of Information Management Data Insights*, *1*(2), doi.org/10.1016/j.jjimei.2021.100015

Kılıç, Ö. ve Yılmaz, İ. (2017). Türkiye'de üniversite kütüphanelerinde bilgi güvenliği yönetimi ve açık erişim sistemleri. *Kastamonu Üniversitesi Kastamonu Eğitim Dergisi, 25*(1), 253-264. doi.org/10.24146/tk.811003

Kim, D. ve Solomon, M. G. (2018). *Fundamentals of information systems security* (3nd ed.). Jones & Bartlett Learning.

Knapp, K. J., Maurer, C. ve Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education*, *28*(2), 101. http://jise.org/Volume28/n2/JISEv28n2p101.html adresinden erişildi.

Kostagiolas, P. A. ve Asonitis, S. (2009). Intangible assets for academic libraries: Definitions, categorization and an exploration of management issues. *Library Management*, *30*(6/7), 419-429. https://www.emerald.com veritabanından erişildi.

Köksoy, F. (2020). Avrupa birliği'nin siber güvenlik politikası: kurumsalcılık mı tutarlılık mı? *Güvenlik Stratejileri Dergisi, 16*(35), 635-674. https://www.ceeol.com/search/article-detail?id=901334 adresinden erişildi.

Krosnick, J. A. ve Fabrigar, L. R. (1997). Designing rating scales for effective measurement in surveys. In L. Lyberg, P. Biemer, M. Collins, L. Decker, E. DeLeeuw, C. Dippo, N. Schwarz & D. Trewin (Eds.), *Survey Measurement and Process Quality* (pp. 141-164). Wiley-Interscience. doi.org/10.1002/9781118490013.ch6

Krosnick, J. A. ve Presser, S. (2010). Questionnaire design. In P. V. Marsden & J. D. Wright (Eds.), *Handbook of Survey Research,* (2nd Ed.). Bradford: Emerald Group Publishing.

Kuchler, H. (2014). *Home Depot attack bigger than Target's.* Financial Times. https://www.ft.com/content/7f9a2b26-3f74-11e4-984b-00144 adresinden erişildi.

Kuchler, H. (2014a). *Home depot attack bigger than target's*. Financial Times. https://www.ft.com/content/7f9a2b26-3f74-11e4-984b-00144feabdc0 adresinden erişildi.

Kuchler, H. (2017). *Yahoo says 2013 cyber breach affected all 3bn accounts.* Financial Times. https://www.ft.com/content/9412c2b0-a87c-11e7-93c5-648314d2c72c adresinden erişildi.

Kurt, H. Ö. (2019). *Kurumlarda bilgi güvenliği yönetimi: Hastane bilgi sistemleri üzerine bir araştırma* (Tez No: 557979) [Yüksek lisans tezi, Necmettin Erbakan Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Kurt, S. G. (2019). *Bilgi güvenliğinin bilgi işlem çalışanları tarafından değerlendirilmesi – Sağlık sektöründe bir çalışma* (Tez No: 566816) [Yüksek lisans tezi, Marmara Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Külcü, Ö. (2000). Kuramsal bilginin oluşumu ve toplumsal bilgiye dönüşümünde epistemoloji bilgi hizmetleri ilişkisi I. *Türk Kütüphaneciliği, 14*(4), 386-411. http://www.tk.org.tr/index.php/tk/article/view/669 adresinden erişildi.

Lev, B. (2001), *Intangibles: Measurement, management and reporting,* Washington, DC: .Brookings Institution Press,

Lim, J. S., Chang, S., Maynard, S. ve Ahmad, A. (2009). *Exploring the relationship between organizational culture and ınformation security culture*. Proceedings of the 7th Australian Information Security Management Conference, 1st to 3rd December 2009 Perth içinde (ss. 88-97). doi: 10.4225/75/57b4065130def

Maiwald, E. (2004). *Fundamentals of network security.* USA: Burr Ridge: McGraw Hill Professional.

Marttin, V. ve Pehlivan, İ. (2010). ISO 27001:2005 Bilgi güvenliği yönetimi standardı ve türkiye'deki bazı kamu kuruluşu uygulamaları üzerine bir inceleme. *Mühendislik Bilimleri ve Tasarım Dergisi, 1 (1)*, 49-56. https://dergipark.org.tr/en/pub/jesd/issue/20866/223911 adresinden erişildi.

McCumber, J. (1991). Information systems security: A comprehensive model. *In Proceedings of the 14th National Computer Security Conference* (pp. 328-337). Baltimore, Maryland, USA: National Institute of Standards and Technology. http://csrc.nist.gov/publications/history/nissc/1991-14th-NCSC-proceedings-vol-1.pdf adresinden erişildi.

McCumber, J. (2004). *Assessing and managing security risk in IT systems: A Structured Methodology* (1nd Ed.). Boca Raton: Auerbach Publications. https://doi.org/10.1201/9780203490426 adresinden erişildi.

McGinn, H. F. (1994). Information assets. *The Bottom Line*, *7*(2), 40-41. doi.org/10.1108/eb025416

Mead, N. R., Shoemaker, D. ve Woody, C. (2013). Principles and measurement models for software assurance. *International Journal of Secure Software Engineering (IJSSE)*, *4*(1), 1-10. doi.10.4018/jsse.2013010101

Meral, S.(2022). *Kamu kurumlarının bilgi güvenliği politikalarının kurumsal bilgi güvenliğinin sağlanması açısından etkinliğinin analiz edilmesi* (Tez No: 751107) [Yüksek lisans tezi, Gazi Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Mete, H. (2010). *SO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bilgi işlem merkezlerinde uygulanması* [Yüksek lisans tezi, Sakarya Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Mishkin, S. and Kuchler, H. (2014, 21 Mayıs). *Ebay reveals cyber attack on database.* Financial Times. https://www.ft.com/content/41a20592-e0f5-11e3-a934-00144feabdc0 adresinden erişildi.

Missier, P., Lalk, G., Verykios, V., Grillo, F., Lorusso, T. ve Angeletti, P. (2003). Improving data quality in practice: a case study in the italian public administration. *Distributed and Parallel Databases*, *13*, 135-160. https://link.springer.com/article/10.1023/A:1021548024224 adresinden erişildi.

Morris, R. ve Thompson, K. (1979). Password security: A case history. *Communications of the ACM, 22*(11), 594-597. doi.org/10.1145/359168.359172

Muharremoğlu, G. (2013). *Kurumsal bilgi güvenliğinde zafiyet, saldırı ve savunma öğelerinin incelenmesi* [Yüksek lisans tezi, İstanbul Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Murgia, M. ve Neville, S. (2017). *NHS was an easy target in global hacking attack*. Financial Times. https://www.ft.com/content/5f45ad06-373c-11e7-99bd adresinden erişildi.

Nachtigal, S. (2009). *E-business ınformation systems security design paradigm and model* (Doctoral dissertation, University of London). https://citeseerx.ist.psu.edu/document adresinden erişildi.

Nayak, U. ve Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security*. Apress.

NIST. (2022a). *NIST publications.* National Institute of Standards and Technogy. https://www.nist.gov/standardsgov/resources/publications adresinden erişildi.

NIST. (2022b). *NIST SP 800 Özel yayınlar*. National Institute of Standards and Technogy. https://www.nist.gov/standardsgov/resources/publications adresinden erişildi.

Nicolas-Rocca, T. S. ve Burkhard, R. J. (2019). Information security in libraries: Examining the effects of knowledge transfer. *Inf. Technol. Libr.(ital)*, *38*(2), 58-71. doi:10.6017/ital.v38i2.10973

North Atlantic Council. (2002). *Security within the north atlantic treaty organization* (Revision 1 C-M 49). Brüksel: North Atlantic Treaty Organization

Nyst, C. ve Falchetta, T. (2017). The Right to Privacy in the Digital Age. *Journal of Human Rights Practice, 9*(1), 104-118. doi.org/10.1093/jhuman/huw026

O'brien, J. A. ve Marakas, G. M. (2006). *Management information systems* (Vol. 6). New York, USA: McGraw-Hill Irwin.

Odabaş, H. (2003). Kurumsal bilgi yönetimi. *Türk Kütüphaneciliği, 17*(4), 357-368. http://eprints.rclis.org/7436/1/64a.pdf adresinden erişildi.

Odabaş, H. (2005). Bilgi yönetimi sistemi. *Bilgi çağı bilgi yönetimi ve bilgi sistemleri* içinde. Çizgi Kitabevi.

Oliveira, S. R., ve Zaiane, O. R. (2002, December). Privacy preserving frequent itemset mining. In *Proceedings of the IEEE ICDM workshop on privacy, security and data mining* (ss.43-54). https://webdocs.cs.ualberta.ca/ adresinden erişildi.

Oluwabunmi, T. ve Madukoma, E. (2022). Information security awareness and ınformation security Compliance in University Libraries in South-West, Nigeria. *Library Philosophy & Practice*. https://web.s.ebscohost.com veritabanından erişildi.

Onaran, B. (2019). *Hastane bilgi sistemlerinin önemi ve özel bir hastane çalışanları üzerinde uygulama* [Yüksek lisans tezi, İstanbul Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Öner, N. (2015). *Bilginin serüveni.* İstanbul: Divan Kitap

Özbilgin, İ. G. ve Özlü, M. (2010). Yazılım geliştirme süreçleri ve ISO 27001 Bilgi *Güvenliği. Akademik Bilişim, 16*. https://ab.org.tr/ab10/bildiri/51.pdf adresinden erişildi.

Özdemir, A. ve Uluyol, Ç. (2019). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, *25*(3), 649-666. doi.org/10.20296/tsadergisi.815635

Özkaya, E., Sarıca, R. ve Durmaz Ş. (2019). *Siber güvenlik: Saldırı & savunma stratejileri.* Buzdağı Yayınları

Özkılıç, Ö. (2005). *İş sağliği ve güvenliği, yönetim sistemleri ve risk değerlendirme metodolojileri*. TİSK Yayınları,

Öztemiz, S. ve Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası, 14*(1), 87-100. doi.org/10.15612/BD.2013.136

Paneva-Marinova, D., Goynov, M., ve Luchev, D. (2017). Multimedia digital library as a constructive block in ecosystems for digital cultural assets. *Digital Presentation and Preservation of Cultural and Scientific Heritage*, *7*, 31-40. https://www.ceeol.com/search/article-detail?id=560880 adresinden erişildi.

Paşaoğlu, C., Güler, H. ve Jafari, M. (2019). Ağ tabanlı veri sızıntısı tespiti ve önlenmesi üzerine bir inceleme. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, *3*(2), 79-92. doi.org/10.33461/uybisbbd.611768

Pathari, V. ve Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security, 20(4)*, 264-280. https://doi.org/10.1108/09685221211267648

Pattanaik, B. B. ve Viswakarma, S. (2014). Set up an online content management system to display press clips at central library, Jawaharlal Nehru University: A strategic approach. *International Journal of Information*, *6*(3), 74-82.

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). New York: Sage Publications. doi.org/10.1002/nur.4770140111

Peltier, T. R. (2016). *Information security policies, procedures, and standards: guidelines for effective information security management*. CRC press.

Phelps, D. C. (2005). Information system security: Self-efficacy and security effectiveness in Florida libraries. (Doctoral dissertation) https://search.proquest.com/ adresinden erişildi.

Pipkin, D. (2000). *Information security: Protecting the global enterprise* (1st ed.). Upper Saddle River, N.J: Prentice Hall.

Planning the ARPANET: 1967-1968. (2021).*The history of computer communications.* https://history of computer communications. info/section/4.7/planning-the-arpanet-1967-1968/ adresinden erişildi.

Polat, E. (2022). *Kurumsal bilgi güvenliğinin örgütsel iletişim, örgütsel bilgi paylaşımı ve kişisel bilgi güvenliği farkındalığı açısından değerlendirilmesi*.(Doktora tezi) YÖK Tez Kataloğu veri tabanından erişildi.

Radack, S. (2004). *Federal information processing standard (fips) 199, standards for security categorization of federal information and information systems* (No. ITL Bulletin March 2004). National Institute of Standards and Technology. https://www.nist.gov/ adresinden erişildi.

Redwine, S. T. (2006). *Software assurance: A guide to the common body of knowledge to produce, acquire and sustain secure software,* (version 1.1.) Washington, DC: US Department of Homeland Security.

Reeds, J. A. ve Weinberger, P. J. (1984). The UNIX system: File security and the UNIX system crypt command. *AT T Bell Laboratories Technical Journal, 63*(8), 1673-1683. doi.org/10.1002/j.1538-7305.1984.tb00059.x

Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. (2014). *T.C. Resmi Gazete,* 31151, 10 Haziran 2020.

Riebe, T., Kaufhold, M. A., ve Reuter, C. (2021). The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An empirical study. *Proceedings of the ACM on Human-Computer Interaction, 5(*CSCW2), 1-30. doi.org/10.1145/3479865.

Ritchie, D. M. (1979a,). 'On the Security of UNIX. *UNIX Supplementary Documents.* https://www.krsaborio.net/unix/research/acrobat/770610.pdf adresinden erişildi.

Ritchie, D. M. (1979b, 16 Ocak). Protection of data file contents. https://patents.google.com/patent/US4135240A/en adresinden erişildi.

Rudasill, L. and Moyer, J. (2004). Cyber-security, cyber-attack, and the development of governmental response: the librarian's view. *New library world*, *105*(7/8), 248-255. doi.org/10.1108/03074800410550995

Saltzer, J. H. ve Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278-1308. doi: 10.1109/PROC.1975.9939

SANS Institute. (2021, Ağustos 17). *Information security policy templates*. (2021). https://www.sans.org/information-security-policy/?category=general adresinden erişildi.

Sanz-Calcedo, J. G., González, A. G., López, O., Salgado, D. R., Cambero, I. ve Herrera, J. M. (2015). Analysis on integrated management of the quality,

environment and safety on the industrial projects. *Procedia Engineering*, *132*, 140-145. doi.org/10.1016/j.proeng.2015.12.490

Schell, R. R., Downey, P. J. ve Popek, G. J. (1973). *Preliminary Notes on the Design of Secure Military Computer Systems*. https://apps.dtic.mil/sti/citations/ADA089433 adresinden erişildi.

Schlienger, T. ve Teufel, S. (2003). Information security culture: From analysis to change. *South African Computer Journal, 31*, 46-52. https://hdl.handle.net/10520/EJC27949 adresinden erişildi.

Schneier, B. (2015). *Secrets and lies: Digital security in a networked world.* John Wiley & Sons.

Sebesta, R. W. (2002). *Programming the world wide web*. Addison-Wesley Longman Publishing.

Security Through Education (2021, Eylü 12). *Social engineering defined.* https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/ adresinden erişildi.

Seferoğlu, S. S., Yıldız Durak, H., Karaoğlan Yılmaz, F. ve Yılmaz, R. (2018). Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme. B. Akkoyunlu, A. İşman, H. F.Odabaşı (editörler),*Eğitim Teknolojileri Okumaları* içinde. (ss.29-43). Pegem Akademi Yayıncılık

Shaaban, A. M., Kristen, E. ve Schmittner, C. (2018). Application of IEC 62443 for IoT components. In *computer safety, reliability, and security: SAFECOMP 2018 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Västerås, Sweden, September 18, 2018,* (pp. 214-223). Springer International Publishing.

Shirey, R. W. (1994). *Security architecture for ınternet protocols. A Guide for protocol designs and standards.* Internet Draft. https://www.academia.edu/2293392/ adersinden erişildi.

Siberay (2021, Temmuz 22). Sosyal mühendislik. (2021, 22 Temmuz). https://www.siberay.com/sosyal-muhendislik adresinden erişildi.

Slade, R. (2006). *Dictionary of information security*. United Kingdom: Syngress Publishing.

Smith, R. E. (2019). *Elementary information security*. Jones & Bartlett Learning.

Solmaz, E. E. (2022). Büyük veri hırsızlıkları ve potansiyel tehditler. G. Alpar ve G. Durmaz (eds.) U*luslararası Sistemin Yarattığı Sorunlar Ve Çözüm Yolları, 30-31 Mayıs, Ankara* içinde (ss. 29-38). Ankara: Stratejik Düşünce Enstitüsü Yayınları

Solomon, M. G. ve Chapple, M. (2004). *Information security ılluminated.* Jones & Bartlett Publishers.

Stewart, J. M., Tittel, E., ve Chapple, M. (2005). *CISSP: Certified Information Systems Security Professional Study Guide*. John Wiley & Sons.

Stoneburner, G., Goguen, A. ve Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800* (30), 800-30. http://www.icsdefender.ir/ adresinden erişildi.

Suganthy, A. ve Maiti, M. (2014). Information security evolution, ımpact and design factors. *International Journal of Computer Applications, 100*, 14-19. doi:10.5120/17496-8028

Sumner, M. (2009). Information security threats: a comparative analysis of impact, probability, and preparedness. *Information Systems Management*, *26*(1), 2-12. http://eprints.rclis.org/7436/ adresinden erişildi.

Sundt, C. (2006). Information security and the law. *Information Security Technical Report*, *11*(1), 2-9. doi.org/10.1016/j.istr.2005.11.003

Sweeney, L. (2002). K-anonymity: A model for protecting privacy. *International journal of uncertainty, fuzziness and knowledge-based systems*, *10* (05), 557-570. doi.org/10.1142/S0218488502001648

Swiderski, F. ve Snyder, W. (2004). *Threat Modeling* (1st ed.). Redmond, Wash: Microsoft Press.

Syafrizal, M., Selamat, S. R. ve Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417-432. https://www.academia.edu/download/78607584/426.pdf adresinden erişildi.

Syahputra, A., Ulina, P. T., Muda, I., Sjuchro, D. W. ve Atmanegara, A. W. (2021). The role of ınformation systems auditing and control association (ISACA) as an ınstitution for ınformation systems auditors, establishing an ethical code for auditors and holder of ısaca certificates. In *Intelligent and Reliable Engineering Systems* (pp. 188-192). CRC Press.

Şahinaslan, E. (2010). *Standartlara dayalı bilgi güvenliği risk analiz ve ölçümleme metodolojisinin bankacılık sektörüne özgü modellenmesi ve uygulama yazılımının geliştirilmesi* [Yüksek lisans tezi, Trakya Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim*, *9*, 11-13. https://www.guvenliweb.org.tr/dosya/cCvJ7.pdf adresinden erişildi.

Şişkin, D. Ş.(2020). *Üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin korunması: Ankara'daki üniversite kütüphanelerinin değerlendirilmesi* (Tez No: 620913) [Yüksek lisans tezi, Hacettepe Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi [CBDDO] (2020). *Bilgi ve iletişim güvenliği rehberi* (Sürüm No: 2020/1,0). T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. https://cbddo.gov.tr/bgrehber adresinden erişildi.

Tabachnick, L.S. and Fidell (2013). *Using Multivariate Statistics* (8nd ed.). Boston: Pearson.

Taherdoost, H. (2022). Understanding cybersecurity frameworks and ınformation security standards-a review and comprehensive overview. *Electronics*, *11*(14), 2181. doi.org/10.3390/electronics11142181

Takçı, H., Akyüz, T., Alper, U., Karabağ, R., Aktaş, F. Ö. ve Soğukpınar, İ. (2010). Bilgi güvenliği yönetiminde risk değerlendirmesi için bir model. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, *3*(1), 47-52. https://dergipark.org.tr/en/pub/tbbmd/issue/22242/238773 adresinden erişildi.

Tamdoğan, O. G. (2009). Enformasyon zincirinde bilgi erişim sistemleri, bilgi erişim sürecinde kütüphane kurumu ve diğer bilgi merkezleri. *Türk Kütüphaneciliği*, *23*(1), 151-168. https://dergipark.org.tr/en/pub/tk/issue/48930/624189 adresinden erişildi.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Doğa Bilimleri Dergisi*, *11*(1), 132-137. https://dergipark.org.tr/en/pub/ksudobil/issue/35406/393310 adresinden erişildi.

Thomson, K. L., Von Solms, R. ve Louw, L. (2006). Cultivating an organizational information security culture. *Computer fraud & security*, *2006*(10), 7-11. https://doi.org/10.1016/S1361-3723(06)70430-4

Tofan, D. C. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, *3*(3), 128-135. http://jmeds.eu/index.php/jmeds/article/view/Information-Security-Standards adresinden erişildi.

Tofan, D. C. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, *3*(3), 128-135.

Tok, H. (2010). *Kamu kurumları için bilgi güvenliği yönetişim modeli* [Yüksek lisans tezi, Gebze Yüksek Teknoloji Enstitüsü]. YÖK Tez Kataloğu veri tabanından erişildi.

Tonta, Y. (2004). Bilgi yönetiminin kavramsal tanımı ve uygulama alanları. *Kütüphaneciliğin Destanı Sempozyumu 21-24 Ekim 2004, Ankara* içinde. https://www.openaccess.hacettepe.edu.tr/xmlui/handle/11655/11631 adresinden erişildi.

TSE. (2021). *2022 yılı performans programı.* Ankara: Türk Standardları Estitüsü. https://statik.tse.org.tr//upload/tr/dosya/dokumanyonetimi/107/07032022184613-1.pdf adresinden erişildi.

Türk Dil Kurumu [TDK] (2021). Güvenlik. *Güncel Türkçe sözlüğünde*. Erişim tarihi: 18 Ocak 2021, https://sozluk.gov.tr/

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu [TÜBİTAK] (2013). *Bilgi güvenliği yönetimi rehberi: işletim ve bakım.* Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi [BİLGEM] Yazılım Teknolojileri Araştırma Enstitüsü. *https://dijitalakademi.bilgem.tubitak.gov.tr* adresinden erişildi.

Türkiye İstatistik Kurumu. (2022). *Kütüphane istatistikleri,2021* (Sayı: 45700). Sosyal İstatistikler Daire Başkanlığı, Türkiye İstatistik Kurumu. https://data.tuik.gov.tr/ adresinden erişildi.

Twentyman, J. (2015). Fear of reputational damage after security leaks may be overhyped. Financial Times. https://www.ft.com/content/b6395d84-cc8f-11e4-b5a5-00144feab7de adresinden erişildi.

United States Government Department of Defense. (1985). *Department of defense trusted computer system evaluation criteria*. The Orange Book: University of Michigan Library.

Vaast, E. (2007). Danger is in the eye of the beholders: social representations of information systems security in healthcare. *The Journal of Strategic Information Systems*, *16*(2), 130-152. doi.org/10.1016/j.jsis.2007.05.003

Vacca, J. R. (2012). *Computer and information security handbook*. Elsevier.

