TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI

DİJİTAL DÖNÜŞÜM OFİSİ

TS ISO/IEC 27001:2017 KONTROLLERİ İLE BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ EŞLEŞTİRME TABLOSU

EKİM 2021

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ

TS ISO/IEC 27001:2017 KONTROLLERİ İLE BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ EŞLEŞTİRME TABLOSU

EKİM 2021

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 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 Kontrollerin 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 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
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 A.8.1.2 Varlıkların sahipliği
Ağ ve Sistem Güvenliği	3.1.1.2	1	Donanım Envanter İçeriğinin Yönetimi	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.1.3	1	Donanım Envanterine Kaydedilmemiş Donanımların Yönetimi	A.8.2.3 Varlıkların kullanımı
Ağ ve Sistem Güvenliği	3.1.1.4	2	Aktif Keşif Araçlarının Kullanılması	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.1.5	2	DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.1.6	2	Kullanım Ömrünü Tamamlayan Cihazların Veri Depolama Üniteleri	A.8.3.2 Ortamın yok edilmesi A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı
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 A.13.1.1 Ağ kontrolleri
Ağ ve Sistem Güvenliği	3.1.1.8	3	Donanım Varlıklarının Kimlik Denetimi için İstemci Sertifikalarının Kullanılması	A.10.1.2 Anahtar yönetimi
Ağ ve Sistem Güvenliği	3.1.1.9	3	Sabit Disk Güvenliği	A.8.3.2 Ortamın yok edilmesi
Ağ ve Sistem Güvenliği	3.1.2.1	1	Yazılım Envanterinin Yönetimi	A.8.1.1 Varlıkların envanteri A.8.1.2 Varlıkların sahipliği
Ağ ve Sistem Güvenliği	3.1.2.2	1	Yazılım Envanter İçeriğinin Yönetimi	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.2.3	1	Yazılımın Üreticisi Tarafından Desteklenmesi	A.8.1.1 Varlık envanteri A.8.2.3 Varlıkların kullanımı

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.2.4	1	Yazılım Envanterine Kaydedilmemiş Yazılımların Yönetimi	A.8.2.3 Varlıkların kullanımı
Ağ ve Sistem Güvenliği	3.1.2.5	2	Yazılım Envanteri Yönetim Araçlarının Kullanımı	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.2.6	3	Yazılım ve Donanım Envanterinin Entegre Edilmesi	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.2.7	3	Beyaz Liste Yönetimi	A.12.6.2 Yazılım kurulumu kısıtlamaları
Ağ ve Sistem Güvenliği	3.1.3.1	1	Yazılım Güncelleme Araçlarının Kullanımı	A.14.2.2 Sistem değişiklik kontrolü prosedürleri
Ağ ve Sistem Güvenliği	3.1.3.2	1	Zararlı Yazılımların Engellenmesi	A.12.6.2 Yazılım kurulumu kısıtlamaları
Ağ ve Sistem Güvenliği	3.1.3.3	1	Zafiyet/Yama Yönetimi	A.12.6.1 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
Ağ ve Sistem Güvenliği	3.1.3.5	1	Son Kullanıcıların Yetkisiz Program Ekleme/Kaldırma İşlemlerinin Engellenmesi	A.12.6.2 Yazılım kurulumu kısıtlamaları
Ağ ve Sistem Güvenliği	3.1.3.6	1	Güvenlik Açıkları için Risk Analizi Tabanlı Önceliklendirme	A.12.6.1 Teknik açıklıkların yönetimi
Ağ ve Sistem Güvenliği	3.1.3.7	1	Güvenlik Sıkılaştırmalarının Yapılması	A.12.5.1 İşletimdeki sistemler üzerine yazılım kurulumu
Ağ ve Sistem Güvenliği	3.1.3.8	2	İşletim Sistemi Yama Yönetimi Araçlarının Kullanımı	A.12.6.1 Teknik açıklıkların yönetimi A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.3.9	2	Zafiyet Tarama Araçlarının Kullanımı	A.12.6.1 Teknik açıklıkların yönetimi A.13.1.1 Ağ kontrolleri
Ağ ve Sistem Güvenliği	3.1.3.10	2	Aktif Portların, Servislerin ve Protokollerin Varlık Envanterinde Tutulması	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.4.1	1	Tekrar Yayınlama (Relay) İşleminin Engellenmesi	A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.4.2	1	SMTP Kimlik Doğrulaması Kullanımı	A.9.4.2 Güvenli oturum açma prosedürleri
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
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 A.13.2.3 Elektronik mesajlaşma
Ağ ve Sistem Güvenliği	3.1.4.5	1	İstenmeyen E-posta (Spam) Koruması	A.12.2.1 Kötücül yazılımlara karşı kontroller
Ağ ve Sistem Güvenliği	3.1.4.6	1	Servis Dışı Bırakma Saldırıları (DoS) Koruması	A.13.1.1 Ağ kontrolleri A.13.1.2 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 A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği A.13.2.3 Elektronik mesajlaşma
Ağ ve Sistem Güvenliği	3.1.4.8	1	Sahte ya da Değiştirilmiş E-Postaların Engellenmesi	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği A.13.2.3 Elektronik mesajlaşma

