TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
**SİBER GÜVENLİK BAŞKANLIĞI**

# TS ISO/IEC 27001 KONTROLLERİ İLE BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ EŞLEŞTİRME TABLOSU

**BELGE ADI:** TS ISO/IEC 27001 KONTROLLERİ İLEBİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ EŞLEŞTİRME TABLOSU

**SÜRÜM NO:** 1.1

**SÜRÜM TARİHİ:** 01.03.2026

**GİZLİLİK DERECESİ:** Tasnif Dışı

| Değişiklik No | Değişiklik Tarihi | Değişiklik Nedeni |
|---|---|---|
| 1.0 | Ekim 2021 | İlk Yayın |
| 1.1 | Mart 2026 | Mülga olan Dijital Dönüşüm Ofisi'nin yetkilerinin Siber Güvenlik Başkanlığı'na devredilmesi nedeniyle doküman üzerinde tasarımsal ve kurumsal değişiklikler yapılmıştır. |

https://www.siberguvenlik.gov.tr

*TS ISO/IEC 27001 Kontrolleri ile Bilgi ve İletişim Güvenliği Rehberi Eşleştirme Tablosu hakkındaki görüş ve öneriler aşağıda yer alan elektronik posta adresine iletilebilir.*

**Elektronik Posta:** bgrehber@siberguvenlik.gov.tr

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
SİBER GÜVENLİK BAŞKANLIĞI

# TS ISO/IEC 27001 KONTROLLERİ İLE BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ EŞLEŞTİRME TABLOSU

# GİRİŞ

Bilgi ve İletişim Güvenliği Rehberi (Rehber) kapsamındaki kurum ve kuruluşlar, hali hazırda yürüttükleri bilgi güvenliği yönetim sistemi (BGYS) süreçlerini, Rehber uygulama süreçlerine entegre etmeli ve bilgi güvenliği risk yönetimi faaliyetleri kapsamında Rehberde tanımlanan tedbirleri uygulamalıdır. Bu bağlamda, kurum ve kuruluşlara Rehber uyum süreci ile BGYS süreçlerinin entegrasyonu çalışmalarında yardımcı olması amacıyla TS ISO/IEC 27001:2017 Standardının (Standart) EK-A Referans Kontrol Amaçları ve Kontrolleri, TS ISO/IEC 27001:2022 Standardının (Standart) EK-A Kontroller ve Öznitelik Değerleri Matrisi ile Rehberde tanımlanan tedbirler arasındaki ilişkiyi ortaya koyan bir eşleştirme tablosu hazırlanmıştır.

Rehberde tanımlanan tedbirler ile eşleştirme tablosunda ilişkilendirilmiş olan standart kontrollerinin bire bir aynı bilgi güvenliği hedefini karşıladığı yönünde bir değerlendirme yapılmamalıdır. Standardın kurum ve kuruluşlara, EK-A Referans Kontrol Amaçları ve Kontrolleri ile EK-A Kontroller ve Öznitelik Değerleri Matrisinin uygulanmasına yönelik izlenebilecek metodolojiler konusunda geniş bir çerçeve çizdiği göz önünde bulundurulduğunda, Rehber tedbir maddesinin ilgili standart kontrolünün bir hedefi olarak uygulanabileceği değerlendirilmelidir. Kurum ve kuruluşlar, TS ISO/IEC 27001:2017 ve TS ISO/IEC 27001:2022 uyumlu BGYS çalışmalarının kapsamı ile Rehber uyum kapsamının aynı olması durumunda BGYS iç tetkik çalışmaları ile Rehber uyum denetimlerinin tek bir denetim altında yürütülmesi sürecine katkı sağlamak amacıyla bu eşleştirme tablosundan faydalanabilir.