Vaidya, J. ve Clifton, C. (2002, July). Privacy preserving association rule mining in vertically partitioned data. In *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 639-644). https://doi.org/10.1145/775047.775142

Van Oorschot, P. C. (2020). *Computer security and the ınternet*. Springer International Publishing.

Volonino, L., Robinson, S. R. ve Volonino, C. P. (2004). *Principles and practice of information security: protecting computers from hackers and lawyers*. Pearson/Prentice Hall.

Vorakulpipat, C., Siwamogsatham, S. ve Pibulyarojana, K. (2010, July). Exploring information security practices in Thailand using ISM-Benchmark. In *PICMET 2010 technology management for global economıc growth* (pp. 1-4). IEEE. https://ieeexplore.ieee.org/abstract/document/5603346 adresinden erişildi.

Vural, Y. (2018). Veri mahremiyeti: saldırılar, korunma ve yeni bir çözüm önerisi. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *4*(2), 21-34. doi.org/10.18640/ubgmd.517767

Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *23*(2), 507-522. https://dergipark.org.tr/en/pub/gazimmfd/issue/6676/88512 adresinden erişildi.

Wang, J. (2009). *Computer network security: Theory and practice* (2009th ed.). Berlin : Beijing: Springer.

Ware, W. H. (1979). *Security controls for computer systems: Report of Defense Science Board Task Force on Computer Security.* https://apps.dtic.mil/sti/citations/ADA076617 adresinden erişildi.

Ware, W. H. (2009). *RAND and theiinformation evolution: A History in essays and vignettes* (Illustrated edition.). Santa Monica, CA: RAND Corporation.

Web Application Security Consortium (WASC). (2007). The WASC Threat Classification v2.0 report (reference). https://help.hcltechsw.com/appscan/Enterprise/10.1.0/topics/r_wasc_threat_classifications_report.html adresinden erişildi.

White, L. N. (2007a). Unseen measures: the need to account for intangibles. *The Bottom Line*, *20*(2), 77-84. doi.org/10.1108/08880450710773011

White, L. N. (2007b). Imperfect reflections: The challenges in implementing human capital assessment in libraries. *The Bottom Line*, *20*(4), 141-147. doi.org/10.1108/08880450710843969

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91-95. doi.org/10.1145/859670.859675

Whitman, M. E. ve Mattord, H. J. (2011). *Roadmap to information security: For IT and infosec managers*. Boston: Cengage Learning.

Whitman, M. E. ve Mattord, H. J. (2018). *Principles of information security* (8nd ed.). Boston: Cengage Learning.

Whitman, M. E. ve Mattord, H. J. (2019). *Management of ınformation security*. Boston: Cengage.

Wilkes, M. V. (1975). *Time-sharing computer systems* (3rd edition.). London: New York: Elsevier Science Ltd.

Wood, C. C. (1997). Part of the foundation for secure systems: Separation of duties policy. *Information Management & Computer Security, 5*(1), 18-19. doi.org/10.1108/09685229710167999

Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security, 2004*(1), 16-17. doi.org/10.1016/S1361-3723(04)00019-3

Workman, M., Bommer, W. H. ve Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. https://doi.org/10.1016/j.chb.2008.04.00

Yanarışık, O. (2020). İç güvenlik ve siber güvenlik. İ. İrdem(ed.) *Güvenlik Yönetimi ve Polislik* içinde (ss.303-327). Ankara: Polis Akademisi Yayınları.

Yavuz, A. ve Gürkan, T. (2019). Bilgi güvenliği tehditleri: yazılım tanımlı ağlar geleneksel bilgisayar ağlarına karşı. *Kırklareli Üniversitesi Mühendislik ve Fen Bilimleri Dergisi*, *5*(2), 200-209. doi.org/10.34186/klujes.643437

Yazıcı, A. ve Sener, C. (2003). Computer and information sciences. *ISCIS 2003: 18th International Symposium, Antalya, Turkey, November 3-5, 2003*, Proceedings. Springer.

Yazıcıoğlu, Y. ve Erdoğan, S. (2014). *Bilimsel araştırma yöntemleri-SPSS uygulamalı* (4. baskı.). Ankara: Detay Yayıncılık.

Yeh, Q. J. and Chang, A. J. T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, *44*(5), 480-491. doi.org/10.1016/j.im.2007.05.003

Yıldırım, B. F. (2019). Sağlığın kişiselleşmesi ve kişisel sağlık bilgi sistemleri. *Bilgi Yönetimi*, *2*(2), 127-135. doi.org/10.33721/by.642698

Yıldız, R. (2022). *ISO/IEC 27001 bilgi güvenliği yönetim sistemleri gereksinimlerinin veri tabanı sistemlerinde uygulanması* (Tez No: 759643) [Yüksek lisans tezi, İstanbul Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Yontar, E. (2000). Norbert Elias'ın insan bilimleri kavramı ve bilgi sosyolojisi. *Toplum ve Bilim, 84*, 112-128. https://iletisim.com.tr/dergiler/toplum-ve-bilim/3/sayi-84-2000-84-bahar-2000/9954 adresinden erişildi.

Yusuf, A., Yusuf, S. ve Zayyana, H. M. (2021). Assessment of information security threats to information systems in Federal University Libraries, Nigeria. *Samaru Journal of Information Studies*, *21*(1), 38-47. https://www.ajol.info/index.php/sjis/article/view/217870 adresinden erişildi.

Yükseköğretim Kurulu.[YÖK] (2022, Kasım). *2022-2023 öğretim yılı yükseköğretim istatistikleri*. Yükseköğretim Bilgi Yönetim Sistemi, Yükseköğretim Kurulu. https://istatistik.yok.gov.tr/ adresinden erişildi.

Yüksel, Z. (2007). *Ağ güvenliği ve güvenlik duvarında VPN ve NAT uygulamaları*. [Yüksek lisans tezi, Yıldız Teknik Üniversitesi]. YÖK Tez Kataloğu veri tabanından erişildi.

Zhang, W. (2006). Digital library intellectual property right evaluation and method. *The Electronic Library*, 25(3), 267-73. https://www.emerald.com veritabanından erişildi.

EKLER

EK-1. 1: Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi Anket Formu

Sayın Katılımcı,

LÜTFEN BU DÖKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ.

Sizi Ali KAVAK tarafından yürütülen "Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi ve Ulusal Model Önerisi" başlıklı **araştırmaya** davet ediyoruz. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz. Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya **katılmama** veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır.

Ali KAVAK

Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Bölümü Doktora Öğrencisi

Çalışmaya İlişkin Anahtar Terimler:

Bilgi Sistemleri: Bilginin toplanması, işlenmesi, saklanması, iletilmesi, görüntülenmesi, yayılması ve düzenlenmesi için tüm altyapı, organizasyon, personel ve bileşenleri ifade eder.

Bilgi Varlığı: Kurumun iş süreçleri için değer taşıyan elektronik veya basılı bilgiler, donanımlar, yazılımlar, internet ve yerel iletişim ağları, fiziksel mekân ve ortamlar, hizmetler, imaj /itibar, insan gibi somut ve soyut şeylerdir.

Kritik Bilgi / Veri: Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesinin kuruma çok ciddi maddi veya manevi zarar vereceği her türlü bilgi/veri.

Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğini sağlamak.

Gizlilik: Bilginin yetkisiz kişilerin erişimine karşı korunması.

Bütünlük: Bilginin tam ve doğru olma durumun korunması.

Erişebilirlik / Kullanabilirlik: Bilgini yetkili kişilerce erişilebilir ve kullanılabilir durumda olması.

Tehdit: Bilgi sistemlerine olumsuz etkisi olabilecek her türlü eylemi, durumu veya olayı ifade eder.

Önlem: Bilgi sistemleri tehditlerini önlemek için uygulanan teknik ve kurumsal eylemleri ifade eder.

Teknolojik Önlemler: Bilgi erişimini korumak, kontrol etmek veya bir bilgi sistemi üzerinden aktarılan verilerin yetkisiz erişimini önlemek için uygulanan donanım, yazılım, ağ, veri ve fiziki teknik mekanizmalardır.

Kurumsal Önlemler: Bilginin bütünlüğünü, gizliliğini ve kullanılabilirliğini korumak, güvenlik bilincinin oluşturmak ve sürdürmek için uygulanan politikalar, prosedürler, idari araçlar ve yöntemlerdir.

Bölüm I: Demografik ve Temel Bilgi Güvenliği Soruları

1- Cinsiyetiniz:

a) Kadın b) Erkek

2- Eğitim durumunuz:

a) İlköğretim / Ortaöğretim b) Ön lisans c) Lisans d) Lisansüstü (Yüksek Lisans/Doktora)

3- Üniversite tahsili varsa son mezuniyet programınız:

a) Bilgi ve Belge Yönetimi /Kütüphanecilik/Arşivcilik/Dokümantasyon ve Enformasyon

b) Bilgisayar / Bilişim / Yazılım ile ilgili bir programlardan herhangi biri

c) Diğer (Lütfen yazınız: . . . . .)

4- Göreviniz:

a) Daire Başkanı c) Öğretim Görevlisi e) Bilgisayar İşletmeni / Bilgi İşlem Uzmanı

b) Şube Müdürü d) Kütüphaneci f) Diğer personel (Lütfen yazınız: . . . . .)

5- Çalıştığınız üniversitenin statüsü:

a) Devlet Üniversitesi b) Vakıf Üniversitesi

6- Üniversite kütüphanelerindeki toplam iş tecrübeniz:

(Lütfen yazınız: . . . . . .yıl)

7- Kütüphanenizde bilgi güvenliği veya bilgi sistemleri güvenliğinden sorumlu personel var mı?

a) Var b) Yok c) Fikrim Yok

8- Kütüphanenizde kullanıcıların kullanımına verilen bilgisayar (lar) var mı?

a) Var b) Yok

9- Kütüphanenizde kullanıcılara sağlanan internet hizmeti var mı?

a) Var b) Yok

10- Lütfen kütüphanenizde kullanılan bilgi sistemlerini belirtiniz.

(Birden fazla seçenek işaretleyebilirsiniz.)

a) Kütüphane Otomasyon Sistemi
b) Veritabanı Erişim ve İstatistik Sistemi
c) Kütüphanelerarası İşbirliği Takip Sistemi (KİTS)
d) Türkiye Belge Sağlama Sistemi (TÜBESS)
e) Açık Erişim Sistemleri
f) Kütüphane Üyelik Bilgi Sistemleri
g) Ulusal Kimlik Doğrulama Sistemleri (Yetkim vb.)
h) İntihal Yazılımları (Turnitin, Ithanticate vb.
i) Diğer (Lütfen yazınız: . . . . .)

11- İşlenen verinin / bilginin kritikliği açısından kütüphanenizdeki bilgi sistemlerinin değeri / önemi nedir?

a) Çok Düşük b) Düşük c) Orta d) Yüksek e) Çok Yüksek f) Fikrim Yok

12- Bilgi güvenliği yönetimi sürecinde standart, politika, prosedür, rehber gibi kurumsal araç ve yöntemler kullanılmakta mıdır?

a) Evet b) Hayır c) Fikrim Yok

13- İşlenen veya depolanan <u>en kritik bilginin</u> açığa çıkması ve yetkisiz kişilerce ele geçirilip ifşa edilmesi durumunda; (Sadece bir seçenek işaretleyiniz!)

a) Herhangi bir zarar oluşmaz.

b) Sadece kütüphane hizmetlerini ve çıkarlarını etkileyecek zararlar gelir.

c) Üniversite çıkarlarına saygınlık derecesinde zararlar gelir fakat telafisi mümkündür.

d) Üniversite çıkarlarına yaşamsal zararlar gelir ve telafisi mümkün değildir.

14- İşlenen veya depolanan <u>en kritik bilginin</u> içeriğinin yetkisiz kişilerce değiştirilerek bütünlüğünün bozulması durumunda; (Sadece bir seçenek işaretleyiniz!)

a) Herhangi bir zarar / olumsuzluk oluşmaz.

b) Sadece kütüphane hizmetlerini ve çıkarlarını etkileyecek zararlar gelir.

c) Üniversite çıkarlarına saygınlık derecesinde zararlar oluşur fakat telafisi mümkündür.

d) Üniversite çıkarlarında yaşamsal zararlar oluşur ve telafisi mümkün değildir.

15- Bir bilgi güvenliği ihlali meydana geldiğinde bilgi sistemlerine veya varlıklarına erişimde hoş görülebilecek devre dışı kalma süresi en fazla ne kadar olur?

a) 1 saatten az b) 1 ile 8 saatten az c) 8 ile 24 saatten az d) 24 saatten fazla

16- Bilgi varlıklarınızın işlediği verinin / bilginin gizlilik, bütünlük ve erişebilirlik unsurlarının tamamını veya bir kısmını etkileyecek olası en kötü senaryoya sahip bir bilgi güvenliği ihlali meydana geldiğinde, söz konusu olay kütüphanenizin <u>kurumsal yapısını hangi seviyede etkiler?</u>

a) Çok Düşük b) Düşük c) Orta d) Yüksek e) Çok Yüksek f) Fikrim Yok

17- Bilgi varlıklarınızın işlediği verinin / bilginin gizlilik, bütünlük ve erişebilirlik unsurlarının tamamını veya bir kısmını etkileyecek olası en kötü senaryoya sahip bir bilgi güvenliği ihlali meydana geldiğinde, söz konusu olay <u>toplumsal yapıyı hangi seviyede etkiler?</u>

a) Çok Düşük b) Düşük c) Orta d) Yüksek e) Çok Yüksek f) Fikrim Yok

18- Bilgi varlıklarınızın işlediği verinin / bilginin gizlilik, bütünlük ve erişebilirlik unsurlarının tamamını veya bir kısmını etkileyecek olası en kötü senaryoya sahip bir bilgi güvenliği ihlali meydana geldiğinde, söz konusu olay <u>kütüphanecilik camiasını hangi seviyede etkiler?</u>

a) Çok Düşük b) Düşük c) Orta d) Yüksek e) Çok Yüksek f) Fikrim Yok

19- Bilgi varlıklarınızın işlediği verinin / bilginin gizlilik, bütünlük ve erişebilirlik unsurlarının tamamını veya bir kısmını etkileyecek olası en kötü senaryoya sahip bir bilgi güvenliği ihlali meydana geldiğinde, söz konusu olay, entegre çalışan dış paydaşlara ait bilgi varlıklarını hangi <u>seviyede etkiler?</u>

a) Çok Düşük b) Düşük c) Orta d) Yüksek e) Çok Yüksek f) Fikrim Yok

20- Kütüphanenizde karşılaşılan veya karşılaşılması olası en yaygın tehdit gurubu nedir?

a) Donanım b) Yazılım c) Ağ d) Veri e) Fiziksel / Çevresel f) İnsan / Diğer

21- Kütüphanenizde karşılaşılan veya karşılaşması olası yaygın tehditler nelerdir?

(Birden fazla seçenek işaretleyebilirsiniz.)

a) Yetkisiz donanım / yazılım kurulumu ve kullanımı

b) Parola saldırıları, çözümleme, çalma

c) Bilgi sistemi arızası ve bakım hatası

d) Bilgi sistemlerini hackleme

e) Yanlış güncelleme, depolama veya yedekleme

f) İletişim hataları (dedikodu, dinleme, yalan vb.)

g) Donanım hırsızlığı, sabotaj ve kasıtlı imha

h) Kimlik doğrulama saldırıları /

i) Virüs, solucan, Truva atı gibi kötü yazılımlar

j) Kimlik hırsızlığı ve dolandırıcılığı tehditleri

k) Reklam, parazit, hırsız ve casus yazılım tehditleri

l) Binaya izinsiz giriş ve yetkisiz erişim tehditleri

m) Uzaktan yönetim aracı saldırıları

n) Doğal afetlere veya hava olaylarına bağlı tehditler

o) E-posta saldırıları

p) Fiziksel belge / evrak / dosya hırsızlığı veya ifşası

q) Web saldırıları

r) Kasıtlı / kasıtsız personel suiistimalleri

Bölüm II: Teknolojik Önlemlerin Varlık / Uygulanma Düzeyini Ölçen Maddeler

22- Aşağıda teknolojik önlemlere (donanım, yazılım, ağ, veri ve fiziksel-çevresel önlemler) ilişkin maddeler bulunmakta olup bu önlemlerin kütüphanenizde uygulanma düzeyini yansıtan en uygun seçeneği (√) işaretleyiniz.

Teknolojik Önlemlerin Varlık / Uygulanma Düzeyi **Yok / Hiç:** Maddede belirtilen önlem yok ve uygulanamamaktadır **Çok Kötü:** Maddede belirtilen önlem var ve çok kötü düzeyde uygulanmaktadır **Kötü:** Maddede belirtilen önlem var ve kötü düzeyde uygulanmaktadır. **Orta:** Maddede belirtilen önlem var ve orta düzeyde uygulanmaktadır **İyi:** Maddede belirtilen önlem var ve iyi düzeyde uygulanmaktadır. **Çok İyi:** Maddede belirtilen önlem var ve çok iyi düzeyde uygulanmaktadır. **Fikrim Yok:** Maddede belirtilen önleme ilişkin herhangi bir bilgim yok.	**Yok / Uygulanmamakta**	**Var/ Uygulanmakta**					**Fikrim Yok**
		Çok Kötü	**Kötü**	**Orta**	**İyi**	**Çok İyi**	
Donanım Güvenliği Önlemleri							
22.1. Veri işleme, depolama ve iletme yeteneğine sahip tüm donanımların güncel envanteri tutulmakta ve kullanım tahsisleri yapılmaktadır.							
22.2. Kütüphane envanterindeki tüm cihaz ve taşınabilir ortamlar, kaybolma veya çalınma riskine karşı şifrelenmektedir.							
22.3. Kritik bilgi içeren taşınabilir cihaz ve ortamlar güvenli şekilde saklanmakta ve kurum dışına çıkarılmasına izin verilmemektedir.							
22.4. Kütüphane envanterinden çıkarılan donanımların veri depolama ünitelerindeki veri / bilgi geri getirilmeyecek şekilde silinmektedir.							
22.5. Kullanım ömrünü tamamlamış veri depolama üniteleri (HDD, SSD, harici bellek, disk vb.) güvenli bir biçimde imha edilmektedir.							
22.6. Yeni tedarik edilen sabit diskler veri kurtarmaya imkân sağlamayacak bir şekilde biçimlendirilerek sisteme dâhil edilmektedir.							
22.7. Bilgi içeren tüm cihaz ve ortamların ısı, nem ve elektromanyetik zararlara maruz kalamaması için çevresel önlemleri alınmaktadır.							
22.8. Onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihaz ve ortamlardaki kritik bilgiler geri getirilmeyecek şekilde silinmektedir.							
22.9. Nesnelerin interneti (IoT) cihazları ile ilgili kurulum, imha ve yeniden kullanıma alma gibi işlemler yetkili personelce yapılmaktadır.							
Yazılım Güvenliği Önlemleri							
22.10. Yazılımların adı, sürümü, yayımcısı, sözleşme, lisans ve edinim tarihi gibi bilgilerden oluşan detaylı yazılım envanteri tutulmaktadır.							
22.11. Yazılım ve uygulamaların kurulumu, yapılandırılması ve güncellemesi yetkili personel tarafından yapılacak şekilde kısıtlanmaktadır.							
22.12. Yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması gibi kontroller kullanılmaktadır.							
22.13. Bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması gibi kontroller uygulanmaktadır.							
22.14. Bilgisayarların ve bilişim sistemlerinin korunması ve taranması için zararlı yazılım tespit uygulamaları (Norton, Mcafee, Bitdefender vb.) kullanılmaktadır.							
22.15. Zararlı yazılım ~~ve~~ saldırı tespit gibi koruma uygulamaları, kullanıcılar tarafından devre dışı bırakılmayacak şekilde yapılandırılmaktadır.							
22.16. Kritik veri işleyen sistem yazılımları, onaylanmamış dosya yüklemelerine ve yetkisiz değişikliklere karşı düzenli olarak gözden geçirilmektedir.							
22.17. Felaket, saldırı, sistem arızası ve kullanıcı hatası kaynaklı veri / bilgi kayıplarına karşı yazılım ve uygulama yedeklemeleri yapılmaktadır.							
22.18. Olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemleri düzenli olarak gözden geçirilmektedir.							
22.19. Bilgi sistemlerinde tespit edilen zararlı yazılımlar ve saldırılar üst yönetime ve bilgi işlem birimine iletilmektedir.							
22.22. Bilgisayarlar, taşınabilir ortamları zararlı yazılım taramasından otomatik olarak geçirilecek ve otomatik olarak çalıştırılmasına izin vermeyecek şekilde yapılandırılmaktadır							
22.22. Kurumsal ve kişisel bilgi içeren uygulamalara ve yazılımlara, kişisel cihaz ve ortamların bağlanmasına izin verilmemektedir.							
Ağ ve İletişim Güvenliği Önlemleri							
22.21. Ağ hizmetlerinin güvenliği için kullanıcı kimlik doğrulama ve şifreleme gibi ağ bağlantısı kontrolleri uygulanmaktadır.							