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
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
Ağ ve Sistem Güvenliği	3.1.4.10	1	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması	A.12.2.1 Kötücül yazılımlara karşı kontroller
Ağ ve Sistem Güvenliği	3.1.4.11	1	Güvenlik Sıkılaştırmalarının Yapılması	A.12.5 İşletimsel yazılımın kontrolü
Ağ ve Sistem Güvenliği	3.1.4.12	1	E-Posta İletişim Güvenliğinin Sağlanması	A.10.1 Kriptografik kontroller A.13.2.1 Bilgi transfer politikaları ve prosedürleri A.13.2.3 Elektronik mesajlaşma
Ağ ve Sistem Güvenliği	3.1.4.13	1	E-Posta Sunucu Mimarisi	A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi A.14.2.5 Güvenli sistem mühendisliği prensipleri
Ağ ve Sistem Güvenliği	3.1.4.14	1	Üçüncü Taraflardan Temin Edilen E-Posta Hizmetleri	A.13.1.2 Ağ hizmetlerinin güvenliği A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme
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 A.12.6.2 Yazılım kurulumu kısıtlamaları
Ağ ve Sistem Güvenliği	3.1.4.16	2	E-Posta İstemcilerinde Betik Kodlarının Kullanımını Sınırlama	A.12.2.1 Kötücül yazılımlara karşı kontroller A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu A.12.6.2 Yazılım kurulumu kısıtlamaları
Ağ ve Sistem Güvenliği	3.1.4.17	2	E-Posta Alışverişlerinin Şifreli ve İmzalı Yapılması	A.10.1 Kriptografik kontroller A.13.2.2 Bilgi transferindeki anlaşmalar A.13.2.3 Elektronik mesajlaşma A.14.1.3 Uygulama hizmet işlemlerinin korunması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.4.18	2	E-Posta Sunucularına Uzaktan Erişim	A.6.2.2 Uzaktan çalışma A.9.4.2 Güvenli oturum açma prosedürleri A.9.4.3 Parola yönetim sistemi
Ağ ve Sistem Güvenliği	3.1.4.19	3	E-Posta Eklerinin Kum Havuzlarında Çalıştırılması	A.12.2.1 Kötücül yazılımlara karşı kontroller
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 A.13.1.2 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
Ağ ve Sistem Güvenliği	3.1.5.3	1	Cihazların Otomatik Kod Çalıştırmasına İzin Vermemesi	A.12.2.1 Kötücül yazılımlara karşı kontroller A.12.5.1 İşletimsel sistemler üzerine 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
Ağ ve Sistem Güvenliği	3.1.5.5	1	İşletim Sistemlerinin Güvenlik Mekanizmalarının Etkinleştirilmesi	A.12.2.1 Kötücül yazılımlara karşı kontroller
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 A.12.4.1 Olay kaydetme A.12.4.3 Yönetici ve operatör kayıtları A.18.1.3 Kayıtların korunması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.5.7	3	DNS Sorgularının Kayıtlarının Tutulması	A.12.2.1 Kötücül yazılımlara karşı kontroller A.12.4.1 Olay kaydetme A.12.4.3 Yönetici ve operatör kayıtları
Ağ ve Sistem Güvenliği	3.1.5.8	3	Komut Satırı Kayıtlarının Tutulması	A.12.2.1 Kötücül yazılımlara karşı kontroller A.12.4.1 Olay kaydetme A.12.4.3 Yönetici ve operatör kayıtları
Ağ ve Sistem Güvenliği	3.1.6.1	1	Ağ Topolojisi	A.13.1.1 Ağ kontrolleri
Ağ ve Sistem Güvenliği	3.1.6.2	1	Ağ Cihazlarının Güvenli Konfigürasyonu	A.9.4.2 Güvenli oturum açma prosedürleri A.13.1.1 Ağ kontrolleri
Ağ ve Sistem Güvenliği	3.1.6.3	1	Ağ Cihazlarında Güvenlik Güncellemelerinin Yapılması	A.13.1.2 Ağ hizmetlerinin güvenliği A.14.2.2 Sistem değişiklik kontrolü prosedürleri
Ağ ve Sistem Güvenliği	3.1.6.4	1	Kara Liste veya Beyaz Liste Kullanımı	A.9.1.2 Ağlara ve ağ hizmetlerine erişim
Ağ ve Sistem Güvenliği	3.1.6.5	1	İzin Verilmeyen Trafiğin Engellenmesi	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği A.13.1.3 Ağlarda ayrım
Ağ ve Sistem Güvenliği	3.1.6.6	1	Ağların İzole Edilmesi	A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği A.13.1.3 Ağlarda ayrım
Ağ ve Sistem Güvenliği	3.1.6.7	1	DoS/DDoS Koruması	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği A.13.1.3 Ağlarda ayrım

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.9	1	Kablosuz Erişim Noktalarının Envanterinin Tutulması	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.6.10	1	Misafir Ağı Yönetimi	A.9.1.1 Erişim kontrol politikası A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.9.4.2 Güvenli oturum açma prosedürleri A.13.1.3 Ağlarda ayrım
Ağ ve Sistem Güvenliği	3.1.6.11	1	Yerel Güvenlik Duvarı Ayarlarının Yapılması	A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.12	1	IP Telefon Kullanımı	A.8.1.3 Varlıkların kabul edilebilir kullanımı A.13.1.2 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 A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
Ağ ve Sistem Güvenliği	3.1.6.14	1	IP Telefon Kullanımında Parola Politikası	A.9.4.3 Parola yönetim sistemi
Ağ ve Sistem Güvenliği	3.1.6.15	2	Ağ Erişim Denetimleri	A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1.1 Ağ kontrolleri
Ağ ve Sistem Güvenliği	3.1.6.16	2	Ağ Cihazlarına Ait Yapılandırmaların Dokümante Edilmesi	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.17	2	Ağ Paketlerinin Kaydedilmesi	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.6.18	2	Ağ Sınır Cihazlarında Kayıt Tutulması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması
Ağ ve Sistem Güvenliği	3.1.6.19	2	Ağ Tabanlı Saldırı Tespit/Engelleme Sistemi Kullanımı	A.12.2.1 Kötücül yazılımlara karşı kontroller A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.20	2	Uygulama Katmanında Filtreleme Yapılması	A.9.4.2 Güvenli oturum açma prosedürleri A.12.2.1 Kötücül yazılımlara karşı kontroller A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.21	2	Ağ Tabanlı URL Filtreleri Kullanımı	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.22	2	URL Kategori Hizmeti Kullanımı	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.23	2	URL'lerin Kayıt Altına Alınması	A.12.4.1 Olay kaydetme A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.24	2	Kurum Ağına Bağlı Kablosuz Erişim Noktalarının Tespiti	A.13.1.1 Ağ kontrolleri A.13.1.2 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 A.13.1.3 Ağlarda ayrım
Ağ ve Sistem Güvenliği	3.1.6.26	2	Eşler Arası Kablosuz Ağ Erişiminin Engellenmesi	A.13.1.1 Ağ kontrolleri A.13.1.2 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 A.13.1.2 Ağ hizmetlerinin güvenliği

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.6.28	2	Uygulama Seviyesi Saldırıların Engellenmesi	A.12.2.1 Kötücül yazılımlara karşı kontroller A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.29	2	IP Telefon Erişim Kontrol Listeleri	A.9.1.1 Erişim kontrol politikası A.9.1.2 Ağlara ve ağ hizmetlerine erişim
Ağ ve Sistem Güvenliği	3.1.6.30	3	Ağ Cihazlarının Yapılandırma Yönetimi	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.31	3	Ağ Cihazlarının Yönetimi	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.6.32	3	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	A.6.2.2 Uzaktan çalışma A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.12.2.1 Kötücül yazılımlara karşı kontroller
Ağ ve Sistem Güvenliği	3.1.6.33	3	Kripto Ağ Cihazlarının Kullanımı	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika A.10.1.2 Anahtar yönetimi
Ağ ve Sistem Güvenliği	3.1.6.34	3	Kablosuz İletişim Güvenliği	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika A.13.1.1 Ağ kontrolleri A.13.1.2 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
Ağ ve Sistem Güvenliği	3.1.6.36	3	Veri Transferi	A.13.2.1 Bilgi transfer politikaları ve prosedürleri A.13.2.2 Bilgi transferindeki anlaşmalar A.13.2.3 Elektronik mesajlaşma A.13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.7.1	1	Veri Sınıflandırma Politikasının Oluşturulması	A.8.2.1 Bilgi sınıflandırması A.8.2.2 Bilgi etiketlemesi A.8.2.3 Varlıkların 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 A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri
Ağ ve Sistem Güvenliği	3.1.7.3	1	Kritik Verinin Envanteri Yönetimi	A.8.1.1 Varlıkların envanteri
Ağ ve Sistem Güvenliği	3.1.7.4	1	Düzenli Olarak Erişilmeyen Kritik Verinin ve Sistemlerin Kaldırılması	A.8.3.2 Ortamın yok edilmesi
Ağ ve Sistem Güvenliği	3.1.7.5	1	Bulut Servislerinin Kullanımı	A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme A.15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme
Ağ ve Sistem Güvenliği	3.1.7.6	1	Taşınabilir Ortam Yönetimi	A.8.1.3 Varlıkların kabul edilebilir kullanımı A.8.3.1 Taşınabilir ortam yönetimi
Ağ ve Sistem Güvenliği	3.1.7.7	1	Ağda Kritik Veri Taşınması	A.13.2.1 Bilgi transfer politikaları ve prosedürleri A.13.2.3 Elektronik mesajlaşma
Ağ ve Sistem Güvenliği	3.1.7.8	2	Ağ İçerisinde Veri Sızıntısı Önleme	A.9.4.1 Bilgiye erişimin kısıtlanması A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.9.4.2 Güvenli oturum açma prosedürleri A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması
Ağ ve Sistem Güvenliği	3.1.7.10	3	Taşınabilir Ortam Engelleme	A.8.1.3 Varlıkların kabul edilebilir kullanımı A.8.3.1 Taşınabilir ortam yönetimi
Ağ ve Sistem Güvenliği	3.1.8.1	1	İz ve Denetim Kayıtlarının Tutulması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
Ağ ve Sistem Güvenliği	3.1.8.2	1	Denetim Kayıtlarının Yönetimi	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
Ağ ve Sistem Güvenliği	3.1.8.3	1	Zaman Sunucusu Kullanımı	A.12.4.4 Saat senkronizasyonu
Ağ ve Sistem Güvenliği	3.1.8.4	1	Detaylı Kayıt Tutulması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
Ağ ve Sistem Güvenliği	3.1.8.5	1	Kayıtlar için Yeterli Depolama Alanı Tahsisi	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması
Ağ ve Sistem Güvenliği	3.1.8.6	2	Merkezi Kayıt Yönetimi	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
Ağ ve Sistem Güvenliği	3.1.8.7	2	Kayıt Analizi Araçları Kullanımı	A.16.1.4 Bilgi güvenliği olaylarında değerlendirme ve karar verme A.16.1.7 Kanıt toplama