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.1.1 | 1 | Donanım Envanterinin Yönetimi | A.8.1.1 Varlıkların envanteri<br>A.8.1.2 Varlıkların sahipliği | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.1.2 | 1 | Donanım Envanter İçeriğinin Yönetimi | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.1.3 | 1 | Donanım Envanterine Kaydedilmemiş Donanımların Yönetimi | A.8.2.3 Varlıkların kullanımı | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.1.4 | 2 | Aktif Keşif Araçlarının Kullanılması | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.1.5 | 2 | DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.1.6 | 2 | Kullanım Ömrünü Tamamlayan Cihazların Veri Depolama Üniteleri | A.8.3.2 Ortamın yok edilmesi<br>A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı | 7.10 Depolama ortamı<br>7.14 Ekipmanların güvenli bir şekilde yok edilmesi veya tekrar kullanılması |
| Ağ ve Sistem Güvenliği | 3.1.1.7 | 2 | Kurum Ağı Bağlantı Noktalarında Kimlik Denetimi Yapılması | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1.1 Ağ kontrolleri | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.1.8 | 3 | Donanım Varlıklarının Kimlik Denetimi için İstemci Sertifikalarının Kullanılması | A.10.1.2 Anahtar yönetimi | 8.24 Kriptografi (şifreleme) kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.1.9 | 3 | Sabit Disk Güvenliği | A.8.3.2 Ortamın yok edilmesi | 7.10 Depolama ortamı |
| Ağ ve Sistem Güvenliği | 3.1.2.1 | 1 | Yazılım Envanterinin Yönetimi | A.8.1.1 Varlıkların envanteri<br>A.8.1.2 Varlıkların sahipliği | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.2.2 | 1 | Yazılım Envanter İçeriğinin Yönetimi | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.2.3 | 1 | Yazılımın Üreticisi Tarafından Desteklenmesi | A.8.1.1 Varlık envanteri<br>A.8.2.3 Varlıkların kullanımı | 5.9 Bilgi envanteri ve diğer ilgili varlıklar<br>5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.2.4 | 1 | Yazılım Envanterine Kaydedilmemiş Yazılımların Yönetimi | A.8.2.3 Varlıkların kullanımı | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.2.5 | 2 | Yazılım Envanteri Yönetim Araçlarının Kullanımı | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.2.6 | 3 | Yazılım ve Donanım Envanterinin Entegre Edilmesi | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.2.7 | 3 | Beyaz Liste Yönetimi | A.12.6.2 Yazılım kurulumu kısıtlamaları | 8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.3.1 | 1 | Yazılım Güncelleme Araçlarının Kullanımı | A.14.2.2 Sistem değişiklik kontrolü prosedürleri | 8.32 Değişiklik yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.3.2 | 1 | Zararlı Yazılımların Engellenmesi | A.12.6.2 Yazılım kurulumu kısıtlamaları | 8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.3.3 | 1 | Zafiyet/Yama Yönetimi | A.12.6.1 Teknik açıklıkların yönetimi | 8.8 Teknik açıklıkların yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.3.4 | 1 | Yüksek ve Üzeri Seviyede Zafiyet İçeren Sunucu/ Uygulamaların Yalıtılması | A.12.6.1 Teknik açıklıkların yönetimi | 8.8 Teknik açıklıkların yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.3.5 | 1 | Son Kullanıcıların Yetkisiz Program Ekleme/Kaldırma İşlemlerinin Engellenmesi | A.12.6.2 Yazılım kurulumu kısıtlamaları | 8.19 İşletim sistemlerine yazılım kurulumu |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.3.6 | 1 | Güvenlik Açıkları için Risk Analizi Tabanlı Önceliklendirme | A.12.6.1 Teknik açıklıkların yönetimi | 8.8 Teknik açıklıkların yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.3.7 | 1 | Güvenlik Sıkılaştırmalarının Yapılması | A.12.5.1 İşletimdeki sistemler üzerine yazılım kurulumu | 8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.3.8 | 2 | İşletim Sistemi Yama Yönetimi Araçlarının Kullanımı | A.12.6.1 Teknik açıklıkların yönetimi<br>A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi | 8.8 Teknik açıklıkların yönetimi<br>8.32 Değişiklik yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.3.9 | 2 | Zafiyet Tarama Araçlarının Kullanımı | A.12.6.1 Teknik açıklıkların yönetimi<br>A.13.1.1 Ağ kontrolleri | 8.8 Teknik açıklıkların yönetimi<br>8.20 Ağ güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.3.10 | 2 | Aktif Portların, Servislerin ve Protokollerin Varlık Envanterinde Tutulması | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.4.1 | 1 | Tekrar Yayınlama (Relay) İşleminin Engellenmesi | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.4.2 | 1 | SMTP Kimlik Doğrulaması Kullanımı | A.9.4.2 Güvenli oturum açma prosedürleri | 8.5 Güvenli kimlik doğrulama |
| Ağ ve Sistem Güvenliği | 3.1.4.3 | 1 | Kurum Tarafından Onaylanan İnternet Tarayıcıları ve E-Posta İstemcilerinin Kullanımı | A.12.6.1 Yazılım kurulumu kısıtlamaları | 8.8 Teknik açıklıkların yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.4.4 | 1 | E-posta İçeriğindeki Zararlı Bağlantılara (URL) Erişimin Engellenmesi | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.13.2.3 Elektronik mesajlaşma | 8.7 Kötü amaçlı yazılıma karşı koruma<br>5.14 Bilgi transferi |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.4.5 | 1 | İstenmeyen E-posta (Spam) Koruması | A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.7 Kötü amaçlı yazılıma karşı koruma |
| Ağ ve Sistem Güvenliği | 3.1.4.6 | 1 | Servis Dışı Bırakma Saldırıları (DoS) Koruması | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.4.7 | 1 | E-posta İçerik Kontrollerinin Yapılması | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.13.2.3 Elektronik mesajlaşma | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>5.14 Bilgi transferi |
| Ağ ve Sistem Güvenliği | 3.1.4.8 | 1 | Sahte ya da Değiştirilmiş E-Postaların Engellenmesi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.13.2.3 Elektronik mesajlaşma | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>5.14 Bilgi transferi |
| Ağ ve Sistem Güvenliği | 3.1.4.9 | 1 | Risk İçeren İzinsiz ve/veya Çalıştırılabilir Dosya Türlerinin Engellenmesi | A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.7 Kötü amaçlı yazılıma karşı koruma |
| Ağ ve Sistem Güvenliği | 3.1.4.10 | 1 | Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması | A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.7 Kötü amaçlı yazılıma karşı koruma |
| Ağ ve Sistem Güvenliği | 3.1.4.11 | 1 | Güvenlik Sıkılaştırmalarının Yapılması | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.4.12 | 1 | E-Posta İletişim Güvenliğinin Sağlanması | A.10.1 Kriptografik kontroller<br>A.13.2.1 Bilgi transfer politikaları ve prosedürleri<br>A.13.2.3 Elektronik mesajlaşma | 8.24 Kriptografi (şifreleme) kullanımı<br>5.14 Bilgi transferi |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.4.13 | 1 | E-Posta Sunucu Mimarisi | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 5.8 Proje yönetiminde bilgi güvenliği<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Ağ ve Sistem Güvenliği | 3.1.4.14 | 1 | Üçüncü Taraflardan Temin Edilen E-Posta Hizmetleri | A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme | 8.21 Ağ hizmetlerinin güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Ağ ve Sistem Güvenliği | 3.1.4.15 | 2 | Onaylı İnternet Tarayıcısı ve E-Posta İstemcisi Eklentilerinin Kullanımı | A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu<br>A.12.6.2 Yazılım kurulumu kısıtlamaları | 8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.4.16 | 2 | E-Posta İstemcilerinde Betik Kodlarının Kullanımını Sınırlama | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu<br>A.12.6.2 Yazılım kurulumu kısıtlamaları | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.4.17 | 2 | E-Posta Alışverişlerinin Şifreli ve İmzalı Yapılması | A.10.1 Kriptografik kontroller<br>A.13.2.2 Bilgi transferindeki anlaşmalar<br>A.13.2.3 Elektronik mesajlaşma<br>A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.24 Kriptografi (şifreleme) kullanımı<br>5.14 Bilgi transferi<br>8.26 Uygulama güvenlik gereklilikleri |
| Ağ ve Sistem Güvenliği | 3.1.4.18 | 2 | E-Posta Sunucularına Uzaktan Erişim | A.6.2.2 Uzaktan çalışma<br>A.9.4.2 Güvenli oturum açma prosedürleri<br>A.9.4.3 Parola yönetim sistemi | 6.7 Uzaktan çalışma<br>8.5 Güvenli kimlik doğrulama<br>5.17 Kimlik doğrulama bilgileri |
| Ağ ve Sistem Güvenliği | 3.1.4.19 | 3 | E-Posta Eklerinin Kum Havuzlarında Çalıştırılması | A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.7 Kötü amaçlı yazılıma karşı koruma |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.5.1 | 1 | Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması ve Merkezi Olarak Yönetilmesi | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.5.2 | 1 | Taşınabilir Disklerin Zararlı Yazılım Taramalarından Geçirilmesi | A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.7 Kötü amaçlı yazılıma karşı koruma |
| Ağ ve Sistem Güvenliği | 3.1.5.3 | 1 | Cihazların Otomatik Kod Çalıştırmasına İzin Vermemesi | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.5.4 | 1 | Zararlı Yazılımdan Korunma Uygulamalarının Yapılandırılması ve Güncel Tutulması | A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.7 Kötü amaçlı yazılıma karşı koruma |
| Ağ ve Sistem Güvenliği | 3.1.5.5 | 1 | İşletim Sistemlerinin Güvenlik Mekanizmalarının Etkinleştirilmesi | A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.7 Kötü amaçlı yazılıma karşı koruma |
| Ağ ve Sistem Güvenliği | 3.1.5.6 | 2 | Zararlı Yazılımdan Korunma Uygulamalarına Ait Kayıtların Merkezi Olarak Tutulması | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.12.4.1 Olay kaydetme<br>A.12.4.3 Yönetici ve operatör kayıtları<br>A.18.1.3 Kayıtların korunması | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.15 Kaydetme (log tutma)<br>5.33 Kayıtların korunması |
| Ağ ve Sistem Güvenliği | 3.1.5.7 | 3 | DNS Sorgularının Kayıtlarının Tutulması | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.12.4.1 Olay kaydetme<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.15 Kaydetme (log tutma) |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.5.8 | 3 | Komut Satırı Kayıtlarının Tutulması | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.12.4.1 Olay kaydetme<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.6.1 | 1 | Ağ Topolojisi | A.13.1.1 Ağ kontrolleri | 8.20 Ağ güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.2 | 1 | Ağ Cihazlarının Güvenli Konfigürasyonu | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.13.1.1 Ağ kontrolleri | 8.5 Güvenli kimlik doğrulama<br>8.20 Ağ güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.3 | 1 | Ağ Cihazlarında Güvenlik Güncellemelerinin Yapılması | A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.14.2.2 Sistem değişiklik kontrolü prosedürleri | 8.21 Ağ hizmetlerinin güvenliği<br>8.32 Değişiklik yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.6.4 | 1 | Kara Liste veya Beyaz Liste Kullanımı | A.9.1.2 Ağlara ve ağ hizmetlerine erişim | 5.15 Erişim kontrolü |
| Ağ ve Sistem Güvenliği | 3.1.6.5 | 1 | İzin Verilmeyen Trafiğin Engellenmesi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.13.1.3 Ağlarda ayrım | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı |
| Ağ ve Sistem Güvenliği | 3.1.6.6 | 1 | Ağların İzole Edilmesi | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.13.1.3 Ağlarda ayrım | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı |
| Ağ ve Sistem Güvenliği | 3.1.6.7 | 1 | DoS/DDoS Koruması | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.13.1.3 Ağlarda ayrım | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.6.8 | 1 | İnternet Ortamından Kurum İçi Kaynaklara Erişim | A.9.1.1 Erişim kontrol politikası<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.9 | 1 | Kablosuz Erişim Noktalarının Envanterinin Tutulması | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.6.10 | 1 | Misafir Ağı Yönetimi | A.9.1.1 Erişim kontrol politikası<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.9.4.2 Güvenli oturum açma prosedürleri<br>A.13.1.3 Ağlarda ayrım | 5.15 Erişim kontrolü<br>8.5 Güvenli kimlik doğrulama<br>8.22 Ağların ayrımı |
| Ağ ve Sistem Güvenliği | 3.1.6.11 | 1 | Yerel Güvenlik Duvarı Ayarlarının Yapılması | A.13.1.2 Ağ hizmetlerinin güvenliği | 8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.12 | 1 | IP Telefon Kullanımı | A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.13 | 1 | IP Telefon Sistemlerine Ait İz Kayıtlarının Tutulması | A.12.3.1 Bilgi yedekleme<br>A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.13 Bilgi yedekleme<br>8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.6.14 | 1 | IP Telefon Kullanımında Parola Politikası | A.9.4.3 Parola yönetim sistemi | 5.17 Kimlik doğrulama bilgileri |
| Ağ ve Sistem Güvenliği | 3.1.6.15 | 2 | Ağ Erişim Denetimleri | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1.1 Ağ kontrolleri | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.6.16 | 2 | Ağ Cihazlarına Ait Yapılandırmaların Dokümante Edilmesi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 5.37 Dokümante edilmiş işletim prosedürleri |
| Ağ ve Sistem Güvenliği | 3.1.6.17 | 2 | Ağ Paketlerinin Kaydedilmesi | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması | 8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.6.18 | 2 | Ağ Sınır Cihazlarında Kayıt Tutulması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması | 8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.6.19 | 2 | Ağ Tabanlı Saldırı Tespit/Engelleme Sistemi Kullanımı | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.20 | 2 | Uygulama Katmanında Filtreleme Yapılması | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.5 Güvenli kimlik doğrulama<br>8.7 Kötü amaçlı yazılıma karşı koruma<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.21 | 2 | Ağ Tabanlı URL Filtreleri Kullanımı | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.22 | 2 | URL Kategori Hizmeti Kullanımı | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.23 | 2 | URL'lerin Kayıt Altına Alınması | A.12.4.1 Olay kaydetme<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.15 Kaydetme (log tutma)<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.6.24 | 2 | Kurum Ağına Bağlı Kablosuz Erişim Noktalarının Tespiti | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.25 | 2 | İstemcilerin Kablosuz Ağ Erişimlerinin Sınırlandırılması | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1.3 Ağlarda ayrım | 5.15 Erişim kontrolü<br>8.22 Ağların ayrımı |
| Ağ ve Sistem Güvenliği | 3.1.6.26 | 2 | Eşler Arası Kablosuz Ağ Erişiminin Engellenmesi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.27 | 2 | Kablosuz Çevre Birimleri Aracılığı ile Yapılan Erişimin Engellenmesi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.28 | 2 | Uygulama Seviyesi Saldırıların Engellenmesi | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.29 | 2 | IP Telefon Erişim Kontrol Listeleri | A.9.1.1 Erişim kontrol politikası<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim | 5.15 Erişim kontrolü |
| Ağ ve Sistem Güvenliği | 3.1.6.30 | 3 | Ağ Cihazlarının Yapılandırma Yönetimi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.31 | 3 | Ağ Cihazlarının Yönetimi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.32 | 3 | Kuruma Uzaktan Bağlanan Cihazların Yönetimi | A.6.2.2 Uzaktan çalışma<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.12.2.1 Kötücül yazılımlara karşı kontroller | 6.7 Uzaktan çalışma<br>5.15 Erişim kontrolü<br>8.7 Kötü amaçlı yazılıma karşı koruma |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.6.33 | 3 | Kripto Ağ Cihazlarının Kullanımı | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.10.1.2 Anahtar yönetimi | 8.24 Kriptografi (şifreleme) kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.6.34 | 3 | Kablosuz İletişim Güvenliği | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.24 Kriptografi (şifreleme) kullanımı<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.6.35 | 3 | Kablosuz Çevre Birimleri Kullanımının Engellenmesi | A.8.1.3 Varlıkların kabul edilebilir kullanımı | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.6.36 | 3 | Veri Transferi | A.13.2.1 Bilgi transfer politikaları ve prosedürleri<br>A.13.2.2 Bilgi transferindeki anlaşmalar<br>A.13.2.3 Elektronik mesajlaşma<br>A.13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları | 5.14 Bilgi transferi<br>6.6 Gizlilik veya ifşa etmeme anlaşmaları |
| Ağ ve Sistem Güvenliği | 3.1.7.1 | 1 | Veri Sınıflandırma Politikasının Oluşturulması | A.8.2.1 Bilgi sınıflandırması<br>A.8.2.2 Bilgi etiketlemesi<br>A.8.2.3 Varlıkların kullanımı | 5.12 Bilgilerin sınıflandırılması<br>5.13 Bilgilerin etiketlenmesi<br>5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.7.2 | 1 | Servis Sağlayıcıdan Alınan Hizmetlerde Veri Güvenliği Hususları | A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme<br>A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması<br>5.21 Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.7.3 | 1 | Kritik Verinin Envanteri Yönetimi | A.8.1.1 Varlıkların envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Ağ ve Sistem Güvenliği | 3.1.7.4 | 1 | Düzenli Olarak Erişilmeyen Kritik Verinin ve Sistemlerin Kaldırılması | A.8.3.2 Ortamın yok edilmesi | 7.10 Depolama ortamı<br>8.10 Bilgi silme |
| Ağ ve Sistem Güvenliği | 3.1.7.5 | 1 | Bulut Servislerinin Kullanımı | A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme<br>A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri<br>A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme<br>A.15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması<br>5.21 Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme<br>5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.7.6 | 1 | Taşınabilir Ortam Yönetimi | A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.8.3.1 Taşınabilir ortam yönetimi | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>7.10 Depolama ortamı |
| Ağ ve Sistem Güvenliği | 3.1.7.7 | 1 | Ağda Kritik Veri Taşınması | A.13.2.1 Bilgi transfer politikaları ve prosedürleri<br>A.13.2.3 Elektronik mesajlaşma | 5.14 Bilgi transferi |
| Ağ ve Sistem Güvenliği | 3.1.7.8 | 2 | Ağ İçerisinde Veri Sızıntısı Önleme | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.3 Bilgi erişim kısıtlaması<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.7.9 | 3 | Durağan Veri Güvenliğinin Sağlanması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.9.4.2 Güvenli oturum açma prosedürleri<br>A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması | 8.3 Bilgi erişim kısıtlaması<br>8.5 Güvenli kimlik doğrulama<br>8.24 Kriptografi (şifreleme) kullanımı<br>8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.7.10 | 3 | Taşınabilir Ortam Engelleme | A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.8.3.1 Taşınabilir ortam yönetimi | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>7.10 Depolama ortamı |
| Ağ ve Sistem Güvenliği | 3.1.8.1 | 1 | İz ve Denetim Kayıtlarının Tutulması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.8.2 | 1 | Denetim Kayıtlarının Yönetimi | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.8.3 | 1 | Zaman Sunucusu Kullanımı | A.12.4.4 Saat senkronizasyonu | 8.17 Saat senkronizasyonu |
| Ağ ve Sistem Güvenliği | 3.1.8.4 | 1 | Detaylı Kayıt Tutulması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.8.5 | 1 | Kayıtlar için Yeterli Depolama Alanı Tahsisi | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması | 8.15 Kaydetme (log tutma) |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.8.6 | 2 | Merkezi Kayıt Yönetimi | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.8.7 | 2 | Kayıt Analizi Araçları Kullanımı | A.16.1.4 Bilgi güvenliği olaylarında değerlendirme ve karar verme<br>A.16.1.7 Kanıt toplama | 5.25 Bilgi güvenliği ihlal olaylarını değerlendirme ve karar verme<br>5.28 Kanıt toplama |
| Ağ ve Sistem Güvenliği | 3.1.8.8 | 2 | Siber Tehdit ve Olay Yönetim Sistemlerinin Düzenli Yapılandırılması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları<br>A.16.1.4 Bilgi güvenliği olaylarında değerlendirme ve karar verme | 8.15 Kaydetme (log tutma)<br>5.25 Bilgi güvenliği ihlal olaylarını değerlendirme ve karar verme |
| Ağ ve Sistem Güvenliği | 3.1.9.1 | 1 | Güncel Sürümlerin Kullanılması | A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu | 8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.9.2 | 1 | Kapasite Planlaması | A.12.1.3 Kapasite yönetimi | 8.6 Kapasite yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.9.3 | 1 | Sanal Makinelerin Yönetilmesi | A.8.3.2 Ortamın yok edilmesi<br>A.13.1.1 Ağ kontrolleri | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>8.20 Ağ güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.9.4 | 1 | İşletim Sistemi Sıkılaştırmalarının ve Güvenlik Kontrollerinin Yapılması | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.12.4.1 Olay kaydetme<br>A.12.6.1 Teknik açıklıkların yönetimi | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.8 Teknik açıklıkların yönetimi<br>8.15 Kaydetme (log tutma)<br>8.19 İşletim sistemlerine yazılım kurulumu |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.9.5 | 1 | Tedarik Edilen Sanallaştırma Hizmeti Ortam Güvenliğinin Sağlanması | A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme<br>A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması<br>5.21 Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme |
| Ağ ve Sistem Güvenliği | 3.1.9.6 | 2 | İmaj Bütünlüğünün Denetlenmesi ve İzlenmesi | A.12.3.1 Bilgi yedekleme<br>A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi | 8.13 Bilgi yedekleme<br>8.32 Değişiklik yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.9.7 | 2 | Sanal Ağ Güvenliği | A.13.1.1 Ağ kontrolleri<br>A.13.2.1 Bilgi transfer politikaları ve prosedürleri | 8.20 Ağ güvenliği<br>5.14 Bilgi transferi |
| Ağ ve Sistem Güvenliği | 3.1.9.8 | 2 | Operasyon ve Test Ortamlarının İzolasyonu | A.9.1.1 Erişim kontrol politikası<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.12.1.4 Geliştirme, test ve işletim ortamların birbirinden ayrılması<br>A.13.1.1 Ağ kontrolleri | 5.15 Erişim kontrolü<br>8.31 Geliştirme, test ve canlı (gerçek) ortamlarının ayrılması<br>8.20 Ağ güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.9.9 | 2 | Sanallaştırma Yönetim Ortamına Erişim | A.9.1.1 Erişim kontrol politikası<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim | 5.15 Erişim kontrolü |
| Ağ ve Sistem Güvenliği | 3.1.9.10 | 2 | Sanallaştırma Ortamı Sertifika Yönetimi | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.10.1.2 Anahtar yönetimi | 8.24 Kriptografi (şifreleme) kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.9.11 | 2 | Sanal Makineler Arası Trafiğin Kontrol Edilmesi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.9.12 | 2 | Depolama Ortamları ile İletişim Güvenliğinin Sağlanması | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.9.13 | 2 | Fiziksel Kaynakların İzole Edilmesi | A.11.2.1 Teçhizat yerleştirme ve koruma | 7.8 Ekipman konumlandırma ve koruma |
| Ağ ve Sistem Güvenliği | 3.1.10.1 | 1 | Siber Olaylara Müdahale Planlarının Hazırlanması | A.16.1.1 Sorumluluklar ve prosedürler<br>A.16.1.5 Bilgi güvenliği ihlal olaylarına yanıt verme | 5.24 Bilgi güvenliği ihlal olayı yönetimi planlaması ve hazırlığı<br>5.26 Bilgi güvenliği ihlal olaylarına yanıt verme |
| Ağ ve Sistem Güvenliği | 3.1.10.2 | 1 | Siber Olay Yönetimi Kapsamında Görev Alacak Personelin Belirlenmesi | A.16.1.1 Sorumluluklar ve prosedürler<br>A.16.1.5 Bilgi güvenliği ihlal olaylarına yanıt verme | 5.24 Bilgi güvenliği ihlal olayı yönetimi planlaması ve hazırlığı<br>5.2 Bilgi güvenliği rolleri ve sorumlulukları<br>5.26 Bilgi güvenliği ihlal olaylarına yanıt verme |