22.23. Ağlar; personel, öğrenci gibi kullanıcı seviyelerine ve bilgi sistemlerine göre birbirinden ayrılmaktadır. (Personel / öğrenci ağı, sunucu / istemci ağı vb.)							
22.24. Misafir cihazlarının yalnızca misafir ağına erişimlerinin olduğu genel ağdan izole edilmiş ayrı bir ağ kullanılmaktadır.							
22.25. Bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemleri kullanılmaktadır.							
22.26. Onaylanmayan ve erişimi yasak olan web sitelerinin bağlantısını engellemek için ağ tabanlı URL filtrelemesi uygulanmaktadır.							
22.27. Ağlar arasında iletişim güvenliğini sağlamak ve uzak kullanıcıları kurum ağlarına güvenli şekilde bağlamak için sanal özel ağ (VPN, ZenMate vb.), uygulama güvenlik duvarı (proxy) gibi güvenli ağ geçitleri kullanılmaktadır.							
22.28. Kritik bilgi işleyen bilgisayar ve diğer sistemlerin wifi, bluetooth, 3G gibi kablosuz ve kablolu ağ bağlantıları sınırlandırılmakta veya engellenmektedir.							
22.29. Elektronik bilgi iletiminde, elektronik haberleşme ile ilgili iş süreçleri, yasal ve güvenlik kontrol gereksinimleri dikkate alınmaktadır.							
22.30. Kurumun ağ yönetim sorumlularının bilgisi olmadan ağa switch, hub, modem veya access point gibi aktif cihazlar dâhil edilmemektedir.							
22.31. Ağ teknolojisi ile çalışan telefon, faks, fotokopi gibi cihazların kayıtları tutulmakta ve kullanıcı sorumluları belirlenmektedir.							
22.32. Kurum ağına bağlanan kullanıcılara ait donanımların erişimleri, port seviyesinde kontrol edilmekte ve zarlı donanımlar engellenmektedir.							
Veri Güvenliği Önlemleri							
22.33. Bilgi yaşam döngüsü içerisinde işlenen, depolanan, iletilen ve imha edilen kritik bilgiler belirlenmekte ve kayıtları tutulmaktadır.							
22.34. Bilgiler; değeri, kritikliği ve gizliliği gibi hassasiyetlere göre (kritik, kişisel ve özel bilgi vb.) sınıflandırılmakta ve uygun sınıflanma etiketi taşımaktadır.							
22.35. Bilgisayar ve taşınabilir ortamlarda (HDD, SSD, harici bellek vb.) muhafaza edilen kritik bilgiler şifrelenmektedir.							
22.36. Kritik ve değerli bilgiler, depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmekte ve saklanmaktadır.							
22.37. Kullanım dışı kalan bilgisayar ve depolama ortamlarındaki kritik bilgiler, yetkili personelce güvenli şekilde silinmektedir.							
22.38. Kritik bilgiye ve bilgi işleme sistemlerine erişimler, en az ayrıcalık ilkesine göre yetkilendirilen personelle kısıtlanmaktadır.							
22.39. Kişisel bilgilerin erişim yetkilendirmeleri önceden belirlenmiş ilke ve yöntemlere göre verilmektedir.							
22.40. Bilgi sistemlerindeki kullanıcı bilgilerinin tedarikçilerce görüntülenmesi ve ihlal edilmemesi karşılıklı sözleşme ile koruma altına alınmaktadır.							
22.41. Personel, tedarikçi ve diğer tüm kullanıcıların bilgi sistemlerindeki bilgilere erişim yetkileri, düzenli aralıklarla gözden geçirilmekte ve kütüphane ile olan ilişkileri, sözleşmeleri veya anlaşmaları sone erdiğinde kaldırılmaktadır.							
22.42. Bilgi sistemi ve hizmetlerinden yararlanacak her kullanıcı için ayrı bir hesap tanımlanmakta ve asla ortak hesap kullanımına izin verilmemektedir.							
22.43. Kullanıcılardan kişisel bilgilerin sistemler arasında veya gerekli hallerde kurum içinde kullanılacağı ile ilgili açık rıza onayı alınmaktadır.							
22.44. Bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin (T.C. numarası, doğum tarihi vb.) üyelik numarası ve şifre olarak kullanılmamaktadır.							
22.45. Bilgi sistemlerine varsayılan kullanıcı hesap parolalarıyla giriş izni verilmemekte, güçlü parola kullanımı uygulanmaktadır.							
22.46. Kritik bilgilerin kurum dışına aktarımı sadece yetkili kullanıcı hesaplarıyla yapılmaktadır.							
22.47. Veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi kimlik doğrulama sistemleri kullanılmaktadır.							
Fiziksel ve Çevresel Güvenlik Önlemleri							
22.48. Kütüphanenin ana giriş ve çıkış kapıları güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile denetlenmektedir.							
22.49. Kritik bilgi barındıran alanların fiziksel güvenlik sınırları belirlenmekte ve kapı, pencere gibi kısımlar güvenlik mekanizmaları ile korunmaktadır.							
22.50. Kütüphanede güvenlik kontrollerini sağlayacak yetkinliğe sahip yeterli sayıda güvenlik personeli çalıştırılmaktadır.							
22.51. Kütüphanenin iç ve dış alanları güvenlik kameraları ile takip edilmektedir.							
22.52. Ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb.) giriş ve çıkışları kayıt altına alınmakta ve sadece ilgili amaçları için erişim izni verilmektedir.							

22.53. Ziyaretçilerin kabul edileceği alanlar personel ve kullanıcı çalışma alanlarından ayrı bir bölgede konumlandırılmaktadır.							
22.54. Refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğu uygulanmaktadır.							
22.55. Kritik bilgilerin işlendiği veya saklandığı alanlara erişim, uygun kontroller (kartlı / şifreli erişim vb.) uygulanarak yetkili kişiler ile sınırlandırılmaktadır.							
22.56. Kütüphane binasına ait pencereler, kapılar ve bahçe alanları, demir parmaklık, çit, kilit, tel örgü gibi dış güvenlik unsurlarıyla kontrol edilmektedir.							
22.57. Bilgi sistemlerinin enerji ve iletişim hizmetlerini taşıyan kablolar, dinleme ve hasara karşı kablo kanalı ve izolasyon malzemeleriyle korunmaktadır.							
22.58. Doğal afetler, kötü niyetli saldırılar ve kazaklara karşı fiziksel koruma önlemleri büyük oranda alınmakta ve personel bilgilendirilmektedir.							
22.59. Elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarları kullanılmaktadır.							
<u>Bölüm III: Kurumsal Önlemlerin Varlık / Uygulanma Düzeyini Ölçen Maddeler</u>							
23- Aşağıda kütüphanenizdeki kurumsal önlemlere (bilgi güvenliği politikaları, prosedürleri, idari araçları ve farkındalık oluşturma uygulamaları) ilişkin maddeler bulunmakta olup bu önlemlerin kütüphanenizde varlık / uygulanma düzeyini yansıtan en uygun seçeneği (√) işaretleyiniz?							
Bilgi Güvenliği Politikaları							
23.1. Personel, kullanıcı ve tedarikçilerin bilgi sistemleri ve varlıklarındaki bilgilerin kabul edilebilir kullanımlarını tanımlayan ilke ve yöntemler							
23.2. Kâğıt veya elektronik ortamda bulunan kritik bilgilere yetkisiz erişim, bunların hasar görmesi ve kaybolması risklerini azaltan temiz masa / ekran ilke ve yöntemleri							
23.3. Kritik bilgi, evrak, yazılım, medya ve diğer bilgi varlıklarının kurum dışına çıkarılması ya da başka ortamlara aktarılması ile ilgili önlemleri temin eden bilgi transferi ilke ve yöntemleri							
23.4. Taşınabilir cihazların kullanılmasıyla ortaya çıkan risklerin yönetilmesini ve üzerlerindeki kayıtlı bilgilerin güvenliğini temin eden ilke ve yöntemler							
23.5. Uzak çalışma alanlarından kurumun bilgi sistemlerinde erişilen, işlenen ve depolanan bilgiyi koruma amacı güden uzaktan çalışma ilke ve yöntemleri							
23.6. Bilgi sistemlerine kaynağı belirli, kişisel ve kötü niyet şüphesi olmayan hangi tür yazılımların kurulabileceğini tanımlayan ilke ve yöntemler							
23.7. Bilgi sistemleri ve varlıklarına erişim sağlayan kullanıcı ve tedarikçilerin haklarını, kısıtlamalarını ve sınırlığını belirleyen erişim kontrol ilke ve yöntemleri							
23.8. Bilginin değeri, kritikliği ve ifşa edilme hassasiyetine uygun seviyelerde korunmasını temin eden bilgi sınıflandırma ve etiketleme ilke ve yöntemleri							
23.9. Kritik bilgi barındıran alan ve sistemlerin korunmasını ve kütüphanenin güvenlik sınırlarını ve önlemlerini tanımlayan fiziksel ve çevresel yöntemleri							
23.10. Olası bir felaket ve ortam hatasından kaynaklanan veri kaybına karşı kritik bilgi, yazılım ve sistemlerin korunmasını amaçlayan bilgi yedekleme ilke ve yöntemleri							
23.11. Bilgi sistemlerinin zararlı yazılım saldırılarından korumak için tespit etme, engelleme ve kurtarma kontrollerini içeren zararlı yazılımlara karşı ilke ve yöntemler							
23.12. Bilgilerin gizliliğinin ve bütünlüğünün korunması için şifreleme kontrollerinin doğru ve etkin kullanımını temin eden ilke ve yöntemler							
23.13. Ağa bağlı sistem ve uygulamalardaki verilerin ve ağ alt yapısının güvenliğini ve yetkisiz erişimlerden korunmasını temin eden ağ yönetimi ilke ve yöntemleri							
23.14. Kişisel kimlik bilgilerinin gizliliğini ve korunmasını temin eden kişisel bilgilerin mahremiyeti ve koruması ilke ve yöntemleri							
23.15. Patentli yazılım ve bilgi varlıklarının yasal kullanım haklarının ilgili yasa ve anlaşmalar çerçevesinde korunmasını temin eden fikri mülkiyet ilke ve yöntemleri							
23.16. Tedarikçilerin kullanıcı ve kuruma ait bilgi varlıklarına erişimi ile ilgili risklerin azaltılmasını ve kritik bilgilerin korunmasını temin eden tedarikçi ilişkileri ilke ve yöntemleri							
Bilgi Güvenliği Prosedürleri							
23.17. Kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması, taşınması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ortam cihazlarının yönetimi ilke ve yöntemleri							
23.18. Sistem ve hizmetlere güvenli erişimi temin etmek için kullanıcı kaydetme, kayıt silme, erişim izni verme, kimlik doğrulama gibi faaliyetlerin belirlendiği kullanıcı erişim ilke ve yöntemleri							
23.19. Sistem ve uygulamalara yetkisiz erişimi engellemek için faaliyetlerin belirlendiği güvenli oturum açma ilke ve yöntemleri							

23.22. Güvenli alanlara sadece yetkili personele erişim izni vermek için uygun giriş kontrollerinin ve faaliyetlerinin belirlendiği fiziksel giriş ilke ve yöntemleri							
23.23. Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir şekilde müdahale edilmesini amaçlayan faaliyetlerin ve yönetim sorumluluklarının belirlendiği ilke ve yöntemler							
23.22. Yıkıcı bir olayı yönetmek ve mevcut durumu korumak veya en az zararla atlatabilme için gereksinim duyulan planlama ve faaliyetlerin belirlendiği iş sürekliliği ve felaket kurtarma ilke ve yöntemleri							
23.23. Kütüphane sistemleri, internet ağı, elektronik posta ve diğer erişimler için güçlü parola kullanımı ve yönetme standartları düzenleyen parola işleme ve kullanımı ilke ve yöntemleri							
23.24. Bilgi varlıklarının kapasitelerinin planlanması ve kapasite kullanımlarının belli sınırlar içinde tutulması faaliyetlerini düzenleyen kapasite yönetimi ilke ve yöntemleri							
23.25. Kullanıcıların doğru ve güvenli e-posta kullanımına yönelik kişisel ve kurumsal faaliyetleri düzenleyen elektronik posta ilke ve yöntemleri							
23.26. Ziyaretçilerin kabulü, dolaşımları ve kütüphaneden ayrılmalarıyla ilgili faaliyetleri düzenleyen ziyaretçi kabul ilke ve yöntemleri							
Bilgi Güvenliği İdari Araçları ve Yöntemleri							
23.27. Bilgi güvenliği politika ve prosedürleri ihlallerinin raporlanması ve ilgili birimlere bildirilmesini düzenleyen kılavuz ve talimatlar							
23.28. Bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi bir disiplin mekanizması							
23.29. Yeni istihdam edilen personele bilgi güvenliği sorumluluklarını ve görevi son bulan personele ise istihdamın sona ermesinden sonra devam ettirmesi gereken bilgi güvenliği sorumluluklarını bildiren talimat ve uygulamalar							
23.30. Kişisel bilgilerin kütüphane bilgi sistemlerine işlenmeden önce ilgili kullanıcının bilgilendirilmesini amaçlayan aydınlatma metni uygulamaları							
23.31. Kişisel bilgilerin kütüphane bilgi sistemlerine işlenme amacının ilgilisine açıkça ifade edilmesini amaçlayan açık rıza yönetimi uygulamaları							
23.32. Bilgi güvenliği tehditlerinden korumaya yönelik ilgili aksiyon planlarını kapsayan risk analizi tabanlı idari araçlar ve uygulamalar (varlık performans analizi, tehdit analizi, risk analizi vb.)							
23.33. Bilgi güvenliği yönetim sisteminizin etkin, güncel, izlenebilir ve gelişime açık yapıda olmasının teminini amaçlayan iç denetim ilke ve uygulamaları							
23.34. Üçüncü taraf tedarikçi firma ve kurumlar ile yapılacak bilgi alışverişinin güvenliğini sağlamaya yönelik yapılan sözleşmelere ilişkin idari ilke ve yöntemler							
Bilgi Güvenliği Farkındalığı Oluşturma Çalışmaları							
23.35. Personelin ve kullanıcıların bilgi güvenliği sorumluluklarını farkında olmalarını ve yerine getirmelerini amaçlayan bilgi güvenliği farkındalık eğitimi çalışmaları							
23.36. Bilgi güvenliği eğitim faaliyetlerinin kapsamının belirlendiği ve ihtiyaçların netleştirildiği eğitim planlama rehberleri							
23.37. Bilgi güvenliği alanında görevlendirilen personelin yetenek ihtiyaç analizinin yapılması ve sonuçlarına göre hizmetçi eğitim uygulamaları							
23.38. Kütüphanenin bilgi güvenliği çerçevesini oluşturan politika, prosedür ve idari yöntemler hakkında tedarikçilerin farkındalığını geliştirme çalışmaları							
23.39. Personel ve kullanıcıların bilgi güvenliği farkındalığını arttırıcı interaktif eğitim çalışmaları							
23.40. Bilgi güvenliği ile ilgili broşür, poster ve kitapçık gibi bilgilendirici doküman çalışmaları							
23.41. Kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması							
23.42. Kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları, fare altlığı, not kâğıtları gibi farkındalık arttırıcı faaliyetler							
23.43. Personele ve kullanıcılara bilgi güvenliği ile ilgili mail ve SMS yoluyla bilgilendirme mesajlarının gönderilmesi							
23.44. Personel ve kullanıcıların bilgi güvenliği hassasiyetlerinin ödüllendirilme çalışmaları							
23.45. Kütüphanenizin bilgi güvenliği politika, prosedür ve idari yöntemleri ile ilgili yapılan güncellemelerin kullanıcılara zamanında bildirilme							

EK-1. 2: Etik Kurul Değerlendirme Formu

T.C.
ÇANKIRI KARATEKİN ÜNİVERSİTESİ
ETİK KURUL DEĞERLENDİRME FORMU

Toplantı No:	29
Araştırmanın Yürütücüsü:	Ali KAVAK
Araştırmanın Başlığı:	Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi ve Ulusal Model Önerisi
Karar Tarihi:	15-12-2022
Kurul Görüşü:	Kabul Edilmiştir. Araştırmanın/Projenin uygulanabilirliği konusunda bilimsel araştırmalar etiği açısından bir sakınca yoktur.

SONUÇ: Kabul Edilmiştir. Araştırmanın/Projenin uygulanabilirliği konusunda bilimsel araştırmalar etiği açısından bir sakınca yoktur.

Başkan
Prof. Dr. Hüseyin ODABAŞ
İMZA

Başkan Yardımcısı
Prof. Dr. Ela Özkan CANBOLAT
İMZA

Üye
Prof. Dr. Gülcihan YILDIRIM
İMZA

Üye
Doç. Dr. Hakan ÇOLAK
İMZA

Üye
Doç. Dr. Bilgehan TEKİN
İMZA

Üye
Doç. Dr. Emine ÇELİKSOY
İMZA

Üye
Dr. Öğr. Üyesi Serap Aslan COBUTOĞLU
İMZA

Üye
Doç. Dr. Haydar KOÇ
İMZA

Çankırı Karatekin Üniversitesi

EK-7. 1: Bilgi Güvenliği Yönetim Sistemi Politikası

Doküman No:	**KÜTÜPHANE.BGYS.POL.01**
Doküman Adı:	**Bilgi Güvenliği Yönetim Sistemi Politikası**

1. AMAÇ

Bu politika, ……Üniversitesi kütüphanelerinin sahip olduğu bilgi varlıklarındaki hassas ve kritik öneme sahip veri / bilgilerin gizlilik, bütünlük ve erişebilirlik kapsamında değerlendirilebilecek tüm bilgi güvenliği tehditlerinden korunması amacıyla yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak yönetilmesini temin etmeyi amaçlamaktadır.

Üniversite kütüphanelerinin kurumsal bilgi güvenliğinin sağlamasına yönelik hazırlanan bu Bilgi Güvenliği Yönetim Sistemi (BGYS) ile, üniversite kütüphaneleriyle ilgili tüm tarafların uyması gerek bilgi güvenliği gereksinimlerinin ve şartlarının çerçevesi ve yazılı kuralları belirlenmektedir.

2. KAPSAM

Bilgi hizmeti sunan ….Üniversitesi kütüphanelerinin iş ve işlemlerin yürütülmesi süreçlerinde kullanılan bilgi varlıklarını korumak amacıyla kurulan ve kullanılan donanım, yazılım, ağ, veri tabanları, bilgi sistemleri gibi teknolojik altyapı ile birlikte insan kaynakları, dokümantasyon, fiziksel ve çevresel yapılar gibi bilgi varlıklarının güvenliğini kapsamaktadır. Bu BGYS ile üniversite kütüphanesine ait bilgiler; izinsiz ve yetkisiz erişime karşı korunur, bilgilerin gizliliği, bütünlüğü ve yetkili kullanıcıların erişimi sağlanır ve ilgili mevzuat ve standartların şartları yerine getirilir.

3. UYGULANABİLİRLİK

BGYS kapsamı içerisinde tutulan tüm bilgi varlıklarıyla ilişkisi olan üniversite kütüphanesi ve ilgili diğer birim çalışanları (bilgi işlem, kalite koordinatörlüğü vb.) çalışanları bu politikayı uygulamakta yükümlü sayılır. Bu politika Üniversite üst yönetimi tarafından onaylanarak yürürlüğe girmiştir.

4. SORUMLULUKLAR

4.1. Üst yönetimin sorumlulukları:

- Bu politikayı gözden geçirmek ve onaylamak.
- BGYS kurulunu ve yöneticisini atamak
- Bilgi güvenliği politikasının kurum içinde uygulanmasına desek vermek

4.2. Birim yönetici(ler)sinin sorumlulukları:

- Birim sahaları içine giren bölümlerde BGYS'yi gerçekleştirmek,
- Personeline, kullanıcılarına ve üçüncü taraflara ait veri/bilgilerin güvenliğini tehlikeye düşüren kasti hareketlerden sorumlulara karşı idari ve hukuki yaptırımları devre sokmak,
- Üçüncü taraf bilgi güvenliği politikalarından haberdar olmak ve bunlarla ilgili kütüphanenin BGYS'sinde gerekli düzenlemeleri yapmak.

4.3. Personelin sorumlulukları:

- BGYS politikasını bilmek ve politikadaki esas ve kurallara uymak,
- Sahip olduğu kişisel ve kurumsal bilgi varlıklarını korumak,
- Bilgi güvenliği tehditlerini ve karşı önlemlerini bilmek

- Bilgi güvenliği ihlal olaylarını tespit etmek ve ilgililere anında iletmek,
- Kendisine tahsis edilen gizli ve kritik bilgi varlıklarını, kullanıcı hesaplarını kurum çıkarına karşı olacak işlemler için kullanmamak,
- Kullanıcılara ve üçüncü taraflara ait kişisel ve kuramsal bilgilerin gizliliği, bütünlüğü ve erişebilirliği ile ilgili güvenlik unsurlarına uymak.
- Kurumun diğer mevzuatları ile belirlenmiş bilgi güvenliği ile ilgili diğer kural ve ilkelere uymak.

5. HEDEFLER ve PRENSİPLER

5.1. BGYS'nin kuruluş ve sürdürülebilirliğini sağlamak amacıyla bu politikada şunları hedeflenmektedir:

- Uygun bilgi güvenliği risk değerlendirme araçlarıyla bilgi varlıklarının kritiklik değerlerini belirlemek,
- Bilgi varlıklarının zayıf noktaları ve onlara karşı gerçekleşebilecek tehditleri anlamak,
- Teknik ve kurumsal bilgi güvenliği önlemlerini almak
- Bilgi güvenliği risklerini kabul edilebilir seviyelere indirmek,
- İlgili mevzuata ve yasalara uymak (KVKK vb.),
- Kurumun itibarını ve bilgi güvenliği imajını korumak,
- Kullanıcıların kişisel bilgi güvenirliğini sağlamak,
- Üçüncü taraf sözleşmelerden kaynaklanan güvenlik gereksinimlerini karşılamak ve temsil ettiği markanın imajını ve haklarını korumak,
- Kurumun temel hizmetlerinin en az kesintiyle devam etmesini sağlamak,
- Bilgi güvenliği işletim ve denetim prosedürlerine, talimatlarına ve diğer dokümanlarına uymak,
- TS ISO/IEC 27001 standartlarının uygunluğunu ve sürdürülmesini sağlamak,
- Personelin ve kullanıcıların bilgi güvenliği bilinç ve farkındalık seviyelerini artırmak..

5.2. BGYS politikası, kuruma ait tüm bilgi varlıkları ve iş süreçlerinde bilgi güvenliği gizlilik, bütünlük ve erişebilirlik unsurlarına uygun önlemler almayı temel prensip edinmektedir. Bu itibarla, dinamik bir BGYS süreci ile bilgi varlıkları kabul edilebilir risk seviyesinin altında tutulmaya çalışılmakta ve bu bilgi varlıkları için uygun önlemler belirlenerek iyileştirme çalışmaları sürdürülmektedir.

6. TAAHÜT VE ONAY

Üst yönetim, BGYS'ye uyulmasını, etkinliğini, sürekli iyileştirilmesini; personelin, kullanıcıların ve üçüncü tarafların katılımını ve uyumunu; risk yönetiminin gerçekleştirilmesini; bilginin gizlilik, bütünlük ve erişilebilirlik unsurlarının korunmasını; yönetim gözden geçirme yoplantılarına iştirak edilmesini; yasal mevzuata, sözleşmemelere ve standartlara uyumun garanti altına alınmasını; kurum kültürünün vazgeçilmez bir parçası olarak uygulanmasının takip edilmesini taahhüt etmektedir.