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.8.8	2	Siber Tehdit ve Olay Yönetim Sistemlerinin Düzenli Yapılandırılması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları A.16.1.4 Bilgi güvenliği olaylarında 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
Ağ ve Sistem Güvenliği	3.1.9.2	1	Kapasite Planlaması	A.12.1.3 Kapasite yönetimi
Ağ ve Sistem Güvenliği	3.1.9.3	1	Sanal Makinelerin Yönetilmesi	A.8.3.2 Ortamın yok edilmesi A.13.1.1 Ağ kontrolleri
Ağ ve Sistem Güvenliği	3.1.9.4	1	İşletim Sistemi Sıkılaştırmalarının ve Güvenlik Kontrollerinin Yapılması	A.12.2.1 Kötücül yazılımlara karşı kontroller A.12.4.1 Olay kaydetme A.12.6.1 Teknik açıklıkların yönetimi
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 A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri
Ağ ve Sistem Güvenliği	3.1.9.6	2	İmaj Bütünlüğünün Denetlenmesi ve İzlenmesi	A.12.3.1 Bilgi yedekleme A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi
Ağ ve Sistem Güvenliği	3.1.9.7	2	Sanal Ağ Güvenliği	A.13.1.1 Ağ kontrolleri A.13.2.1 Bilgi transfer politikaları ve prosedürleri
Ağ ve Sistem Güvenliği	3.1.9.8	2	Operasyon ve Test Ortamlarının İzolasyonu	A.9.1.1 Erişim kontrol politikası A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.12.1.4 Geliştirme, test ve işletim ortamların birbirinden ayrılması A.13.1.1 Ağ kontrolleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.9.9	2	Sanallaştırma Yönetim Ortamına Erişim	A.9.1.1 Erişim kontrol politikası A.9.1.2 Ağlara ve ağ hizmetlerine erişim
Ağ ve Sistem Güvenliği	3.1.9.10	2	Sanallaştırma Ortamı Sertifika Yönetimi	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika A.10.1.2 Anahtar yönetimi
Ağ ve Sistem Güvenliği	3.1.9.11	2	Sanal Makineler Arası Trafiğin Kontrol Edilmesi	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.9.12	2	Depolama Ortamları ile İletişim Güvenliğinin Sağlanması	A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Ağ ve Sistem Güvenliği	3.1.9.13	2	Fiziksel Kaynakların İzole Edilmesi	A.11.2.1 Teçhizat yerleştirme ve koruma
Ağ ve Sistem Güvenliği	3.1.10.1	1	Siber Olaylara Müdahale Planlarının Hazırlanması	A.16.1.1 Sorumluluklar ve prosedürler A.16.1.5 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 A.16.1.5 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 A.16.1.1 Sorumluluklar ve prosedürler
Ağ ve Sistem Güvenliği	3.1.10.4	1	Siber Tehdit Bildirimlerinin Yönetilmesi	A.16.1.3 Bilgi güvenliği açıklıklarının 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
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 A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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
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 A.16.1.6 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 A.18.1.3 Kayıtların korunması A.18.2.3 Teknik uyum gözden geçirmesi
Ağ ve Sistem Güvenliği	3.1.11.2	1	Sızma Testlerinin Kullanıcı Profillerine Göre Gerçekleştirilmesi	A.12.6.1 Teknik açıklıkların yönetimi A.18.2.3 Teknik uyum gözden geçirmesi
Ağ ve Sistem Güvenliği	3.1.11.3	1	Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi	A.12.6.1 Teknik açıklıkların yönetimi A.18.2.3 Teknik uyum gözden geçirmesi
Ağ ve Sistem Güvenliği	3.1.11.4	1	Sızma Testi için Oluşturulan Hesapların Yönetimi	A.9.2.1 Kullanıcı kaydetme ve kayıt silme A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi
Ağ ve Sistem Güvenliği	3.1.11.5	1	Doğrulama Testlerinin Yaptırılması	A.6.1.2 Görevlerin ayrılığı A.18.2.3 Teknik uyum gözden geçirmesi
Ağ ve Sistem Güvenliği	3.1.11.6	1	Sızma Testi ve Güvenlik Denetimi Bulgularının Seviyelendirilmesi	A.12.6.1 Teknik açıklıkların yönetimi A.18.2.3 Teknik uyum gözden geçirmesi
Ağ ve Sistem Güvenliği	3.1.11.7	2	Test Ortamlarının Hazırlanması	A.12.7.1 Bilgi sistemleri tetkik kontrolleri
Ağ ve Sistem Güvenliği	3.1.11.8	2	Sızma Testleri ve Güvenlik Denetimlerinin Periyodu	A.12.6.1 Teknik açıklıkların yönetimi A.18.2.3 Teknik uyum gözden geçirmesi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.11.9	3	Düzenli Kırmızı Takım Tatbikatlarının Yapılması	A.12.6.1 Teknik açıklıkların yönetimi A.16.1.2 Bilgi güvenliği olaylarının raporlanması A.16.1.3 Bilgi güvenliği açıklıklarının raporlanması A.18.2.3 Teknik uyum gözden geçirmesi
Ağ ve Sistem Güvenliği	3.1.11.10	3	Kurum Ağına Eklenen Yazılımın ve Donanımın Kontrolü	A.12.6.1 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 A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.12.4.1 Olay kaydetme
Ağ ve Sistem Güvenliği	3.1.12.2	1	Kullanıcı Hesaplarının Yönetimi	A.9.2.1 Kullanıcı kaydetme ve kayıt silme A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi
Ağ ve Sistem Güvenliği	3.1.12.3	1	Başarısız Oturum Açma Denemelerinin Yönetimi	A.9.4.2 Güvenli oturum açma prosedürleri A.12.4.1 Olay kaydetme
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 A.14.2.6 Güvenli geliştirme ortamı
Ağ ve Sistem Güvenliği	3.1.12.5	1	Yönetici Hesaplarının Kullanımı	A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.12.4.1 Olay kaydetme
Ağ ve Sistem Güvenliği	3.1.12.6	1	İşlem Yapılmayan Oturumların Sonlandırılması	A.9.4.2 Güvenli oturum açma prosedürleri
Ağ ve Sistem Güvenliği	3.1.12.7	1	Kimlik Doğrulama	A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.9.4.2 Güvenli oturum açma prosedürleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.12.8	1	Kullanıcı Yetkilerinin Güncellenmesi	A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi
Ağ ve Sistem Güvenliği	3.1.12.9	1	Kurum Dışı Paydaşların Uzaktan Erişimi	A.6.2.2 Uzaktan çalışma A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.9.4.2 Güvenli oturum açma prosedürleri A.12.4.1 Olay kaydetme A.13.1.2 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 A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi
Ağ ve Sistem Güvenliği	3.1.12.11	2	Yönetici Hesaplarının İşletimi	A.9.1.1 Erişim kontrol politikası A.9.2.2 Kullanıcı erişimine izin verme A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.9.4.2 Güvenli oturum açma prosedürleri A.12.4.1 Olay kaydetme A.12.4.3 Yönetici ve operatör kayıtları
Ağ ve Sistem Güvenliği	3.1.12.12	2	Betik Dillerinin Kullanımına Yönelik Erişimin Sınırlandırılması	A.12.2.1 Kötücül yazılımlara karşı kontroller A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu A.12.6.2 Yazılım kurulumu kısıtlamaları
Ağ ve Sistem Güvenliği	3.1.12.13	2	Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması	A.8.1.1 Varlık envanteri A.8.1.2 Varlıkların sahipliği