| Ağ ve Sistem Güvenliği | 3.1.10.3 | 1 | İletişim Bilgileri Dokümanının Hazırlanması | A.6.1.3 Otoritelerle iletişim<br>A.16.1.1 Sorumluluklar ve prosedürler | 5.5 Yetkililerle iletişim |
| Ağ ve Sistem Güvenliği | 3.1.10.4 | 1 | Siber Tehdit Bildirimlerinin Yönetilmesi | A.16.1.3 Bilgi güvenliği açıklıklarının raporlanması | 6.8 Bilgi güvenliği olayı raporlanması |
| Ağ ve Sistem Güvenliği | 3.1.10.5 | 1 | Siber Olayların Raporlarının Standardize Edilmesi ve Yayınlanması | A.16.1.2 Bilgi güvenliği olaylarının raporlanması | 6.8 Bilgi güvenliği olayı raporlanması |
| Ağ ve Sistem Güvenliği | 3.1.10.6 | 1 | Üçüncü Taraflardan Alınan Siber Olay Yönetim Hizmetleri | A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.10.7 | 2 | SOME Personeli için Periyodik Siber Olay Tatbikatlarının Yapılması | A.16.1.6 Bilgi güvenliği ihlal olaylarından ders çıkarma | 5.27 Bilgi güvenliği ihlal olaylarından ders çıkarma |
| Ağ ve Sistem Güvenliği | 3.1.10.8 | 3 | Siber Olay Yönetimi Puanlama ve Önceliklendirme | A.16.1.4 Bilgi güvenliği olaylarında değerlendirme ve karar verme<br>A.16.1.6 Bilgi güvenliği ihlal olaylarından ders çıkarma | 5.25 Bilgi güvenliği ihlal olaylarını değerlendirme ve karar verme<br>5.27 Bilgi güvenliği ihlal olaylarından ders çıkarma |
| Ağ ve Sistem Güvenliği | 3.1.11.1 | 1 | Sızma Testleri ve Güvenlik Denetimlerinin Gerçekleştirilmesi | A.12.6.1 Teknik açıklıkların yönetimi<br>A.18.1.3 Kayıtların korunması<br>A.18.2.3 Teknik uyum gözden geçirmesi | 8.8 Teknik açıklıkların yönetimi<br>5.33 Kayıtların korunması<br>5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk |
| Ağ ve Sistem Güvenliği | 3.1.11.2 | 1 | Sızma Testlerinin Kullanıcı Profillerine Göre Gerçekleştirilmesi | A.12.6.1 Teknik açıklıkların yönetimi<br>A.18.2.3 Teknik uyum gözden geçirmesi | 8.8 Teknik açıklıkların yönetimi<br>5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk |
| Ağ ve Sistem Güvenliği | 3.1.11.3 | 1 | Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi | A.12.6.1 Teknik açıklıkların yönetimi<br>A.18.2.3 Teknik uyum gözden geçirmesi | 8.8 Teknik açıklıkların yönetimi<br>5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk |
| Ağ ve Sistem Güvenliği | 3.1.11.4 | 1 | Sızma Testi için Oluşturulan Hesapların Yönetimi | A.9.2.1 Kullanıcı kaydetme ve kayıt silme<br>A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi | 5.16 Kimlik yönetimi<br>5.18 Erişim hakları |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.11.5 | 1 | Doğrulama Testlerinin Yaptırılması | A.6.1.2 Görevlerin ayrılığı<br>A.18.2.3 Teknik uyum gözden geçirmesi | 5.3 Görevlerin ayrılığı<br>5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk<br>8.8 Teknik açıklıkların yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.11.6 | 1 | Sızma Testi ve Güvenlik Denetimi Bulgularının Seviyelendirilmesi | A.12.6.1 Teknik açıklıkların yönetimi<br>A.18.2.3 Teknik uyum gözden geçirmesi | 5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk<br>8.8 Teknik açıklıkların yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.11.7 | 2 | Test Ortamlarının Hazırlanması | A.12.7.1 Bilgi sistemleri tetkik kontrolleri | 8.34 Tetkik testi sırasında bilgi sistemlerinin korunması |
| Ağ ve Sistem Güvenliği | 3.1.11.8 | 2 | Sızma Testleri ve Güvenlik Denetimlerinin Periyodu | A.12.6.1 Teknik açıklıkların yönetimi<br>A.18.2.3 Teknik uyum gözden geçirmesi | 5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk<br>8.8 Teknik açıklıkların yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.11.9 | 3 | Düzenli Kırmızı Takım Tatbikatlarının Yapılması | A.12.6.1 Teknik açıklıkların yönetimi<br>A.16.1.2 Bilgi güvenliği olaylarının raporlanması<br>A.16.1.3 Bilgi güvenliği açıklıklarının raporlanması<br>A.18.2.3 Teknik uyum gözden geçirmesi | 5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk<br>8.8 Teknik açıklıkların yönetimi<br>6.8 Bilgi güvenliği olayı raporlanması |
| Ağ ve Sistem Güvenliği | 3.1.11.10 | 3 | Kurum Ağına Eklenen Yazılımın ve Donanımın Kontrolü | A.12.6.1 Teknik açıklıkların yönetimi | 8.8 Teknik açıklıkların yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.12.1 | 1 | Erişim Kontrol Politikasının Oluşturulması ve Uygulanması | A.9.1.1 Erişim kontrol politikası<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.12.4.1 Olay kaydetme | 5.15 Erişim kontrolü<br>8.15 Kaydetme (log tutma) |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.12.2 | 1 | Kullanıcı Hesaplarının Yönetimi | A.9.2.1 Kullanıcı kaydetme ve kayıt silme<br>A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi | 5.16 Kimlik yönetimi<br>5.17 Kimlik doğrulama bilgileri |
| Ağ ve Sistem Güvenliği | 3.1.12.3 | 1 | Başarısız Oturum Açma Denemelerinin Yönetimi | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.12.4.1 Olay kaydetme | 8.5 Güvenli kimlik doğrulama<br>8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.12.4 | 1 | Varsayılan Kullanıcıların ve Parolaların Değiştirilmesi | A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi<br>A.14.2.6 Güvenli geliştirme ortamı | 5.17 Kimlik doğrulama bilgileri<br>8.31 Geliştirme, test ve canlı (gerçek) ortamlarının ayrılması |
| Ağ ve Sistem Güvenliği | 3.1.12.5 | 1 | Yönetici Hesaplarının Kullanımı | A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.12.4.1 Olay kaydetme | 8.2 Ayrıcalıklı erişim hakları<br>8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.12.6 | 1 | İşlem Yapılmayan Oturumların Sonlandırılması | A.9.4.2 Güvenli oturum açma prosedürleri | 8.5 Güvenli kimlik doğrulama |
| Ağ ve Sistem Güvenliği | 3.1.12.7 | 1 | Kimlik Doğrulama | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.9.4.2 Güvenli oturum açma prosedürleri | 5.15 Erişim kontrolü<br>8.5 Güvenli kimlik doğrulama |
| Ağ ve Sistem Güvenliği | 3.1.12.8 | 1 | Kullanıcı Yetkilerinin Güncellenmesi | A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi | 8.2 Ayrıcalıklı erişim hakları<br>5.18 Erişim hakları |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.12.9 | 1 | Kurum Dışı Paydaşların Uzaktan Erişimi | A.6.2.2 Uzaktan çalışma<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.9.4.2 Güvenli oturum açma prosedürleri<br>A.12.4.1 Olay kaydetme<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 6.7 Uzaktan çalışma<br>5.15 Erişim kontrolü<br>8.5 Güvenli kimlik doğrulama<br>8.15 Kaydetme (log tutma)<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.12.10 | 2 | Kullanılmayan Hesapların Devre Dışı Bırakılması | A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi | 5.18 Erişim hakları |
| Ağ ve Sistem Güvenliği | 3.1.12.11 | 2 | Yönetici Hesaplarının İşletimi | A.9.1.1 Erişim kontrol politikası<br>A.9.2.2 Kullanıcı erişimine izin verme<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.9.4.2 Güvenli oturum açma prosedürleri<br>A.12.4.1 Olay kaydetme<br>A.12.4.3 Yönetici ve operatör kayıtları | 5.15 Erişim kontrolü<br>5.18 Erişim hakları<br>8.2 Ayrıcalıklı erişim hakları<br>8.5 Güvenli kimlik doğrulama<br>8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.12.12 | 2 | Betik Dillerinin Kullanımına Yönelik Erişimin Sınırlandırılması | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu<br>A.12.6.2 Yazılım kurulumu kısıtlamaları | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.12.13 | 2 | Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması | A.8.1.1 Varlık envanteri<br>A.8.1.2 Varlıkların sahipliği | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.12.14 | 2 | Merkezi Kimlik Doğrulama | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.9.4.2 Güvenli oturum açma prosedürleri | 5.15 Erişim kontrolü<br>8.5 Güvenli kimlik doğrulama |
| Ağ ve Sistem Güvenliği | 3.1.12.15 | 2 | Çok Faktörlü Kimlik Doğrulama Yapılması | A.6.2.2 Uzaktan çalışma<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.9.4.2 Güvenli oturum açma prosedürleri | 6.7 Uzaktan çalışma<br>5.15 Erişim kontrolü<br>8.5 Güvenli kimlik doğrulama |
| Ağ ve Sistem Güvenliği | 3.1.12.16 | 2 | Kimlik Doğrulama Bilgilerinin Güvenli Olarak Saklanması | A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi | 5.17 Kimlik doğrulama bilgileri |
| Ağ ve Sistem Güvenliği | 3.1.12.17 | 2 | Servis Hesaplarının Yönetimi | A.9.2.2 Kullanıcı erişimine izin verme<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi | 5.18 Erişim hakları<br>8.2 Ayrıcalıklı erişim hakları |
| Ağ ve Sistem Güvenliği | 3.1.12.18 | 3 | Hesap Giriş Davranışlarında Değişikliklerin Saptanması | A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.12.4.1 Olay kaydetme | 5.18 Erişim hakları<br>8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.12.19 | 3 | Oturum Kayıtlarının Tutulması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması | 8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.12.20 | 3 | Sistem Yöneticisi Görevlerinin Güvenliği | A.9.2.1 Kullanıcı kaydetme ve kayıt silme<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.12.4.3 Yönetici ve operatör kayıtları | 5.16 Kimlik yönetimi<br>8.2 Ayrıcalıklı erişim hakları<br>5.18 Erişim hakları<br>8.15 Kaydetme (log tutma) |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.12.21 | 3 | Veri ve Parola Güvenliğinin Sağlanması | A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi<br>A.9.3.1 Gizli kimlik doğrulama bilgisinin kullanımı<br>A.9.4.3 Parola yönetim sistemi | 5.17 Kimlik doğrulama bilgileri |
| Ağ ve Sistem Güvenliği | 3.1.13.1 | 1 | Yedekleme Planının Oluşturulması | A.12.3.1 Bilgi yedekleme<br>A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması | 8.13 Bilgi yedekleme<br>5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.2 | 1 | Yedekleme Planının Periyodik Olarak Gözden Geçirilmesi | A.12.3.1 Bilgi yedekleme<br>A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması<br>A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi | 8.13 Bilgi yedekleme<br>5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.3 | 1 | Yedekleme İşlemleri için İz Kayıtlarının Oluşturulması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması | 8.15 Kaydetme (log tutma) |
| Ağ ve Sistem Güvenliği | 3.1.13.4 | 1 | Yedekten Geri Dönüş Testleri | A.12.3.1 Bilgi yedekleme<br>A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi | 8.13 Bilgi yedekleme<br>5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.5 | 2 | Yedekleme Medyalarının Saklanması, Güvenliği ve İmhası | A.8.3.2 Ortamın yok edilmesi<br>A.8.3.3 Fiziksel ortam aktarımı<br>A.11.2.5 Varlıkların taşınması<br>A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı<br>A.12.3.1 Bilgi yedekleme | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>7.14 Ekipmanların güvenli bir şekilde yok edilmesi veya tekrar kullanılması<br>8.13 Bilgi yedekleme |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.13.6 | 2 | İş Sürekliliği Kapsamının Tanımlanması | A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması | 5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.7 | 2 | İş Sürekliliği Planlarının Hazırlanması | A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması<br>A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi | 5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.8 | 2 | İş Sürekliliği Kapsamında Rol ve Sorumlulukların Tanımlanması | A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları<br>A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması<br>A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması | 5.2 Bilgi güvenliği rolleri ve sorumlulukları<br>5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.9 | 2 | İş Sürekliliği Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması | A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme<br>A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması<br>A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması<br>5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.10 | 2 | İş Sürekliliği Planlarının Test Edilmesi | A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi | 5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.11 | 2 | İş Sürekliliği Planlarının Güvenli Muhafazası | A.12.3.1 Bilgi yedekleme | 8.13 Bilgi yedekleme |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.13.12 | 2 | Felaket Kurtarma Planlarının Hazırlanması | A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması<br>A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması<br>A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi | 5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.13 | 2 | Felaket Kurtarma Planları Kapsamında Rol ve Sorumlulukların Tanımlanması | A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları<br>A.6.1.3 Otoritelerle iletişim<br>A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması<br>A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması | 5.2 Bilgi güvenliği rolleri ve sorumlulukları<br>5.5 Yetkililerle iletişim<br>5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.14 | 2 | Felaket Kurtarma Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması | A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme<br>A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması<br>A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması<br>5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.15 | 2 | Felaket Kurtarma Planlarının Test Edilmesi | A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi | 5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.16 | 2 | Felaket Kurtarma Planlarının Güvenli Muhafazası | A.12.3.1 Bilgi Yedekleme<br>A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması | 8.13 Bilgi yedekleme<br>5.29 Kesinti sırasında bilgi güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.13.17 | 3 | Kritik Sistem Sürekliliğinin Sağlanması | A.17.2.1 Bilgi işleme olanaklarının erişilebilirliği | 8.14 Bilgi işleme tesislerinin yedek fazlalığı<br>5.30 İş sürekliliği için BİT hazırlığı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.13.18 | 3 | Felaket Kurtarma Merkezi Oluşturulması | A.17.2.1 Bilgi işleme olanaklarının erişilebilirliği | 8.14 Bilgi işleme tesislerinin yedek fazlalığı<br>5.30 İş sürekliliği için BİT hazırlığı |
| Ağ ve Sistem Güvenliği | 3.1.14.1 | 1 | Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması | A.6.2.2 Uzaktan çalışma | 6.7 Uzaktan çalışma |
| Ağ ve Sistem Güvenliği | 3.1.14.2 | 1 | Ekipman Güvenliğinin Sağlanması | A.6.2.2 Uzaktan çalışma<br>A.11.2.6 Kuruluş dışındaki teçhizat ve varlıkların güvenliği | 6.7 Uzaktan çalışma<br>7.9 Kuruluş dışındaki varlıkların güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.14.3 | 1 | Dosya Paylaşımı | A.6.2.2 Uzaktan çalışma | 6.7 Uzaktan çalışma |
| Ağ ve Sistem Güvenliği | 3.1.14.4 | 1 | Farkındalık Eğitimlerinin Verilmesi | A.6.2.2 Uzaktan çalışma<br>A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi | 6.7 Uzaktan çalışma<br>6.3 Bilgi güvenliği farkındalığı, eğitim ve öğretim |
| Ağ ve Sistem Güvenliği | 3.1.14.5 | 1 | Zararlı Yazılımdan Korunma Uygulamaları | A.6.2.2 Uzaktan çalışma<br>A.12.2.1 Kötücül yazılımlara karşı kontroller | 6.7 Uzaktan çalışma<br>8.7 Kötü amaçlı yazılıma karşı koruma |
| Ağ ve Sistem Güvenliği | 3.1.14.6 | 1 | Güncel İşletim Sistemi ve Uygulamaların Kullanılması | A.6.2.2 Uzaktan çalışma<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.12.5 İşletimsel yazılımın kontrolü | 6.7 Uzaktan çalışma<br>5.15 Erişim kontrolü<br>8.9 Konfigürasyon (yapılandırma) yönetimi |
| Ağ ve Sistem Güvenliği | 3.1.14.7 | 1 | Kurum Kaynaklarına Uzaktan Erişim | A.6.2.2 Uzaktan çalışma<br>A.9.4.2 Güvenli oturum açma prosedürleri | 6.7 Uzaktan çalışma<br>8.5 Güvenli kimlik doğrulama |
| Ağ ve Sistem Güvenliği | 3.1.14.8 | 1 | Video Konferans Uygulamalarının Kullanımı | A.8.2.3 Varlıkların kullanımı<br>A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.14.9 | 1 | Güçlü Parola Kullanımı | A.9.4.3 Parola yönetim sistemi | 5.17 Kimlik doğrulama bilgileri |
| Ağ ve Sistem Güvenliği | 3.1.14.10 | 1 | Güncel Video Konferans Uygulamalarının Kullanılması | A.12.5.1 İşletimdeki sistemler üzerine yazılım kurulumu | 8.19 İşletim sistemlerine yazılım kurulumu |
| Ağ ve Sistem Güvenliği | 3.1.14.11 | 1 | Video Konferans Görüşmelerine Yetkisiz Katılım | A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması | 8.26 Uygulama güvenlik gereklilikleri |
| Ağ ve Sistem Güvenliği | 3.1.14.12 | 1 | Video Konferans Paylaşım İşlemleri ve Sohbet Özelliği | A.13.2.1 Bilgi transfer politikaları ve prosedürleri<br>A.13.2.3 Elektronik mesajlaşma<br>A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması<br>A.14.1.3 Uygulama hizmet işlemlerinin korunması | 5.14 Bilgi transferi<br>8.26 Uygulama güvenlik gereklilikleri |
| Ağ ve Sistem Güvenliği | 3.1.14.13 | 1 | Video Konferans Katılımcı Yönetimi | - | - |
| Ağ ve Sistem Güvenliği | 3.1.14.14 | 1 | Video Konferans Toplantı Odası İsimlendirmeleri | - | - |
| Ağ ve Sistem Güvenliği | 3.1.14.15 | 1 | Kullanıcı Bilgisayarında Güvenlik Duvarının Aktif Olması | A.6.2.2 Uzaktan çalışma<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 6.7 Uzaktan çalışma<br>8.21 Ağ hizmetlerinin güvenliği |
| Ağ ve Sistem Güvenliği | 3.1.14.16 | 2 | Bekleme Odası Özelliğinin Bulunması | - | - |
| Ağ ve Sistem Güvenliği | 3.1.14.17 | 3 | Uç Nokta Seviyesinde Veri Sızıntısının Önlenmesi | A.6.2.2 Uzaktan çalışma | 6.7 Uzaktan çalışma<br>8.12 Veri sızıntısı önleme |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Ağ ve Sistem Güvenliği | 3.1.14.18 | 3 | Erişimin Kurum Bilgisayarları ile Sınırlandırılması | A.6.2.2 Uzaktan çalışma<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika | 6.7 Uzaktan çalışma<br>5.15 Erişim kontrolü<br>8.24 Kriptografi (şifreleme) kullanımı |
| Ağ ve Sistem Güvenliği | 3.1.14.19 | 3 | Kuruma Uzaktan Bağlanan Cihazların Yönetimi | A.6.2.1 Mobil cihaz politikası<br>A.6.2.2 Uzaktan çalışma<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.1 Kullanıcı uç nokta cihazları<br>6.7 Uzaktan çalışma<br>5.15 Erişim kontrolü<br>8.7 Kötü amaçlı yazılıma karşı koruma |
| Uygulama ve Veri Güvenliği | 3.2.1.1 | 1 | Kullanıcı Yönetiminin Yapılabilmesi | A.9.2.1 Kullanıcı kaydetme ve kayıt silme<br>A.9.2.2 Kullanıcı erişimine izin verme | 5.16 Kimlik yönetimi<br>5.18 Erişim hakları |
| Uygulama ve Veri Güvenliği | 3.2.1.2 | 1 | Ortak Hesap Kullanılmaması | A.9.2.1 Kullanıcı kaydetme ve kayıt silme<br>A.12.4.1 Olay kaydetme | 5.16 Kimlik yönetimi<br>8.15 Kaydetme (log tutma) |
| Uygulama ve Veri Güvenliği | 3.2.1.3 | 1 | Kimlik Doğrulama İşlemleri için İz Kayıtlarının Oluşturulması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması | 8.15 Kaydetme (log tutma) |
| Uygulama ve Veri Güvenliği | 3.2.1.4 | 1 | Kimlik Doğrulama Bilgilerinin Güvenliği | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.9.4.3 Parola yönetim sistemi | 8.5 Güvenli kimlik doğrulama<br>5.17 Kimlik doğrulama bilgileri |
| Uygulama ve Veri Güvenliği | 3.2.1.5 | 1 | İlk Parolanın Belirlenmesi | A.9.4.3 Parola yönetim sistemi<br>A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi | 5.17 Kimlik doğrulama bilgileri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.1.6 | 1 | Varsayılan Kullanıcı Adı ve Parolaların Kullanılmaması | A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi<br>A.9.4.3 Parola yönetim sistemi<br>A.12.4.1 Olay kaydetme | 5.17 Kimlik doğrulama bilgileri<br>8.15 Kaydetme (log tutma) |
| Uygulama ve Veri Güvenliği | 3.2.1.7 | 1 | Kaynak Kodda Kimlik Doğrulama Bilgilerinin Bulunmaması | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi | 5.8 Proje yönetiminde bilgi güvenliği |
| Uygulama ve Veri Güvenliği | 3.2.1.8 | 1 | Parola Yönetimi | A.9.4.3 Parola yönetim sistemi | 5.17 Kimlik doğrulama bilgileri |
| Uygulama ve Veri Güvenliği | 3.2.1.9 | 1 | Kimlik Doğrulama Fonksiyonlarına Yapılacak Saldırılara Karşı Önlem Alınması | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması<br>A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.5 Güvenli kimlik doğrulama<br>8.26 Uygulama güvenlik gereklilikleri |
| Uygulama ve Veri Güvenliği | 3.2.1.10 | 2 | Güçlü Kimlik Doğrulama Yöntemlerinin Desteklenmesi | A.9.4.2 Güvenli oturum açma prosedürleri | 8.5 Güvenli kimlik doğrulama |
| Uygulama ve Veri Güvenliği | 3.2.1.11 | 2 | Hesap Kurtarma Seçeneklerinin Güvenliği | A.9.4.2 Güvenli oturum açma prosedürleri | 8.5 Güvenli kimlik doğrulama |
| Uygulama ve Veri Güvenliği | 3.2.1.12 | 2 | Kullanılmayan Hesapların Tespiti | A.9.2.1 Kullanıcı kaydetme ve kayıt silme<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi | 5.16 Kimlik yönetimi<br>8.2 Ayrıcalıklı erişim hakları<br>5.18 Erişim hakları |
| Uygulama ve Veri Güvenliği | 3.2.1.13 | 2 | Merkezi Kimlik Doğrulama Mekanizmalarının Kullanılması | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 8.5 Güvenli kimlik doğrulama<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.2.1 | 1 | Kimlik Doğrulama İşlemleri Sonrasında Yeni Bir Oturum ve Yeni Bir Oturum Kimliğinin Üretilmesi | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.2.2 | 1 | Oturum Kimliğinin Doğrulanması ve Güvenliğinin Sağlanması | A.14.1.3 Uygulama hizmet işlemlerinin korunması<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 8.26 Uygulama güvenlik gereklilikleri<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.2.3 | 1 | Kullanıcı Oturumlarının Sonlandırılması | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 8.5 Güvenli kimlik doğrulama<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.2.4 | 1 | Oturum Güvenlik Mekanizmalarının Kullanılması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.2.5 | 3 | Kullanıcıların Aktif Oturumlarını Yönetebilmesi | A.14.2.5 Güvenli sistem mühendisliği esasları | 8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.3.1 | 1 | Yetki Denetimi | A.9.2.2 Kullanıcı erişimine izin verme<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi veya düzenlenmesi<br>A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.9.2.6 Erişim haklarının kaldırılması<br>A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması | 5.18 Erişim hakları<br>8.2 Ayrıcalıklı erişim hakları<br>8.3 Bilgi erişim kısıtlaması<br>8.26 Uygulama güvenlik gereklilikleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.3.2 | 1 | Kritik Veriye ve Kaynaklara Erişimlerin Kayıt Altına Alınması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Uygulama ve Veri Güvenliği | 3.2.3.3 | 1 | En Az Yetki Prensibinin Uygulanması | A.9.2.2 Kullanıcı erişimine izin verme<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.9.4.1 Bilgiye erişimin kısıtlanması | 5.18 Erişim hakları<br>8.2 Ayrıcalıklı erişim hakları<br>8.3 Bilgi erişim kısıtlaması |
| Uygulama ve Veri Güvenliği | 3.2.3.4 | 3 | İçerik Duyarlı ve Gelişmiş Erişim Denetimi | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 5.8 Proje yönetiminde bilgi güvenliği<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.4.1 | 1 | Yapılandırma Dosyaları, Denetim Kayıtları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Konumda Depolanmaması | A.12.4.2 Kayıt bilgisinin korunması<br>A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.15 Kaydetme (log tutma)<br>8.26 Uygulama güvenlik gereklilikleri |
| Uygulama ve Veri Güvenliği | 3.2.4.2 | 1 | Uygulama Bileşenlerine Dış Kaynaklardan Erişimin Kısıtlanması | A.9.4.1 Bilgiye erişimin kısıtlanması | 8.3 Bilgi erişim kısıtlaması |
| Uygulama ve Veri Güvenliği | 3.2.4.3 | 1 | İstemci Ön Bellekleme İşlevinin Kritik Veri için Kapatılması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 8.3 Bilgi erişim kısıtlaması<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.4.4 | 1 | Uygulamanın Kullandığı Kaynakların Güvensiz Ortamlarda Saklanmaması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.14.2.1 Güvenli geliştirme politikası | 8.3 Bilgi erişim kısıtlaması<br>8.25 Güvenli geliştirme yaşam döngüsü |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.4.5 | 1 | Güvenilmeyen Kaynaklardan Alınan Dosyaların Denetlenmesi | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.26 Uygulama güvenlik gereklilikleri<br>8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>8.28 Güvenli kodlama |