Üst Yönetim, Üniversite Kütüphaneleri BGYS Politikasının uygulanmasının ve denetlenmesinin, güvenlik ihlallerinde de gerekli idari ve hukuki yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan etmektedir.

EK-7. 2: Bilgi Varlıklarının Sınıflandırılması ve Kritiklik Derecesi Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.02
Doküman Adı:	Bilgi Varlıklarının Sınıflandırılması ve Kritiklik Derecesi Politikası

1. AMAÇ

Bu politika, … Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığının bilgi varlıklarının uygun bir şekilde sınıflandırılarak ve gizli / kritik bilgilerin derecesi belirlenerek güvenliğinin sağlanmasını amaçlamaktadır.

2. KAPSAM

Bu politikadaki uygulama kuralları, kütüphanede ve ilgili birimlerde çalışan tüm personel için geçerlidir

3. SORUMLULUKLAR

Bu politikanın uygulanmasından üst yönetimi, birim yöneticileri ve personel sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Bilgi varlıkları; kurum mevzuatı, yasal şartlar, bilginin kritikliği, bilginin ifşası veya değiştirilmesi gibi hassasiyet derecelerine göre sınıflandırılmakta; bilgi varlığına işlenen verinin gizlilik, bütünlük ve erişebilirlik unsurları bakımından değerleri ile bu bilgi varlıklarında gerçekleşebilecek güvenlik ihlallerinin etki alanlarına göre ise krtiklik derecesi belirlenmektedir.

4.2. **Bilgi** varlıkları gizlilik derecelerine göre dört düzeyde (gizli, hizmete özel, kişiye özel, genel) sınıflandırılmaktadır:

- *GİZLİ / KRİTİK:* Kritik ve gizli bilgi varlıklarını belirtir. Gizli bilgi varlıkları, açığa çıkması veya yetkisiz kişilerin erişimi durumunda kurum için sorun yaratacak kurumsal ve kişisel bilgileri içermektedir. Bu bilgiler sadece yetkili kişilerin erişimine açıktır. Bu nedenle bu bilgiler bilgi güvenliği önlemi yöntem ve mekanizmaları ile korunmaktadır. Bu bilgilerin gizlilik, bütünlük ve erişebilirdik unsurlarının korunması esastır. Bu bilgilerin korunması için oluşturulan ilgili dokümanlardaki kural ve ilkelere uyulması gerekir.
- *HİZMETE ÖZEL:* İçerdiği bilgi itibarıyla gizlilik derecesine sahip olmayan, ancak kurumda bilmesi gereken personel haricindeki personel tarafından bilinmesinde kurumun itibarını ve imajını etkileyecek bilgi varlıklarının sınıflandırılmasında kullanılır.
- *KİŞİYE ÖZEL:* Kişisel Verileri Korunması Kanunu (KVKK) çerçevesinde özel nitelikli kişisel veri kapsamına giren tüm bilgiler için kullanılır
- *GENEL:* Gizlilik derecesi olmayan ve özel olarak korunması gerekmeyen bilgi varlıları için kullanılır.

4.3. Bilgi varlıkları gizlilik / kritiklik derecesine göre ise üç düzeyde (düşük, orta, yüksek) değerlendirilmektedir:

- *DÜŞÜK:* İzinsiz ve yetkisiz olarak işlenmesi, kullanılması, açıklanması veya paylaşılması durumunda, kişisel ve kurumsal güvenlik açısından düşük düzeyde zarar verebilecek yapıdaki gizli ve kritik bilgiler için kullanılır. Kabul edilebilir risk düzeyi bulunmakta ve hizmetin durumuna göre aksiyon alınmalıdır.
- *ORTA:* İzinsiz ve yetkisiz olarak işlenmesi, kullanılması, açıklanması veya paylaşılması durumunda, kişisel ve kurumsal güvenlik açısından orta düzeyde zarar verebilecek yapıdaki gizli ve kritik bilgiler için kullanılır. Dikkate değer risk düzeyi bulunmakta ve orta vadede aksiyon alınmalıdır.
- *YÜKSEK:* İzinsiz ve yetkisiz olarak işlenmesi, kullanılması, açıklanması veya paylaşılması durumunda, kişisel ve kurumsal güvenlik açısından yüksek düzeyde zarar verebilecek yapıdaki gizli ve kritik bilgiler için kullanılır. Kabul edilemez risk düzeyi bulunmakta ve hemen aksiyon alınmalıdır.

5. HEDEFLER ve PRENSİPLER

- Bilgi güvenliği yönetim sisteminin basalı bir biçimde yürütülmesini sağlamak.
- Bilgi varlılarının güvenliğinin sağlamak,
- Personelin ve kullanıcıların bilgi güvenliğini sağlamak,
- Kurumun itibarını ve imajını korumak.

6. YÖNETİMİN TAAHÜTÜ VE ONAYI

Üst Yönetim, bu politikanın uygulanmasının ve denetlenmesinin, güvenlik ihlallerinde de gerekli idari ve hukuki yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan etmektedir.

EK-7. 3: Bilgi Transferi Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.03
Doküman Adı:	Bilgi Transferi Politikası

1. AMAÇ

Kurum bünyesinde bulunan bilgi, evrak, medya, yazılım ve diğer varlıkların dışarı çıkarılması (gönderilmesi), yer değişimi ya da başka ortamlara aktarılması durumunda izlenecek yöntemleri ve kuralları belirlemek

2. KAPSAM

Kurum, kurumun üçüncü taraflar ve şahıslarla yapacağı bilgi değişiminde (transferi); kurumun çalışanları ile üçüncü taraflar ve şahıslar bu politikanın kapsamındadır.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından kurumun bilgi varlıklarını ve bilgi varlıklarına erişme yetkisi verilmiş kurum personeli ile kurum dışı kullanıcıları sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Gizli bilgilerin bir medya üzerinde ya da elektronik posta ile üçüncü taraflarla paylaşımı kontrolü bir şekilde BGYS Yöneticisi ya da birim yöneticisi onayıyla olmalıdır.

4.2. Flash bellek, CD, DVD gibi medyalar Bilgi Sistemlerince virüs taramasından geçirilerek ve kullanım onayı verilmeden kullanılmamalıdır. Elektronik bilgi alışverişi yapmak üzere kuruluşlar arası bir ağ kurulmadan önce bir gizlilik sözleşmesi imzalanmalıdır.

4.3. Bilgi içeren ortamlar için; aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı önlemler alınmalıdır.

4.4. Bilgi varlıklarının taşınması için bir yetkilendirme sistemi olmalıdır.

5. İLGİLİ DOKÜMANLAR

- Tedarikçi Güvenliği Politikası

EK-7. 4: Fikri Mülkiyet Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.04
Doküman Adı:	Fikri Mülkiyet Politikası

1. AMAÇ

Kuruma ve üçüncü kişilere ait olan fikri hakların korunması ve ihlallerin önlenmesi için uyulacak kuralları tanımlamaktır.

2. KAPSAM

Kurum ve üçüncü şahıslara ait tüm fikri mülkiyet (marka, patent, lisans, vb.) haklarını kapsamaktadır.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından kurumun bilgi varlıklarını ve bilgi varlıklarına erişme yetkisi verilmiş kurum personeli ile kurum dışı kullanıcıları sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Kurumda kullanılan tüm yazılımlar lisanslı olmalıdır.

4.2. Yazılım yüklemeleri, kopyalamalar vb. işlemler bilgi teknolojileri bölümü tarafından yapılmalıdır.

4.3. Kurum ve üçüncü şahıslara ait markaların kullanımı, ticari markalar ve coğrafi işaretlere ilişkin uluslararası yasalara uygun biçimde yapılmalıdır.

4.4. Kuruma ve üçüncü şahıslara ait fikri mülkiyet haklarının ihlal edildiği durumlarda güvenlik "ihlal olayı bildirimi" prosedürü işletilmelidir.

5. İLGİLİ DOKÜMANLAR

- Bilgi Güvenliği İşletim Prosedürleri/İhlal Olayları Yönetimi Prosedürü
- Bilgi Transferi Politikası

EK-7. 5: Fiziksel ve Çevresel Güvenlik Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.05
Doküman Adı:	Fiziksel ve Çevresel Güvenlik Politikası

1. AMAÇ

Bu politika kurum bilgi varlıklarının korunması amacıyla ofis ortamı, sistem odasına, muhasebe, insan kaynakları bölümleri, arşiv, vb. kurumsal bilgilerin bulundurulduğu yerlerin korunmasına ilişkin kuralları belirlemektir.

2. KAPSAM

Kurum binaları, ofisler, sistem odaları vb. bilgi varlıklarının bulunduğu fiziksel ortamlar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından BGYS Komitesi, BGYS Yöneticisi ve bilgi teknolojileri bölümü sorumludur. Tüm kurum çalışanları, geçici görevliler ve kurum bilgi varlıklarına erişimi yetkisi olan herkes bu politikadaki kurallara uymak zorundadır.

4. UYGULAMA / POLİTİKA

4.1. Kurum tesislerinin fiziksel olarak korunması; giriş/çıkış bariyerleri, kartlı giriş sistemleri, kameralar, güvenlik görevlileri vb. araçlarla sağlanmalıdır.

4.2. Kuruma gelen ziyaretçilerin ve yetkisiz kişilerin güvenli alanlara girişi kontrol edilmeli ve bu işlem sorumlu kişiler gözetiminde gerçekleştirilmelidir.

4.3. Fiziksel güvenliği sağlamak için kritik alanlara giriş önlemleri alınır. Server (Sunucu) bilgisayarların bulunduğu sistem odasının güvenlik önlemleri alınmalıdır.

5. İLGİLİ DOKÜMANLAR

- Bilgi Güvenliği İşletim Prosedürleri
- İhlal Olayları Yönetimi Prosedürü

EK-7. 6: Güvenli Sistem Mühendisliği Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.06
Doküman Adı:	Güvenli Sistem Mühendisliği Politikası

1. AMAÇ

Bu politika bilgi teknolojileri sistemlerinin (donanım, yazılım, destek, vb.) tasarımı ya da satın alma sürecinde güvenlik konularını sağlamayı amaçlar.

2. KAPSAM

Bu politika kurumun yazılım, donanım ve güvenlik sistemlerinin tasarım ve edinimi sürecini kapsar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından bilgi teknolojileri bölümü (IT), BGYS Yöneticisi, BGYS Komitesi ve satın alma yöneticileri sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Güvenli sistem mühendisliği, IT (bilgi teknolojileri) projelerinin güvenli bir şekilde tasarlanması ve sürdürülmesiyle ilgili bir konudur.

4.2. Bilgi teknolojileri projeleri belli aşamalar temelinde tasarlanmalı ve sürdürülmelidir:

- Başlangıç; Gereksinimlerin tanımlanması,
- Geliştirme; Sistem tasarımı ya da satın alınması. Güvenlik gereksinimlerinin tanımlanması,
- Uygulama; Sistemin test edilerek kurulması,
- İşletim / Bakım; Sistemin çalıştırılarak, performansının izlenmesi ve ölçülmesi,

4.3. Bilgi teknolojileri sistemlerinin satın alma ya da geliştirme sürecinde güvenlik gereksinimleri tanımlanmalı ve dokümante edilmelidir.

4.4. Uygulama (yazılım) geliştirme ve bakım süreci için güvenlik gereksinimlerini içeren yöntemler belirlenip dokümante edilmelidir.

4. İLGİLİ DOKÜMANLAR

- Tedarikçi Güvenliği Politikası

EK-7. 7: İnsan Kaynakları Güvenliği Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.07
Doküman Adı:	İnsan Kaynakları Güvenliği Politikası

1. AMAÇ

Bu politika insan kaynakları süreçlerinin BGYS ile olan gereksinimlerini belirlemeyi amaçlar.

2. KAPSAM

İnsan kaynakları süreçleri ve BGYS süreçlerini kapsar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından insan kaynakları bölümü, bilgi teknolojileri bölümü, BGYS Yöneticisi, BGYS Komitesi sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Kurum çalışanlarının işe giriş ve çıkış aşamasında izlenecek adımlar belli prosedürlere bağlanmalıdır.

4.2. Teknik işlemler (hesapların açılması, Internet erişim, yetkilendirme ve benzer konular) bilgi teknolojilerine (IT) bildirilmelidir.

4.3. İşe alınacak personelden alınan bilgiler ve belgeler doğrulanmalıdır.

4.4. İşe alımda bilgi güvenliği sorumluluklarını belirten Hizmet Sözleşmesi, Bilgi Güvenliği Politikası ve Varlıkların Kabul Edilebilir Kullanımına ilişkin dokümanlar imzalattırılmalıdır.

4.5. Personele verilen bilgi varlıkları (telefon, bilgisayar, vb.) takip edilmelidir.

4.6. Çalışanların düzenli olarak bilgi güvenliği "farkındalık" eğitimi alması sağlanmalıdır.

4.7. Bilgi güvenliğine ilişkin kuralları düzenli olarak çalışanlara duyurulmalıdır.

4.8. Disiplin süreçlerine bilgi güvenliği ihlalleri ve BGYS kuralları da eklenmelidir

5. İLGİLİ DOKÜMANLAR

- Eğitim/Farkındalık Eğitimi Prosedürü
- İnsan Kaynakları Bölümü İlgili Dokümanları

EK-7. 8: İzleme, Ölçme, Analiz ve Değerlendirme Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.08
Doküman Adı:	İzleme, Ölçme, Analiz ve Değerlendirme Politikası

1. AMAÇ

Bu prosedürün amacı, kurumumuzda uygulanan Bilgi Güvenliği Yönetim Sistemi (BGYS) süreçleri içerisinde yapılan faaliyetlerin performanslarının ölçülmesi ve denetlenmesidir.

2. KAPSAM

Bilgi Güvenliği Yönetim Sistemi ile ilgili tüm faaliyetleri kapsar.

3. SORUMLULUKLAR

Bilgi Güvenliği Yönetim Sistemi ile ilgili tüm faaliyetleri kapsar.

4. UYGULAMA / POLİTİKA

4.1. Nelerin izleneceği ve ölçüleceği belirlenmelidir. İzlenecek tipik konular şunlar olabilir: İnternet ve diğer erişimler, yedekleme işlemleri, kapasite kullanımı, sızma testi (penetrasyon testi) sonuçları, iç ağ zayıflık taraması, bilgi güvenliği ihlal olayları, iç tetkik sonuçları, bilgi güvenliği farkındalık eğitimlerinin etkinliği, diğer aktiviteler.

4.2. Değerlendirme kriterleri belirlenmelidir. Tipik kriterler şunlardır:

- Uygunsuzluk sayısı: BGYS hizmetlerinin sunulması sırasında ortaya çıkan hatalı durumlar yönünden izlenir. Bulunan uygunsuzluk ve açılan düzeltici faaliyet sayısının az olması bir başarı kriteridir.
- İhlal olayları sayısı: Bilgi güvenliği politika ve prosedürlerine aykırı hareketler ve saldırılar izlenir. Tespit edilen ihlal sayısının az olması başarı kriteridir.
- Sistemin durma (kesinti) zamanları: Güvenlikle ilgili olarak servislerin durma sayıları ve süreleri. Bu bilgiler sunucu işletim sistemleri ve ilgili yazılımların loglarından izlenir. Hizmet kesintisi süresinin az olması başarı kriteridir.
- Kapasite kullanımı: Sistemlerin kapasitelerinin uygun şekilde kullanılması - kapasitenin aşılmaması bir başarı kriteridir.
- Bütçeye uyma: BGYS planlaması sürecinde yapılan bütçe harcamalarının içinde kalınıp kalınmadığı denetlenir. Bütçeyi aşmamak başarı kriteridir.
- Risklerin düşürülmesi: İşlenen risk sayısı ve risklerin düşürme oranları başarı kriteridir. Kullanıcı Anketleri: Kullanıcıların BGYS'den memnun olmaları başarı kriteridir.
- İç Tetkikler: İç tetkik sonuçlarına göre bulunan uygunsuzlukların azlığı başarı kriteridir. Penetrasyon testi sonuçları: Bulunan zayıflıkların ve açıkların sayıca az olması başarı kriteridir.
- İç ağ teknik açıklık taraması sonuçları: Bulunan zayıflıkların ve açıkların sayıca az olması başarı kriteridir.
- Yedekleme işlemleri: Düzenli olarak yapılan yedekleme işlemleri başarı kriteridir. Tatbikat sayıları; Düzenli olarak yapılan başarılı iş sürekliliği tatbikatları bir başarı kriteridir.

5. İLGİLİ DOKÜMANLAR

- Bilgi Güvenliği İşletim Prosedürleri
- Teknik Açıklık Yönetimi Prosedürü
- Performans Raporu İzleme, Ölçme, Analiz Ve Değerlendirme Prosedürü

EK-7. 9: Sürekli İyileştirme Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.09
Doküman Adı:	Sürekli İyileştirme Politikası

1. AMAÇ

Bilgi Güvenliği Yönetim Sistemlerinin uygunluğunu ve etkinliğini kontrol etmek için gerekli olan iyileştirme faaliyetlerinin etkin bir biçimde yürütülmesini ve yaygınlaştırılmasını sağlamak.

2. KAPSAM

Tüm BGYS faaliyetlerini kapsar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından BGYS Komitesi, BGYS Yöneticisi ve bilgi teknolojileri bölümü ve diğer bölüm yöneticileri sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Başta BGYS komitesi olmak üzere her bölüm, tespit ettiği "iyileştirme" fırsatlarını belirlemeli ve bunları BGYS Yöneticisi ile paylaşmalıdır.

4.2. BGYS Yöneticisi bölümlerden gelen iyileştirme taleplerini değerlendirmeli ve gerekiyorsa "düzeltici faaliyet" yapmalıdır.

5. İLGİLİ DOKÜMANLAR

- İzleme, Ölçme, Analiz Ve Değerlendirme Politikası
- Düzeltici Faaliyet Prosedürü
- Sürekli İyileştirme Ve Politikası

EK-7. 10: Tedarikçi ve Üçüncü Taraf Güvenliği Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.10
Doküman Adı:	Tedarikçi ve Üçüncü Taraf Güvenliği Politikası

1. AMAÇ

Bu politikanın amacı tedarikçi şirketler ve üçüncü taraf şirketlerle, kurumlar ve kişilerle olan işlemlerde ve bilgi alışverişinde bilgi güvenliğinin sağlanmasıdır.

2. KAPSAM

Tüm kurum ve BGYS süreçlerinden satın alma ve hizmet tedarikleri ayrıca üçüncü taraflarla yapılan bilgi alışverişi ve yapılan diğer işlemler.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından başta satın alma ve bilgi teknolojileri bölümü olmak üzere tüm çalışanlar ve üçüncü taraflar sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Kurum tedarikçilerle ilgili olarak bilgi güvenliği bakımından kendi şartlarını belirlemelidir.

4.2. Tedarikçi firma seçiminde ISO/IEC 27001 standardının aranması vb. koşullar olmalıdır.

4.3. Tedarikçi firma ve yetkilileriyle "gizlilik anlaşmaları imzalanmalıdır.

4.4. Üçüncü taraflarla herhangi bilgi alışverişi yapılmadan önce bir gizlilik anlaşması yapılmalıdır.

4.5. Kurumun ağına bağlanacak olan üçüncü taraflardan belli güvenlik gereksinimleri (Anti virüs, şifreleme vb.) istenmelidir.

4.6. Gizli bilgilerin dağıtımını içeren kurallar belirlenmeli ve üçüncü taraflara bu bilgiler iletilmeden önce taraflarla bu kurallar üzerinde anlaşılmalıdır.

5. İLGİLİ DOKÜMANLAR

- Gizlilik Sözleşmesi

EK-7. 11: Temiz Masaüstü ve Temiz Ekran Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.11
Doküman Adı:	Temiz Masaüstü ve Temiz Ekran Politikası

1. AMAÇ

Bilgi varlıklarının - ofislerdeki masalar ve bilgisayar ekranları - bilgi güvenliği ihlalleri oluşturacak biçimde kullanılmasını engellemek.

2. KAPSAM

Kurumdaki tüm bilgi varlıkları dâhildir.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından tüm kurum çalışanları sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Tüm çalışanlar ve bilgisayar kullanıcıları, ofis masalarını, dolaplarını ve bilgisayar ekranlarını bilgilere yetkisiz erişime engel olacak şekilde düzenlemelidir.

4.2. Gizli olarak sınıflandırılmış evraklar, flash bellek, CD, DVD vb bilgi saklama ortamları ofislerde açıkta bırakılmamalıdır.

4.3. Gizli olarak sınıflandırılmış evraklar çöp kutusuna atılmadan önce kâğıt imha makinelerinden geçirilmelidir.

4.4. Bilgisayar başından ayrılmadan önce ekranlar parola ile kilitli konuma getirilir. (Windows işletim sistemi kullanılan bilgisayarlarda Windows Logo Tuşu + L ya da CTRL+ALT+DEL tuşları kullanılır.)

4.5. Kullanıcı hesaplarına ait bilgiler - parolalar - kâğıtlara yazılıp bir yere asılmamalıdır. Ekranlara, duvarlara ve benzeri yerlere (herkesin göreceği şekilde) not kâğıtları yapıştırılmamalıdır.

4.6. Bilgisayar ekranlarında çok sayıda program simgesi konulmamalıdır.

4.7. Bilgisayarlarda çok sayıda program açık olarak bırakılmamalıdır.

4.8. El terminalleri ve mobil cihazlar kullanılmadığı sürelerde kapalı/kilitli tutulmalıdır.

5. İLGİLİ DOKÜMANLAR

- Fiziksel ve Çevresel Güvenlik Politikası

EK-7. 12: Uyum Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.12
Doküman Adı:	Uyum Politikası

1. AMAÇ

Kurumun ve çalışanların ilgili yasa ve yönetmeliklere uygun davranmasını sağlamak.

2. KAPSAM

Kurum yönetimi, tüm faaliyetler ve tüm çalışanlar.

3. SORUMLULUKLAR

Üst yönetim, yöneticiler ve tüm çalışanlar.

4. UYGULAMA / POLİTİKA

4.1. Uyum politikası T.C. Anayasası, Ceza Kanunları, İlgili Yönetmelikler ve Kurumun üçüncü taraflarla yaptığı Sözleşme şartların uymayı amaçlar.