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.9.4.2 Güvenli oturum açma prosedürleri
Ağ ve Sistem Güvenliği	3.1.12.15	2	Çok Faktörlü Kimlik Doğrulama Yapılması	A.6.2.2 Uzaktan çalışma A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.9.4.2 Güvenli oturum açma prosedürleri
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
Ağ ve Sistem Güvenliği	3.1.12.17	2	Servis Hesaplarının Yönetimi	A.9.2.2 Kullanıcı erişimine izin verme A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi
Ağ ve Sistem Güvenliği	3.1.12.18	3	Hesap Giriş Davranışlarında Değişikliklerin Saptanması	A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi A.12.4.1 Olay kaydetme
Ağ ve Sistem Güvenliği	3.1.12.19	3	Oturum Kayıtlarının Tutulması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması
Ağ ve Sistem Güvenliği	3.1.12.20	3	Sistem Yöneticisi Görevlerinin Güvenliği	A.9.2.1 Kullanıcı kaydetme ve kayıt silme A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi A.12.4.3 Yönetici ve operatör kayıtları
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 A.9.3.1 Gizli kimlik doğrulama bilgisinin kullanımı A.9.4.3 Parola yönetim sistemi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.13.1	1	Yedekleme Planının Oluşturulması	A.12.3.1 Bilgi yedekleme A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması
Ağ ve Sistem Güvenliği	3.1.13.2	1	Yedekleme Planının Periyodik Olarak Gözden Geçirilmesi	A.12.3.1 Bilgi yedekleme A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi
Ağ ve Sistem Güvenliği	3.1.13.3	1	Yedekleme İşlemleri için İz Kayıtlarının Oluşturulması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması
Ağ ve Sistem Güvenliği	3.1.13.4	1	Yedekten Geri Dönüş Testleri	A.12.3.1 Bilgi yedekleme A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi
Ağ ve Sistem Güvenliği	3.1.13.5	2	Yedekleme Medyalarının Saklanması, Güvenliği ve İmhası	A.8.3.2 Ortamın yok edilmesi A.8.3.3 Fiziksel ortam aktarımı A.11.2.5 Varlıkların taşınması A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı A.12.3.1 Bilgi yedekleme
Ağ ve Sistem Güvenliği	3.1.13.6	2	İş Sürekliliği Kapsamının Tanımlanması	A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması
Ağ ve Sistem Güvenliği	3.1.13.7	2	İş Sürekliliği Planlarının Hazırlanması	A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi
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 A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
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 A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması
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
Ağ ve Sistem Güvenliği	3.1.13.11	2	İş Sürekliliği Planlarının Güvenli Muhafazası	A.12.3.1 Bilgi yedekleme
Ağ ve Sistem Güvenliği	3.1.13.12	2	Felaket Kurtarma Planlarının Hazırlanması	A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi
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 A.6.1.3 Otoritelerle iletişim A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması
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 A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması
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