| Uygulama ve Veri Güvenliği | 3.2.4.6 | 1 | Kaynaklara Erişimin Kısıtlanması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.3 Bilgi erişim kısıtlaması<br>8.7 Kötü amaçlı yazılıma karşı koruma<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.4.7 | 2 | Açık Kaynak Kod Tabanının Kurum Bünyesinde Tutulması | A.9.4.5 Program kaynak koduna erişim kontrolü | 8.4 Kaynak koduna erişim |
| Uygulama ve Veri Güvenliği | 3.2.5.1 | 1 | Uygulamada Güvenlik Güncellemeleri ve Yamaları Yüklenmiş Bileşenlerin Kullanılması | A.14.2.2 Sistem değişiklik kontrolü prosedürleri<br>A.14.2.4 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar | 8.32 Değişiklik yönetimi |
| Uygulama ve Veri Güvenliği | 3.2.5.2 | 1 | Kaynak Paylaşım ve İçerik Güvenliği Sıkılaştırmaları | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 8.3 Bilgi erişim kısıtlaması<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.5.3 | 1 | Kurulumların Korumalı ve Ayrıştırılmış Şekilde Yapılması | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 5.8 Proje yönetiminde bilgi güvenliği<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.5.4 | 1 | Sunuculara ve Çalışma Ortamlarına Sadece Uygulamanın ve Yetkili Kullanıcıların Erişebilmesi | A.9.2 Kullanıcı erişim yönetimi | 8.1 Kullanıcı uç nokta cihazları<br>8.2 Ayrıcalıklı erişim hakları<br>8.3 Bilgi erişim kısıtlaması<br>8.4 Kaynak koduna erişim |
| Uygulama ve Veri Güvenliği | 3.2.5.5 | 1 | Sunucular Arası İletişimde İhtiyaç Duyulan En Az Yetkiye Sahip Hesapların Kullanılması | A.9.2.2 Kullanıcı erişimine izin verme<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.9.4.1 Bilgiye erişimin kısıtlanması | 5.18 Erişim hakları<br>8.2 Ayrıcalıklı erişim hakları<br>8.3 Bilgi erişim kısıtlaması |
| Uygulama ve Veri Güvenliği | 3.2.5.6 | 1 | İşletimdeki Sistemler Üzerinde Uygulama Kurulumu | A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu<br>A.12.6.2 Yazılım kurulumu kısıtlamaları | 8.19 İşletim sistemlerine yazılım kurulumu |
| Uygulama ve Veri Güvenliği | 3.2.5.7 | 2 | Güvenli Derleme | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.5.8 | 2 | Yapılandırma Değişikliklerinin İzlenmesi | A.9.4.5 Program kaynak koduna erişim kontrolü<br>A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.14.2.2 Sistem değişiklik kontrolü prosedürleri<br>A.14.2.4 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar | 8.4 Kaynak koduna erişim<br>8.15 Kaydetme (log tutma)<br>8.32 Değişiklik yönetimi |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.5.9 | 2 | Sistem Kaynaklarının Azalması Durumunda Uyarı Verilmesi | A.12.1.3 Kapasite yönetimi | 8.6 Kapasite yönetimi |
| Uygulama ve Veri Güvenliği | 3.2.5.10 | 2 | Anahtarlar ve Parolaların Değiştirilebilir Olması | A.9.4.3 Parola yönetim sistemi<br>A.10.1 Kriptografik kontroller<br>A.12.5.1 İşletimdeki sistemler üzerine yazılım kurulumu | 5.17 Kimlik doğrulama bilgileri<br>8.24 Kriptografi (şifreleme) kullanımı<br>8.19 İşletim sistemlerine yazılım kurulumu |
| Uygulama ve Veri Güvenliği | 3.2.5.11 | 3 | Sunucular Arası İletişimin Şifreli Olması | A.10.1 Kriptografik kontroller<br>A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.24 Kriptografi (şifreleme) kullanımı<br>8.21 Ağ hizmetlerinin güvenliği<br>8.26 Uygulama güvenlik gereklilikleri |
| Uygulama ve Veri Güvenliği | 3.2.6.1 | 1 | Güvenlik Gereksinimleri ve Tasarımı | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 5.8 Proje yönetiminde bilgi güvenliği<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>8.28 Güvenli kodlama<br>8.30 Dış kaynak yoluyla geliştirme<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Uygulama ve Veri Güvenliği | 3.2.6.2 | 1 | Test ve Geliştirme Ortamında Gerçek Veri Kullanılmaması | A.14.2.6 Güvenli geliştirme ortamı<br>A.14.3.1 Test verisinin korunması | 8.31 Geliştirme, test ve canlı (gerçek) ortamlarının ayrılması<br>8.33 Test bilgisi |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.6.3 | 1 | Tedarik Edilen Uygulamalarda Kullanım Amacına Uygun Olmayan Özellik/Arka Kapı Bulunmaması | A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme<br>A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması<br>5.21 Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme |
| Uygulama ve Veri Güvenliği | 3.2.6.4 | 1 | Arayüzün Türkçe Dil Desteğine Sahip Olması | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi | 5.8 Proje yönetiminde bilgi güvenliği |
| Uygulama ve Veri Güvenliği | 3.2.6.5 | 1 | Güncel İstemci ve Sunucu Teknolojilerinin Kullanılması | A.12.6.1 Teknik açıklıkların yönetimi<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi | 8.8 Teknik açıklıkların yönetimi<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.32 Değişiklik yönetimi |
| Uygulama ve Veri Güvenliği | 3.2.6.6 | 1 | Uygulama Güvenlik Testlerinin Yapılması | A.14.2.8 Sistem güvenlik testi<br>A.14.2.9 Sistem kabul testi<br>A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme | 8.29 Geliştirme ve kabul aşamasında güvenlik testleri<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Uygulama ve Veri Güvenliği | 3.2.6.7 | 2 | Kaynak Kod Güvenlik Analizlerinin Yapılması | A.14.2.8 Sistem güvenlik testi<br>A.14.2.9 Sistem kabul testi | 8.29 Geliştirme ve kabul aşamasında güvenlik testleri |
| Uygulama ve Veri Güvenliği | 3.2.6.8 | 2 | Güvenli Yazılım Geliştirme Süreçlerinin Uygulanması | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.14.2 Geliştirme ve destek proseslerinde güvenlik | 5.8 Proje yönetiminde bilgi güvenliği<br>8.28 Güvenli kodlama<br>8.25 Güvenli geliştirme yaşam döngüsü |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.7.1 | 1 | Ortak Hesap Kullanılmaması ve En Az Yetki Prensibinin Uygulanması | A.9.2 Kullanıcı erişim yönetimi<br>A.9.4.1 Bilgiye erişimin kısıtlanması | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması |
| Uygulama ve Veri Güvenliği | 3.2.7.2 | 1 | Bulut Depolama Hizmetlerinde Kurumsal Verilerin Bulundurulmaması | - | 5.23 Bulut hizmetlerinin kullanımı için bilgi güvenliği |
| Uygulama ve Veri Güvenliği | 3.2.7.3 | 1 | Veri Tabanlarına ve Verinin Saklandığı Ortamlara Yalnızca Yetkili Kullanıcıların Erişebilmesi | A.9.2 Kullanıcı erişim yönetimi<br>A.9.4.1 Bilgiye erişimin kısıtlanması | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması |
| Uygulama ve Veri Güvenliği | 3.2.7.4 | 1 | Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması | A.9.2.2 Kullanıcı erişimine izin verme | 5.18 Erişim hakları |
| Uygulama ve Veri Güvenliği | 3.2.7.5 | 1 | Veri Tabanlarında Varsayılan Kullanıcı ve Parolaların Kullanılmaması | A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi | 5.17 Kimlik doğrulama bilgileri |
| Uygulama ve Veri Güvenliği | 3.2.7.6 | 1 | Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.9.4.3 Parola yönetim sistemi | 8.5 Güvenli kimlik doğrulama<br>5.17 Kimlik doğrulama bilgileri |
| Uygulama ve Veri Güvenliği | 3.2.7.7 | 1 | Test ve Geliştirme Ortamında Kullanılan Veri Tabanı Üzerinde Gerçek Veri Bulundurulmaması | A.14.2.6 Güvenli geliştirme ortamı<br>A.14.3.1 Test verisinin korunması | 8.31 Geliştirme, test ve canlı (gerçek) ortamlarının ayrılması<br>8.33 Test bilgisi |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.7.8 | 1 | Kullanıcıların Denetim Kayıtları Üzerinde Değişiklik Yapmasının Engellenmesi | A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıt kayıtları<br>A.18.1.3 Kayıtların korunması | 8.2 Ayrıcalıklı erişim hakları<br>8.15 Kaydetme (log tutma)<br>5.33 Kayıtların korunması |
| Uygulama ve Veri Güvenliği | 3.2.7.9 | 1 | Veri Tabanı Versiyonunun Güncel ve Güvenlik Yamalarının Yüklü Olması | A.12.6.1 Teknik açıklıkların yönetimi<br>A.14.2.2 Sistem değişiklik kontrolü prosedürleri<br>A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi | 8.8 Teknik açıklıkların yönetimi<br>8.32 Değişiklik yönetimi |
| Uygulama ve Veri Güvenliği | 3.2.7.10 | 1 | Veri Tabanı Üzerinde Özel Nitelikli Kişisel Verinin Açık Metin Olarak Tutulmaması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.10.1 Kriptografik kontroller<br>A.18.1.5 Kriptografik kontrollerin düzenlenmesi | 8.3 Bilgi erişim kısıtlaması<br>8.24 Kriptografi (şifreleme) kullanımı<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Uygulama ve Veri Güvenliği | 3.2.7.11 | 1 | Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması | A.6.2.2 Uzaktan çalışma<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi | 6.7 Uzaktan çalışma<br>8.2 Ayrıcalıklı erişim hakları |
| Uygulama ve Veri Güvenliği | 3.2.7.12 | 1 | Ayrıcalıkların Roller ve/veya Profiller Üzerinden Verilmesi | A.9.2 Kullanıcı erişim yönetimi<br>A.9.4.1 Bilgiye erişimin kısıtlanması | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması |
| Uygulama ve Veri Güvenliği | 3.2.7.13 | 1 | Veri Kurtarma Prosedürünün Hazırlanması | A.12.3.1 Bilgi yedekleme<br>A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması | 8.13 Bilgi yedekleme<br>5.8 Proje yönetiminde bilgi güvenliği<br>5.29 Kesinti sırasında bilgi güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.7.14 | 1 | Yedeklerin Güvenliğinin Sağlanması | A.9.2 Kullanıcı erişim yönetimi<br>A.12.3 Yedekleme | 5.15 Erişim kontrolü<br>8.13 Bilgi yedekleme<br>8.24 Kriptografi (şifreleme) kullanımı |
| Uygulama ve Veri Güvenliği | 3.2.7.15 | 1 | Varsayılan Yapılandırmaların Kullanılmaması | A.12.5 İşletimsel yazılımın kontrolü<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.7.16 | 2 | Yetkili Kullanıcı İşlemlerinin Kaydedilmesi | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Uygulama ve Veri Güvenliği | 3.2.7.17 | 2 | Kritik Tablolar ve Görüntüler Üzerindeki Yetkilerin Denetlenmesi | A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi | 5.18 Erişim hakları |
| Uygulama ve Veri Güvenliği | 3.2.7.18 | 3 | Tüm Kullanıcı İşlemlerinin Kaydedilmesi | A.12.4 Kaydetme ve izleme | 8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Uygulama ve Veri Güvenliği | 3.2.7.19 | 3 | Saklama Gereksinimi Sona Eren Kritik Verinin Güvenli Silinmesi | A.8.3.2 Ortamın yok edilmesi | 7.10 Depolama ortamı<br>8.10 Bilgi silme |
| Uygulama ve Veri Güvenliği | 3.2.7.20 | 3 | İşlenmesi Asıl Amaç Olmayan Verilerin Veri Tabanı Sunucusundan Maskelenerek Sunulması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.3 Bilgi erişim kısıtlaması<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>8.11 Veri maskeleme |
| Uygulama ve Veri Güvenliği | 3.2.7.21 | 3 | Veri Tabanına Gönderilen Sorguların Kontrol Edilmesi | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.7.22 | 3 | Kritik Veri İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.18.1.3 Kayıtların korunması | 8.3 Bilgi erişim kısıtlaması<br>8.24 Kriptografi (şifreleme) kullanımı<br>5.33 Kayıtların korunması |
| Uygulama ve Veri Güvenliği | 3.2.8.1 | 1 | Hataların Yakalanması ve Varsayılan Olarak Güvenli Duruma Geçmesi | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.5 Güvenli kimlik doğrulama<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.8.2 | 1 | Hataların ve Tanımlanan Olayların İz Kayıtlarının Oluşturulabilmesi | A.12.4 Kaydetme ve izleme | 8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Uygulama ve Veri Güvenliği | 3.2.8.3 | 1 | Özel Nitelikli Kişisel Veri İçeren Hata Mesajının veya İz Kaydının Üretilmemesi | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri<br>A.18.1.3 Kayıtların korunması | 8.3 Bilgi erişim kısıtlaması<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>5.33 Kayıtların korunması |
| Uygulama ve Veri Güvenliği | 3.2.8.4 | 1 | İz Kayıtlarında Olayların Zaman Bilgisinin Yer Alması | A.12.4.4 Saat senkronizasyonu | 8.17 Saat senkronizasyonu |
| Uygulama ve Veri Güvenliği | 3.2.8.5 | 1 | İz Kayıtlarının Güvenliğinin Sağlanması | A.12.4.2 Kayıt bilgisinin korunması<br>A.18.1.3 Kayıtların korunması | 8.15 Kaydetme (log tutma)<br>5.33 Kayıtların korunması |
| Uygulama ve Veri Güvenliği | 3.2.8.6 | 1 | İz Kayıtlarının Saldırı Vektörü Olarak Kullanımının Engellenmesi | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.9.1 | 1 | SSL/TLS Protokolünün Güvenli Kullanılması | A.10.1 Kriptografik kontroller<br>A.12.5 İşletimsel yazılımın kontrolü | 8.24 Kriptografi (şifreleme) kullanımı<br>8.9 Konfigürasyon (yapılandırma) yönetimi |
| Uygulama ve Veri Güvenliği | 3.2.9.2 | 1 | Sertifika Denetimlerinin Yapılması | A.10.1 Kriptografik kontroller<br>A.12.5 İşletimsel yazılımın kontrolü | 8.24 Kriptografi (şifreleme) kullanımı<br>8.9 Konfigürasyon (yapılandırma) yönetimi |
| Uygulama ve Veri Güvenliği | 3.2.9.3 | 2 | HSTS Kullanılması | A.14.2.1 Güvenli geliştirme politikası<br>A.10.1 Kriptografik kontroller | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.24 Kriptografi (şifreleme) kullanımı |
| Uygulama ve Veri Güvenliği | 3.2.9.4 | 3 | Hatalı Sertifikaların Tespiti | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Uygulama ve Veri Güvenliği | 3.2.9.5 | 3 | SSL/TLS Hata İz Kayıtları | A.12.4 Kaydetme ve izleme | 8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Uygulama ve Veri Güvenliği | 3.2.9.6 | 3 | Kritik Verinin Şifrelenmesi | A.10.1 Kriptografik kontroller<br>A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 8.24 Kriptografi (şifreleme) kullanımı<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Uygulama ve Veri Güvenliği | 3.2.9.7 | 3 | Kurum Tarafından Onaylanmış Sertifikaların Kullanılması | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Uygulama ve Veri Güvenliği | 3.2.10.1 | 1 | Sunucu Tarafında Girdi Doğrulama Denetiminin Yapılması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.2 | 1 | Girdi Doğrulama Hataları için İz Kaydının Oluşturulması | A.12.4 Kaydetme ve izleme | 8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.10.3 | 1 | Uygulamanın Yetkisiz Olarak Program Çalıştırmasının Engellenmesi | A.12.2 Kötücül yazılımlardan koruma | 8.7 Kötü amaçlı yazılıma karşı koruma |
| Uygulama ve Veri Güvenliği | 3.2.10.4 | 1 | Kritik Bilgilerin Formlarda Bulunan Gizli Alanlarda Saklanmaması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.5 | 1 | CSRF Saldırılarına Karşı Önlem Alınması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.6 | 1 | Veri Tabanına Erişimde Kullanılan Dile Karşı Enjeksiyon Saldırılarının Önlenmesi | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.7 | 1 | İşletim Sistemi Komut Enjeksiyonu Açıklarının Önlenmesi | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.8 | 1 | Bellek Taşması Saldırılarının Önlenmesi | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.10.9 | 1 | Dosya İçerme Açıklarının Önlenmesi | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.10 | 1 | XML Tabanlı Saldırıların Önlenmesi | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.11 | 1 | Yapısal Olmayan Veri için Karakterlerin Denetlenmesi | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.12 | 1 | Girdi Denetimi Yapılması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.13 | 1 | Yüklenen Dosyaların Denetlenmesi | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.14 | 2 | İsteklerin Öngörülmeyen Büyüklükte Olup Olmadığının Kontrol Edilebilmesi | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.10.15 | 3 | TS ISO/IEC 19790-24759 Onaylı Kriptografik Modüllerin ve Rastgele Sayı Üreteçlerinin Kullanılması | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Uygulama ve Veri Güvenliği | 3.2.10.16 | 3 | Karakter Kodlamasının Tespiti | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.10.17 | 3 | Uygulama Seviyesi Servis Dışı Bırakma Saldırılarının Engellenmesi | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.11.1 | 1 | Web Servislerinin Güvenli Protokol Üzerinden Sunulması | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Uygulama ve Veri Güvenliği | 3.2.11.2 | 1 | Web Servisi Yapılandırmalarının Yetkili Kullanıcılar Tarafından Yapılması ve Yönetilmesi | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.9.2.2 Kullanıcı erişimine izin verme<br>A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi | 5.15 Erişim kontrolü<br>5.18 Erişim hakları<br>8.2 Ayrıcalıklı erişim hakları |
| Uygulama ve Veri Güvenliği | 3.2.11.3 | 1 | Web Servis Çağrılarında Kimlik Doğrulama ve Yetkilendirme Kontrolü | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.9.4.2 Güvenli oturum açma prosedürleri | 8.3 Bilgi erişim kısıtlaması<br>8.5 Güvenli kimlik doğrulama |
| Uygulama ve Veri Güvenliği | 3.2.11.4 | 1 | Sunulan Web Servislerin Girdi-Çıktı Denetimlerinin Yapılması | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Uygulama ve Veri Güvenliği | 3.2.11.5 | 1 | Web Servis Yapılandırma ve Yönetim İşlemleri | A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.2 Ayrıcalıklı erişim hakları<br>8.7 Kötü amaçlı yazılıma karşı koruma<br>8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.11.6 | 2 | Entegre Olunan Sistemin Web Servislerinin Beklenen Şekilde Çalıştığının Doğrulanması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.11.7 | 2 | Uygulamanın Kararlılığının Sağlanması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.11.8 | 2 | Web Servisi Çağrı Sayısının ve Kaynak Kullanımının Sınırlandırılması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Uygulama ve Veri Güvenliği | 3.2.11.9 | 3 | Dış Sistemler / Uygulamalar Arası Çağrıların Kayıt Altına Alınması | A.12.4 Kaydetme ve izleme | 8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Uygulama ve Veri Güvenliği | 3.2.11.10 | 3 | Kritik Altyapı Sistemleri ile Güvenli İletişimin Sağlanması | A.10.1 Kriptografik kontroller<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri<br>A.17.1 Bilgi güvenliği sürekliliği | 8.24 Kriptografi (şifreleme) kullanımı<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>5.29 Kesinti sırasında bilgi güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.1 | 1 | Akıllı Telefon ve Tabletlerin Kabul Edilebilir Kullanımı | A.6.2.1 Mobil cihaz politikası<br>A.6.2.2 Uzaktan çalışma<br>A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.8.3.1 Taşınabilir ortam yönetimi | 8.1 Kullanıcı uç nokta cihazları<br>6.7 Uzaktan çalışma<br>5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>7.10 Depolama ortamı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.2 | 1 | Mobil Cihazlarda Jailbreak veya Rootlama İşleminin Yapılmaması | A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.9.4.4 Ayrıcalıklı destek programlarının kullanımı | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>8.18 Ayrıcalıklı destek programların kullanımı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.3 | 1 | Kullanıcılara Uygulama İzinleri Hakkında Eğitim Verilmesi | A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi | 6.3 Bilgi güvenliği farkındalığı, eğitim ve öğretim |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.4 | 1 | Mobil Cihaz Envanterinin Tutulması | A.8.1.1 Varlıkların envanteri<br>A.8.1.2 Varlıkların sahipliği | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.5 | 1 | Halka Açık Şarj İstasyonlarının Kullanılmaması | A.6.2.1 Mobil cihaz politikası<br>A.8.1.3 Varlıkların kabul edilebilir kullanımı | 8.1 Kullanıcı uç nokta cihazları<br>5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.6 | 2 | Cihazın Uzaktan Fabrika Ayarlarına Döndürülmesi | A.6.2.1 Mobil cihaz politikası | 8.1 Kullanıcı uç nokta cihazları |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.7 | 2 | Tamire Verilen Cihazlarda Bulunan Verinin Silinmesi | A.6.2.1 Mobil cihaz politikası<br>A.8.3.2 Ortamın yok edilmesi | 8.1 Kullanıcı uç nokta cihazları<br>7.10 Depolama ortamı<br>8.10 Bilgi silme |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.8 | 3 | Güvenlik Yazılımlarının Yüklenmesi | A.6.2.1 Mobil cihaz politikası<br>A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.1 Kullanıcı uç nokta cihazları<br>8.7 Kötü amaçlı yazılıma karşı koruma |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.9 | 3 | Taşınabilir Cihaz Yönetimi | A.6.2.1 Mobil cihaz politikası<br>A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi | 8.1 Kullanıcı uç nokta cihazları<br>5.8 Proje yönetiminde bilgi güvenliği |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.10 | 3 | Taşınabilir Cihazların Ayrı Sistemlerde Kullanılması | A.6.2.1 Mobil cihaz politikası<br>A.6.2.2 Uzaktan çalışma<br>A.8.1.3 Varlıkların kabul edilebilir kullanımı | 8.1 Kullanıcı uç nokta cihazları<br>6.7 Uzaktan çalışma<br>5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.11 | 3 | Parola Politikaları | A.6.2.1 Mobil cihaz politikası<br>A.9.4.3 Parola yönetim sistemi | 8.1 Kullanıcı uç nokta cihazları<br>5.17 Kimlik doğrulama bilgileri |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.12 | 3 | Çok Sayıda Hatalı Giriş Denemesi Yapılması Halinde Cihaz İçindeki Verinin Silinmesi | A.6.2.1 Mobil cihaz politikası<br>A.9.4.2 Güvenli oturum açma prosedürleri | 8.1 Kullanıcı uç nokta cihazları<br>8.5 Güvenli kimlik doğrulama |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.13 | 3 | Desteklenen Cihaz Listesinin Oluşturulması | A.8.1.1 Varlıkların envanteri<br>A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.12.2 Kötücül yazılımlardan koruma | 5.9 Bilgi envanteri ve diğer ilgili varlıklar<br>8.3 Bilgi erişim kısıtlaması<br>8.7 Kötü amaçlı yazılıma karşı koruma |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.14 | 3 | Güncel Olmayan Cihazların Sistemlere Erişiminin Engellenmesi | A.6.2.1 Mobil cihaz politikası<br>A.9.1 Erişim kontrolünün iş gereklilikleri | 8.1 Kullanıcı uç nokta cihazları<br>8.3 Bilgi erişim kısıtlaması |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.1.15 | 3 | Seyahat Kullanım Politikasının Tanımlanması | A.6.2.1 Mobil cihaz politikası<br>A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 8.1 Kullanıcı uç nokta cihazları<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.2.1 | 1 | Taşınabilir Bilgisayarların Kabul Edilebilir Kullanımı | A.6.2.1 Mobil cihaz politikası<br>A.6.2.2 Uzaktan çalışma<br>A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.8.3.1 Taşınabilir ortam yönetimi | 8.1 Kullanıcı uç nokta cihazları<br>6.7 Uzaktan çalışma<br>5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>7.10 Depolama ortamı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.2.2 | 1 | Güvenlik Yazılımlarının Yüklenmesi | A.12.2.1 Kötücül yazılımlara karşı kontroller | 8.7 Kötü amaçlı yazılıma karşı koruma |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.2.3 | 1 | Tamire Verilen Taşınabilir Bilgisayarlarda Bulunan Verinin Silinmesi | A.6.2.1 Mobil cihaz politikası<br>A.8.3.1 Taşınabilir ortam yönetimi<br>A.8.3.2 Ortamın yok edilmesi | 8.1 Kullanıcı uç nokta cihazları<br>7.10 Depolama ortamı<br>8.10 Bilgi silme |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.2.4 | 2 | Disk Şifreleme | A.8.3.1 Taşınabilir ortam yönetimi | 7.10 Depolama ortamı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.2.5 | 3 | Harici Depolama Ortamlarına Erişimin Yönetimi | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.6.2.1 Mobil cihaz politikası | 8.3 Bilgi erişim kısıtlaması<br>8.1 Kullanıcı uç nokta cihazları |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.2.6 | 3 | Taşınabilir Bilgisayar Yönetimi | A.6.2.1 Mobil cihaz politikası<br>A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi | 8.1 Kullanıcı uç nokta cihazları<br>5.8 Proje yönetiminde bilgi güvenliği |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.2.7 | 3 | Güncel Olmayan Bilgisayarların Sistemlere Erişiminin Engellenmesi | A.6.2.1 Mobil cihaz politikası<br>A.9.1 Erişim kontrolünün iş gereklilikleri | 8.1 Kullanıcı uç nokta cihazları<br>8.3 Bilgi erişim kısıtlaması |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.2.8 | 3 | Seyahat Kullanım Politikasının Tanımlanması | A.6.2.1 Mobil cihaz politikası<br>A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 8.1 Kullanıcı uç nokta cihazları<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.3.1 | 1 | Taşınabilir Ortamların Kabul Edilebilir Kullanımı | A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.8.3.1 Taşınabilir ortam yönetimi | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>7.10 Depolama ortamı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.3.2 | 1 | Taşınabilir Ortamların Saklama ve Kullanım Koşulları | A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.8.3.1 Taşınabilir ortam yönetimi | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>7.10 Depolama ortamı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.3.3 | 2 | Taşınabilir Ortamların Barındırdığı Verilerin Güvenliği | A.8.1.3 Varlıkların kabul edilebilir kullanımı<br>A.8.3.1 Taşınabilir ortam yönetimi | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı<br>7.10 Depolama ortamı |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.3.4 | 2 | Taşınabilir Ortamların Güvenli İmhası | A.8.3.2 Ortamın yok edilmesi | 7.10 Depolama ortamı<br>8.10 Bilgi silme |