4.2. Anayasanın özel hayatın gizliliği ve kişisel haklara yönelin maddeleri.

4.3. Türk Ceza Kanunun ilgili maddeleri:

4.4. 5237: 5237 sayılı Türk Ceza Kanunu'nun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde belirtilen yükümlülüklerin yerine getirilmesi.

4.5. 5809: 5809 sayılı elektronik haberleşme kanunu çerçevesinde belirtilen bilgi güvenliği ile ilgili yükümlülüklerin yerine getirilmesi.

4.6. 5651: 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu temelinde kurumun sağladığı İnternet erişim hizmetinin loglanması gerekmektedir.

4.7. 6698: 6698 sayılı Kişisel Verilerin Korunması Kanunu ("6698 sayılı Kanun") uyarınca, kişisel verilerin korunması gerekmektedir.

4.8. Kurumun (ÖRNEK A.Ş) iş ortakları, tedarikçiler, müşteriler vb. üçüncü taraflarla yaptığı sözleşmelerden doğan yükümlülüklerini yerine getirmek zorundadır.

5. İLGİLİ DOKÜMANLAR

- BGYS Politikası
- Varlıkların Kabul Edilebilir Kullanımı Politikası

EK-7. 13: Varlıkların Kabul Edilebilir Kullanımı Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.13
Doküman Adı:	Varlıkların Kabul Edilebilir Kullanımı Politikası

1. AMAÇ

Kurum bilgi varlıklarının doğru ve güvenli kullanımını sağlamak.

2. KAPSAM

Kurumun bütün çalışanları ve bütün bilgi varlıklarını kapsamaktadır.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından BGYS Komitesi, BGYS Yöneticisi ve bilgi teknolojileri bölümü sorumludur. Tüm kurum çalışanları, geçici görevliler ve kurum bilgi varlıklarına erişimi yetkisi olan herkes bu politikadaki kurallara uymak zorundadır.

4. UYGULAMA / POLİTİKA

4.1. Varlıkların kabul edilebilir politikası bilgi varlıkları türlerine göre (bilgisayarlar, internet, elektronik posta, telefon, faks, mobil cihazlar) ayrı ayrı belirtilebilir.

4.2. Genel Kurallar

- Kurumun bilgi varlıkları (bilgisayarlar, yazıcılar, İnternet, elektronik posta, telefon, faks, mobil cihazlar, vb.) yalnızca kurum işlerinin yürütülmesi için kullanılmalıdır. Bu sistemlerin yasa dışı ya da kuruma zarar verecek şekilde kullanılması yasaktır.
- Kurum bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve denetleme gibi işlemleri yapabilecektir.
- Kullanıcıların, bilgisayar sistemi, İnternet ve elektronik posta sistemini kullanmak için sahip olduğu kimlik bilgilerini ve parolalarını başkalarına vermeleri yasaktır.
- Kuruma ait olan bir bilgi varlığı (donanım, yazılım, flash bellek, evrak vb.) BGYS Yöneticisi ya da bölüm yöneticisinin izni olmadan dışarı çıkarılamaz. Kurumun internet bağlantısı ve elektronik posta hizmeti ilgili yasa ve düzenlemelere uygun bir şekilde kullanılmalıdır.
- Elektronik posta kullanım kuralları belirlenmelidir.
- Cep telefonlarının kullanım kuralları belirlenmelidir.

4.3. Internet Kullanım Kuralları

- Sadece izin verilen sitelere erişim yapılmalıdır.
- Internet erişim loglanmalıdır (kaydedilmelidir).

- Sosyal medya kullanımı kısıtlanmalıdır.
- Ziyaretçi Internet erişimi 5651 yasasına göre loglanmalıdır.

4.4. Elektronik Posta Kullanım Kuralları

- Elektronik posta iletişimi formel bir şekilde yapılmalıdır. Mesajlar kısa ve öz olarak düzenlenmelidir. Ayrıca mesajlarda alıcının organizasyon içindeki konumuna göre uygun bir hitap dili kullanılmalıdır. Mesaj içeriğinin ardından gönderenin adı soyadı, görevi ve iletişim bilgileri mutlaka olmalıdır. Kurumsal bilgilerin paylaşıldığını üçüncü taraflarla kurumsal anlaşmalar ve kişilerle de gizlilik anlaşması yapılmalıdır.
- Elektronik postaların ekleri (attach), boyut ve içerik olarak sınırlı olmalıdır. Gelen postaları belli klasörlerde saklanmalıdır. Belli konularda gelen elektronik postaları biriktirmek üzere uygun klasörler oluşturmalı ve gönderilen ve alınan önemli elektronik postalar uygun klasör yapısı için saklanmalıdır.
- Çalışanların tatilde oldukları sürede elektronik postalarının yönlendirileceği alternatif kişiler olmalıdır. Ayrıca "out of Office" gibi imkânlar kullanılmalıdır. 4.3. Cihazların Kullanımı
- Bilgisayar, yazıcı, telefon ve bilgi işleyen tüm cihazları varsa talimatına uygun olarak kullanılmalıdır.
- Kullanıcılar sadece kendilerine ait (izinlerinin olduğu ve/veya yetkilerinin olduğu) cihazları kullanabilirler.
- Ortak kullanılan yazıcı ve diğer cihazların kullanımında güvenlik kurallarına dikkat edilmelidir. Kullandıktan sonra yazıcıların üzerinde artık kâğıt bırakılmamalıdır.
- Cihazların dışarı çıkarılmaları izin dâhilinde olmalıdır.

4.5. Telefonla İletişim:

- Telefonla iletişim mümkün olan en kısa ve öz biçimde yapılır. Kurum içi görüşmelerde dâhili hatlar tercih edilmelidir.
- Kuruma ait sabit telefonlar ve cep telefonları özel işlemler için kullanılmamalıdır.

5. İLGİLİ DOKÜMANLAR

- BGYS Politikası

EK-7. 14: Ziyaretçi Kabul Politikası

Doküman No:	KÜTÜPHANE.BGYS.POL.14
Doküman Adı:	Ziyaretçi Kabul Politikası

1. AMAÇ

Dışarıdan gelen ziyaretçilerin kabulü, kuruluş içinde dolaşmaları ve kuruluştan ayrılmalarıyla ile ilgili kuralları belirlemek.

2. KAPSAM

Kurum yönetimi, tüm faaliyetler ve tüm çalışanlar.

3. SORUMLULUKLAR

Tüm kurum çalışanları, geçici görevliler ve kurum bilgi varlıklarına Bu politikanın uygulanmasından BGYS Komitesi, BGYS Yöneticisi ve bilgi teknolojileri bölümü sorumludur.

4. UYGULAMA / POLİTİKA

4.1. Dışarıdan ziyaret amaçlı gelen kişiler kuruluş girişinde karşılanmalı, kimlik bilgileri ve ziyaret bilgileri (kimle ve ne için gibi) kaydedilmelidir. Ziyaretçilere bilgi güvenliği kurallarını da içeren bir ziyaretçi bilgisi (doküman verilerek ya da video izlettirilerek) verilmelidir.

4.2. Ziyaretçilere bir "ziyaretçi kartı" verilmeli ve kartın kurumdan ayrılıncaya kadar takılması sağlanmalıdır.

4.3. Ziyaretçilerin mümkünse bir refakatçı ile kurum için dolaşması sağlanmalıdır. Ziyaretçiler için görüşme odasında görüşme yapılması sağlanmalıdır. Ziyaretçilerin fotoğraf çekmeleri, flash bellek kullanmaları, bilgisayar kullanmaları, yazıcı vb. ofis cihazlarını kullanmaları engellenmelidir.

4.4. Dokümanların oluşturulması, saklanması, duyurulması vb. çalışmalar kuruma göre farklılık gösterecektir. Her zaman belirttiğimiz gibi bir hastane, bir üniversite, bir fabrika ve bir hukuk bürosu BGYS kurabilir ve bunların hepsi ISO/IEC 27001 standardı uygunluk belgesi alabilir. Her birinin personeli, alt yapısı, organizasyonu farklı olacaktır. Bu anlamda yapılacak çalışmalar (dokümantasyon) farklı olacaktır.

4.5. Ziyaretçi kabul politikası da her şirkete göre farklı olacaktır ancak önemli olan ziyaretçinin kimliğinin ve ziyaret amacının kaydının yapılması, ziyaretçinin şirketin gizli bilgilerine erişmesinin engellenmesi ve bir bilgi güvenliği ihlali yapmasına izin verilmemelidir

5. İLGİLİ DOKÜMANLAR

- Fiziksel ve Çevresel Güvenlik Politikası

EK-7. 15: Bilgi Sınıflandırma ve Etiketleme Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.2
Doküman Adı:	Bilgi Sınıflandırma ve Etiketleme Prosedürü

1. AMAÇ

Bu prosedürün amacı, bilgi varlıklarının, gerekli güvenlik düzeyine uygun olarak sınıflandırılması ve etiketlenmesinin sağlanmasıdır.

2. KAPSAM

Kurumun tüm bilgi varlıklarını kapsar.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından BGYS Komitesi, BGYS Yöneticisi ve bilgi teknolojileri bölümü sorumludur. Tüm kurum çalışanları, geçici görevliler ve kurum bilgi varlıklarına erişimi yetkisi olan herkes bu prosedürdeki kurallara uymak zorundadır.

4. UYGULAMA / POLİTİKA

4.1. Varlık Envanterinin Hazırlanması

6. Varlık envanterinde varlıklara ilişkin sınıflandırma ve etiketleme bilgisi yer almalıdır.
7. Etiketleme aşağıdaki gibi yapılmalıdır.
    - GİZLİ: Uygun etiket gerekir. Kapak sayfası, alt bilgi, üst bilgi, konu vb. alanlarda GİZLİ yazılabilir. KIRMIZI renkli etiket yapıştırılır.
    - KİŞİYE ÖZEL: Uygun etiket gerekir. Kapak sayfası, alt bilgi, üst bilgi, konu vb. alanlarda gizlilik etiketi belirtilmelidir. TURUNCU renkli etiket yapıştırılır.
    - HİZMETE ÖZEL: Uygun etiket gerekir. Kapak sayfası, alt bilgi, üst bilgi, konu vb. alanlarda gizlilik etiketi belirtilmelidir. SARI renkli etiket yapıştırılır.
    - GENEL: Etiket gerekmez. YEŞİL renkli etiket yapıştırılır.

4.2. Uygulama Şekli;

- Etiketleme işlemi de sınıflandırmaya uygun olarak fiziksel varlıkların üzerinde renkli ya da yazılı etiketlerin yapıştırılmasıyla sağlanır. Dolaplara ya da klasörlere içerdiği evraklara göre de belli etiketler yapıştırılabilir. Basılı raporlar üzerinde sınıflandırma (GİZLİ ya da HİZMETE ÖZEL) bilgi olabilir.

5. İLGİLİ DOKÜMANLAR

- Varlıkların Kabul Edilebilir Kullanımı Politikası
- Varlık Envanteri Listesi

EK-7. 16: BGYS Doküman Kayıtların Kontrolü Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.03
Doküman Adı:	Üniversite Kütüphaneleri BGYS Doküman Kayıtların Kontrolü Prosedürü

1. AMAÇ

Bu prosedürde dokümanların nasıl yazılacağı; doküman yapısı, içeriği, güncelleme sistemi vb. işlemler ayrıca dağıtımı ve saklanmasına ilişkin bütün detaylar tanımlanmaktadır.

2. KAPSAM

Bu politikadaki uygulama kuralları, kütüphanede ve ilgili birimlerde çalışan tüm personel için geçerlidir

3. UYGULANABİLİRLİK

BGYS kapsamı içerisinde tutulan tüm bilgi varlıklarıyla ilişkisi olan üniversite kütüphanesi ve ilgili diğer birim çalışanları (bilgi işlem, kalite koordinatörlüğü vb.) çalışanları bu politikayı uygulamakta yükümlü sayılır. Bu politika Üniversite üst yönetimi tarafından onaylanarak yürürlüğe girmiştir.

4. SORUMLULUKLAR

Prosedürün uygulamasından BGYS kurulunda görev yapan tüm personel sorumludur.

5. UYGULAMA

Bu prosedürde şu uygulama başlıkları oluşturulur:

- Dokümanların Sayfa Yapısı
- Dokümanların Tür Kodu Kısaltmaları
- Dokümanların Onaylanması
- Dokümanların Saklanması, Yayımlanması, Dağıtımı
- Dokümanların Revizyonu (Değişiklik-Yenileme, İptali
- Dış Kaynaklı Dokümanlar
- Kayıtların Kontrolü

6. İLGİLİ DOKÜMANLAR

- Doküman Revizyon Formu
- Değişiklik İstek Formu

EK-7. 17: BGYS Düzeltici Faaliyet Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.04
Doküman Adı:	BGYS Düzeltici Faaliyet Prosedürü

1. AMAÇ

Bilgi Güvenliği Yönetim Sistemi (BGYS) sisteminde "uygunsuzluklar" bulunduğunda gerekli Düzeltici Faaliyetlerin (DF) uygulanmasını sağlamaktır.

2. KAPSAM

BGYS tüm süreçlerini ve işleyişini kapsamaktadır.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından BGYS kurulu ve yöneticisi ve bilgi teknolojileri bölümü sorumludur.

4. UYGULAMA

4.1. Düzeltici Faaliyetin Açılması

ISO/IEC 27001:2013 standardına uygunsuzluk, ayrıca yasalara, müşteri gereksinimlerin ve sözleşme koşullarına uygunsuzlukların tespit edilmesi nedeniyle düzeltici faaliyet başlatılabilir. Bu işlem için DÜZELTİCİ FAALİYET TALEP FORMU düzenlenir. Bu form BGYS Yöneticisi tarafından onaylanarak düzeltme işlemi başlar.

4.2. Düzeltici Faaliyetin Uygulanması (Çözüm) Uygunsuzluğun nedeni belirlenir.

- Kök neden analizi yapılır.
- Çözümü için yapılacak işlemler belirlenir.
- Düzeltme işlemi yapılır
- Sorunun gelecekte tekrar etmemesi için gerekli önlemler alınmalıdır.
- Yapılan çalışmalar takip edilir ve gerekirse ek süre verilebilir.

4.3. Düzeltici Faaliyetin Kapatılması

Düzeltici faaliyetin tamamlanmasının ardından BGYS Yöneticisi yaptığı kontrole göre düzeltici faaliyetin tamamlandığından emin olur ve faaliyeti kapatır.

Düzeltici faaliyetin kapatma işleminin ardından BGYS Yöneticisi, düzeltmeyi talep eden kişi ya da bölüme ilgili faaliyetin yapıldığını ve işlemin kapatıldığını belirtir.

5. İLGİLİ DOKÜMANLAR

- Düzeltici faaliyet Talep Formu
- İç Denetim Prosedürü

EK-7. 18: Eğitim / Farkındalık Eğitimi Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.05
Doküman Adı:	Eğitim / Farkındalık Eğitimi Prosedürü

1. AMAÇ

BGYS Komitesi, IT bölümü ve çalışanların "Bilgi Güvenliği Farkındalık" eğitimlerini düzenlemek.

2. KAPSAM

BGYS Komitesi ve tüm çalışanları kapsar.

3. SORUMLULUKLAR

BGYS Yöneticisi ve İnsan Kaynakları bölümü yetkilileri.

4. UYGULAMA / POLİTİKA

4.1. Eğitimlerin Planlanması

Eğitimler, teknik bilişim eğitimleri, ISO/IEC 27001 eğitimleri ve kullanıcılar için bilgi güvenliği "farkındalık" eğitimleri yıllık olarak planlanır.

4.2. Eğitimlerin Gerçekleştirilmesi

Tüm personele ve yeni girenlere farkındalık eğitimi verilmelidir. Farkındalık eğitimi en az dört saat olmak üzere yapılmalıdır. İçerik olarak; kullanıcıların internet ve bilgisayar risklerine karşı riskleri içermelidir. Ayrıca ISO/ IEC 27001:2013'in dokümanları (özellikle varlık kullanım politikaları ve diğer kuralları) hakkında genel bilgileri içermelidir. Eğitimlerin katılım formu mutlaka tutulmalıdır. Eğitim sonu anketi düzenlenmelidir.

4.3. Eğitimlerin Değerlendirilmesi

Katılımcıların eğitim sonu değerlendirmelerinden eğitimin performansı ölçülmelidir. Eğitim değerlendirmeleri Yönetimin Gözden Geçirme (YGG) toplantılarında görüşülmelidir.

5. İLGİLİ DOKÜMANLAR

- Eğitim Katılım Formu
- Yıllık Eğitim Planı

EK-7. 19: Fikri Mülkiyet Haklarının Korunması Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.06
Doküman Adı:	Fikri Mülkiyet Haklarının Korunması Prosedürü

1. AMAÇ

Kuruma ve üçüncü kişilere ait olan fikri hakların korunması ve ihlallerin önlenmesi için yapılacak işlemler tanımlamaktır.

2. KAPSAM

Tüm kurum süreçlerini kapsar.

3. SORUMLULUKLAR

Tüm kurum çalışanları sorumludur.

4. UYGULAMA

4.1. Kuruma Ait Fikri Mülkiyet Haklarının Korunması

- Kurumun ürün ve hizmetlerine ait fikri mülkiyet hakları sadece kurum tarafından kullanılır.
- Kurumun ürün ve hizmetlerine ait fikri mülkiyet haklarının ihlal edilmesi durumunda yetkililere bildirilmelidir.

4.2. Üçüncü Kişilere Ait Fikri Mülkiyet Haklarının Korunması

- Üçüncü kişilere ait fikri mülkiyet haklarının ilgili firmalara ait olması nedeniyle hatalı kullanım yapılmamalıdır.
- Kurum tarafından satın alınmamış ya da yasal biçimde edinilmemiş yazılımlar, elektronik yayınlar (e-kitap, ses, video, vb.) kurum bilgisayarları üzerine kopyalanamaz ve paylaşılamaz.
- Üçüncü kişilere ait fikri mülkiyet haklarının ihlal edilmesi durumunda yetkililere bildirilmelidir.

5. İLGİLİ DOKÜMANLAR

- Fikri Mülkiyet Politikası
- İlgili Yasa Ve Düzenlemelerine Uyum Prosedürü

EK-7. 20: İç Denetim Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.07
Doküman Adı:	İç Denetim Prosedürü

1. AMAÇ

Bu prosedürün amacı, bilgi güvenliği denetimlerin (iç tetkik) nasıl yapılacağını açıklamaktır.

2. KAPSAM

Kurumun ISO/IEC 27001 kapsamı içindeki tüm birimler.

3. SORUMLULUKLAR

BGYS Yöneticisi, bölüm yöneticileri (müdürleri) ve tüm çalışanlar.

4. UYGULAMA

4.1. İç Tetkiklerin Planlanması

- BGYS Yöneticisi ve BGYS Komitesi toplanarak iç tetkik için planlama yapar. Uygun iç tetkik tarihini belirler.
- İç tetkikte görev alacak personel belirlenir.
- İç tetkik tarihleri ve görevliler ilgili birimlere duyurulur.

4.2. İç Tetkik Soru Listelerinin Hazırlanması

- İç tetkik yapılacak alana (bölüme) göre uygun soru listeleri hazırlanır.
- İç Tetkikçi bu soru listelerini kullanarak denetimi yapar ve raporunu hazırlar.

4.3. İç Tetkiklerin Gerçekleştirilmesi

- İç tetkikler kuruma uygun şekilde belli alanlara ayrılabilir.

4.4. Tipik olarak;

- Tüm Birimlerin Ortak Denetimi (İlgili sorular hazırlanır)
- Bilgi İşlem Altyapısının (Teknik) Denetimi (İlgili sorular hazırlanır)
- Fiziksel ve Çevresel Güvenlik Denetimi(İlgili sorular hazırlanır)

4.5. İç Tetkiklerin Raporlanması

- İç tetkiklerin yapılması sürecinde bulunan uygunsuzluklar UYGUNSUZLUK TESPİT/BİLDİRİM FORMU doldurulur.
- Ardından tüm sonuçlar bir İÇ TETKİK RAPORU ile üst yönetime sunulur.

5. İLGİLİ DOKÜMANLAR

- Uygunsuzluk Tespit/Bildirim Formu
- İlgili Dokümanlar

EK-7. 21: İhlal Olayları Yönetim Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.08
Doküman Adı:	İhlal Olayları Yönetim Prosedürü

1. AMAÇ

Bu prosedürün amacı, bilgi güvenliği ihlal olaylarının bildirilmesini ve ihlallere karşı yapılacak işlemleri tanımlamak.

2. KAPSAM

Kurum bilgi varlıklarının kullanıldığı tüm alanlar.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından BGYS Komitesi, BGYS Yöneticisi ve bilgi teknolojileri bölümü sorumludur. Tüm kurum çalışanları, geçici görevliler ve kurum bilgi varlıklarına erişimi yetkisi olan herkes bu prosedürdeki kurallara uymak zorundadır.

4. UYGULAMA

Bilgi güvenliği ihlal olaylarının yönetimi bilgi güvenliği yönetim sistemi (BGYS) süreçleri içinde en önemlilerinden birisidir. Çünkü güvenliğin tam olarak sağlanması için ihlal olaylarının belirlenmesi ve değerlendirilmesi gerekir.

4.1. İhlal Olaylarının Tanımlanması

BGYS başta olmak üzere kurum iş süreçlerinin tümüne ya da bir kısmına olumsuz olarak etki eden yazılım, donanım ve insan kaynağı temelli her türlü olay güvenlik ihlal olayı olarak tanımlanmalıdır.

Aşağıda tipik ihlal olayları yer almaktadır

- Bilgi güvenliği kurallarına uymamak. Varlık kullanım kurallarına uymamak
- Kullanıcıların bilgisayarlarını başıboş (kilitlemeden) bırakması.
- Yetkisiz erişim.
- Bilgi hırsızlığı.
- Yetkisiz bilgi kopyalama.
- Parola paylaşımı.
- Elektronik posta ve internet erişiminde kurum çıkarlarına ters düşen işlemler yapmak.
- Fiziksel ve çevresel koşulların kullanımının gerektirdiği kurallara uymamak.
- Flash belleklerin izinsiz kullanımı.
- Varlıkların izinsiz dışarı çıkarılması.
- Gizli evrakların ortalıkta bırakılması.
- Varlık imha kurallarına uymamak.
- İş sözleşmesinin bitmesine rağmen şirket bilgi varlıklarına erişmek ya da kullanmak.