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.13.16	2	Felaket Kurtarma Planlarının Güvenli Muhafazası	A.12.3.1 Bilgi Yedekleme A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması
Ağ ve Sistem Güvenliği	3.1.13.17	3	Kritik Sistem Sürekliliğinin Sağlanması	A.17.2.1 Bilgi işleme olanaklarının erişilebilirliği
Ağ ve Sistem Güvenliği	3.1.13.18	3	Felaket Kurtarma Merkezi Oluşturulması	A.17.2.1 Bilgi işleme olanaklarının erişilebilirliği
Ağ ve Sistem Güvenliği	3.1.14.1	1	Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması	A.6.2.2 Uzaktan çalışma
Ağ ve Sistem Güvenliği	3.1.14.2	1	Ekipman Güvenliğinin Sağlanması	A.6.2.2 Uzaktan çalışma A.11.2.6 Kuruluş dışındaki teçhizat ve varlıkların güvenliği
Ağ ve Sistem Güvenliği	3.1.14.3	1	Dosya Paylaşımı	A.6.2.2 Uzaktan çalışma
Ağ ve Sistem Güvenliği	3.1.14.4	1	Farkındalık Eğitimlerinin Verilmesi	A.6.2.2 Uzaktan çalışma A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi
Ağ ve Sistem Güvenliği	3.1.14.5	1	Zararlı Yazılımdan Korunma Uygulamaları	A.6.2.2 Uzaktan çalışma A.12.2.1 Kötücül yazılımlara karşı kontroller
Ağ ve Sistem Güvenliği	3.1.14.6	1	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	A.6.2.2 Uzaktan çalışma A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.12.5 İşletimsel yazılımın kontrolü
Ağ ve Sistem Güvenliği	3.1.14.7	1	Kurum Kaynaklarına Uzaktan Erişim	A.6.2.2 Uzaktan çalışma A.9.4.2 Güvenli oturum açma prosedürleri
Ağ ve Sistem Güvenliği	3.1.14.8	1	Video Konferans Uygulamalarının Kullanımı	A.8.2.3 Varlıkların kullanımı A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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
Ağ ve Sistem Güvenliği	3.1.14.10	1	Güncel Video Konferans Uygulamalarının Kullanılması	A.12.5.1 İşletimdeki sistemler üzerine 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
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 A.13.2.3 Elektronik mesajlaşma A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması A.14.1.3 Uygulama hizmet işlemlerinin korunması
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 A.13.1.2 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
Ağ ve Sistem Güvenliği	3.1.14.18	3	Erişimin Kurum Bilgisayarları ile Sınırlandırılması	A.6.2.2 Uzaktan çalışma A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Ağ ve Sistem Güvenliği	3.1.14.19	3	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	A.6.2.1 Mobil cihaz politikası A.6.2.2 Uzaktan çalışma A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.12.2.1 Kötücül yazılımlara karşı kontroller
Uygulama ve Veri Güvenliği	3.2.1.1	1	Kullanıcı Yönetiminin Yapılabilmesi	A.9.2.1 Kullanıcı kaydetme ve kayıt silme A.9.2.2 Kullanıcı erişimine izin verme
Uygulama ve Veri Güvenliği	3.2.1.2	1	Ortak Hesap Kullanılmaması	A.9.2.1 Kullanıcı kaydetme ve kayıt silme A.12.4.1 Olay kaydetme
Uygulama ve Veri Güvenliği	3.2.1.3	1	Kimlik Doğrulama İşlemleri için İz Kayıtlarının Oluşturulması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması
Uygulama ve Veri Güvenliği	3.2.1.4	1	Kimlik Doğrulama Bilgilerinin Güvenliği	A.9.4.2 Güvenli oturum açma prosedürleri A.9.4.3 Parola yönetim sistemi
Uygulama ve Veri Güvenliği	3.2.1.5	1	İlk Parolanın Belirlenmesi	A.9.4.3 Parola yönetim sistemi A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi
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 A.9.4.3 Parola yönetim sistemi A.12.4.1 Olay kaydetme
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
Uygulama ve Veri Güvenliği	3.2.1.8	1	Parola Yönetimi	A.9.4.3 Parola yönetim sistemi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
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 A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması A.14.1.3 Uygulama hizmet işlemlerinin korunması
Uygulama ve Veri Güvenliği	3.2.1.10	2	Güçlü Kimlik Doğrulama Yöntemlerinin Desteklenmesi	A.9.4.2 Güvenli oturum açma prosedürleri
Uygulama ve Veri Güvenliği	3.2.1.11	2	Hesap Kurtarma Seçeneklerinin Güvenliği	A.9.4.2 Güvenli oturum açma prosedürleri
Uygulama ve Veri Güvenliği	3.2.1.12	2	Kullanılmayan Hesapların Tespiti	A.9.2.1 Kullanıcı kaydetme ve kayıt silme A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi
Uygulama ve Veri Güvenliği	3.2.1.13	2	Merkezi Kimlik Doğrulama Mekanizmalarının Kullanılması	A.9.4.2 Güvenli oturum açma prosedürleri A.14.2.5 Güvenli sistem mühendisliği esasları
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 A.14.2.5 Güvenli sistem mühendisliği esasları
Uygulama ve Veri Güvenliği	3.2.2.2	1	Oturum Kimliğinin Doğrulanması ve Güvenliğinin Sağlanması	A.14.1.3 Uygulama hizmet işlemlerinin korunması A.14.2.5 Güvenli sistem mühendisliği esasları
Uygulama ve Veri Güvenliği	3.2.2.3	1	Kullanıcı Oturumlarının Sonlandırılması	A.9.4.2 Güvenli oturum açma prosedürleri A.14.2.5 Güvenli sistem mühendisliği esasları

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Uygulama ve Veri Güvenliği	3.2.2.4	1	Oturum Güvenlik Mekanizmalarının Kullanılması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği esasları
Uygulama ve Veri Güvenliği	3.2.2.5	3	Kullanıcıların Aktif Oturumlarını Yönetebilmesi	A.14.2.5 Güvenli sistem mühendisliği esasları
Uygulama ve Veri Güvenliği	3.2.3.1	1	Yetki Denetimi	A.9.2.2 Kullanıcı erişimine izin verme A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi veya düzenlenmesi A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi A.9.2.6 Erişim haklarının kaldırılması A.9.4.1 Bilgiye erişimin kısıtlanması A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması
Uygulama ve Veri Güvenliği	3.2.3.2	1	Kritik Veriye ve Kaynaklara Erişimlerin Kayıt Altına Alınması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
Uygulama ve Veri Güvenliği	3.2.3.3	1	En Az Yetki Prensibinin Uygulanması	A.9.2.2 Kullanıcı erişimine izin verme A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.9.4.1 Bilgiye erişimin kısıtlanması
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 A.14.2.5 Güvenli sistem mühendisliği esasları
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 A.14.1.3 Uygulama hizmet işlemlerinin korunması
Uygulama ve Veri Güvenliği	3.2.4.2	1	Uygulama Bileşenlerine Dış Kaynaklardan Erişimin Kısıtlanması	A.9.4.1 Bilgiye erişimin kısıtlanması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Uygulama ve Veri Güvenliği	3.2.4.3	1	İstemci Ön Bellekleme İşlevinin Kritik Veri için Kapatılması	A.9.4.1 Bilgiye erişimin kısıtlanması A.14.2.5 Güvenli sistem mühendisliği esasları
Uygulama ve Veri Güvenliği	3.2.4.4	1	Uygulamanın Kullandığı Kaynakların Güvensiz Ortamlarda Saklanmaması	A.9.4.1 Bilgiye erişimin kısıtlanması A.14.2.1 Güvenli geliştirme politikası
Uygulama ve Veri Güvenliği	3.2.4.5	1	Güvenilmeyen Kaynaklardan Alınan Dosyaların Denetlenmesi	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.4.6	1	Kaynaklara Erişimin Kısıtlanması	A.9.4.1 Bilgiye erişimin kısıtlanması A.12.2.1 Kötücül yazılımlara karşı kontroller A.14.2.5 Güvenli sistem mühendisliği prensipleri
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
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 A.14.2.4 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar
Uygulama ve Veri Güvenliği	3.2.5.2	1	Kaynak Paylaşım ve İçerik Güvenliği Sıkılaştırmaları	A.9.1 Erişim kontrolünün iş gereklilikleri A.14.2.5 Güvenli sistem mühendisliği esasları
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 A.14.2.5 Güvenli sistem mühendisliği prensipleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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
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 A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.9.4.1 Bilgiye erişimin kısıtlanması
Uygulama ve Veri Güvenliği	3.2.5.6	1	İşletimdeki Sistemler Üzerinde Uygulama Kurulumu	A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu A.12.6.2 Yazılım kurulumu kısıtlamaları
Uygulama ve Veri Güvenliği	3.2.5.7	2	Güvenli Derleme	A.12.2.1 Kötücül yazılımlara karşı kontroller A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.5.8	2	Yapılandırma Değişikliklerinin İzlenmesi	A.9.4.5 Program kaynak koduna erişim kontrolü A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.14.2.2 Sistem değişiklik kontrolü prosedürleri A.14.2.4 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar
Uygulama ve Veri Güvenliği	3.2.5.9	2	Sistem Kaynaklarının Azalması Durumunda Uyarı Verilmesi	A.12.1.3 Kapasite yönetimi
Uygulama ve Veri Güvenliği	3.2.5.10	2	Anahtarlar ve Parolaların Değiştirilebilir Olması	A.9.4.3 Parola yönetim sistemi A.10.1 Kriptografik kontroller A.12.5.1 İşletimdeki sistemler üzerine yazılım kurulumu