| Taşınabilir Cihaz ve Ortam Güvenliği | 3.3.3.5 | 2 | Taşınabilir Ortam Bilgisinin Yedeklenmesi | A.8.3.1 Taşınabilir ortam yönetimi<br>A.12.3.1 Bilgi yedekleme | 7.10 Depolama ortamı<br>8.13 Bilgi yedekleme |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.1 | 1 | Ağ Portlarının Kısıtlanması | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.3 Bilgi erişim kısıtlaması<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.2 | 1 | Ağ Servislerinin Güvenlik Kontrolleri | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.14.2.8 Sistem güvenlik testi<br>A.18.2.3 Teknik uyum gözden geçirmesi | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.29 Geliştirme ve kabul aşamasında güvenlik testleri<br>5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk<br>8.8 Teknik açıklıkların yönetimi |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.3 | 1 | Güvenli Yapılandırma | A.12.1.1 Yazılı işletim prosedürleri | 5.37 Dokümante edilmiş işletim prosedürleri |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.4 | 1 | Cihazın Güvenli İmhası veya Tekrar Kullanımı | A.8.3.2 Ortamın yok edilmesi | 7.10 Depolama ortamı<br>8.10 Bilgi silme |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.5 | 1 | Yetkisiz Cihazların Kurum Ağına Bağlanmasının Engellenmesi | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1 Ağ güvenliği yönetimi | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.6 | 2 | Cihaz Güvenlik Duvarının Aktifleştirilmesi | A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.7 | 2 | Kablosuz Erişim Noktalarına Güvenli Bağlantı | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1 Ağ güvenliği yönetimi | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.8 | 2 | Cihazların Merkezi Yönetimi | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi | 5.8 Proje yönetiminde bilgi güvenliği |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.1.9 | 3 | Ağ Üzerinden Gönderilen Verinin Şifrelenmesi | A.10.1 Kriptografik kontroller<br>A.13.1.1 Ağ kontrolleri<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.24 Kriptografi (şifreleme) kullanımı<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.2.1 | 1 | Veri Yedekleme | A.12.3 Yedekleme | 8.13 Bilgi yedekleme |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.2.2 | 1 | Verilere Yetkili Erişim | A.9.2 Kullanıcı erişim yönetimi | 5.15 Erişim kontrolü |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.2.3 | 3 | Kullanılan Cihazlardan Kritik Verinin Temizlenmesi | A.8.3.2 Ortamın yok edilmesi<br>A.11.2.7 Teçhizatın güvenli olarak yok edilmesi veya tekrar kullanımı | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>7.14 Ekipmanların güvenli bir şekilde yok edilmesi veya tekrar kullanılması |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.3.1 | 1 | Oturum Sonlandırma İşlemlerinin Aktifleştirilmesi | A.14.2.5 Güvenli sistem mühendisliği esasları | 8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.3.2 | 1 | Kimlik Doğrulama Politikası | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.9.4.2 Güvenli oturum açma prosedürleri | 8.3 Bilgi erişim kısıtlaması<br>8.5 Güvenli kimlik doğrulama |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.3.3 | 1 | Kullanıcı Yetki Sınırlaması | A.9.2 Kullanıcı erişim yönetimi | 5.15 Erişim kontrolü |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.3.4 | 1 | Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi | A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi | 5.17 Kimlik doğrulama bilgileri |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.3.5 | 1 | Sıfırlama Mekanizmaları | A.9.2 Kullanıcı erişim yönetimi<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 5.15 Erişim kontrolü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.4.1 | 1 | Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi | A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi | 5.17 Kimlik doğrulama bilgileri |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.4.2 | 1 | API ve Bağlantı Güvenliği | A.9.1 Erişim kontrolünün iş gereklilikleri | 8.3 Bilgi erişim kısıtlaması |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.4.3 | 2 | Web Uygulama Güvenlik Duvarı Kullanımı | A.13.1.1 Ağ kontrolleri | 8.20 Ağ güvenliği |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.4.4 | 2 | Sistem API'lerinde Güvenli Haberleşme Protokolü Kullanımı | A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.26 Uygulama güvenlik gereklilikleri |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.5.1 | 1 | Güncellemelerin Kontrolü | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.5.2 | 1 | Cihazlara Fiziksel Erişimin Kısıtlanması | A.11.1.2 Fiziksel giriş kontrolleri<br>A.11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması, | 7.2 Fiziksel giriş<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.5.3 | 3 | Gömülü İşletim Sistemi İçin Kod Analiz Raporu Alınması | A.12.6.1 Teknik açıklıkların yönetimi<br>A.14.2.7 Dışardan sağlanan geliştirme<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme<br>A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme | 8.8 Teknik açıklıkların yönetimi<br>8.30 Dış kaynak yoluyla geliştirme<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.5.4 | 3 | Elektromanyetik Sızıntılara Karşı Güvenlik Önlemlerinin Alınması | A.11.2.1 Teçhizat yerleştirme ve koruma | 7.8 Ekipman konumlandırma ve koruma |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.5.5 | 3 | Tersine Mühendisliğe Karşı Koruma | A.14.2.5 Güvenli sistem mühendisliği esasları<br>A.14.2.9 Sistem kabul testi | 8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>8.29 Geliştirme ve kabul aşamasında güvenlik testleri |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.5.6 | 3 | Güvenli Önyükleme | A.14.2.5 Güvenli sistem mühendisliği esasları | 8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği | 3.4.5.7 | 3 | Güncellemelerin Güvenilir Kanallar Üzerinden Yapılması | A.12.5.1 İşletimdeki sistemler üzerine yazılım kurulumu<br>A.12.6.2 Yazılım kurulumu kısıtlamaları | 8.19 İşletim sistemlerine yazılım kurulumu |
| Personel Güvenliği | 3.5.1.1 | 1 | Güvenlik Soruşturmalarının Yapılması | A.7.1 İstihdam öncesi | 6.1 Tarama |
| Personel Güvenliği | 3.5.1.2 | 1 | Varlıkların Kabul Edilebilir Kullanım Kurallarının Tanımlanması | A.7.1.2 İstihdam hüküm ve koşulları<br>A.8.1.3 Varlıkların kabul edilebilir kullanımı | 6.2 İstihdam hüküm ve koşulları<br>5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Personel Güvenliği | 3.5.1.3 | 1 | Temiz Masa Temiz Ekran Politikasının Tanımlanması | A.11.2.9 Temiz masa temiz ekran politikası | 7.7 Temiz masa ve temiz ekran |
| Personel Güvenliği | 3.5.1.4 | 1 | Sözleşmelerde Bilgi Güvenliği Hususlarının Yer Alması | A.7.1.2 İstihdam hüküm ve koşulları | 6.2 İstihdam hüküm ve koşulları |
| Personel Güvenliği | 3.5.1.5 | 1 | Sosyal Medya Kullanım Politikasının Uygulanması | A.5.1.1 Bilgi güvenliği politikaları<br>A.5.1.2 Bilgi güvenliği için politikaların gözden geçirilmesi<br>A.7.1.2 İstihdam hüküm ve koşulları | 5.1 Bilgi güvenliği politikaları<br>6.2 İstihdam hüküm ve koşulları |
| Personel Güvenliği | 3.5.1.6 | 1 | Bilgi Güvenliği İhlal Olayına Yönelik Disiplin Sürecinin Tanımlanması | A.7.2.3 Disiplin prosesi | 6.4 Disiplin süreci |
| Personel Güvenliği | 3.5.1.7 | 1 | Rol, Sorumluluk ve Asgari Yetkinliklerin Tanımlanması | A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları | 5.2 Bilgi güvenliği rolleri ve sorumlulukları |
| Personel Güvenliği | 3.5.1.8 | 1 | İstihdam Sorumluluklarının Sonlandırılması veya Değiştirilmesi | A.7.3 İstihdamın sonlandırılması ve değiştirilmesi | 6.5 İstihdamın sona ermesinden veya değiştirilmesinden sonraki sorumluluklar<br>5.11 Varlıkların iadesi |
| Personel Güvenliği | 3.5.1.9 | 1 | Gizlilik ile İlgili Gereksinimlerin Personele Tebliğ Edilmesi | A.5.1.1 Bilgi güvenliği politikaları<br>A.5.1.2 Bilgi güvenliği için politikaların gözden geçirilmesi<br>A.7.1.2 İstihdam hüküm ve koşulları | 5.1 Bilgi güvenliği politikaları<br>6.2 İstihdam hüküm ve koşulları |
| Personel Güvenliği | 3.5.2.1 | 1 | Farkındalık Eğitimleri Verilmesi | A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi | 6.3 Bilgi güvenliği farkındalığı, eğitim ve öğretim |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Personel Güvenliği | 3.5.2.2 | 1 | Olayların Tespiti ve Raporlanmasına Yönelik Eğitimlerin Verilmesi | A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi<br>A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi | 6.3 Bilgi güvenliği farkındalığı, eğitim ve öğretim |
| Personel Güvenliği | 3.5.2.3 | 2 | Yetenek İhtiyaç Analizi Yapılması | A.7.2.1 Yönetim sorumlulukları<br>A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi | 5.4 Yönetim sorumlulukları<br>6.3 Bilgi güvenliği farkındalığı, eğitim ve öğretim |
| Personel Güvenliği | 3.5.3.1 | 1 | Tedarikçi İlişkilerinde Bilgi Güvenliği Politikasının Tanımlanması | A.5.1.1 Bilgi güvenliği politikaları<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 5.1 Bilgi güvenliği politikaları<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Personel Güvenliği | 3.5.3.2 | 1 | Demo ve Kavram İspatı Çalışmalarında Gizlilik Taahhütnamesi | A.13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 6.6 Gizlilik veya ifşa etmeme anlaşmaları<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Personel Güvenliği | 3.5.3.3 | 1 | Tedarikçi Sözleşmelerinde Bilgi Güvenliğinin Ele Alınması | A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme<br>A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri | 5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması<br>5.21 Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme |
| Personel Güvenliği | 3.5.3.4 | 1 | Tedarik Zinciri Güvenliği | A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri | 5.21 Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Personel Güvenliği | 3.5.3.5 | 1 | Kabul Kriterlerinin Belirlenmesi | A.14.2.7 Dışardan sağlanan geliştirme<br>A.14.2.9 Sistem kabul testi<br>A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme | 8.30 Dış kaynak yoluyla geliştirme<br>8.29 Geliştirme ve kabul aşamasında güvenlik testleri<br>5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |
| Personel Güvenliği | 3.5.3.6 | 1 | İletişim Metotlarının Belirlenmesi | A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme | 5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Personel Güvenliği | 3.5.3.7 | 1 | Yüklenici Tarafından Tedarik Edilen Ürün/Hizmet Değişikliklerinin Yönetimi | A.15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme | 5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |
| Personel Güvenliği | 3.5.3.8 | 1 | Ana Yüklenici ve Alt Yüklenici Sorumluluklarının Netleştirilmesi | A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Personel Güvenliği | 3.5.3.9 | 1 | Tedarikçi Hizmetlerinin İzlenmesi | A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme | 5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |
| Personel Güvenliği | 3.5.3.10 | 2 | Tedarik Zinciri İzleme Sürecinin Oluşturulması | A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri<br>A.15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme | 5.21 Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme<br>5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |
| Fiziksel Mekânların Güvenliği | 3.6.1.1 | 1 | Fiziksel Güvenlik Sınırı | A.11.1.1 Fiziksel güvenlik sınırı<br>A.11.1.2 Fiziksel giriş kontrolleri | 7.1 Fiziksel güvenlik sınırları<br>7.2 Fiziksel giriş |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Fiziksel Mekânların Güvenliği | 3.6.1.2 | 1 | Güvenlik Biriminin Yeterliliği | A.11.1.1 Fiziksel güvenlik sınırı<br>A.11.1.2 Fiziksel giriş kontrolleri<br>A.18.2.1 Bilgi güvenliğinin bağımsız gözden geçirilmesi | 7.1 Fiziksel güvenlik sınırları<br>7.2 Fiziksel giriş<br>5.35 Bilgi güvenliğinin bağımsız gözden geçirilmesi |
| Fiziksel Mekânların Güvenliği | 3.6.1.3 | 1 | Fiziksel Giriş ve Çıkış Kontrolleri | A.11.1.2 Fiziksel giriş kontrolleri | 7.2 Fiziksel giriş |
| Fiziksel Mekânların Güvenliği | 3.6.1.4 | 1 | Dış Güvenlik Unsurlarının Kontrolü | A.11.1.4 Dış ve çevresel tehditlere karşı koruma | 7.5 Fiziksel ve çevresel tehditlere karşı koruma |
| Fiziksel Mekânların Güvenliği | 3.6.1.5 | 1 | Ziyaretçi Giriş Çıkış Kontrolleri | A.11.1.2 Fiziksel giriş kontrolleri | 7.2 Fiziksel giriş |
| Fiziksel Mekânların Güvenliği | 3.6.1.6 | 1 | Yetkisiz Fiziksel Erişim Durumunda İzlenecek Sürecin Tanımlanması | A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirmelerin yönetimi | 5.24 Bilgi güvenliği ihlal olayı yönetimi planlaması ve hazırlığı |
| Fiziksel Mekânların Güvenliği | 3.6.1.7 | 1 | Kablolama Güvenliği | A.11.2.3 Kablo güvenliği | 7.12 Kablo güvenliği |
| Fiziksel Mekânların Güvenliği | 3.6.1.8 | 1 | Dış ve Çevresel Tehditlere Karşı Koruma | A.11.1.4 Dış ve çevresel tehditlere karşı koruma<br>A.11.2.2 Destekleyici altyapı hizmetleri | 7.5 Fiziksel ve çevresel tehditlere karşı koruma<br>7.11 Destekleyici altyapı hizmetleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Fiziksel Mekânların Güvenliği | 3.6.1.9 | 1 | Kamera Sistemleri | A.9.2 Kullanıcı erişim yönetimi<br>A.11.1 Güvenli alanlar<br>A.11.2.1 Teçhizat yerleştirme ve koruma<br>A.13.1.1 Ağ kontrolleri<br>A.18.1.3 Kayıtların korunması | 5.15 Erişim kontrolü<br>7.1 Fiziksel güvenlik sınırları<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.6 Güvenli alanlarda çalışma<br>7.8 Ekipman konumlandırma ve koruma<br>8.20 Ağ güvenliği<br>5.33 Kayıtların korunması |
| Fiziksel Mekânların Güvenliği | 3.6.1.10 | 2 | Çalışma Alanlarının Güvenliği | A.11.1 Güvenli alanlar | 7.1 Fiziksel güvenlik sınırları<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.6 Güvenli alanlarda çalışma |
| Fiziksel Mekânların Güvenliği | 3.6.1.11 | 2 | Destekleyici Altyapı Hizmetleri | A.11.2.2 Destekleyici altyapı hizmetleri | 7.11 Destekleyici altyapı hizmetleri |
| Fiziksel Mekânların Güvenliği | 3.6.1.12 | 3 | Fiziksel Güvenlik Sistemleri Verilerinin Siber Olay Tespitinde Kullanılması | A.12.4 Kaydetme ve izleme | 8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Fiziksel Mekânların Güvenliği | 3.6.1.13 | 3 | Ziyaretçi Fiziksel Erişim Güvenliği | A.11.1.2 Fiziksel giriş kontrolleri | 7.2 Fiziksel giriş |
| Fiziksel Mekânların Güvenliği | 3.6.1.14 | 3 | Fiziksel Erişim Güvenliği | A. 11.1.2 Fiziksel giriş kontrolleri<br>A.11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması<br>A.11.1.5 Güvenli alanlarda çalışma | 7.2 Fiziksel giriş<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.6 Güvenli alanlarda çalışma |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Fiziksel Mekânların Güvenliği | 3.6.2.1 | 1 | Sistem Odası/Veri Merkezi Güvenliği Politikası | A.5.1.1 Bilgi güvenliği politikaları<br>A.11.1 Güvenli alanlar | 5.1 Bilgi güvenliği politikaları<br>7.1 Fiziksel güvenlik sınırları<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.6 Güvenli alanlarda çalışma |
| Fiziksel Mekânların Güvenliği | 3.6.2.2 | 1 | Fiziksel Varlıkların Sistem Odası/Veri Merkezi Dışına Transferi | A.11.2.5 Varlıkların taşınması<br>A.11.2.6 Teçhizat ve kuruluş dışındaki varlıkların güvenliği | 7.10 Depolama ortamı<br>7.9 Kuruluş dışındaki varlıkların güvenliği |
| Fiziksel Mekânların Güvenliği | 3.6.2.3 | 1 | Güvenli Alan Yetkilendirmesinin Yapılması | A.9.2 Kullanıcı erişim yönetimi<br>A.11.1 Güvenli alanlar | 5.15 Erişim kontrolü<br>7.1 Fiziksel güvenlik sınırları<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.6 Güvenli alanlarda çalışma |
| Fiziksel Mekânların Güvenliği | 3.6.2.4 | 1 | Üçüncü Taraf Hizmetlerin Güvenliği | A.11.1.2 Fiziksel giriş kontrolleri | 7.2 Fiziksel giriş |
| Fiziksel Mekânların Güvenliği | 3.6.2.5 | 1 | Ortam Koşullarının Kontrolü | A.11.1.4 Dış ve çevresel tehditlere karşı koruma<br>A.11.2.2 Destekleyici altyapı hizmetleri<br>A.13.1.1 Ağ kontrolleri | 7.5 Fiziksel ve çevresel tehditlere karşı koruma<br>7.11 Destekleyici altyapı hizmetleri<br>8.20 Ağ güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Fiziksel Mekânların Güvenliği | 3.6.2.6 | 1 | Kamera Sistemleri | A.9.2 Kullanıcı erişim yönetimi<br>A.11.1 Güvenli alanlar<br>A.11.2.1 Teçhizat yerleştirme ve koruma<br>A.13.1.1 Ağ kontrolleri<br>A.18.1.3 Kayıtların korunması | 5.15 Erişim kontrolü<br>7.1 Fiziksel güvenlik sınırları,<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama,<br>7.6 Güvenli alanlarda çalışma<br>7.8 Ekipman konumlandırma ve koruma<br>8.20 Ağ güvenliği<br>5.33 Kayıtların korunması |
| Fiziksel Mekânların Güvenliği | 3.6.2.7 | 1 | Destekleyici Altyapı Hizmetleri | A.11.2.2 Destekleyici altyapı hizmetleri<br>A.11.2.4 Teçhizat bakımı | 7.11 Destekleyici altyapı hizmetleri<br>7.13 Ekipman bakımı |
| Fiziksel Mekânların Güvenliği | 3.6.2.8 | 1 | Dış ve Çevresel Tehditlere Karşı Koruma | A.11.1 Güvenli alanlar<br>A.11.2.1 Teçhizat yerleştirme ve koruma<br>A.11.2.2 Destekleyici altyapı hizmetleri | 7.1 Fiziksel güvenlik sınırları,<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.6 Güvenli alanlarda çalışma<br>7.8 Ekipman konumlandırma ve koruma<br>7.11 Destekleyici altyapı hizmetleri |
| Fiziksel Mekânların Güvenliği | 3.6.2.9 | 1 | Donanım Bakımı ve Güvenliği | A.11.2.1 Teçhizat yerleştirme ve koruma<br>A.11.2.4 Teçhizat bakımı | 7.8 Ekipman konumlandırma ve koruma<br>7.13 Ekipman bakımı |
| Fiziksel Mekânların Güvenliği | 3.6.2.10 | 1 | Kablolama Güvenliği | A.11.2.3 Kablo güvenliği | 7.12 Kablo güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Fiziksel Mekânların Güvenliği | 3.6.2.11 | 1 | Fiziksel Giriş Kontrolleri | A.11.1.2 Fiziksel giriş kontrolleri<br>A.12.4 Kaydetme ve izleme | 7.2 Fiziksel giriş<br>8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Fiziksel Mekânların Güvenliği | 3.6.2.12 | 2 | Ortam Koşullarının Gerçek Zamanlı İzlenmesi | A.11.1.4 Dış ve çevresel tehditlere karşı koruma<br>A.11.2.2 Destekleyici altyapı hizmetleri | 7.5 Fiziksel ve çevresel tehditlere karşı koruma<br>7.11 Destekleyici altyapı hizmetleri |
| Fiziksel Mekânların Güvenliği | 3.6.2.13 | 2 | Siber Olay Tespitinde İz Kayıtlarının Kullanılması | A.12.4 Kaydetme ve izleme | 8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Fiziksel Mekânların Güvenliği | 3.6.2.14 | 3 | Kontrollü Erişim Noktalarının Oluşturulması | A.11.1.2 Fiziksel giriş kontrolleri | 7.2 Fiziksel giriş |
| Fiziksel Mekânların Güvenliği | 3.6.2.15 | 3 | İklimlendirme Kontrolü | A.11.2.2 Destekleyici altyapı hizmetleri<br>A.11.2.4 Teçhizat bakımı | 7.11 Destekleyici altyapı hizmetleri<br>7.13 Ekipman bakımı |
| Fiziksel Mekânların Güvenliği | 3.6.3.1 | 1 | Sistem Odası/Veri Merkezi Cihaz Yerleşim Planı | A.8.1.1 Varlık envanteri | 5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Fiziksel Mekânların Güvenliği | 3.6.3.2 | 2 | Gizlilik Seviyeli Bilgi İşleyen Cihazların TEMPEST Onayı | A.11.2.1 Teçhizat yerleştirme ve koruma<br>A.8.1.1 Varlık envanteri | 7.8 Ekipman konumlandırma ve koruma<br>5.9 Bilgi envanteri ve diğer ilgili varlıklar |
| Fiziksel Mekânların Güvenliği | 3.6.3.3 | 3 | TEMPEST Tesisat Kurallarına Uyum | A.11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması<br>A.11.2.1 Teçhizat yerleştirme ve koruma<br>A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.8 Ekipman konumlandırma ve koruma<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kişisel Verilerin Güvenliği | 4.1.1.1 | 1 | Kişisel Veri İşleme Envanterinin Hazırlanması ve Yönetimi | A.8.1.1 Varlık envanteri<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 5.9 Bilgi envanteri ve diğer ilgili varlıklar<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.1.2 | 1 | Kişisel Veri Saklama ve İmha Politikasının Hazırlanması | A.5.1.1 Bilgi güvenliği politikaları<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 5.1 Bilgi güvenliği politikaları<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.1.3 | 1 | Kişisel Verilerin Veri Tabanlarında Birincil Anahtar Olarak Kullanılmaması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği esasları<br>A.14.2.6 Güvenli geliştirme ortamı | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>8.31 Geliştirme, test ve canlı (gerçek) ortamlarının ayrılması |
| Kişisel Verilerin Güvenliği | 4.1.1.4 | 1 | Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması | A.9.1.1 Erişim kontrol politikası<br>A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.13.2.1 Bilgi transfer politikaları ve prosedürleri | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması<br>5.14 Bilgi transferi |
| Kişisel Verilerin Güvenliği | 4.1.1.5 | 1 | Kişisel Verilerin Güvensiz Ortamlarda Saklanmaması | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.18.1.3 Kayıtların korunması | 5.8 Proje yönetiminde bilgi güvenliği<br>5.33 Kayıtların korunması |
| Kişisel Verilerin Güvenliği | 4.1.1.6 | 1 | Kişisel Veri Üzerinde Girdi/Çıktı Denetimi Yapılması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği esasları<br>A.14.2.8 Sistem güvenlik testi | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>8.29 Geliştirme ve kabul aşamasında güvenlik testleri |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kişisel Verilerin Güvenliği | 4.1.1.7 | 1 | Kişisel Verinin Gizli Alanlarda Saklanmaması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği esasları<br>A.14.2.8 Sistem güvenlik testi<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>8.29 Geliştirme ve kabul aşamasında güvenlik testleri<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.1.8 | 1 | Hata Mesajlarında Mahremiyetin Korunması | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği esasları<br>A.14.2.8 Sistem güvenlik testi<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>8.29 Geliştirme ve kabul aşamasında güvenlik testleri<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.1.9 | 1 | Özel Nitelikli Kişisel Verinin Saklanması | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.18.1.3 Kayıtların korunması<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması<br>A.18.1.5 Kriptografik kontrollerin düzenlenmesi | 8.24 Kriptografi (şifreleme) kullanımı<br>5.33 Kayıtların korunması<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kişisel Verilerin Güvenliği | 4.1.1.10 | 1 | Geçici Olarak Tutulan Kişisel Verinin Yok Edilmesi | A.14.2.1 Güvenli geliştirme politikası<br>A.14.2.5 Güvenli sistem mühendisliği esasları<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kişisel Verilerin Güvenliği | 4.1.1.11 | 2 | Veri Tabanı Tasarımı | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.14.2.1 Güvenli geliştirme politikası | 5.8 Proje yönetiminde bilgi güvenliği<br>8.25 Güvenli geliştirme yaşam döngüsü |