4.2. İhlal Olayının Tespiti/Bildirimi

- Güvenlik ihlal olayları bildirimi kullanıcılar tarafından İHLAL TESPİT/BİLDİRİM FORMU aracılığıyla yapılabilir.
- Güvenlik ihlal olayları bilgi sistemlerinin incelemesi sonucu tespit edilebilir.

4.3. İhlal Olayının Değerlendirilmesi ve Karar Verme

- Her bir güvenlik ihlal olayı BGYS Yöneticisi tarafından değerlendirilerek gerekli yanıt verilmelidir.
- Değerlendirme sürecinde olayın kanıtları incelenmeli, varsa sorumluları ve şahitler dinlenmelidir.
- İhlal olayları belli bir önem derecesine göre sınıflandırılmalıdır.

4.4. İhlal Olaylarının Derecesi:

- Yüksek: Kritik varlıkları etkileyen olaylar. Olay raporlanmalı. BGYS Yöneticisi ve üst yönetime bildirilmeli. Gerekli işlemler (yasal işlemler, kurum disiplin işlemleri) başlatılmalıdır
- Orta: Kritik varlıkların etkilenmediği, ancak kuruma zarar verebilecek olaylar. Olay raporlanmalı, İnsan Kaynaklarına ya da ilgili birimlere bildirilmelidir
- Düşük: Genel olarak kuruma ve bilgi varlıklarına zarar vermeyen olaylar. Olay raporlanmalı.

4.5. Kanıt Toplama

İhlal olayının değerlendirme sürecinde olaya ilişkin kanıt toplanır. Kanıtlar şunlardır:

- Bilgisayar ortamındaki erişimler, loglar, dosyalar ve diğer işlemler.
- Elde edilen dosyalar, ekran görüntüleri vb.
- Kamera görüntüleri.
- Şahitlerin ifadeleri.

Kanıt toplama işlemi mümkünse şahit huzurunda gerçekleştirilmelidir. Kanıt toplama sürecinde şu kurallara uyulmalıdır.

- İşlemlerin yasal yollarla yapılması gerekir.
- Olayın zamanı ve teknik detayları belirlenmelidir.
- Elektronik kayıtların bir kopyasının alınması gerekir.

4.6. İhlal Olayına Yanıt Verme

- İhlal olaylarının ardından gerekli tutanaklar tutulmalı ve karşılıklı olarak imzalanmalıdır. Olaylar üst yönetime, İnsan Kaynakları yöneticilerine ve gerekirse emniyet (bilişim arı polisi) birimlerine bildirilmelidir.

4.7. İhlal Olayının Raporlanması

- İhlal olayına yapılan müdahalenin ardından bir rapor (İHLAL OLAYI RAPORU) hazırlanmalıdır. İhlal olayının ardından "uygunsuzluk tespiti" söz konusu ise gerekli düzeltme faaliyeti başlatılmalıdır.

5. İLGİLİ DOKÜMANLAR

- İhlal Olayı Tespit/Bildirim Formu İhlal Olayı Raporu

EK-7. 22: İletişim Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.09
Doküman Adı:	İletişim Prosedürü

1. AMAÇ

BGYS süreçleriyle ilgili olarak kurum içerisinde iç ve dış paydaşlarla (iletişim kurulacak birimler, tedarikçiler, vb.) iletişimin nasıl yapılacağı belirlenmelidir.

2. KAPSAM

Kurum bilgi varlıklarının kullanıldığı tüm alanlar.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından BGYS Komitesi, BGYS Yöneticisi ve bilgi teknolojileri bölümü sorumludur. Tüm kurum çalışanları, geçici görevliler ve kurum bilgi varlıklarına erişimi yetkisi olan herkes bu prosedürdeki kurallara uymak zorundadır.

4. UYGULAMA / POLİTİKA

4.1. Genel Kurallar

- BGYS süreçleriyle ilgili olarak; kurum içerisinde iç ve dış paydaşlarla (iletişim kurulacak birimler, tedarikçiler, vb.) iletişimin nasıl yapılacağı belirlenmelidir. İletişim konuları, sorumluluklar vb. detayların BGYS prosedürlerinde tanımlı olması beklenir. ● ●
- Gizli bilgilerin konu edildiği iletişimlerde gizli bilgilerin güvenliğinin sağlanması gerekir.
- Bilgi güvenliği ihlal olayı olduğunda yapılacak iletişim (kimle, nasıl ve ne zaman) belirlenmelidir.
- Acil durumlarda (yangın, deprem, saldırı, vb. iş sürekliliğini tehlikeye atan durumlarda) yapılacak iletişim (kimle, nasıl ve ne zaman) belirlenmelidir. İletişim sürecinde yasalara ve kişilik haklarına uyulmalıdır.
- İletişim kanalı telefon, elektronik posta, Internet ve diğer uygun ortamlardır. Kurumsal iletişimde öncelikle elektronik posta (e-mail) tercih edilmelidir.
- İletişim formel bir şekilde yapılmalıdır. Mesajlar kısa ve öz olarak düzenlenmelidir. Ayrıca mesajlarda alıcının organizasyon içindeki konumuna göre uygun bir hitap dili kullanılmalıdır.

4.2. İletişimin Türleri (Şekilleri)

ISO/IEC 27001:2013 aşağıdaki şekillerde "iletişim" yapmamızı önermektedir:

- İç/dış birimlerle (paydaşlarla) yapılacak iletişim (kimle, nasıl ve ne zaman) belirlenmelidir.
- Otoritelerle (polis, yangın, belediye, vb.) yapılacak iletişim (kimle, nasıl ve ne zaman) belirlenmelidir.
- Özel ilgi grupları (forumlar, bilgi güvenliği kurumları) yapılacak iletişim (kimle, nasıl ve ne zaman) belirlenmelidir.

4.2.1. İç İletişim

- İç iletişim, BGYS Komitesi, BGYS Yöneticisi ve ilgili birimlerin kurum içinde yapacağı iletişimi belirler.
- İç iletişim birçok araçla yapılabilir; panolar, telefon, toplantılar, doküman yayınlama, elektronik posta, web siteleri vb.
- İç iletişim için uygun bir planlama yapılmalıdır.

4.2.2. Dış İletişim

- Diş iletişim yine belirtilen araçlarla kurum dışından kişilerle ve kurumlarla yapılan iletişimdir.
- Diş iletişimde gizli bilgilerin kullanımı yetkililer tarafından izin verilmedikçe yasaklanmalıdır.
- Gizlilik anlaşması imzalanmalıdır.

4.2.3. Otoritelerle İletişim

- Otoritelerle (polis, yangın, Telekom, belediye, vb.) yapılacak iletişim (kimle, nasıl ve ne zaman) belirlenmelidir.

5. İLGİLİ DOKÜMANLAR

- İhlal Olayları Yönetim Prosedürü

EK-7. 23: İzleme, Ölçme, Analiz ve Değerlendirme Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.10
Doküman Adı:	İzleme, Ölçme, Analiz ve Değerlendirme Prosedürü

1. AMAÇ

Bu prosedürün amacı, BGYS'nin başarımına ilişkin olarak izleme, ölçme ve değerlendirme işlemlerini tanımlamak.

2. KAPSAM

Başarımı ölçülebilecek olan bütün BGYS bileşenleri.

3. SORUMLULUKLAR

BGYS Yöneticisi ve BGYS Komitesi.

4. UYGULAMA / POLİTİKA

4.1. Değerlendirme kriterleri belirlenmelidir. Tipik kriterler şunlardır:

- Uygunsuzluk sayısı: BGYS hizmetlerinin sunulması sırasında ortaya çıkan hatalı durumlar izlenir. Bulunan uygunsuzluk ve açılan düzeltici faaliyet sayısının az olması bir başarı kriteridir.
- İhlal olayları sayısı: Bilgi güvenliği politika ve prosedürlerine aykırı hareketler ve saldırılar izlenir. Tespit edilen ihlal sayısının az olması başarı kriteridir. Sistemin durma (kesinti) zamanları: Güvenlikle ilgili olarak servislerin durma sayıları ve süreleri. Bu bilgiler sunucu işletim sistemleri ve ilgili yazılımların loglarından izlenir. Hizmet kesintisi süresinin az olması başarı kriteridir.
- Kapasite kullanımı: Sistemlerin kapasitelerinin uygun şekilde kullanılması - kapasitenin aşılmaması bir başarı kriteridir.
- Bütçeye uyma: BGYS planlaması sürecinde yapılan bütçe harcamalarının içinde kalınıp kalınmadığı denetlenir. Bütçeyi aşmamak başarı kriteridir.
- Risklerin düşürülmesi: İşlenen risk sayısı ve risklerin düşürme oranları başarı kriteridir. Kullanıcı Anketleri: Kullanıcıların BGYS'den memnun olmaları başarı kriteridir.
- İç Tetkikler: İç tetkik sonuçlarına göre bulunan uygunsuzlukların azlığı başarı kriteridir. Penetrasyon testi sonuçları: Bulunan zayıflıkların ve açıkların sayıca az olması başarı kriteridir.
- İç ağ teknik açıklık taraması sonuçları: Bulunan zayıflıkların ve açıkların sayıca az olması başarı kriteridir.
- Loglama işlemleri: Tutulan ve izlenen loglama işlemlerinin düzenli olarak yapılması bir başarı kriteridir.
- Yedekleme işlemleri: Düzenli olarak yapılan yedekleme işlemleri başarı kriteridir. Tatbikat sayıları; Düzenli olarak yapılan başarılı iş sürekliliği tatbikatları bir başarı kriteridir.

4.2. Raporlama yapılmalıdır. Raporlarda şu konulara yer verilmelidir;

- Ölçme işlemi, işlem sayıları ve zaman temelinde kurulacak bir metrik sistemi ile takip edilmelidir.
- Performans izleme bilgileri, önceki değerler, deneyimler ve sektörler ortalamalara göre karşılaştırılarak değerlendirilmelidir.
- Her ay performansa yönelik olarak PERFORMANS RAPORU düzenlenerek ve üst yönetime sunulmalıdır.
- Yönetim Gözden Geçirme toplantılarında performans raporları değerlendirilir

5. İLGİLİ DOKÜMANLAR

- İzleme ve Ölçme Planı Performans Raporu

EK-7. 24: Varlık Yönetimi Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.11
Doküman Adı:	Varlık Yönetimi Prosedürü

1. AMAÇ

Bu prosedürün amacı, BGYS sistemi içinde varlıkların envantere alınması, sahipliği, kullanılması/el değiştirmesi, taşınması ve ömrünü tamamladığında imha edilmesi için gerekli işlemlerini belirlemektir.

2. KAPSAM

Tüm bilgi varlıklarını kapsar.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından BGYS Komitesi, BGYS Yöneticisi ve bilgi teknolojileri bölümü sorumludur. Tüm kurum çalışanları, geçici görevliler ve kurum bilgi varlıklarına erişimi yetkisi olan herkes bu prosedürdeki kurallara uymak zorundadır.

4. UYGULAMA / POLİTİKA

4.1. Varlık Envanterinin Oluşturulması

- BGYS Komitesi çalışmaları temelinde; kurum departman sorumlularından varlık listeleri alınır.
- Bilgi işlem bölümü ile birlikte çalışarak donanım, yazılım, ağ aygıtları gibi varlıkların listesi elde edilir.
- Varlık envanteri oluşturulur.
- Varlıklar uygun şekilde kategorilere ayrılır. Her varlığın değeri Gizlilik, Bütünlük ve Erişilebilirlik (GBE) temelinde hesaplanır.
- Envanterde ayrıca varlıkların Sahiplik, Varlık Sınıfı, Gizlilik Sınıfı ve bulunduğu yer gibi bilgiler yer alabilir.
- Uygun zamanlarda varlık envanteri güncellenir.

4.2. Varlıkların Kullanımı

- Varlık envanterine kaydedilerek değerleri belirlenen varlıkların sahipleri tarafından uygun şekilde kullanılması gerekir.
- Varlıkların kullanımına ilişkin "varlıkların kabul edilebilir kullanımı" politikası ve diğer ilgili dokümanlara (talimat ve prosedürler) uyulmalıdır.

4.3. Varlıkların İadesi

- Kurum çalışanlarına verilen varlıklar, iş akdinin sona ermesiyle birlikte geri alınması gerekir. Bu işlem genellikle uygun bir form aracılığıyla yapılır. Bu form aracılığıyla verilen varlıkların kontrol edilerek geri alınması ve karşılıklı onaylanması işlemi yapılır. ●
- Varlıkların iadesi ve varlık yönetimine ilişkin uygulamalar hakkında daha geniş bilgi için bu bölümde yer alan “varlıkların kabul edilebilir kullanımı" politikası, zimmet formu, varlık imha tutanağı ve varlıklarla ilgili diğer dokümanlara bakınız.

4.3. Varlıkların İmhası

- Varlık yönetimi sürecinde bir diğer işlem de işlevi ya da kullanım ömrü dolan bir varlığın (bir donanım, bir evrak, bir saklama birimi, vb.) uygun bir biçimde imha edilmesi gereğidir. Örneğin bastırılmış gizli bir evrakın yok edilmesi onu çöpe atarak olmaz. O evrakın "evrak imha/öğütme makinesi" aracılığıyla okunamaz duruma getirilmesi gerekir. Benzer şekilde bir donanımın da bir daha kullanımı mümkün olmayacak şekilde imha edilmesi gerekir. Bu işlemler için özel hizmetler alınabileceği gibi uygun şekilde kırım yaparak ve bu işlemin bir tutanağı (fotoğrafı ile birlikte) tutularak işlem yapılmalıdır.

4.4. Varlıkların Taşınması

- Bir varlığın taşınması için ilgili birim yetkilisinden izin alınmalıdır. Kritik varlıkların bakıma gönderilmesi sürecinde gerekli güvenlik önlemleri alınmalıdır. ●
- Sistem odası, sunucu bilgisayar vb. kritik bilgi varlıkların taşınmadan önce taşıma işleminin bir tutanağı hazırlanmalı, BGYS Yöneticisi ve Genel Müdür tarafından onaylanmalıdır.

5. İLGİLİ DOKÜMANLAR

- Varlık Envanteri, Varlıkların Kabul Edilebilir Kullanımı Politikası

EK-7. 25: Yönetimin Gözden Geçirme (YGG) Prosedürü

Doküman No:	KÜTÜPHANE.BGYS.PR.12
Doküman Adı:	Yönetimin Gözden Geçirme (YGG) Prosedürü

1. AMAÇ

BGYS'nin etkinliğini gözden geçirmek.

2. KAPSAM

BGYS Süreçlerini kapamaktadır.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından BGYS Yöneticisi ve BGYS Komitesi ve yöneticiler sorumludur. Toplantılar aşağıdaki yönetimin üyelerinin aktif katılımı ile yapılır:

- Genel Müdür
- BGYS Yöneticisi
- BGYS Komitesi
- Bölüm Yöneticileri
- İnsan Kaynakları Yöneticisi
- Diğer ilgili kişiler

4. UYGULAMA / POLİTİKA

4.1. Genel

Yönetimin Gözden Geçirme (YGG), ISO/IEC 27001:2013 ve BGYS'nin başarılı bir şekilde yürütülmesini sağlamak üzere üst yönetimin katılımıyla yapılan toplantılardır.

4.2. Toplantının Zamanı (Periyodu)

Yönetim gözden geçirme toplantısı senede en az bir kere yapılmalıdır. Özel durumlarda toplantılar daha sık yapılabilir.

4.3. Toplantının Duyurulması

Toplantının zamanı BGYS Yöneticisi tarafından belirlenir ve en az on beş gün öncesinden üst yönetime (genel müdür) bildirilir.

4.4. Toplantının Gündemi

- Toplantılarda görüşülen konular genel olarak aşağıda belirtilen maddeleri içerir;
- Bilgi Güvenliği Politikası ‘nın gözden geçirilmesi
- Risk Yönetim metodolojisinin gözden geçirilmesi
- Risk işleme planının gözden geçirilmesi
- Düşürülen risklerin açıklanması
- Güncel risk raporunun değerlendirilmesi
- Güvenlik ihlal olaylarının değerlendirilmesi
- İş sürekliliği stratejisinin gözden geçirilmesi
- İş sürekliliği tatbikat sonuçlarının değerlendirilmesi
- Bilgi güvenliği farkındalık çalışmalarının gözden geçirilmesi
- İç tetkik (denetim) raporlarının değerlendirilmesi
- Varlık Envanteri, varlık sahiplik ve kullanıcı erişim haklarının gözden geçirilmesi İzleme ve ölçme sonuçları,
- Üçüncü taraflardan geri bildirimlerin değerlendirilmesi (varsa)
- Donanımların kapasitesi ve ileriye dönük olarak planlaması Yedekleme donanımlarının gözden geçirilmesi
- Gizlilik anlaşmalarının gözden geçirilmesi
- Personel politikalarının ve insan kaynakları uygulamalarının gözden geçirilmesi Diğer konular.
- Kaynakların ve bütçenin değerlendirilmesi.

4.5. Toplantı Tutanağı

- YGG toplantısında gündem maddeleri ile ilgili kararlar alınır. Toplantının sonucunda, toplantıda görüşülen tüm konular ve alınan kararlar BGYS Yöneticisi tarafından kayıt altına alınır ve Genel Müdür onayına sunulur.

5. İLGİLİ DOKÜMANLAR

- İzleme, Ölçme, Analiz Ve Değerlendirme Prosedürü, İç Tetkik Prosedürü

EK-7. 26: BGYS Dokümanının Kapsam ve Bağlam Dokümanı

Doküman No:	KÜTÜPHANE. BGYS. DOK. 01
Doküman Adı:	Üniversite Kütüphaneleri BGYS Belgesi Kapsamı ve Bağlamı

Bilgi hizmeti sunan ….Üniversitesi kütüphanelerinin iş ve işlemlerin yürütülmesi süreçlerinde kullanılan bilgi varlıklarını korumak amacıyla kurulan ve kullanılan donanım, yazılım, ağ, veri tabanları, bilgi sistemleri gibi teknolojik altyapı ile birlikte insan kaynakları, dokümantasyon, fiziksel ve çevresel yapılar gibi bilgi varlıklarının güvenliğini kapsamaktadır.

Kütüphanenin altyapısı, personeli ve kurum kültürüne ilişkin iç bağlamı şu konuları içermektedir:

- Bilgi teknolojileri kaynaklı bilgi güvenliği riskleri ve tehditleri.
- Çevresel / fiziksel faktörler ve insan kaynaklı bilgi güvenliği riskleri ve tehditleri.

Kütüphanenin yasal konuları, çevre şartları ve teknolojik gelişmelere karşı ilişkileri belirleyen dış bağlam ise şu konuları içermektedir:

- Sözleşmeler ve hizmet anlaşmaları.
- Kullanıcı beklentileri.
- Üçüncü tarafın sözleşme gereği beklentileri.
- Doğal afetler, grev, lokavt gibi dış riskler.
- Mevzuat ve düzenleyici yapıların diğer şartları.

EK-7. 27:Gizlilik Sözleşmesi Formu

Doküman No:	KÜTÜPHANE.BGYS.FRM.01
Doküman Adı:	**Gizlilik Sözleşmesi Formu**

Gizlilik sözleşmesi hukuki bir metindir. Tarafların belirtilen “gizli bilgileri" ifşa etmemesi üzerinde aralarında imzaladığı bir anlaşmadır. Tedarikçiler, danışmanlar, kritik personel vb. gizli bilgileri kullanan ya da erişen kişilerle yapılır.

Genel olarak yapısı şu şekildedir:

Taraflar: Sözleşmenin tarafları, kurum (bilgi veren) ve karşı taraf (bilgiyi alan şirket ya da kişi)

Gizli bilgi: Gizli bilgi, kurumun sahip olduğu her türlü bilgiyi ifade eder. Gizli bilgi basılı, sözlü ya da bilgisayar ortamında olabilir. Tipik olarak aşağıdaki bilgi unsuları gizli bilgi olarak bu anlaşmada yer alır:

- Tasarım
- İş süreçleri
- Fikirler, fikri mülkiyet hakları
- Metotlar
- Ticari sırlar
- Teknik bilgiler
- Müşteri bilgileri
- Tedarikçi bilgileri
- Ürün özellikleri
- Personel bilgileri
- Bilgisayar sistemleri
- Muhasebe kayıtları
- Sözleşmeler, taahhütnameler vb. hukuki metinler.

Tarafların yükümlülükleri: Gizli bilgileri ifşa etmeme.

Cezai şart: Sözleşme hükümlerine uyulmadığında belli bir maddi (para) karşılık olarak cezai şart uygulanır.