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Uygulama ve Veri Güvenliği	3.2.5.11	3	Sunucular Arası İletişimin Şifreli Olması	A.10.1 Kriptografik kontroller A.13.1.2 Ağ hizmetlerinin güvenliği A.14.1.3 Uygulama hizmet işlemlerinin korunması
Uygulama ve Veri Güvenliği	3.2.6.1	1	Güvenlik Gereksinimleri ve Tasarımı	A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Uygulama ve Veri Güvenliği	3.2.6.2	1	Test ve Geliştirme Ortamında Gerçek Veri Kullanılmaması	A.14.2.6 Güvenli geliştirme ortamı A.14.3.1 Test verisinin korunması
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 A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri
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
Uygulama ve Veri Güvenliği	3.2.6.5	1	Güncel İstemci ve Sunucu Teknolojilerinin Kullanılması	A.12.6.1 Teknik açıklıkların yönetimi A.14.2.1 Güvenli geliştirme politikası A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi
Uygulama ve Veri Güvenliği	3.2.6.6	1	Uygulama Güvenlik Testlerinin Yapılması	A.14.2.8 Sistem güvenlik testi A.14.2.9 Sistem kabul testi A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme
Uygulama ve Veri Güvenliği	3.2.6.7	2	Kaynak Kod Güvenlik Analizlerinin Yapılması	A.14.2.8 Sistem güvenlik testi A.14.2.9 Sistem kabul testi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Uygulama ve Veri Güvenliği	3.2.6.8	2	Güvenli Yazılım Geliştirme Süreçlerinin Uygulanması	A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi A.14.2 Geliştirme ve destek proseslerinde güvenlik
Uygulama ve Veri Güvenliği	3.2.7.1	1	Ortak Hesap Kullanılmaması ve En Az Yetki Prensibinin Uygulanması	A.9.2 Kullanıcı erişim yönetimi A.9.4.1 Bilgiye erişimin kısıtlanması
Uygulama ve Veri Güvenliği	3.2.7.2	1	Bulut Depolama Hizmetlerinde Kurumsal Verilerin Bulundurulmaması	-
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 A.9.4.1 Bilgiye erişimin kısıtlanması
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
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
Uygulama ve Veri Güvenliği	3.2.7.6	1	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	A.9.4.2 Güvenli oturum açma prosedürleri A.9.4.3 Parola yönetim sistemi
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 A.14.3.1 Test verisinin korunması
Uygulama ve Veri Güvenliği	3.2.7.8	1	Kullanıcıların Denetim Kayıtları Üzerinde Değişiklik Yapmasının Engellenmesi	A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıt kayıtları A.18.1.3 Kayıtların korunması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
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 A.14.2.2 Sistem değişiklik kontrolü prosedürleri A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi
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 A.10.1 Kriptografik kontroller A.18.1.5 Kriptografik kontrollerin düzenlenmesi
Uygulama ve Veri Güvenliği	3.2.7.11	1	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	A.6.2.2 Uzaktan çalışma A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
Uygulama ve Veri Güvenliği	3.2.7.12	1	Ayrıcalıkların Roller ve/veya Profiller Üzerinden Verilmesi	A.9.2 Kullanıcı erişim yönetimi A.9.4.1 Bilgiye erişimin kısıtlanması
Uygulama ve Veri Güvenliği	3.2.7.13	1	Veri Kurtarma Prosedürünün Hazırlanması	A.12.3.1 Bilgi yedekleme A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması
Uygulama ve Veri Güvenliği	3.2.7.14	1	Yedeklerin Güvenliğinin Sağlanması	A.9.2 Kullanıcı erişim yönetimi A.12.3 Yedekleme
Uygulama ve Veri Güvenliği	3.2.7.15	1	Varsayılan Yapılandırmaların Kullanılmaması	A.12.5 İşletimsel yazılımın kontrolü A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.7.16	2	Yetkili Kullanıcı İşlemlerinin Kaydedilmesi	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
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

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Uygulama ve Veri Güvenliği	3.2.7.18	3	Tüm Kullanıcı İşlemlerinin Kaydedilmesi	A.12.4 Kaydetme ve izleme
Uygulama ve Veri Güvenliği	3.2.7.19	3	Saklama Gereksinimi Sona Eren Kritik Verinin Güvenli Silinmesi	A.8.3.2 Ortamın yok edilmesi
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 A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.7.21	3	Veri Tabanına Gönderilen Sorguların Kontrol Edilmesi	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
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 A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika A.18.1.3 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 A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.8.2	1	Hataların ve Tanımlanan Olayların İz Kayıtlarının Oluşturulabilmesi	A.12.4 Kaydetme ve izleme
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 A.14.2.5 Güvenli sistem mühendisliği prensipleri A.18.1.3 Kayıtların korunması
Uygulama ve Veri Güvenliği	3.2.8.4	1	İz Kayıtlarında Olayların Zaman Bilgisinin Yer Alması	A.12.4.4 Saat senkronizasyonu

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Uygulama ve Veri Güvenliği	3.2.8.5	1	İz Kayıtlarının Güvenliğinin Sağlanması	A.12.4.2 Kayıt bilgisinin korunması A.18.1.3 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 A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.9.1	1	SSL/TLS Protokolünün Güvenli Kullanılması	A.10.1 Kriptografik kontroller A.12.5 İşletimsel yazılımın kontrolü
Uygulama ve Veri Güvenliği	3.2.9.2	1	Sertifika Denetimlerinin Yapılması	A.10.1 Kriptografik kontroller A.12.5 İşletimsel yazılımın kontrolü
Uygulama ve Veri Güvenliği	3.2.9.3	2	HSTS Kullanılması	A.14.2.1 Güvenli geliştirme politikası A.10.1 Kriptografik kontroller
Uygulama ve Veri Güvenliği	3.2.9.4	3	Hatalı Sertifikaların Tespiti	A.12.5 İşletimsel yazılımın kontrolü
Uygulama ve Veri Güvenliği	3.2.9.5	3	SSL/TLS Hata İz Kayıtları	A.12.4 Kaydetme ve izleme
Uygulama ve Veri Güvenliği	3.2.9.6	3	Kritik Verinin Şifrelenmesi	A.10.1 Kriptografik kontroller A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama
Uygulama ve Veri Güvenliği	3.2.9.7	3	Kurum Tarafından Onaylanmış Sertifikaların Kullanılması	A.10.1 Kriptografik kontroller
Uygulama ve Veri Güvenliği	3.2.10.1	1	Sunucu Tarafında Girdi Doğrulama Denetiminin Yapılması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.2	1	Girdi Doğrulama Hataları için İz Kaydının Oluşturulması	A.12.4 Kaydetme ve izleme