| Kişisel Verilerin Güvenliği | 4.1.2.1 | 1 | Erişimlerin Kayıt Altına Alınması | A.9.4.2 Güvenli oturum açma prosedürleri<br>A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 8.5 Güvenli kimlik doğrulama<br>8.15 Kaydetme (log tutma)<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.2.2 | 1 | Erişim Kayıtlarının Arşivlenmesi | A.12.3.1 Bilgi yedekleme<br>A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 8.13 Bilgi yedekleme<br>8.15 Kaydetme (log tutma)<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.2.3 | 1 | Erişim Kayıtlarının Güvenliğinin Sağlanması | A.12.4.2 Kayıt bilgisinin korunması | 8.15 Kaydetme (log tutma) |
| Kişisel Verilerin Güvenliği | 4.1.2.4 | 1 | Erişim Kayıtlarının Aktarımı | A.13.2.1 Bilgi transfer politikaları ve prosedürleri | 5.14 Bilgi transferi |
| Kişisel Verilerin Güvenliği | 4.1.2.5 | 2 | Yetkisiz Erişimlerin Tespiti | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.12.4.2 Kayıt bilgisinin korunması | 8.3 Bilgi erişim kısıtlaması<br>8.15 Kaydetme (log tutma) |
| Kişisel Verilerin Güvenliği | 4.1.2.6 | 3 | Erişim Kayıtlarında Özel Nitelikli Kişisel Veri Bulundurulmaması | A.12.4.1 Olay kaydetme<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 8.15 Kaydetme (log tutma)<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kişisel Verilerin Güvenliği | 4.1.3.1 | 1 | Yetkilendirme Mekanizmasının Kullanılması | A.9.2 Kullanıcı erişim yönetimi<br>A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.3.2 | 1 | Kimlik Doğrulama Mekanizmasının Kullanılması | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 8.3 Bilgi erişim kısıtlaması<br>8.26 Uygulama güvenlik gereklilikleri<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.3.3 | 1 | Erişimin Sınırlandırılması | A.9.1.1 Erişim kontrol politikası<br>A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.9.4.2 Güvenli oturum açma prosedürleri | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması<br>8.5 Güvenli kimlik doğrulama |
| Kişisel Verilerin Güvenliği | 4.1.3.4 | 1 | Erişim Denetim Politikalarının Oluşturulması | A.5.1.1 Bilgi güvenliği politikaları<br>A.9.1.1 Erişim kontrol politikası | 5.1 Bilgi güvenliği politikaları<br>5.15 Erişim kontrolü |
| Kişisel Verilerin Güvenliği | 4.1.3.5 | 2 | Çok Faktörlü Kimlik Doğrulama Mekanizmasının Kullanılması | A.9.4.2 Güvenli oturum açma prosedürleri | 8.5 Güvenli kimlik doğrulama |
| Kişisel Verilerin Güvenliği | 4.1.3.6 | 2 | Dış Sistemler / Uygulamalar Arası Veri Akışı için Erişimlerin Doğrulanması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.12.4.1 Olay kaydetme<br>A.13.2.1 Bilgi transfer politikaları ve prosedürleri | 8.3 Bilgi erişim kısıtlaması<br>8.15 Kaydetme (log tutma)<br>5.14 Bilgi transferi |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kişisel Verilerin Güvenliği | 4.1.3.7 | 3 | Alt Bileşenler Arasında Veri Akışı için Erişimlerin Doğrulanması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.13.2.1 Bilgi transfer politikaları ve prosedürleri | 8.3 Bilgi erişim kısıtlaması<br>5.14 Bilgi transferi |
| Kişisel Verilerin Güvenliği | 4.1.4.1 | 1 | İletişimin Şifrelenmesi | A.10.1 Kriptografik kontroller<br>A.13.1 Ağ güvenliği yönetimi<br>A.13.2.1 Bilgi transfer politikaları ve prosedürleri | 8.24 Kriptografi (şifreleme) kullanımı<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı<br>5.14 Bilgi transferi |
| Kişisel Verilerin Güvenliği | 4.1.4.2 | 2 | Verinin Maskelenmesi | A.18.1.3 Kayıtların korunması<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 5.33 Kayıtların korunması<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması<br>8.11 Veri maskeleme |
| Kişisel Verilerin Güvenliği | 4.1.4.3 | 2 | Verinin Bütünlüğünün Korunması | A.9.2 Kullanıcı erişim yönetimi<br>A.10.1 Kriptografik kontroller | 5.15 Erişim kontrolü<br>8.24 Kriptografi (şifreleme) kullanımı |
| Kişisel Verilerin Güvenliği | 4.1.4.4 | 3 | Sistemin Alt Bileşenleri Arasındaki İletişimin Şifreli Yapılması | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.13.2.1 Bilgi transfer politikaları ve prosedürleri<br>A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.24 Kriptografi (şifreleme) kullanımı<br>8.21 Ağ hizmetlerinin güvenliği<br>5.14 Bilgi transferi<br>8.26 Uygulama güvenlik gereklilikleri |
| Kişisel Verilerin Güvenliği | 4.1.5.1 | 1 | Sistem Yedeklerinin Yetkili Kullanıcılar Tarafından Alınması | A.9.1.1 Erişim kontrol politikası<br>A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.12.3.1 Bilgi Yedekleme<br>A.12.4.1 Olay Kaydetme | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması<br>8.13 Bilgi yedekleme<br>8.15 Kaydetme (log tutma) |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kişisel Verilerin Güvenliği | 4.1.5.2 | 1 | Kişisel Verilerin Silinmesi | A.8.3.2 Ortamın yok edilmesi<br>A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>7.14 Ekipmanların güvenli bir şekilde yok edilmesi veya tekrar kullanılması |
| Kişisel Verilerin Güvenliği | 4.1.5.3 | 1 | Kişisel Verilerin Yok Edilmesi | A.8.3.2 Ortamın yok edilmesi<br>A.5.1.1 Bilgi güvenliği politikaları<br>A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>5.1 Bilgi güvenliği politikaları<br>5.18 Erişim hakları<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.5.4 | 1 | Kişisel Verilerin Anonim Hale Getirilmesi | A.5.1.1 Bilgi güvenliği politikaları<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 5.1 Bilgi güvenliği politikaları<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.5.5 | 1 | Kişisel Veri Barındıran Yedeklerin Güvenliğinin Sağlanması | A.12.3.1 Bilgi Yedekleme<br>A.12.4.1 Olay Kaydetme | 8.13 Bilgi yedekleme<br>8.15 Kaydetme (log tutma) |
| Kişisel Verilerin Güvenliği | 4.1.5.6 | 2 | Kişisel Veri Barındıran Yedeklerin Yok Edilmesi | A.8.3.2 Ortamın yok edilmesi<br>A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>7.14 Ekipmanların güvenli bir şekilde yok edilmesi veya tekrar kullanılması |
| Kişisel Verilerin Güvenliği | 4.1.6.1 | 1 | Aydınlatmanın Doğru Zamanda Yapılması | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kişisel Verilerin Güvenliği | 4.1.6.2 | 1 | Aydınlatmanın Yerine Getirildiğinin İspat Edilmesi | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.6.3 | 2 | Uygulama Üzerinden Aydınlatma Metninin Güncellenmesi | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.12.4.1 Olay Kaydetme | 5.8 Proje yönetiminde bilgi güvenliği<br>8.15 Kaydetme (log tutma) |
| Kişisel Verilerin Güvenliği | 4.1.7.1 | 1 | Açık Rıza Unsurlarının Belirlenmesi | A.18.1 Yasal ve sözleşmeye tabi gereksinimlere uyum<br>A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler<br>5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması |
| Kişisel Verilerin Güvenliği | 4.1.7.2 | 1 | Açık Rızanın Kayıt Altına Alınması | A.12.4.1 Olay Kaydetme<br>A.18.1.3 Kayıtların korunması | 8.15 Kaydetme (log tutma)<br>5.33 Kayıtların korunması |
| Kişisel Verilerin Güvenliği | 4.1.7.3 | 1 | Açık Rıza Durumunun Sorgulanması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.12.4.1 Olay Kaydetme | 8.3 Bilgi erişim kısıtlaması<br>8.15 Kaydetme (log tutma) |
| Kişisel Verilerin Güvenliği | 4.1.7.4 | 3 | Uygulama Üzerinden Açık Rıza Alınması | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi | 5.8 Proje yönetiminde bilgi güvenliği |
| Kişisel Verilerin Güvenliği | 4.1.7.5 | 3 | Açık Rıza Metninin Güncellenmesi | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama<br>A.18.1.3 Kayıtların korunması | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler<br>5.33 Kayıtların korunması |
| Kişisel Verilerin Güvenliği | 4.1.7.6 | 3 | Açık Rıza ile İlgili Taleplerin Yönetilmesi | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kişisel Verilerin Güvenliği | 4.1.7.7 | 3 | Islak İmzalı Açık Rıza Metninin Saklanması | A.18.1.3 Kayıtların korunması | 5.33 Kayıtların korunması |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kişisel Verilerin Güvenliği | 4.1.8.1 | 1 | İlgili Kişinin Başvuru Hakkının Yönetilmesi | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kişisel Verilerin Güvenliği | 4.1.8.2 | 1 | Kişisel Veriye Yapılan İşlemlerin Elde Edilmesi | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kişisel Verilerin Güvenliği | 4.1.8.3 | 1 | Güncelleme, Anonimleştirme, Silme ve Yok Etme İşlemlerinin Gerçekleştirilmesi | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kişisel Verilerin Güvenliği | 4.1.8.4 | 1 | Kişisel Verinin Aktarıldığı Üçüncü Tarafların Tespit Edilmesi | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama<br>A.18.1.3 Kayıtların korunması | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler<br>5.33 Kayıtların korunması |
| Kişisel Verilerin Güvenliği | 4.1.8.5 | 2 | Kişisel Verisi Etkilenen veya Etkilenmesi Muhtemel Kişilerin Bilgilendirilmesi | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Anlık Mesajlaşma Güvenliği | 4.2.1.1 | 1 | Mesajlaşma Uygulaması Seçimi | A.13.2.3 Elektronik mesajlaşma | 5.14 Bilgi transferi |
| Anlık Mesajlaşma Güvenliği | 4.2.1.2 | 1 | İletim Ortamı Güvenliği | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Anlık Mesajlaşma Güvenliği | 4.2.1.3 | 1 | Gizlilik Dereceli Veri Paylaşımı | A.13.2.1 Bilgi transfer politikaları ve prosedürleri | 5.14 Bilgi transferi |
| Anlık Mesajlaşma Güvenliği | 4.2.1.4 | 1 | Çoklu Cihaz Kullanımı | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.9.4.2 Güvenli oturum açma prosedürleri | 8.3 Bilgi erişim kısıtlaması<br>8.5 Güvenli kimlik doğrulama |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Anlık Mesajlaşma Güvenliği | 4.2.1.5 | 2 | Uçtan Uca Şifreleme | A.10.1 Kriptografik kontroller<br>A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.24 Kriptografi (şifreleme) kullanımı<br>8.26 Uygulama güvenlik gereklilikleri |
| Anlık Mesajlaşma Güvenliği | 4.2.1.6 | 2 | Şifreleme Anahtarlarının Saklanması | A.10.1.2 Anahtar yönetimi<br>A.18.1.3 Kayıtların korunması | 8.24 Kriptografi (şifreleme) kullanımı<br>5.33 Kayıtların korunması |
| Anlık Mesajlaşma Güvenliği | 4.2.1.7 | 2 | Yönetim Arayüzüne Erişim | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.12.4.1 Olay Kaydetme | 8.3 Bilgi erişim kısıtlaması<br>8.15 Kaydetme (log tutma) |
| Anlık Mesajlaşma Güvenliği | 4.2.1.8 | 3 | Cihaz Üzerindeki Verinin Şifrelenmesi | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.18.1.3 Kayıtların korunması | 8.24 Kriptografi (şifreleme) kullanımı<br>5.33 Kayıtların korunması |
| Anlık Mesajlaşma Güvenliği | 4.2.1.9 | 3 | Kritik Haberleşmenin Güvenliği | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Bulut Bilişim Güvenliği | 4.3.1.1 | 1 | Bulut Hizmeti Kullanımı | A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği<br>A.15.2 Tedarikçi hizmet sağlama yönetimi<br>A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.23 Bulut hizmetlerinin kullanımı için bilgi güvenliği<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Bulut Bilişim Güvenliği | 4.3.1.2 | 1 | Hizmet Kapsamı ile Rol ve Sorumlulukların Belirlenmesi | A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Bulut Bilişim Güvenliği | 4.3.1.3 | 1 | Veri İletimi Güvenliği | A.14.1.3 Uygulama hizmet işlemlerinin korunması<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 8.26 Uygulama güvenlik gereklilikleri<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Bulut Bilişim Güvenliği | 4.3.1.4 | 1 | Kaynakların İzole Edilmesi | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 8.3 Bilgi erişim kısıtlaması<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği |
| Bulut Bilişim Güvenliği | 4.3.1.5 | 1 | İmajların İmha Edilmesi | A.8.3.2 Ortamın yok edilmesi<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği |
| Bulut Bilişim Güvenliği | 4.3.1.6 | 1 | Sanal Makineye Ait Belleklerin İmhası | A.8.3.2 Ortamın yok edilmesi<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği |
| Bulut Bilişim Güvenliği | 4.3.1.7 | 1 | Bulut Ortamı Güvenliği | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği<br>A.15.2 Tedarikçi hizmet sağlama yönetimi | 5.15 Erişim kontrolü<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |
| Bulut Bilişim Güvenliği | 4.3.1.8 | 1 | Sanal Makineye Ait Disk Bölgelerinin İmhası | A.8.3.2 Ortamın yok edilmesi<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği |
| Bulut Bilişim Güvenliği | 4.3.1.9 | 1 | İş Sürekliliğinin Sağlanması | A.12.3 Yedekleme<br>A.15.2 Tedarikçi hizmet sağlama yönetimi<br>A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları | 8.13 Bilgi yedekleme<br>5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi<br>5.30 İş sürekliliği için BİT hazırlığı |
| Bulut Bilişim Güvenliği | 4.3.1.10 | 1 | Erişim Yetkilerinin Yönetiminin Sağlanması | A.9.2 Kullanıcı erişim yönetimi<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 5.15 Erişim kontrolü<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Bulut Bilişim Güvenliği | 4.3.1.11 | 1 | Hizmetin Sonlandırılması Hususları | A.8.3.2 Ortamın yok edilmesi<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 7.10 Depolama ortamı<br>8.10 Bilgi silme<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği |
| Bulut Bilişim Güvenliği | 4.3.1.12 | 2 | Güvenli Veri Depolama Politikasının Uygulanması | A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği |
| Bulut Bilişim Güvenliği | 4.3.1.13 | 2 | Bulut Ortamı İşlem Kayıtlarının Tutulması | A.12.4.1 Olay Kaydetme<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği<br>A.18.1.3 Kayıtların korunması | 8.15 Kaydetme (log tutma)<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.33 Kayıtların korunması |
| Bulut Bilişim Güvenliği | 4.3.1.14 | 3 | Kaynakların Fiziksel Olarak İzole Edilmesi | A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği<br>A.15.2 Tedarikçi hizmet sağlama yönetimi | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |
| Kripto Uygulamaları Güvenliği | 4.4.1.1 | 1 | Kriptografik Algoritma Tipinin Seçilmesi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.1.2 | 1 | Kripto Uygulama, Cihaz ve Sistemlerin Kriptografik Algoritma Güvenliği | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.1.3 | 1 | Standart Kriptografik Algoritmaları İçeren Kripto Modüllerinin Güvenliği | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.1.4 | 3 | Milli Kriptografik Algoritmaların Gerçeklendiği Kripto Cihazlarının Tedariki | A.10.1 Kriptografik kontroller<br>A.18.1.5 Kriptografik kontrollerin düzenlenmesi | 8.24 Kriptografi (şifreleme) kullanımı<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kripto Uygulamaları Güvenliği | 4.4.2.1 | 1 | Kriptografik Anahtara İlişkin Güvenlik Gereksinimleri Analizi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.2 | 1 | Kriptografik Anahtarların Üretilmesi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.3 | 1 | Anahtar Üretim ve Dağıtım Cihazlarına Erişim | A.9.2 Kullanıcı erişim yönetimi<br>A.10.1 Kriptografik kontroller<br>A.11.1.2 Fiziksel giriş kontrolleri<br>A.12.4 Kaydetme ve izleme | 5.15 Erişim kontrolü<br>8.24 Kriptografi (şifreleme) kullanımı<br>7.2 Fiziksel giriş<br>8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Kripto Uygulamaları Güvenliği | 4.4.2.4 | 1 | Güvenli Yedekleme | A.10.1 Kriptografik kontroller<br>A.11.1.2 Fiziksel giriş kontrolleri<br>A.12.4 Kaydetme ve izleme | 8.24 Kriptografi (şifreleme) kullanımı<br>7.2 Fiziksel giriş<br>8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Kripto Uygulamaları Güvenliği | 4.4.2.5 | 1 | Kriptografik Anahtarlara Erişim Kontrolü | A.9.2 Kullanıcı erişim yönetimi<br>A.10.1 Kriptografik kontroller<br>A.12.4 Kaydetme ve izleme | 5.15 Erişim kontrolü<br>8.24 Kriptografi (şifreleme) kullanımı<br>8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Kripto Uygulamaları Güvenliği | 4.4.2.6 | 1 | Kriptografik Anahtarların Revize Edilmesi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.7 | 1 | Güvenli Anahtar Ulaştırma / İletimi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kripto Uygulamaları Güvenliği | 4.4.2.8 | 1 | Anahtar Taşıma Cihazlarının Muhafazası ve Cihaza Erişim | A.9.2 Kullanıcı erişim yönetimi<br>A.10.1 Kriptografik kontroller<br>A.12.4 Kaydetme ve izleme | 5.15 Erişim kontrolü<br>8.24 Kriptografi (şifreleme) kullanımı<br>8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Kripto Uygulamaları Güvenliği | 4.4.2.9 | 1 | Anahtar Üretim Ortamlarına Güvenli Erişim | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.10 | 1 | İz Kayıtlarının Oluşturulması | A.12.4 Kaydetme ve izleme<br>A.16.1.7 Kanıt toplama | 8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri<br>5.28 Kanıt toplama |
| Kripto Uygulamaları Güvenliği | 4.4.2.11 | 1 | Kriptografik Anahtarların İptal Edilmesi/Güvenli Yok Edilmesi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.12 | 1 | Kriptografik Anahtar Sorumlusu Zimmet Tutanağının Hazırlanması | A.8.1.2 Varlıkların sahipliği<br>A.10.1 Kriptografik kontroller | 5.9 Bilgi envanteri ve diğer ilgili varlıklar<br>8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.13 | 1 | Kriptografik Anahtar Yetkilendirme | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.14 | 1 | Anahtarların Üretim Yerinden Sonra Kopyalanamaması ve Çoğaltılamaması | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.15 | 1 | Anahtarlara Açık Metin Olarak Erişilmemesi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.16 | 1 | İhlal Raporlama | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.17 | 1 | Yedek Anahtar | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kripto Uygulamaları Güvenliği | 4.4.2.18 | 1 | Anahtar Üretim ve Yönetim Sistemi Testi | A.10.1 Kriptografik kontroller<br>A.18.1.5 Kriptografik kontrollerin düzenlenmesi | 8.24 Kriptografi (şifreleme) kullanımı<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kripto Uygulamaları Güvenliği | 4.4.2.19 | 2 | Güvenli Anahtar Saklama | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.20 | 3 | Anahtar Taşıma Cihazlarında Yapılan Tüm Anahtar İşlemlerinin Kaydının Tutulması | A.10.1 Kriptografik kontroller<br>A.12.4 Kaydetme ve izleme | 8.24 Kriptografi (şifreleme) kullanımı<br>8.15 Kaydetme (log tutma)<br>8.16 İzleme faaliyetleri |
| Kripto Uygulamaları Güvenliği | 4.4.2.21 | 3 | Anahtar Taşıma Cihazlarında Bulunan Anahtarın Onaylı Kriptografik Yöntemlerle Şifreli Olarak Tutulması | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.22 | 3 | Anahtar Alma ve Depolama İşlemlerinde Bütünlük Hatası Oluşması Durumunda Anahtar Malzemesinin İmha Edilmesi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.23 | 3 | Kripto Güvenlik Belgesi Kontrolü | A.9.2 Kullanıcı erişim yönetimi<br>A.10.1 Kriptografik kontroller | 5.15 Erişim kontrolü<br>8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.24 | 3 | Anahtar Kimliği | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.2.25 | 3 | Anahtar Sayımı | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kripto Uygulamaları Güvenliği | 4.4.2.26 | 3 | Anahtar Üretim ve Yönetim Sistemi Testi | A.10.1 Kriptografik kontroller<br>A.18.1.5 Kriptografik kontrollerin düzenlenmesi | 8.24 Kriptografi (şifreleme) kullanımı<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kripto Uygulamaları Güvenliği | 4.4.3.1 | 1 | Güvensiz Ağlar Üzerinden Güvenli Haberleşme | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.10.1 Kriptografik kontroller | 8.3 Bilgi erişim kısıtlaması<br>8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.3.2 | 1 | Envanter Yönetimi | A.8.1.1 Varlık envanteri<br>A.9.2 Kullanıcı erişim yönetimi | 5.9 Bilgi envanteri ve diğer ilgili varlıklar<br>5.15 Erişim kontrolü |
| Kripto Uygulamaları Güvenliği | 4.4.3.3 | 1 | Güvenlik Değerlendirme ve Onay Durumu Yönetimi | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.3.4 | 2 | Kripto Protokollerinin En Güncel ve Güvenilir Versiyonlarının Kullanımı | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.3.5 | 2 | Envanter Yönetim Araçları ile Kriptografik Ürünlerin Yönetimi ve İzlenmesi | A.9.2 Kullanıcı erişim yönetimi<br>A.10.1 Kriptografik kontroller | 5.15 Erişim kontrolü<br>8.24 Kriptografi (şifreleme) kullanımı |
| Kripto Uygulamaları Güvenliği | 4.4.3.6 | 3 | Kripto Cihazları TEMPEST Laboratuvar Onayı | A.10.1 Kriptografik kontroller<br>A.12.6.1 Teknik açıklıkların yönetimi | 8.24 Kriptografi (şifreleme) kullanımı<br>8.8 Teknik açıklıkların yönetimi |
| Kripto Uygulamaları Güvenliği | 4.4.3.7 | 3 | Kripto Cihazları Kripto Analiz Laboratuvar Onayı | A.10.1 Kriptografik kontroller<br>A.18.1.5 Kriptografik kontrollerin düzenlenmesi | 8.24 Kriptografi (şifreleme) kullanımı<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kripto Uygulamaları Güvenliği | 4.4.3.8 | 3 | Kripto Cihazları COMSEC Laboratuvar Onayı | A.10.1 Kriptografik kontroller<br>A.18.1.5 Kriptografik kontrollerin düzenlenmesi | 8.24 Kriptografi (şifreleme) kullanımı<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kritik Altyapılar Güvenliği | 4.5.1 | - | Aşağıda listelenen rehber ana başlıklarında yer alan tedbirler uygulanır:<br>Ağ ve Sistem Güvenliği<br>Uygulama ve Veri Güvenliği<br>Taşınabilir Cihaz ve Ortam Güvenliği<br>Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği<br>Personel Güvenliği<br>Fiziksel Mekânların Güvenliği | - | - |
| Kritik Altyapılar Güvenliği | 4.5.2.1 | 1 | Cihaz Konfigürasyonları | A.14.2.5 Güvenli sistem mühendisliği esasları | 8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Kritik Altyapılar Güvenliği | 4.5.2.2 | 1 | Ağ Erişim Kontrolü | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.9.2 Kullanıcı erişim yönetimi | 5.15 Erişim kontrolü |
| Kritik Altyapılar Güvenliği | 4.5.2.3 | 1 | Ağ Segmentasyonu | A.13.1.3 Ağlarda ayrım | 8.22 Ağların ayrımı |
| Kritik Altyapılar Güvenliği | 4.5.2.4 | 1 | Kimlik Doğrulama | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.9.2 Kullanıcı erişim yönetimi | 8.3 Bilgi erişim kısıtlaması<br>5.15 Erişim kontrolü |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kritik Altyapılar Güvenliği | 4.5.2.5 | 1 | Erişim Yönetimi | A.6.2.2 Uzaktan çalışma<br>A.13.1.1 Ağ kontrolleri | 6.7 Uzaktan çalışma<br>8.20 Ağ güvenliği |
| Kritik Altyapılar Güvenliği | 4.5.2.6 | 1 | Fiziksel Erişim Güvenliği | A.11 Fiziksel ve çevresel güvenlik | 7.1 Fiziksel güvenlik sınırları<br>7.2 Fiziksel giriş<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.4 Fiziksel güvenlik izleme<br>7.5 Fiziksel ve çevresel tehditlere karşı koruma |
| Kritik Altyapılar Güvenliği | 4.5.2.7 | 1 | Sistem Sürekliliğinin Sağlanması | A.17.2 Yedek fazlalıklar | 5.29 Kesinti sırasında bilgi güvenliği |
| Kritik Altyapılar Güvenliği | 4.5.2.8 | 1 | Veri Manipülasyonunun Engellenmesi | A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.26 Uygulama güvenlik gereklilikleri |
| Kritik Altyapılar Güvenliği | 4.5.2.9 | 1 | Kullanıcı Erişim Yönetimi | A.6.2.2 Uzaktan çalışma<br>A.9.2 Kullanıcı erişim yönetimi | 6.7 Uzaktan çalışma<br>5.15 Erişim kontrolü |
| Kritik Altyapılar Güvenliği | 4.5.2.10 | 1 | SSL/TLS Korumalı İletişim | A.13.1.2 Ağ hizmetlerinin güvenliği<br>A.14.1.3 Uygulama hizmet işlemlerinin korunması | 8.21 Ağ hizmetlerinin güvenliği<br>8.26 Uygulama güvenlik gereklilikleri |
| Kritik Altyapılar Güvenliği | 4.5.2.11 | 1 | GPS İletişim ve Senkronizasyonun un Güvenliği | - | 8.20 Ağ güvenliği |
| Kritik Altyapılar Güvenliği | 4.5.2.12 | 1 | Ekipman Güvenliğinin Sağlanması | A.13.1.2 Ağ hizmetlerinin güvenliği | 8.21 Ağ hizmetlerinin güvenliği |
| Kritik Altyapılar Güvenliği | 4.5.2.13 | 1 | Tehdit İstihbaratı Yönetimi | A.6.1.4 Özel ilgi grupları ile iletişim | 5.6 Özel ilgi gruplarıyla iletişim |
| Kritik Altyapılar Güvenliği | 4.5.2.14 | 1 | Otoritelerle İletişim | A.6.1.3 Otoritelerle iletişim | 5.5 Yetkililerle iletişim |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kritik Altyapılar Güvenliği | 4.5.2.15 | 2 | Veri İletimi | A.13.2.1 Bilgi transfer politikaları ve prosedürleri<br>A.13.2.2 Bilgi transferindeki anlaşmalar | 5.14 Bilgi transferi |