Özel şartlar: …

Onay:

EK-7. 28: BGYS Fark Analizi Formu

Doküman No:	KÜTÜPHANE.BGYS.FRM.02
Doküman Adı	BGYS Fark Analizi Formu

S. N.	Donanım Güvenliği Kontrolleri	Evet	Fikrim Yok	Hayır
1	Kurum bünyesinde detaylı ve güncel bir donanım envanter yönetimi yapılmakta mıdır?			
2	Donanım envanter içeriği yönetimi (sahiplik, erişim yetkisi, değişiklik kaydı, güncelleme vb.) yürütülmekte midir?			
3	Donanım envanterine kaydedilmiş tüm donanımların belirli bir politika/prosedür kapsamında yönetilmekte midir?			
4	Kurum ağına bağlanan donanımları keşif amaçlı araçlar kullanılmakta mıdır?			
5	Tespit edilen yeni donanımlar, donanım envanterine kaydedilmekte midir?			
6	Cihazların veri depolama ünitelerini güvenli silme yöntemleri kullanılmaktadır?			
7	Kullanım ömrünü tamamlayan cihazların ve veri depolama ünitelerinnin güvenli biçimde imha yöntemlerinin belirlendiği politika / prosedür kullanılmakta mıdır?			
8	Kuruma ait güvenli ağlara bağlanan donanımlar 802.1x ve NAC çözümleri kullanılarak kimlik doğrulama denetimi yapılmakta mıdır?			
9	Kurum ağına bağlanan donanımlar için istemci sertifikalar ile kimlik doğrulama denetimi yapılmakta mıdır?			
10	Kurumdaki donanımlarda kullanılmak için temin edilen sabit disklerin sisteme dâhil edilmeden önce güvenli silme işlemlerine tabi tutulmakta mıdır?			
11	Kurumdaki depolama aygıt ve ortamları için belirli bir politika yürütülmekte midir?			
12	Eskiyen veya zafiyet içerdiği tespit edilen donanımların yerlerine yeni ve güvenli donanımlar sağlanıyor mu?			
13	Diğer (…)			

S. N.	Yazılım Güvenliği Kontrolleri	Evet	Fikrim Yok	Hayır
1	Yazılım envanteri tutulmakta mıdır?			
2	Yazılım envanter yönetimiyle ilgili faaliyetleri içeren prosedürler bulunmakta mıdır?			
3	Yazılım envanter içerik (isim, versiyon, lisans bilgileri vb.) yönetimi sağlanmakta mıdır?			
4	Kurum tarafından onaylanmayan yazılımların kullanımına yönelik ilke ve yöntemler bulunmakta mıdır?			
5	Yazılım ve donanım envanter sistemleri birbirine entegre yürütülmekte midir?			
6	Kullanılmasına izin verilen yazılımlar için beyaz liste yönetimi kullanılmakta mıdır?			
7	Yazılım güvenlik güncellemeleri zamanında yapılmakta mıdır?			
8	Yazılım güncellemeleri yazılım güncelleme araçlarıyla otomatik takip edilmekte midir?			
9	Kullanıcıların yazılım yükleme yetkisi kısıtlanmakta mıdır?			
10	Zararlı yazılımdan korunma uygulamaları kullanılmakta mıdır?			
11	Zararlı yazılımdan korunma politikaları bulunmakta mıdır?			
12	Bilgisayarların diskleri zararlı yazılım taramasından otomatik geçilmekte midir?			
13	Bilgisayarlar otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılmakta mıdır?			
14	Tespit edilen zararlı yazılımlar ilgili bildirimler bildirilip kayıt altına alınmakta mıdır?			
15	Uygulamalarda, kimlik doğrulama mekanizması kullanılmakta mıdır?			
16	Uygulamalarda, kullanıcı hesaplarını yönetme ara yüzleri kullanılmakta mıdır?			
17	Uygulamalardaki kullanıcı hesapları denetlenip kilitlenebiliyor mu?			
18	Kimlik doğrulama uygulamalarının güvenliği sağlanmakta mıdır?			

19	Kimlik doğrulama mekanizmalarında elektronik imza gibi güçlü yöntemler kullanılabilmekte midir?			
20	Uygulamaların çalıştığı bilgisayarlardan dış kaynaklara uzaktan bağlantı sağlanabilmekte midir?			
21	Uygulamanın çalıştığı sunuculardan uygulama ile ilişkili olmayan kaynak ve sistemlere uzaktan bağlantı ve erişim engelleniyor mu?			
22	Uygulamaların çalıştığı bilgisayarlara uzak masaüstü ile dışarıdan erişilebilmekte midir?			
23	Yazılım güvenlik gereksinim ve tasarımları tanımlanmış mıdır?			
24	Kullanılan veya tedarik edilen uygulamalar için sızma testleri yapılmakta mıdır?			
25	Yeni uygulamalar devreye alınmadan önce kaynak kod analizinden geçirilmekte midir?			
26	Diğer (…)			
S. N.	**Ağ Güvenliği Kontrolleri**	**Evet**	**Fikrim Yok**	**Hayır**
1	Kurum ağlarına ait kullanım metotları bulunmakta mıdır?			
2	Donanım ve yazılım envanteri ile ağlar eşleşmekte midir?			
3	Ağ cihazları iyi uygulama standartlarına ve üretici tavsiyelerine uygun yapılandırılmakta mıdır?			
4	Ağ sistemlerinde varsayılan parola ve kullanıcı adları kullanılmakta mıdır?			
5	Ağ altyapısındaki donanımlar yine ağ üzerinden kontrol edilebilmekte midir?			
6	Ağ cihazlarının üreticisi tarafından yayımlanmış güncel sürümler kullanılmakta mıdır?			
7	Ağ sisteminde beyaz ve kara liste yapısı kullanılmakta mıdır?			
8	Ağ içerisindeki bağlantı trafiği kontrol edilebilmekte midir?			
9	Bilgi güvenliği gereksinimleri doğrultusunda kurum ağları katmanlara (genel, kullanıcı, misafir vb.) ayrılmakta mıdır?			
10	İnternet ortamından kurum içi kaynaklara erişim sağlanabilmekte midir?			
11	Kurum içi kaynaklara dışarıdan erişim için VPN teknolojileri kullanılmakta mıdır?			
12	Kurum ağına bağlı yetkili kablosuz erişim noktaları tespit edilebilmekte midir?			
13	Kurum ağından izole edilmiş bir misafir ağı kullanılmakta mıdır?			
14	Ağ sistem güvenlik duvarlarıyla korunmakta mıdır?			
15	IP telefon sistemlerinde kimlik sahteciliği saldırılarına karşı güvenlik önlemleri alınmakta mıdır?			
16	Ağlardan gelebilecek saldırılara karşı tespit ve engelleme araçları kullanılmakta mıdır?			
17	Ağ trafiği, yetkisiz bağlantıları engellemek amacıyla filtreleme ve kimlik doğrulama sistemleri kullanılmakta mıdır?			
18	Kurumda tüm bilgi sistemleri için ağ tabanlı URL filtreleme ve sınıflandırma servisi kullanılmakta mıdır?			
19	Kurum ağına bağlı yetkisiz kablosuz erişimlerin tespiti için kontrol araçları kullanılmakta mıdır?			
20	Donanımların, kayıtsız kablosuz çevre birimleri aracılığı ile yetkisiz erişimleri kısıtlanabilmekte midir?			
21	Ağ cihazlarının yönetimi için çok faktörlü kimlik doğrulama mekanizmaları kullanılmakta mıdır?			
22	Kurum politikalarına uymayan donanımlara ağ bağlantısı sağlanmakta mıdır?			
23	Kritik ağ ortamları için kripto ağ cihazları kullanılmakta mıdır?			
24	Kablosuz ağlardan kritik veri taşınırken kimlik doğrulama protokolü uygulanmakta mıdır?			
25	Kritik veri işleyen kapalı ağlara, kablosuz klavye ve fare gibi çevre birimlerin takılmasına izin verilmekte midir?			
26	Düzenli olarak erişilmeyen sistemlerin ağ bağlantıları kesilmekte midir?			
27	Diğer (…)			
S. N.	**Veri Güvenliği Kontrolleri**	**Evet**	**Fikrim Yok**	**Hayır**
1	Kritik verilerin envanteri tutulmakta mıdır?			
2	Düzenli olarak erişilmeyen kritik verilere ait sistemler ihtiyaç duyulana kadar ağ ile bağlantısı kesilmekte midir?			
3	Ağlarda kritik veri taşınmakta mıdır?			
4	Kritik verinin güvenlik politikalarına uymayan bir şekilde kullanılmasına yönelik bir önlem uygulanmakta mıdır?			
5	Kullanılmayan veri ortamlarında yer alan kritik verilerin güvenliği sağlanmakta mıdır?			
6	Bilgi varlıklarında yer alan sistemlerin varsayılan parolaları değiştirilmekte midir?			
7	Bilgi sistemlerinde kullanılmayan hesaplar silinmekte midir?			
8	Sistem yöneticileri için uygulamalarda ayrı bir hesap tanımlanmakta mıdır?			
9	Uygulamalarda işlem yapılmayan oturumlar belirli bir süre sonra sonlandırılmakta mıdır?			
10	Bilgi varlıklarına erişimlerde kimlik doğrulama araçları ve sistemleri kullanılmakta mıdır?			
11	Uygulamalarda görevi sona eren hesaplar silinmekte midir?			
12	Kritik ve gizli verilerin işlendiği ve saklandığı sistemler üzerinde yapılan işlemler takip edilmekte midir?			
13	Sistem yetkilendirmeleri düzenli olarak takip edilmekte midir?			

14	Parola ve veri ve güvenliği için otomatik kontrol ve yönetim aracı kullanılmakta mıdır?			
15	Aynı hesabın birden fazla kullanıcı tarafından kullanılmasına izin verilmekte midir?			
16	Kullanıcı parolaları kriptografik yöntemler ile saklanmaktadır?			
17	İlk parola belirleme sürecinde ve iletiminde güvenli yöntemler kullanılmakta mıdır?			
18	Kullanıcı, ilk parolayı kullandıktan sonra değişiklik yapmasına zorlanıyor mu?			
19	Uygulamanın kullandığı bilgi sistemlerinde varsayılan kullanıcı bulunmakta mıdır?			
20	Uygulama kodlarında herhangi bir kullanıcıya ait bilgiler (parola, kullanıcı adı, anahtar vb.) bulunmakta mıdır?			
21	Kullanıcıların parola değiştirme işleminde mevcut parolası üzerinden doğrulama isteniliyor mu?			
22	Parolamı unuttum, süresi dolmuş parolanın güncellenmesi, görüntü güncelleme, devre dışı kayıp simge ve yardım masası yöntemleri ile yapılan hesap kurtarma yöntemlerinin güvenliği sağlanmakta mıdır?			
23	Belirli bir süre hiç kullanılmamış hesaplar tespit edilmekte midir?			
24	Kimlik doğrulamada merkezi kimlik ve doğrulama sistemi kullanılmakta mıdır?			
25	Kimlik doğrulama için E-Devlet sistemi uygulanmakta mıdır?			
26	Kimlik doğrulama yapmak amacıyla sızma testleri yapılmakta mıdır?			
27	Kullanıcı oturumu kapatıldığında oturumun sonlandığı kontrol edilmekte midir?			
28	Kullanıcı oturumlarında işlem yapılmadan beklenecek süre veya oturum kimliğinin geçerlilik süresi gibi kısıtlamalar uygulanmakta mıdır?			
29	Geçerlilik süresi belirlenene oturumlarda işlem yapılmadan beklenen geçerlilik süresi sonunda oturum otomatik sonlanmakta mıdır?			
30	Oturum güvenliği için güvenlik araçları kullanılmakta mıdır?			
31	Uygulamalara erişim için yetki matrisi tanımlanmış mıdır?			
32	Kritik verilere erişimlerin kayıtları tutulmakta mıdır?			
33	Kullanıcılara yetkileri, görevleri ve gereksinimleri doğrultusunda en az yetki prensipleri uygulanmakta mıdır?			
34	Güvenilmeyen kaynaklardan ve kullanıcıdan gelen dosyalar denetlenmekte midir?			
35	Veri kaynaklarına erişim kısıtlanmakta mıdır?			
36	Veri erişim kontrol politikaları kullanılmakta mıdır?			
37	Verilerin kategorilere ayrılması ve sınıflandırılması için politikalar bulunmakta mıdır?			
38	Diğer (…)			

S. N.	**Fiziksel ve Çevresel Güvenlik Kontrolleri**	**Evet**	**Fikrim Yok**	**Hayır**
1	Kritik bilgi ve bilgi işleme olanakları barındıran alanların fiziksel güvenlik sınırları tanımlanmış mıdır?			
2	Kritik bilgi ve bilgi işleme olanakları barındıran alanların giriş ve çıkış noktalarında güvenlik kontrol mekanizması bulunmakta mıdır?			
3	Kuruma fiziksel giriş ve çıkış kontrolleri yapılmakta mıdır?			
4	Binalara ait bütün pencereler, kapılar, dış duvarlar gibi güvenlik altına alınması gereken yerler dış güvenlik kontrolleri ve mekanizmaları ile takip edilmekte midir?			
5	Ziyaretçi giriş çıkış kontrolleri yapılmakta mıdır?			
6	Ziyaretçi bilgileri kayıt altına alınmakta mıdır?			
7	Yetkisiz fiziksel erişim tespit edildiğinde izlenecek güvenlik adımları tanımlanmış mı?			
8	Enerji ve ağların kablolama güvenliğini sağlamakta mıdır?			
9	Doğal afet önlem planları yapılmış mı?			
10	Acil durum eylem planları yapılmış mı?			
11	Dış ve çevresel tehditlere karşı koruma planları yapılmış mı?			
12	Kapalı devre kamera güvenlik sistemi kullanılıyor mu?			
13	Binalardaki çalışma alanlarının güvenliği ile ilgili önlemler geliştirilmiş mi?			
14	Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği ortamlarında mobil ve veri transferi özelliğine sahip cihazların kullanılmamasına dikkat ediliyor mu?			
15	Donanım ve altyapı sistemlerinin periyodik bakımları yapılıyor mu?			
16	Ziyaretçi kabul prosedürü tanımlanmış mıdır?			
17	Ziyaretçilerin giriş ve çıkışlarında refakatçi gözlemi yapılmakta mıdır?			
18	Personel ve kullanıcılar için fiziksel erişim güvenliği sağlanıyor mu?			
19	Fiziksel bilgi varlıklarının kurum dışına çıkarılmalarında gerekli onay ve yetkilendirme alınıyor mu?			
20	Güvenli alanlara erişim yetkilendirilmeleri yapılıyor mu?			
21	Güvenli alanlarda veya kritik bilgi işleme ortamlarında üçüncü taraf hizmetlerinin yerine getirilmesi için gerekli güvenlik tedbirleri alınıyor mu?			
22	Üçüncü taraf personelinin yaptığı işlemler kayıt altına alınmakta mıdır?			
23	Veri merkezlerinde iklimlendirme ve duman kontrol sistemleri kullanılmakta mıdır?			
24	Gizlilik seviyeli bilgi işleyen cihazların fiziksel güvenliği sağlanmakta mıdır?			
	Diğer (…)			

S. N.	Kurumsal Güvenlik Kontrolleri (Politikalar / Prosedürler / İdari Araç ve Yöntemler)	Evet	Fikrim Yok	Hayır
1	Donanım güvenliği politikası oluşturulmuş mu?			
2	Yazılım güvenliği politikası oluşturulmuş mu?			
3	Ağ güvenliği politikası oluşturulmuş mu?			
4	Veri güvenliği politikası oluşturulmuş mu?			
5	Anti-virüs politikası oluşturulmuş mu?			
6	Donanım / teçhizat bakım politikası oluşturulmuş mu?			
7	E-posta politikası oluşturulmuş mu?			
8	Erişim kontrolü politikası oluşturulmuş mu?			
9	İş sürekliliği politikası oluşturulmuş mu?			
10	Kablosuz iletişim politikası oluşturulmuş mu?			
11	Kendi cihazını getirme politikası oluşturulmuş mu?			
12	Kriptografik kullanım politikası oluşturulmuş mu?			
13	Mobil cihazların güvenliği politikası oluşturulmuş mu?			
14	İhlal olayları kaydetme/izleme politikası oluşturulmuş mu?			
15	Ortam araçları işleme/yok etme politikası oluşturulmuş mu?			
16	Parola politikası oluşturulmuş mu?			
17	Teknik açıklık yönetimi politikası oluşturulmuş mu?			
18	Uzaktan çalışma/erişim politikası oluşturulmuş mu?			
19	Yedekleme ve kurtarma politikası oluşturulmuş mu?			
20	Değişiklik yönetimi prosedürü oluşturulmuş mu?			
21	Donanım ve teçhizat bakım prosedürü oluşturulmuş mu?			
22	Erişim kontrolü prosedürü oluşturulmuş mu?			
23	İş sürekliliği yönetimi prosedürü oluşturulmuş mu?			
24	Kapasite yönetimi prosedürü oluşturulmuş mu?			
25	Kullanıcı tanımlama prosedürü oluşturulmuş mu?			
26	Kurumsal parolaları koruma prosedürü oluşturulmuş mu?			
27	Olayları kaydetme/izleme prosedürü oluşturulmuş mu?			
28	Sistem güvenliğini sağlama prosedürü oluşturulmuş mu?			
29	Sistem planlama/kabulü prosedürü oluşturulmuş mu?			
30	Taşınabilir cihaz/ortam prosedürü oluşturulmuş mu?			
31	Teknik açıklık yönetimi prosedürü oluşturulmuş mu?			
32	Zararlı yazılımlardan koruma prosedürü oluşturulmuş mu?			
33	Bilgi güvenliği açıklık testi talimatı oluşturulmuş mu?			
34	Bilgi güvenliği testleri uygulama oluşturulmuş mu?			
35	Bilgisayar kullanım talimatı oluşturulmuş mu?			
36	Donanım / teçhizat bakım talimatı oluşturulmuş mu?			
37	Fotokopi / yazıcı kullanım talimatı oluşturulmuş mu?			
38	Faks cihazı kullanım talimatı oluşturulmuş mu?			
39	İhlal olayı müdahale talimatı oluşturulmuş mu?			
40	Bilgi kaynağı kullanım talimatı oluşturulmuş mu?			
41	Acil durum müdahale talimatı oluşturulmuş mu?			
42	Yazılım kurulumu talimatı oluşturulmuş mu?			
43	Kullanıcı hesabı kaydetme/silme oluşturulmuş mu?			
44	Oturum açma talimatı oluşturulmuş mu?			
45	İklimlendirme cihazları kullanım oluşturulmuş mu?			
46	Yangın cihazları kullanım/bakım oluşturulmuş mu?			
47	Yedekleme talimatı oluşturulmuş mu?			
48	Acil durum/felaket planı oluşturulmuş mu?			
49	Değişiklik istek formu oluşturulmuş mu?			
50	Kapasite planı oluşturulmuş mu?			
51	Donanım/teçhizat bakım formu oluşturulmuş mu?			
52	Kontrol listeleri oluşturulmuş mu?			
53	Yıllık denetim raporu oluşturulmuş mu?			
54	Ziyaretçi formu oluşturulmuş mu?			
55	İş etki analizi formu oluşturulmuş mu?			
56	İş sürekliliği planı oluşturulmuş mu?			
57	Kullanıcı erişim/yetkiler listesi oluşturulmuş mu?			
58	Tetkik açıklık raporu oluşturulmuş mu?			
	…..			

EK-7. 29: Bilgi Güvenliği Risk Belirleme Formu

Doküman No:	KÜTÜPHANE.BGYS.FRM.03
Doküman Adı:	Üniversite Kütüphaneleri Bilgi Güvenliği Risk Belirleme Formu

Soru Maddesi	Evet	Hayır	Hiç	Çok az	Sık sık	Açıklama
Bilgisayarlarınız ne sıklıkla arsızlanıyor?						
Bilgisayarlarınıza siber saldırı ve tehdit oluştu mu?						
Hiç fiziksel veya elektronik veri / bilgi dosyası kaybettiniz mi?						
Bilgisayar destek hizmetleri yeterli mi?						
Ağ kullanımında kısıtlama var mı?						
Personel ve kullanıcı bilgisayarları ayrı mı?						
Oturum açma bilgileriniz başkaları tarafından biliniyor mu?						
Mobil cihazlar kütüphane dışına çıkarılıyor mu?						
Kütüphane bilgi sistemlerine uzaktan bağlantı yapılıyor mu?						
Fiziksel bilgi ortamları kilitli ortamlarda muhafaza ediliyor mu?						
Evrak imhası için evrak imha makinesi kullanılıyor mu?						
İşleriniz ile ilgili dışarıya veri ve bilgi varlığı taşıyor musunuz?						
Kritik bilgiler içeren hatalı bir elektronik posta yolladınız mı?						
Üçüncü taraf firma ve şirketler ile doküman paylaşımı yapıyor musunuz?						
Arızalı donanımları dış servislere gönderirken içindeki bilgiler yedeklenerek siliniyor mu?						
Kişisel verilerin bulunduğu bilgi varlıklarına erişim güvenliği önlemleri alınıyor mu?						
Taşınabilir depolama aygıtları kurum dışına çıkarılıyor mu?						
Misafir ağ uygulaması kullanılıyor mu?						
Misafir giriş kartı uygulaması var mı?						
Diğer (…)						
Diğer (…)						

EK-7. 30: İç Denetim Ortak Soru Formu

Doküman No:	KÜTÜPHANE.BGYS.FRM.04
Doküman Adı:	İç Denetim Ortak Soru Formu

Soru Maddesi	**Evet**	**Hayır**	**Majör Hata**	**Minör Hata**	**Gözlem**
Bilgi Güvenliği Politikası (ları) var mı, biliniyor mu?					
Bilgi Güvenliği (BGYS, ISO/IEC 27001) Farkındalık Eğitimi alınmış mı?					
Bilgi varlıklarına (bilgisayarlar, yazılımlar, dosyalar, elektronik postalar, vb.) ilişkin kurallar var mı?					
Giriş çıkış işlemleri kilitli/şifreli kapılar aracılığıyla mı yapılıyor?					
Bilgisayar kullanımında güvenlik önlemleri var mı?					
Parola politikası ya da parola kullanım kuralları var mı? Temiz masaüstü kuralları var mı, uyuluyor mu?					
Bilgi sınıflandırma ve etiketleme yapılıyor mu? Gizli evrak statüsüne neler giriyor ve gizli evraklar nasıl saklanıyor?					
İnternet üzerinde kısıtlamalar var mı? İstediğini download edebiliyor mu? İstediği siteye girebiliyor mu?					
Kurum için online bankacılık yapılıyor mu? Bankaya elektronik posta gönderiliyor mu? Şifreli mi?					
Elektronik posta kuralları var mı? Kurumun “disclaimer" eki var mı?					
Ortak klasör kullanılıyor mu? İzinleri düzenlenmiş mi? Herkes erişebiliyor mu?					
Gizli evrakların imhası için kâğıt imha makinesi kullanılıyor mu?					
Mobil cihaz kullanım kuralları var mı, uyuluyor mu?					
Uzak bağlantı yapılıyor mu? Güvenli mi?					
Flash bellek kullanımı yapılıyor mu? Güvenliği nasıl sağlanıyor?					
Tedarikçi ilişkilerinde bilgi güvenliği nasıl sağlanıyor.					
Gizlilik anlaşması biliniyor ve yapılıyor mu?					
Bilgi Teknolojileriyle destek/bildirim vb. işlemler için iletişim nasıl kuruluyor?					
Arşiv odası var mı? Nasıl kullanılıyor ve güvenliği nasıl sağlanıyor?					
Ziyaretçilerle nasıl görüşülüyor? Ziyaretçi internete girebiliyor mu? Otoritelerle iletişim (acil durum) nasıl yapılıyor?					
BGYS ile ilgili disiplin yönetmeliği var mı? Biliniyor mu?					
Bir uygunsuzluk ya da ihlal olduğunda nasıl bildiriliyor?					
İşe giriş sürecinde bilgi güvenliği politikası, BGYS ve ISO/IEC 27001 ile ilgili bir evrak imzalanıyor mu?					