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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
Uygulama ve Veri Güvenliği	3.2.10.4	1	Kritik Bilgilerin Formlarda Bulunan Gizli Alanlarda Saklanmaması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.5	1	CSRF Saldırılarına Karşı Önlem Alınması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
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 A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.7	1	İşletim Sistemi Komut Enjeksiyonu Açıklarının Önlenmesi	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.8	1	Bellek Taşması Saldırılarının Önlenmesi	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.9	1	Dosya İçerme Açıklarının Önlenmesi	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.10	1	XML Tabanlı Saldırıların Önlenmesi	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Uygulama ve Veri Güvenliği	3.2.10.11	1	Yapısal Olmayan Veri için Karakterlerin Denetlenmesi	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.12	1	Girdi Denetimi Yapılması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.13	1	Yüklenen Dosyaların Denetlenmesi	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.14	2	İsteklerin Öngörülmeyen Büyüklükte Olup Olmadığının Kontrol Edilebilmesi	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
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
Uygulama ve Veri Güvenliği	3.2.10.16	3	Karakter Kodlamasının Tespiti	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.10.17	3	Uygulama Seviyesi Servis Dışı Bırakma Saldırılarının Engellenmesi	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.11.1	1	Web Servislerinin Güvenli Protokol Üzerinden Sunulması	A.10.1 Kriptografik kontroller

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
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 A.9.2.2 Kullanıcı erişimine izin verme A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
Uygulama ve Veri Güvenliği	3.2.11.3	1	Web Servis Çağrılarında Kimlik Doğrulama ve Yetkilendirme Kontrolü	A.9.4.1 Bilgiye erişimin kısıtlanması A.9.4.2 Güvenli oturum açma prosedürleri
Uygulama ve Veri Güvenliği	3.2.11.4	1	Sunulan Web Servislerin Girdi-Çıktı Denetimlerinin Yapılması	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.11.5	1	Web Servis Yapılandırma ve Yönetim İşlemleri	A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
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 A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.11.7	2	Uygulamanın Kararlılığının Sağlanması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.11.8	2	Web Servisi Çağrı Sayısının ve Kaynak Kullanımının Sınırlandırılması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği prensipleri
Uygulama ve Veri Güvenliği	3.2.11.9	3	Dış Sistemler / Uygulamalar Arası Çağrıların Kayıt Altına Alınması	A.12.4 Kaydetme ve izleme

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Uygulama ve Veri Güvenliği	3.2.11.10	3	Kritik Altyapı Sistemleri ile Güvenli İletişimin Sağlanması	A.10.1 Kriptografik kontroller A.14.2.5 Güvenli sistem mühendisliği prensipleri A.17.1 Bilgi güvenliği sürekliliği
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.1	1	Akıllı Telefon ve Tabletlerin Kabul Edilebilir Kullanımı	A.6.2.1 Mobil cihaz politikası A.6.2.2 Uzaktan çalışma A.8.1.3 Varlıkların kabul edilebilir kullanımı A.8.3.1 Taşınabilir ortam yönetimi
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 A.9.4.4 Ayrıcalıklı destek programlarının 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
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.4	1	Mobil Cihaz Envanterinin Tutulması	A.8.1.1 Varlıkların envanteri A.8.1.2 Varlıkların sahipliği
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.5	1	Halka Açık Şarj İstasyonlarının Kullanılmaması	A.6.2.1 Mobil cihaz politikası A.8.1.3 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
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.7	2	Tamire Verilen Cihazlarda Bulunan Verinin Silinmesi	A.6.2.1 Mobil cihaz politikası A.8.3.2 Ortamın yok edilmesi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.8	3	Güvenlik Yazılımlarının Yüklenmesi	A.6.2.1 Mobil cihaz politikası A.12.2.1 Kötücül yazılımlara karşı kontroller

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.10	3	Taşınabilir Cihazların Ayrı Sistemlerde Kullanılması	A.6.2.1 Mobil cihaz politikası A.6.2.2 Uzaktan çalışma A.8.1.3 Varlıkların kabul edilebilir kullanımı
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.11	3	Parola Politikaları	A.6.2.1 Mobil cihaz politikası A.9.4.3 Parola yönetim sistemi
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 A.9.4.2 Güvenli oturum açma prosedürleri
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.13	3	Desteklenen Cihaz Listesinin Oluşturulması	A.8.1.1 Varlıkların envanteri A.9.1 Erişim kontrolünün iş gereklilikleri A.12.2 Kötücül yazılımlardan koruma
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.14	3	Güncel Olmayan Cihazların Sistemlere Erişiminin Engellenmesi	A.6.2.1 Mobil cihaz politikası A.9.1 Erişim kontrolünün iş gereklilikleri
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.1.15	3	Seyahat Kullanım Politikasının Tanımlanması	A.6.2.1 Mobil cihaz politikası A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.2.1	1	Taşınabilir Bilgisayarların Kabul Edilebilir Kullanımı	A.6.2.1 Mobil cihaz politikası A.6.2.2 Uzaktan çalışma A.8.1.3 Varlıkların kabul edilebilir kullanımı A.8.3.1 Taşınabilir ortam yönetimi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.2.2	1	Güvenlik Yazılımlarının Yüklenmesi	A.12.2.1 Kötücül yazılımlara karşı kontroller