| Kritik Altyapılar Güvenliği | 4.5.3.1 | 1 | Hizmet Güvenliği ve Sürekliliği | A.17.1 Bilgi güvenliği sürekliliği | 5.29 Kesinti sırasında bilgi güvenliği |
| Kritik Altyapılar Güvenliği | 4.5.3.2 | 1 | Üçüncü Taraflara İlişkin Güvenlik Gereksinimleri | A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme | 5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması |
| Kritik Altyapılar Güvenliği | 4.5.3.3 | 1 | Altyapı Servislerinin Güvenliği | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2 Geliştirme ve destek süreçlerinde güvenlik | 8.7 Kötü amaçlı yazılıma karşı koruma<br>5.8 Proje yönetiminde bilgi güvenliği<br>8.25 Güvenli geliştirme yaşam döngüsü |
| Kritik Altyapılar Güvenliği | 4.5.3.4 | 1 | Sahtecilik İşlemlerini Tespit ve Önleme | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.18.1.3 Kayıtların korunması | 8.7 Kötü amaçlı yazılıma karşı koruma<br>5.33 Kayıtların korunması |
| Kritik Altyapılar Güvenliği | 4.5.3.5 | 1 | Sinyalleşme Trafiğinin Güvenliği | A.13.1 Ağ güvenliği yönetimi | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı<br>8.24 Kriptografi (şifreleme) kullanımı |
| Kritik Altyapılar Güvenliği | 4.5.3.6 | 1 | Güvenilir İletişimin Tesisi | A.13.1 Ağ güvenliği yönetimi | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı<br>8.24 Kriptografi (şifreleme) kullanımı |
| Kritik Altyapılar Güvenliği | 4.5.3.7 | 1 | Sıkılaştırma Faaliyetleri | A.12.1 İşletim prosedürleri ve sorumlulukları | 8.9 Konfigürasyon (yapılandırma) yönetimi |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kritik Altyapılar Güvenliği | 4.5.3.8 | 1 | Ekipman Arızalarının İzlenmesi | A.11.2.1 Teçhizat yerleştirme ve koruma<br>A.11.2.2 Destekleyici altyapı hizmetleri | 7.8 Ekipman konumlandırma ve koruma<br>7.11 Destekleyici altyapı hizmetleri |
| Kritik Altyapılar Güvenliği | 4.5.3.9 | 1 | Ekipman Güvenliğinin Sağlanması | A.11.1 Güvenli alanlar<br>A.11.2 Teçhizat | 7.1 Fiziksel güvenlik sınırları<br>7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama<br>7.6 Güvenli alanlarda çalışma<br>7.8 Ekipman konumlandırma ve koruma |
| Kritik Altyapılar Güvenliği | 4.5.3.10 | 1 | Tehdit İstihbaratı Yönetimi | A.6.1.4 Özel ilgi grupları ile iletişim | 5.6 Özel ilgi gruplarıyla iletişim<br>5.7 Tehdit İstihbaratı |
| Kritik Altyapılar Güvenliği | 4.5.3.11 | 1 | Otoritelerle İletişim | A.6.1.3 Otoritelerle iletişim | 5.5 Yetkililerle iletişim |
| Kritik Altyapılar Güvenliği | 4.5.3.12 | 1 | Arayan Hat Bilgisi Kullanımı | A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | 5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Kritik Altyapılar Güvenliği | 4.5.3.13 | 1 | İnternet Değişim Noktası | A.13.1 Ağ güvenliği yönetimi | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı<br>8.23 Web filtreleme |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Kritik Altyapılar Güvenliği | 4.5.3.14 | 3 | Kritik Haberleşme Güvenliği | A.13.1 Ağ güvenliği yönetimi<br>A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama<br>A.18.1.5 Kriptografik kontrollerin düzenlenmesi | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı<br>8.23 Web filtreleme<br>5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler |
| Yeni Geliştirmeler ve Tedarik | 4.6.1.1 | 1 | Politika ve Prosedürlerin Tanımlanması | A.8.1.1 Varlık envanteri<br>A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği<br>A.15.2 Tedarikçi hizmet sağlama yönetimi | 5.9 Bilgi envanteri ve diğer ilgili varlıklar<br>5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |
| Yeni Geliştirmeler ve Tedarik | 4.6.1.2 | 1 | Yazılım Varlık Envanterine Kayıt Edilmemiş Yazılımların Yönetimi | A.8.2.3 Varlıkların kullanımı | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Yeni Geliştirmeler ve Tedarik | 4.6.1.3 | 1 | Donanım Varlık Envanterine Kayıt Edilmemiş Donanımların Yönetimi | A.8.2.3 Varlıkların kullanımı | 5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı |
| Yeni Geliştirmeler ve Tedarik | 4.6.1.4 | 1 | Arayüzün Türkçe Dil Desteğine Sahip Olması | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi | 5.8 Proje yönetiminde bilgi güvenliği |
| Yeni Geliştirmeler ve Tedarik | 4.6.1.5 | 2 | Alt Yüklenici Yönetimi | A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği<br>A.15.2 Tedarikçi hizmet sağlama yönetimi | 5.19 Tedarikçi ilişkilerinde bilgi güvenliği<br>5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Yeni Geliştirmeler ve Tedarik | 4.6.1.6 | 2 | Fonksiyonel ve Fonksiyonel Olmayan Testlerin Yapılması | A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri<br>A.14.2 Geliştirme ve destek süreçlerinde güvenlik | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.28 Güvenli kodlama<br>8.25 Güvenli geliştirme yaşam döngüsü |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.1 | 1 | Kurulum Güvenliği | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.19 İşletim sistemlerine yazılım kurulumu |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.2 | 1 | Servis Güvenliği | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.12.5 İşletimsel yazılımın kontrolü | 8.3 Bilgi erişim kısıtlaması<br>8.9 Konfigürasyon (yapılandırma) yönetimi |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.3 | 1 | Güncel İşletim Sistemi ve Uygulamaların Kullanılması | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.19 İşletim sistemlerine yazılım kurulumu |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.4 | 1 | Şifreli Haberleşen Servislerin Kullanılması | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika | 8.24 Kriptografi (şifreleme) kullanımı |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.5 | 1 | Parola Politikasının Belirlenmesi | A.9.4.3 Parola yönetim sistemi | 5.17 Kimlik doğrulama bilgileri |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.6 | 1 | Son Kullanıcı Bilgisayarlarında Ağ Erişiminin Kısıtlanması | A.9.1 Erişim kontrolünün iş gereklilikleri | 8.3 Bilgi erişim kısıtlaması<br>5.15 Erişim kontrolü |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.7 | 1 | Hata ve Sorun Bilgilerinin Üretici ile Paylaşılmaması | A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi<br>A.12.5 İşletimsel yazılımın kontrolü | 5.8 Proje yönetiminde bilgi güvenliği<br>8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.19 İşletim sistemlerine yazılım kurulumu |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.8 | 1 | Kablosuz Ağ Arayüzlerinin Kapatılması | A.12.5 İşletimsel yazılımın kontrolü<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.19 İşletim sistemlerine yazılım kurulumu<br>8.21 Ağ hizmetlerinin güvenliği |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.9 | 1 | Sistem Üzerinde Düzenli Olarak Zafiyet ve Zararlı Yazılım Taraması Yapılması | A.12.2.1 Kötücül yazılımlara karşı kontroller<br>A.13.1.2 Ağ hizmetlerinin güvenliği | 8.7 Kötü amaçlı yazılıma karşı koruma<br>8.21 Ağ hizmetlerinin güvenliği |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.10 | 1 | Yerel Güvenlik Duvarı Ayarlarının Yapılması | 13.1.2 Ağ hizmetlerinin güvenliği | 8.21 Ağ hizmetlerinin güvenliği |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.11 | 1 | Sunucularda Zaman Senkronizasyonun un Sağlanması | A.12.4.4 Saat senkronizasyonu | 8.17 Saat senkronizasyonu |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.12 | 1 | Güvenli Süreç (Process) İşleme Ayarlarının Yapılması | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.19 İşletim sistemlerine yazılım kurulumu |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.13 | 2 | Kullanılmayan Uygulamaların Kaldırılması | A.12.1.3 Kapasite yönetimi<br>A.13.1.1 Ağ kontrolleri | 8.6 Kapasite yönetimi<br>8.20 Ağ güvenliği |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.14 | 2 | Merkezi Güncelleme Sunucusu | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.19 İşletim sistemlerine yazılım kurulumu |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.15 | 2 | IPv6 Pasif Hale Getirilmesi | A.9.1.2 Ağlara ve ağ hizmetlerine erişim | 5.15 Erişim kontrolü |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.16 | 2 | Sistem İz Kayıtlarının Aktif Edilmesi | A.12.4.1 Olay kaydetme<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.17 | 2 | Sistem İz Kayıtlarının Merkezi Bir Sunucuda Toplanması | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.18 | 2 | Merkezi Kimlik Yönetimi Servisinin Kullanılması | A.9.2.2 Kullanıcı erişimine izin verme | 5.18 Erişim hakları |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.19 | 3 | Sunucularda Çalışan Servislerin Takibi | A.12.4.1 Olay kaydetme | 8.15 Kaydetme (log tutma) |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.20 | 3 | Bilgisayar Tabanlı Saldırı Tespit ve Engelleme Sistemlerinin Kullanılması | A.12.4.1 Olay kaydetme<br>A.12.6.1 Teknik açıklıkların yönetimi | 8.15 Kaydetme (log tutma)<br>8.8 Teknik açıklıkların yönetimi |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.21 | 3 | Disk Kotalarının Belirlenmesi | - | 8.6 Kapasite yönetimi |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.1.22 | 3 | Disk Seviyesinde Şifreleme Yapılması | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika | 8.24 Kriptografi (şifreleme) kullanımı |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.2.1 | 1 | Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi | - | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.2.2 | 1 | Yetkili Kullanıcı Hesap Yönetimi | A.9.2 Kullanıcı erişim yönetimi<br>A.12.5 İşletimsel yazılımın kontrolü | 5.15 Erişim kontrolü<br>8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.5 Güvenli kimlik doğrulama |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.2.3 | 2 | Dosya Sistemi Güvenli Erişim Düzenlemeleri | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.12.5 İşletimsel yazılımın kontrolü | 8.3 Bilgi erişim kısıtlaması<br>8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.19 İşletim sistemlerine yazılım kurulumu |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.2.4 | 2 | Güvenli Disk Bölümlendirme | - | 8.6 Kapasite yönetimi |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.2.5 | 2 | Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi | - | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.2.6 | 2 | Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması | A.12.5 İşletimsel yazılımın kontrolü | 5.33 Kayıtların korunması<br>8.9 Konfigürasyon (yapılandırma) yönetimi |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.2.7 | 2 | Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması | A.9.4.2 Güvenli oturum açma prosedürleri | 8.5 Güvenli kimlik doğrulama |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.2.8 | 3 | Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi | A.9.4 Sistem ve uygulama erişim kontrolü | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.1 | 1 | Kullanıcı Haklarının Kısıtlanması | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.12.5 İşletimsel yazılımın kontrolü | 8.3 Bilgi erişim kısıtlaması<br>8.9 Konfigürasyon (yapılandırma) yönetimi<br>5.15 Erişim kontrolü |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.2 | 1 | Otomatik Güncellemenin Aktif Olması | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.1 Kullanıcı uç nokta cihazları |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.3 | 1 | SMB Protokolü Güvenliği | A.9.1 Erişim kontrolünün iş gereklilikleri | 8.1 Kullanıcı uç nokta cihazları<br>8.20 Ağ güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.4 | 1 | Yerel Yönetici Hesapları Yönetimi | A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi | 8.2 Ayrıcalıklı erişim hakları |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.5 | 1 | Ayrıcalıklı Hesap Sayılarının Sınırlandırılması | A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi | 8.2 Ayrıcalıklı erişim hakları |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.6 | 1 | Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi | A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi | 8.2 Ayrıcalıklı erişim hakları<br>5.17 Kimlik doğrulama bilgileri |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.7 | 2 | Kullanılmayan Hesapların Devre Dışı Bırakılması | A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi<br>A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi | 5.18 Erişim hakları |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.8 | 2 | Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması | A.9.2 Kullanıcı erişim yönetimi | 5.15 Erişim kontrolü |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.9 | 2 | Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması | A.9.2 Kullanıcı erişim yönetimi | 5.15 Erişim kontrolü<br>8.18 Ayrıcalıklı destek programların kullanımı |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.10 | 2 | Aktif Dizin Sorguları Güvenliği | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika | 8.24 Kriptografi (şifreleme) kullanımı |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.11 | 2 | Yönetici Hesaplarının İzlenmesi | A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi<br>A.12.4.1 Olay kaydetme<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.2 Ayrıcalıklı erişim hakları<br>8.15 Kaydetme (log tutma) |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.12 | 2 | Güvenli Yönetici İş İstasyonu Kullanımı | - | 8.2 Ayrıcalıklı erişim hakları<br>8.18 Ayrıcalıklı destek programların kullanımı<br>5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması |
| İşletim Sistemi Sıkılaştırma Tedbirleri | 5.1.3.13 | 2 | Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.9.2 Kullanıcı erişim yönetimi | 8.3 Bilgi erişim kısıtlaması<br>5.15 Erişim kontrolü<br>8.18 Ayrıcalıklı destek programların kullanımı |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.1 | 1 | Güncelleme ve Yama Yönetimi | A.12.5 İşletimsel yazılımın kontrolü<br>A.12.6 Teknik açıklık yönetimi | 8.8 Teknik açıklıkların yönetimi<br>8.19 İşletim sistemlerine yazılım kurulumu |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.2 | 1 | Veri Tabanı Parametrelerinin Güvenli Yapılandırılması | A.12.5 İşletimsel yazılımın kontrolü<br>A.14.2.5 Güvenli sistem mühendisliği prensipleri | 8.9 Konfigürasyon (yapılandırma) yönetimi<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.3 | 1 | Varsayılan Hesap ve Parolaların Kullanılmaması | A.5.1.1 Bilgi güvenliği politikaları<br>A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi | 5.1 Bilgi güvenliği politikaları<br>5.17 Kimlik doğrulama bilgileri |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.4 | 1 | Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması | A.9.4.3 Parola yönetim sistemi | 5.17 Kimlik doğrulama bilgileri |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.5 | 1 | Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması | A.6.2.2 Uzaktan çalışma<br>A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1 Ağ güvenliği yönetimi | 6.7 Uzaktan çalışma<br>5.15 Erişim kontrolü<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.6 | 1 | Kullanılmayan Hesapların Kapatılması | A.9.2 Kullanıcı erişim yönetimi | 5.15 Erişim kontrolü<br>6.1 Tarama |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.7 | 1 | Anonim Hesapların Bulunmaması | A.9.2 Kullanıcı erişim yönetimi | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.8 | 1 | Veri Tabanı Rol ve Yetkilerinin Kısıtlanması | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.9.2 Kullanıcı erişim yönetimi | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.9 | 1 | Veri Tabanı Yönetim Sisteminin İşletim Sistemi Üzerindeki Ayrıcalıklarının Sınırlandırılması | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.9.2 Kullanıcı erişim yönetimi | 8.3 Bilgi erişim kısıtlaması<br>5.15 Erişim kontrolü |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.10 | 1 | Komut/Sorgu Geçmişi Kayıtlarının Güvenliğinin Sağlanması | A.18.1.3 Kayıtların korunması | 5.33 Kayıtların korunması |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.11 | 1 | Yedeklerin Güvenliğinin Sağlanması | A.9.2 Kullanıcı erişim yönetimi<br>A.12.3 Yedekleme | 8.3 Bilgi erişim kısıtlaması<br>5.15 Erişim kontrolü<br>8.13 Bilgi yedekleme<br>8.24 Kriptografi (şifreleme) kullanımı |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.12 | 1 | Adanmış Sunucu Kullanılması | A.12.5 İşletimsel yazılımın kontrolü | - |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.13 | 1 | Kurulum Dosyalarının Güvenilir Kaynaklardan Temin Edilmesi | A.12.5 İşletimsel yazılımın kontrolü | 8.19 İşletim sistemlerine yazılım kurulumu |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.14 | 1 | Örnek Verilerin Silinmesi | A.12.5 İşletimsel yazılımın kontrolü | 8.10 Bilgi silme |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.15 | 2 | Veri Tabanı Sistem Dosyalarının ve İz Kayıtlarının Aynı Disk Bölümü Üzerinde Bulunmaması | A.18.1.3 Kayıtların korunması | 5.33 Kayıtların korunması |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.16 | 2 | Veri Tabanında Tablo ve Nesne Düzeyinde Yetkilendirme Yapılması | A.9.1 Erişim kontrolünün iş gereklilikleri | 5.2 Bilgi güvenliği rolleri ve sorumlulukları<br>5.15 Erişim kontrolü |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.17 | 2 | İşletim Sistemi Üzerinde Veri Tabanı Servisi Çalıştıran Kullanıcıların Yönetici Haklarına Sahip Olmaması | A.9.2 Kullanıcı erişim yönetimi | 5.15 Erişim kontrolü<br>5.2 Bilgi güvenliği rolleri ve sorumlulukları |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.18 | 2 | Kümeleme veya Replikasyon İçinde Bulunan Veri Tabanı Sunucuları Arası İletişimin Güvenliğinin Sağlanması | A.9.2 Kullanıcı erişim yönetimi<br>A.13.1 Ağ güvenliği yönetimi | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.19 | 2 | Merkezi Kimlik Doğrulama Sisteminin Kullanılması | A.9.2.2 Kullanıcı erişimine izin verme | 5.18 Erişim hakları |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.20 | 3 | Kritik Bilgi İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması | A.9.4.1 Bilgiye erişimin kısıtlanması<br>A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika | 8.3 Bilgi erişim kısıtlaması<br>8.24 Kriptografi (şifreleme) kullanımı |
| Veri Tabanı Sıkılaştırma Tedbirleri | 5.2.1.21 | 3 | Veri Tabanı Sunucusu ile İstemci Arasındaki İletişimin Şifreli Olması | A.13.1 Ağ güvenliği yönetimi | 8.20 Ağ güvenliği<br>8.21 Ağ hizmetlerinin güvenliği<br>8.22 Ağların ayrımı<br>8.24 Kriptografi (şifreleme) kullanımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.1 | 1 | Güncel Web Sunucu Yazılımlarının Kullanılması | A.12.5 İşletimsel yazılımın kontrolü | 8.8 Teknik açıklıkların yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.2 | 1 | WebDAV Desteğinin Kaldırılması | A.12.5 İşletimsel yazılımın kontrolü | 8.8 Teknik açıklıkların yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.3 | 1 | Web Sunucusu Kullanıcı Yönetimi | A.9.2 Kullanıcı erişim yönetimi<br>A.12.5 İşletimsel yazılımın kontrolü | 5.15 Erişim kontrolü<br>8.2 Ayrıcalıklı erişim hakları<br>5.17 Kimlik doğrulama bilgileri |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.4 | 1 | Web Sunucusunun Bilgi İfşalarını Önleyecek Şekilde Yapılandırılması | A.12.5 İşletimsel yazılımın kontrolü | 8.12 Veri sızıntısı önleme |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.5 | 1 | Desteklenen HTTP Metotlarının Kısıtlanması | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.6 | 1 | Dizin Listelemenin Pasif Hale Getirilmesi | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.7 | 1 | Debug Modunun Kapalı Olması | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.8 | 1 | İstek Limitlerinin Tanımlanması | A.12.5 İşletimsel yazılımın kontrolü | 8.6 Kapasite yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.9 | 1 | İz Kayıtlarının Alınması | A.12.4.1 Olay kaydetme<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.10 | 1 | Yazma İzni Olan Dizinlerin Kısıtlanması | A.9.2 Kullanıcı erişim yönetimi<br>A.12.5 İşletimsel yazılımın kontrolü | 5.15 Erişim kontrolü<br>8.3 Bilgi erişim kısıtlaması |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.11 | 1 | SSL/TLS Kullanımı | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika | 8.24 Kriptografi (şifreleme) kullanımı |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.12 | 1 | İsteklerin HTTP'den HTTPS'e Yönlendirilmesi | A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika<br>A.12.5 İşletimsel yazılımın kontrolü | 8.24 Kriptografi (şifreleme) kullanımı |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.13 | 1 | Kullanılmayan Modüllerin Kaldırılması | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.14 | 1 | Açık Portların Kısıtlanması | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.12.5 İşletimsel yazılımın kontrolü | 5.15 Erişim kontrolü<br>8.20 Ağ güvenliği |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.15 | 1 | Kaynak Kullanım Optimizasyonu | A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması<br>A.14.2.5 Güvenli sistem mühendisliği esasları | 8.26 Uygulama güvenlik gereklilikleri<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.16 | 1 | Sunucunun Korumalı ve Ayrıştırılmış Şekilde Kurulumu | A.9.1.2 Ağlara ve ağ hizmetlerine erişim<br>A.13.1.3 Ağlarda ayrım | 5.15 Erişim kontrolü<br>8.22 Ağların ayrımı |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.17 | 1 | Sunucuda Koruyucu HTTP Başlıklarının Kullanımı | A.14.2.5 Güvenli sistem mühendisliği esasları | 8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.18 | 1 | Sunucunun Özel Anahtarının (Private Key) Korunması | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.19 | 2 | İz Kayıtlarının Merkezi Kayıt Sistemine Gönderilmesi | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.1.20 | 2 | Sunucuya IP Adresi Üzerinden Erişimlerin Engellenmesi | A.9.1 Erişim kontrolünün iş gereklilikleri | 8.20 Ağ güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.1 | 1 | Güncel Sanallaştırma Yazılımının Kullanılması | A.12.5 İşletimsel yazılımın kontrolü | 8.8 Teknik açıklıkların yönetimi<br>8.9 Konfigürasyon (yapılandırma) yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.2 | 1 | Konteynerların /Sanal Makinelerin Çalıştığı Ana Makine Üzerinde Sıkılaştırmaların Yapılması | A.12.5 İşletimsel yazılımın kontrolü | 8.9 Konfigürasyon (yapılandırma) yönetimi |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.3 | 1 | Sanal Makineler Arasında Zaman Senkronizasyonun un Sağlanması | A.12.4.4 Saat senkronizasyonu | 8.17 Saat senkronizasyonu |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.4 | 1 | Sanallaştırma Yazılımı Güvenlik Duvarının Aktif Olması | A.13.1.2 Ağ hizmetlerinin güvenliği | 8.21 Ağ hizmetlerinin güvenliği |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.5 | 1 | Mantıksal Birim Numarası (LUN) Maskelemesi Yapılması | A.14.2.1 Güvenli geliştirme politikası | 8.25 Güvenli geliştirme yaşam döngüsü<br>8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.6 | 1 | Sanallaştırma Ünitesi Üzerinden Konsol Erişimlerinin Kısıtlanması | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.9.2 Kullanıcı erişim yönetimi | 8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri<br>5.15 Erişim kontrolü |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.7 | 1 | Sanallaştırma Ünitesinde Kullanıcı Yetkilendirme | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.9.2 Kullanıcı erişim yönetimi | 8.2 Ayrıcalıklı erişim hakları<br>5.15 Erişim kontrolü |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.8 | 1 | Gereksiz Hizmetlerin ve Kullanılmayan Donanımların Kaldırılması | A.12.1.3 Kapasite yönetimi<br>A.13.1.1 Ağ kontrolleri | 8.6 Kapasite yönetimi<br>8.20 Ağ güvenliği |

| BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ | | | | TS ISO/IEC 27001:2017 | TS ISO/IEC 27001:2022 |
|---|---|---|---|---|---|
| Varlık Grubu Ana Başlığı | Tedbir No | Tedbir Seviyesi | Tedbir Adı | | |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.9 | 1 | Sanal Makineler Üzerindeki Diskler için Disk Küçültme Konfigürasyonuna Erişimin Kısıtlanması | A.9.1 Erişim kontrolünün iş gereklilikleri<br>A.9.2 Kullanıcı erişim yönetimi | 8.2 Ayrıcalıklı erişim hakları<br>5.15 Erişim kontrolü |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.10 | 2 | Sanallaştırma Yazılımının Merkezi Olarak Güncellenmesi | A.12.5 İşletimsel yazılımın kontrolü | 8.19 İşletim sistemlerine yazılım kurulumu |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.11 | 2 | Sanal Makineler için İz Kayıtlarının Yönetilmesi | A.12.4.1 Olay kaydetme<br>A.12.4.2 Kayıt bilgisinin korunması<br>A.12.4.3 Yönetici ve operatör kayıtları | 8.15 Kaydetme (log tutma) |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.12 | 2 | Sanal Makinelerin Güvenli İmhası | A.8.3.2 Ortamın yok edilmesi | 7.10 Depolama ortamı |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.13 | 2 | Hipervizörler Tarafından Sunulan Bellek Paylaşımı Özelliklerinin Kullanımı | - | 8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.14 | 2 | Sunucu Yedeklerinin Alınması | A.12.3 Yedekleme | 8.13 Bilgi yedekleme |
| Sunucu Sıkılaştırma Tedbirleri | 5.3.2.15 | 3 | Disk ve İmajların Şifreli Olarak Saklanması | A.10.1 Kriptografik kontroller | 8.24 Kriptografi (şifreleme) kullanımı |

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI

**SİBER GÜVENLİK BAŞKANLIĞI**