EK-7. 31: BGYS Fark Analizi Değerlendirme Raporu

Doküman No:	KÜTÜPHANE.BGYS.RPR.01
Doküman Adı:	BGYS Fark Analizi Değerlendirme Raporu

Ana Kategori	Fark Bulguları	Fark (%0 - %100)
Politika	Fark analizi testinde bu kategori ile ilgili maddelerden çoğunun (örneğin, madde 5-6-10-… gibi) mevcut durumda olmadığı ya da geçekleştirildiği sonucu elde edilmiştir.	Politika hazırlanmış ancak duyurulmamış %50 olumsuz
Donanım	Donanımların mevcut durumda bilgi güvenliği ile ilgili kontrolleri iyi kurgulanamamıştır (madde 5-6-3-9-15 gibi)	Donanım güvenliği iyi kurgulanmamış % 20
Farkındalık	Çalışanların bilgi güvenliği ile ilgili farkındalığı gelişmemiştir.	Bilgi güvenliği farkındalık eğitimi verilmemiş. % 0
…	…	…

EK-7. 32:Bilgi Varlıkları Envanter Listesi

Doküman No:	KÜTÜPHANE.BGYS.LST.01
Doküman Adı:	Üniversite Kütüphaneleri Bilgi Varlıkları Envanter Listesi

Varlık Kategorileri	Alt Varlık Grupları	Açıklama
DONANIMLAR	Bilgisayarlar	Varlık hakkında ek bilgi
	Yazıcılar / Tarayıcılar / Fotokopi makinaları	“
	Telefonlar	“
	Mobil cihazlar	
	Depolama / Yedekleme aygıtları	“
	IoT cihazları	
	Kesintisiz güç kaynakları / Jeneratörler	“
	Kütüphane otomasyon cihazları	“
	Kamera ve Kayıt cihazları	“
	Sanal / Dijitalleştirme makinaları	“
	Engelsiz kütüphane cihazları	“
	Kapı ve oda güvenlik cihazlar	“
	Ve diğer donanımlar (eklenebilir)	“
YAZILIMLAR	İşletim sistemleri	Varlık hakkında ek bilgi
	Kütüphane otomasyon yazılımları	“
	Kullanıcı yazılımları	“
	Özel yazılımlar	“
	Bilgi veri tabanı yazılımları	“
	Uygulamalar / Araçlar	“
	Ve diğer yazılımlar (eklenebilir)	“
AĞ SİSTEMLERİ	Anahtarlar (Switch)	Varlık hakkında ek bilgi
	Yönlendiriciler (Reuters)	“
	Tekrarlayıcılar (Repeater)	“
	Ağ depolama aygıtları	“
	Güvenlik duvarı cihazları (Firewall)	“
	Modemler	“
	Erişim Noktası (Access Point)	“
	Ve diğer ağ sistemleri (eklenebilir)	“
VERİ / BİLGİ ORTAMLARI (İNSAN / PERSONEL)	Elektronik dosyalar	Varlık hakkında ek bilgi
	Basılı evraklar	“
	Kurumsal belgeler	“
	Medyalar(CD, DVD, flash bellek)	“
	Arşiv	“
	Formlar	“
	Bilgi kaynakları	“
	Bilgi / Katalog kartları	“
	Kişisel veri belgeleri / dosyaları	
	Veri konusu kişiler	
	Kritik / hassas bilgiler	

	Üçüncü taraf sözleşmeleri / bilgileri	
	Taşınır / Taşınmaz bilgiler	
	Satın alma belgeleri / dosyaları	
	Kişisel veriler	
	Personel özlük bilgileri	
	Bilgi işlem VE BGYS yöneticileri	
	BGYS yöneticileri	
	Ve diğer veri/bilgiler (eklenebilir)	
FİZİKSEL/ ÇEVRESEL ORTAMLAR	Bina	
	İç mekân alanları	
	Dış çevre koruma ürünleri	
	Doğal afetler	
	Yangın söndürme cihazları	
	Dolaplar / Raflar / Diğer Tefrişat	
	İklimlendirme cihazları	
	Altyapı sistemleri	
	Ve diğer fiziksel varlıklar (eklenebilir)	
SOYUT VARLIKLAR	İtibar	
	İmaj	
	Diğer (eklenebilir)	

EK-7. 33: BGYS Kurumsal Dokümanlar Listesi

LOGO	…….…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.LST.02
		Yayım Tarihi	
BGYS Dokümanı	BGYS Kurumsal Dokümanlar Listesi	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

Dok. Kodu	Doküman adı	Dok. Kodu	Doküman adı
ANA DOKÜMANLAR (DOK)			
BGYS.DOK.01	Ana Doküman listesi	BGYS.DOK.07	Risk Değerlendirme Raporu
BGYS.DOK.02	BGYS Kurumsal Roller Ve Yetkiler	BGYS.DOK.08	Risk İşleme Planı
BGYS.DOK.03	BGYS Süreçleri Etkileşim Şeması	BGYS.DOK.09	Uygulanabilirlik Durum Çizelgesi
BGYS.DOK.04	BGYS İletişim Planı	BGYS.DOK.10	Bilgi Varlıkları Envanteri
BGYS.DOK.05	BGYS Kapsam ve Bağlamı	BGYS.DOK.11	BGYS Hedefleri ve Planlama Formu
BGYS.DOK.06	Risk Değerlendirme Metodolojisi	BGYS.DOK.12	Diğer (……..)
POLİTİKALAR (POL)			
BGYS.POL.01	BGYS Politikası	BGYS.POL.09	Personel Güvenliği Politikası
BGYS.POL.02	BGYS İşletim Politikaları*	BGYS.POL.10	İzleme, Ölçme ve Değerlendirme Pol.
BGYS.POL.03	Bilgi Sınıflama ve Kritiklik Politikası	BGYS.POL.11	Sürekli İyileştirme Politikası
BGYS.POL.04	Bilgi Transferleri Politikası	BGYS.POL.12	Tedarikçi ve Üçüncü Taraf Politikası
BGYS.POL.05	Fikri Mülkiyet Politikası	BGYS.POL.13	Temiz Masaüstü ve Ekran Poltikası
BGYS.POL.06	Fiziksel/Çevresel Güvenlik Politikası	BGYS.POL.14	Uyum Politikası
BGYS.POL.07	Güvenli Sistem Politikası	BGYS.POL.15	Ziyaretçi Kabul Politikası
BGYS.POL.08	Varlıkların Kabul Ed. Kullanımı Pol.	BGYS.POL.16	Diğer (…….. Politikası)
PROSEDÜRLER (PR)			
BGYS.PRS.01	BGYS İşletim Prosedürleri*	BGYS.PRS.09	İletişim Prosedürü
BGYS.PRS.02	Bilgi Sınıflama ve Etiketleme Pr.	BGYS.PRS.10	Risk İşleme Prosedürü
BGYS.PRS.03	Doküman ve Kayıtların Kontrolü Pr.	BGYS.PRS.11	Varlık Yönetimi Prosedürü
BGYS.PRS.04	Düzeltici Faaliyet Prosedürü	BGYS.PRS.12	Yönetimi Gözden Geçirme Prosedürü
BGYS.PRS.05	Farkındalık Eğitimi Prosedürü	BGYS.PRS.13	İzleme, Ölçme ve Değerlendirme Pr.
BGYS.PRS.06	Fikri Mülkiyet Hakları Korunma Pr.	BGYS.PRS.14	Proje Yönetim Prosedürü
BGYS.PRS.07	İç Tetkik Prosedürü	BGYS.PRS.15	Bilgi güvenliği Eğitim Prosedürü
BGYS.PRS.08	İhlal Olayları Yönetim Prosedürü	BGYS.PRS.16	Diğer (…….. Prosedürü)
TALİMATLAR (TLM)			
BGYS.TLM.01	BGYS İşletim Talimatları*	BGYS.TLM.02	Diğer (…….. Talimatı)
FORMLAR (FRM)			
BGYS.FRM.01	Risk Bildirim ve Değerlendirme Frm	BGYS.FRM.06	İhlal Olayı Tespit/Bildirim Formu
BGYS.FRM.02	Değişiklik İstek Formu	BGYS.FRM.07	Tederiköi Değerlendirme Formu
BGYS.FRM.03	Doküman Revizyon Talep Formu	BGYS.FRM.08	Uygunsuzluk Tespit/Bildirim Formu
BGYS.FRM.04	Düzeltici Faaliyet Talep Formu	BGYS.FRM.09	Zimmet Formu
BGYS.FRM.05	Eğitim Katılım Formu	BGYS.FRM.10	Diğer (…….. Formu)
TABLOLAR (TBL) / LİSTELER (LST) / ÇİZELGELER (ÇİZ) / PLANLAR (PLN)			
BGYS.LST.01	BGYS Kurulu Listesi	BGYS.ÇİZ.02	Temel Performans Kriter Çizelgesi
BGYS.LST.02	BGYS Dokümanlar Listesi	BGYS.PLN.01	İç Tetkik Planı
BGYS.LST.03	İç Tetkik Soru Listesi	BGYS.PLN.02	İzleme ve Ölçme Planı
BGYS.TBL.01	Doküman Dağıtım Tablosu	BGYS.PLN.03	Risk İşleme Planı
BGYS.TBL.02	Doküman Saklama Süreleri Tablosu	BGYS.PLN.04	Yıllık Eğitim Planı
BGYS.ÇİZ.01	Doküman Revizyon Takip Çizelgesi		Diğer (…….. Çizelge/Plan/Tablo)
İŞ AKIŞLARI (İA) / GÖREV TANIMLARI (GT)			
BGYS.İA.01	İhlal Olayları Yönetimi İş Akışı	BGYS.İA.04	Varlık Yönetimi İş Akışı
BGYS.İA.02	İş Sürekliliği İş Akışı	BGYS.GT.01	BGYS Yöneticisi Görev Tanımı
BGYS.İA.03	Risk Yönetimi İş Akışı	BGYS.	Diğer (…….. Görev tanımı/İş Akışı)
KAYIT VE RAPOR ŞABLONLARI		**BİLGİ EDİNME DOKÜMANLARI**	
BGYS.RPR.01	Eğitim Kayıtları / Raporu	Posterler	
BGYS.RPR.02	İç Tetkik Raporu	Ziyaretçi Bilgilendirme Kartı	
BGYS.RPR.03	İhlal Olayları Raporu	Varlık Sınıflandırma / Etiketleme Kartı	
BGYS.RPR.04	Performans Raporu	Masa / Dolap / Raf Taahhüt Kartı	
BGYS.RPR.05	Risk İşleme Kayıtları / Raporu	Bilgilendirme Çıkartmaları	
BGYS.TTK.01	Varlık İmha Tutanağı	Farkındalık Metinleri	
(*) ile belirtilen politika, prosedür ve talimatlar "Bilgi Güvenliği Teknik Dokümanları (EK-11)"de ayrıntılı olarak listelenmektedir.			

EK-7. 34: BGYS Teknik Dokümanlar Listesi

LOGO	……..…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.LST.06
		Yayım Tarihi	
BGYS Dokümanı	BGYS Teknik Dokümanlar Listesi	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

Dok. Kodu	Doküman adı	Dok. Kodu	Doküman adı
BİLGİ GÜVENLİĞİ POLİTİKALARI			
BG.POL.03.01	Donanım Güvenliği Politikası	BG.POL.03.11	Kendi Cihazını Getirme Politikası
BG.POL.03.02	Yazılım Güvenliği Politikası	BG.POL.03.12	Kriptografik Kullanım Politikası
BG.POL.03.03	Ağ Güvenliği Politikası	BG.POL.03.13	Mobil Cihazların Güvenliği Pol.
BG.POL.03.04	Veri Güvenliği Politikası	BG.POL.03.14	İhlal Olayları Kaydetme/İzleme Pol.
BG.POL.03.05	Anti-Virüs Politikası	BG.POL.03.15	Ortam araçları İşleme/Yok Etme Pol.
BG.POL.03.06	Donanım / Teçhizat Bakım Pol.	BG.POL.03.16	Parola Politikası
BG.POL.03.07	E-Posta Politikası	BG.POL.03.17	Teknik Açıklık Yönetimi politikası
BG.POL.03.08	Erişim Kontrolü Politikası	BG.POL.03.18	Uzaktan Çalışma/Erişim politikası
BG.POL.03.09	İş Sürekliliği Politikası	BG.POL.03.19	Yedekleme ve Kurtarma Politikası
BG.POL.03.10	Kablosuz İletişim Politikası	BG.POL.03.20	Diğer (…….. Politikası)
BİLGİ GÜVENLİĞİ PROSEDÜRLERİ			
BG.PRS.01.01	Değişiklik Yönetimi Prosedürü	BG.PRS.01.08	Olayları Kaydetme/İzleme Prosedürü
BG.PRS.01.02	Donanım ve Teçhizat Bakım Pros.	BG.PRS.01.09	Sistem Güvenliğini Sağlama Pros.
BG.PRS.01.03	Erişim Kontrolü Prosedürü	BG.PRS.01.10	Sistem Planlama/Kabulü Prosedürü
BG.PRS.01.04	İş Sürekliliği Yönetimi Prosedürü	BG.PRS.01.11	Taşınabilir Cihaz/Ortam Prosedürü
BG.PRS.01.05	Kapasite Yönetimi Prosedürü	BG.PRS.01.12	Teknik Açıklık Yönetimi Prosedürü
BG.PRS.01.06	Kullanıcı Tanımlama Prosedürü	BG.PRS.01.13	Zararlı yazılımlardan Koruma Pros.
BG.PRS.01.07	Kurumsal Parolaları Koruma Pros.	BG.PRS.01.14	Diğer (…….. Prosedürü)
BİLGİ GÜVENLİĞİ TALİMATLARI			
BG.TLM.01.01	Bilgi Güvenliği Açıklık Testi Talim.	BG.TLM.01.09	Acil Durum Müdahale Talimatı
BG.TLM.01.02	Bilgi Güvenliği Testleri Uygulama	BG.TLM.01.10	Yazılım Kurulumu Talimatı
BG.TLM.01.03	Bilgisayar Kullanım Talimatı	BG.TLM.01.11	Kullanıcı Hesabı Kaydetme/Silme
BG.TLM.01.04	Donanım / Teçhizat Bakım Talimatı	BG.TLM.01.12	Oturum Açma Talimatı
BG.TLM.01.05	Fotokopi / Yazıcı Kullanım Tal.	BG.TLM.01.13	İklimlendirme Cihazları Kullanım
BG.TLM.01.06	Faks Cihazı Kullanım Talimatı	BG.TLM.01.14	Yangın Cihazları Kullanım/Bakım
BG.TLM.01.07	İhlal Olayı Müdahale Talimatı	BG.TLM.01.15	Yedekleme Talimatı
BG.TLM.01.08	Bilgi Kaynağı Kullanım Talimatı	BG.TLM.01.16	Diğer (…….. Talimatı)
BİLGİ GÜVENLİĞİ DİĞER DOKÜMANLARI (BG.DD)			
BG.DD.01	Acil Durum/Felaket Planı	BG.DD.07	Ziyaretçi Formu
BG.DD.02	Değişiklik İstek Formu	BG.DD.08	İş Etki analizi Formu
BG.DD.03	Kapasite Planı	BG.DD.09	İş Sürekliliği Planı
BG.DD.04	Donanım/Teçhizat Bakım Formu	BG.DD.10	Kullanıcı Erişim/Yetkiler Listesi
BG.DD.05	Kontrol Listeleri	BG.DD.11	Tetkik Açıklık Raporu
BG.DD.06	Yıllık Denetim Raporu	BG.DD.12	Diğer (……..)

EK-7. 35: İhlal Olayı Tespit / Bildirim Formu

LOGO	…….…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.FRM.01
		Yayım Tarihi	
BGYS Dokümanı	İhlal Olayı Tespit / Bildirim Formu	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

İhlal Olayını Bildiren Kişinin:

Adı Soyadı	
Birimi	
Görevi	
Tarih	

İhlal Olayının Tanımı

Açıklama	
Yer	
Tarih / Saat	
İlgili Süreç	
Önem Derecesi(Düşük-Orta-Yüksek:	
Şahit	

Olayın Türü

Yetkisiz Giriş		Donanım hırsızlığı / Sabotaj / Kasıtlı imha	
Yazılım indirme		Oturum açma bilgilerinin çalınması	
Web sitesinin Hack edilmesi		Kişisel bilgilerin ifşa edilmesi	
Fikri haklara karşı yapılan eylem		Parola saldırısı, çalma	
Yazılım kopyalama		İletişim hataları (dedikodu, yalan, dinleme vb.)	
Virüs /Solucan /Trojan		Kimlik doğrulama saldırıları	
E-Posta ile saldırıya Uğrama		Kimlik hırsızlığı	
Güvenlik açıklarından faydalanma		Binaya izinsiz giriş	
Personel suiistimali		Fiziksel belge / dosya / evrak hırsızlığı	
Yazılım yanlış güncelleme		Casus yazılım tehditleri	
Bilgi sistemi arızası / bakım hatası		Diğer (…)	

Değerlendirme

BGYS Yönetici Görüşleri	
Teknik Personel Görüşleri	
Diğer (…Görüşleri)	

Hazırlayan:	Onaylayan:

EK-7. 36: İç Denetim Uygunsuzluk Tespit / Bildirim Formu

LOGO	…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.FRM.02
		Yayım Tarihi	
BGYS Dokümanı	İç Denetim Uygunsuzluk Tespit / Bildirim Formu	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

Denetim Yapan Kişinin:

Adı Soyadı	
Kurumu	
Görevi	
Tarih	

Uygunsuzluğun Tanımı

Açıklama	**Güvenlik Önleminin Adı**	**Majör / Minör / Gözlem**

Uygunsuzluğun Tespit Şekli

İç Denetim	
Çalışan Birimi	
Diğer (…)	

Hazırlayan:	Onaylayan:

EK-7. 37: Düzeltici Faaliyet Talep Formu

LOGO	…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.FRM.03
		Yayım Tarihi	
BGYS Dokümanı	Düzeltici Faaliyet Talep Formu	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

İhlal Olayını Bildiren Kişinin:

Adı Soyadı	
Birimi	
Görevi	
Tarih	

Uygunsuzluğun Tanımı

Açıklama	
İlgili Süreç	

Kök Neden Analizi

Kök Neden	

Değerlendirme

BGYS Yönetici Görüşleri	
Teknik Personel Görüşleri	
Diğer (…Görüşleri)	
Açılma Tarihi	
Kapatılma Tarihi	

Hazırlayan:	Onaylayan:

EK-7. 38: BGYS Risk Bildirim ve Talep Formu

LOGO	…….…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.FRM.04
		Yayım Tarihi	
BGYS Dokümanı	BGYS Risk Bildirim ve Talep Formu	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

Bildirimi Yapan:

Adı Soyadı	
Birimi	
Görevi	
Tarih	

Tehlikenin tanımı Tanımı

Açıklama	
Olasılığı (1 – 5)	
Sıklığı (1 – 5)	
Etkisi (1 – 5)	
Öneriler	
Not: 1 düşük, 5 yüksek	

Değerlendirme

BGYS Yönetici Görüşleri	
Diğer (…Görüşleri)	

Hazırlayan:	Onaylayan:

EK-7. 39: Değişiklik İzleme Formu

LOGO	…….…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.FRM.05
		Yayım Tarihi	
BGYS Dokümanı	Değişiklik İzleme Formu	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

Bildirimi Yapan:

Adı Soyadı	
Birimi	
Görevi	
Tarih	

Değişiklik İsteği

Açıklama	
İstek Nedeni	
Gerekli İşlemler	

Değerlendirme

BGYS Yönetici Görüşleri	
Diğer (…Görüşleri)	

Hazırlayan:	Onaylayan:

EK-7. 40: Doküman Revizyon Talep Formu

LOGO	…….…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.FRM.06
		Yayım Tarihi	
BGYS Dokümanı	Doküman Revizyon Talep Formu	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

Bildirimi Yapan:

Adı Soyadı	
Birimi	
Görevi	
Tarih	

Revizyon İsteği

Doküman No	
Doküman Adı	
Açıklama	
Değişiklik İstek Nedeni	

Değerlendirme

BGYS Yönetici Görüşleri	
Diğer (…Görüşleri)	

Hazırlayan:	Onaylayan:

EK-7. 41: Tedarikçi Değerlendirme Formu

LOGO	…….. Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı	Doküman No:	BGYS.FRM.07
		Yayım Tarihi	
BGYS Dokümanı	Tedarikçi Değerlendirme Formu	Revizyon Tarihi / No:	
		Gizlilik Düzeyi:	

Tedarikçi Kurumlar

Firma Adı	Bilgi Güvenliği Uygulamaları (50 puan)	Bilgi Güvenliği Farkındalığı (50 puan)

Not: 100 puan üzerinden değerlendirme yapılır.

Değerlendirme

BGYS Yönetici Görüşleri	
Diğer (…Görüşleri)	

Hazırlayan:	Onaylayan:

EK-7. 42: Özgeçmiş

KİŞİSEL BİLGİLER

Adı Soyadı	Ali KAVAK
Doğum Yeri	
Doğum Tarihi	

LİSANS EĞİTİM BİLGİLERİ

Üniversite	Ondokuz Mayıs Üniversitesi
Fakülte	Fen - Edebiyat Fakültesi
Bölüm	Bilgi ve Belge Yönetimi

Üniversite	Atatürk Üniversitesi
Fakülte	Edebiyat Fakültesi
Bölüm	Bilgi ve Belge Yönetimi

YÜKSEK LİSANS EĞİTİM BİLGİLERİ

Üniversite	Atatürk Üniversitesi
Enstitü	Eğitim Bilimleri Enstitüsü
Bölüm	Türkçe Eğitimi A.B.D.

Üniversite	Çankırı Karatekin Üniversitesi
Enstitü	Sosyal Bilimler Enstitüsü
Bölüm	Bilgi ve Belge Yönetimi A.B.D.

YABANCI DİL BİLGİSİ

Üniversite	60

İŞ DENEYİMİ

Üniversite	
Enstitü	Öğretim Görevlisi
Bölüm	4 yıl

KATILDIĞI

Kurslar	Pedagojik Formasyon Sertifikası
	Türkçenin Yabancı Dil Olarak Öğretimi Sertifikası

İLETİŞİM

Adres	
E-mail	