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.2.3	1	Tamire Verilen Taşınabilir Bilgisayarlarda Bulunan Verinin Silinmesi	A.6.2.1 Mobil cihaz politikası A.8.3.1 Taşınabilir ortam yönetimi A.8.3.2 Ortamın yok edilmesi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.2.4	2	Disk Şifreleme	A.8.3.1 Taşınabilir ortam yönetimi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.2.5	3	Harici Depolama Ortamlarına Erişimin Yönetimi	A.9.1 Erişim kontrolünün iş gereklilikleri A.6.2.1 Mobil cihaz politikası
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.2.6	3	Taşınabilir Bilgisayar Yönetimi	A.6.2.1 Mobil cihaz politikası A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.2.7	3	Güncel Olmayan Bilgisayarların Sistemlere Erişiminin Engellenmesi	A.6.2.1 Mobil cihaz politikası A.9.1 Erişim kontrolünün iş gereklilikleri
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.2.8	3	Seyahat Kullanım Politikasının Tanımlanması	A.6.2.1 Mobil cihaz politikası A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.3.1	1	Taşınabilir Ortamların Kabul Edilebilir Kullanımı	A.8.1.3 Varlıkların kabul edilebilir kullanımı A.8.3.1 Taşınabilir ortam yönetimi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.3.2	1	Taşınabilir Ortamların Saklama ve Kullanım Koşulları	A.8.1.3 Varlıkların kabul edilebilir kullanımı A.8.3.1 Taşınabilir ortam yönetimi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.3.3	2	Taşınabilir Ortamların Barındırdığı Verilerin Güvenliği	A.8.1.3 Varlıkların kabul edilebilir kullanımı A.8.3.1 Taşınabilir ortam yönetimi
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.3.4	2	Taşınabilir Ortamların Güvenli İmhası	A.8.3.2 Ortamın yok edilmesi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Taşınabilir Cihaz ve Ortam Güvenliği	3.3.3.5	2	Taşınabilir Ortam Bilgisinin Yedeklenmesi	A.8.3.1 Taşınabilir ortam yönetimi A.12.3.1 Bilgi yedekleme
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.1.1	1	Ağ Portlarının Kısıtlanması	A.9.1 Erişim kontrolünün iş gereklilikleri A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.1.2	1	Ağ Servislerinin Güvenlik Kontrolleri	A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği A.14.2.8 Sistem güvenlik testi A.18.2.3 Teknik uyum gözden geçirmesi
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.1.3	1	Güvenli Yapılandırma	A.12.1.1 Yazılı 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
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 A.13.1 Ağ güvenliği yönetimi
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.1.6	2	Cihaz Güvenlik Duvarının Aktifleştirilmesi	A.13.1.1 Ağ kontrolleri A.13.1.2 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 A.13.1 Ağ güvenliği yönetimi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.1.9	3	Ağ Üzerinden Gönderilen Verinin Şifrelenmesi	A.10.1 Kriptografik kontroller A.13.1.1 Ağ kontrolleri A.13.1.2 Ağ hizmetlerinin güvenliği
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.2.1	1	Veri Yedekleme	A.12.3 Yedekleme
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.2.2	1	Verilere Yetkili Erişim	A.9.2 Kullanıcı erişim yönetimi
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.2.3	3	Kullanılan Cihazlardan Kritik Verinin Temizlenmesi	A.8.3.2 Ortamın yok edilmesi A.11.2.7 Teçhizatın güvenli olarak yok edilmesi veya tekrar kullanımı
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.3.1	1	Oturum Sonlandırma İşlemlerinin Aktifleştirilmesi	A.14.2.5 Güvenli sistem mühendisliği esasları
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.3.2	1	Kimlik Doğrulama Politikası	A.9.4.1 Bilgiye erişimin kısıtlanması A.9.4.2 Güvenli oturum açma prosedürleri
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.3.3	1	Kullanıcı Yetki Sınırlaması	A.9.2 Kullanıcı erişim yönetimi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.3.5	1	Sıfırlama Mekanizmaları	A.9.2 Kullanıcı erişim yönetimi A.14.2.5 Güvenli sistem mühendisliği esasları
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
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.4.2	1	API ve Bağlantı Güvenliği	A.9.1 Erişim kontrolünün iş gereklilikleri
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.4.3	2	Web Uygulama Güvenlik Duvarı Kullanımı	A.13.1.1 Ağ kontrolleri
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
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.5.1	1	Güncellemelerin Kontrolü	A.12.5 İşletimsel yazılımın kontrolü
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.5.2	1	Cihazlara Fiziksel Erişimin Kısıtlanması	A.11.1.2 Fiziksel giriş kontrolleri A.11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması,

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.14.2.7 Dışardan sağlanan geliştirme A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.5.4	3	Elektromanyetik Sızıntılara Karşı Güvenlik Önlemlerinin Alınması	A.11.2.1 Teçhizat yerleştirme ve koruma
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.5.5	3	Tersine Mühendisliğe Karşı Koruma	A.14.2.5 Güvenli sistem mühendisliği esasları A.14.2.9 Sistem kabul testi
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.5.6	3	Güvenli Önyükleme	A.14.2.5 Güvenli sistem mühendisliği esasları
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	3.4.5.7	3	Güncellemelerin Güvenilir Kanallar Üzerinden Yapılması	A.12.5.1 İşletimdeki sistemler üzerine yazılım kurulumu A.12.6.2 Yazılım kurulumu kısıtlamaları
Personel Güvenliği	3.5.1.1	1	Güvenlik Soruşturmalarının Yapılması	A.7.1 İstihdam öncesi
Personel Güvenliği	3.5.1.2	1	Varlıkların Kabul Edilebilir Kullanım Kurallarının Tanımlanması	A.7.1.2 İstihdam hüküm ve koşulları A.8.1.3 Varlıkların kabul edilebilir kullanımı
Personel Güvenliği	3.5.1.3	1	Temiz Masa Temiz Ekran Politikasının Tanımlanması	A.11.2.9 Temiz masa temiz ekran politikası
Personel Güvenliği	3.5.1.4	1	Sözleşmelerde Bilgi Güvenliği Hususlarının Yer Alması	A.7.1.2 İstihdam hüküm ve koşulları

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Personel Güvenliği	3.5.1.5	1	Sosyal Medya Kullanım Politikasının Uygulanması	A.5.1.1 Bilgi güvenliği politikaları A.5.1.2 Bilgi güvenliği için politikaların gözden geçirilmesi A.7.1.2 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
Personel Güvenliği	3.5.1.7	1	Rol, Sorumluluk ve Asgari Yetkinliklerin Tanımlanması	A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları
Personel Güvenliği	3.5.1.8	1	İstihdam Sorumluluklarının Sonlandırılması veya Değiştirilmesi	A.7.3 İstihdamın sonlandırılması ve değiştirilmesi
Personel Güvenliği	3.5.1.9	1	Gizlilik ile İlgili Gereksinimlerin Personele Tebliğ Edilmesi	A.5.1.1 Bilgi güvenliği politikaları A.5.1.2 Bilgi güvenliği için politikaların gözden geçirilmesi A.7.1.2 İstihdam hüküm ve koşulları
Personel Güvenliği	3.5.2.1	1	Farkındalık Eğitimleri Verilmesi	A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi
Personel Güvenliği	3.5.2.2	1	Olayların Tespiti ve Raporlanmasına Yönelik Eğitimlerin Verilmesi	A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi
Personel Güvenliği	3.5.2.3	2	Yetenek İhtiyaç Analizi Yapılması	A.7.2.1 Yönetim sorumlulukları A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi
Personel Güvenliği	3.5.3.1	1	Tedarikçi İlişkilerinde Bilgi Güvenliği Politikasının Tanımlanması	A.5.1.1 Bilgi güvenliği politikaları A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Personel Güvenliği	3.5.3.2	1	Demo ve Kavram İspatı Çalışmalarında Gizlilik Taahhütnamesi	A.13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Personel Güvenliği	3.5.3.3	1	Tedarikçi Sözleşmelerinde Bilgi Güvenliğinin Ele Alınması	A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri
Personel Güvenliği	3.5.3.4	1	Tedarik Zinciri Güvenliği	A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri
Personel Güvenliği	3.5.3.5	1	Kabul Kriterlerinin Belirlenmesi	A.14.2.7 Dışardan sağlanan geliştirme A.14.2.9 Sistem kabul testi A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme
Personel Güvenliği	3.5.3.6	1	İletişim Metotlarının Belirlenmesi	A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme
Personel Güvenliği	3.5.3.7	1	Yüklenici Tarafından Tedarik Edilen Ürün/Hizmet Değişikliklerinin Yönetimi	A.15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme
Personel Güvenliği	3.5.3.8	1	Ana Yüklenici ve Alt Yüklenici Sorumluluklarının Netleştirilmesi	A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Personel Güvenliği	3.5.3.9	1	Tedarikçi Hizmetlerinin İzlenmesi	A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme
Personel Güvenliği	3.5.3.10	2	Tedarik Zinciri İzleme Sürecinin Oluşturulması	A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri A.15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme
Fiziksel Mekânların Güvenliği	3.6.1.1	1	Fiziksel Güvenlik Sınırı	A.11.1.1 Fiziksel güvenlik sınırı A.11.1.2 Fiziksel giriş kontrolleri
Fiziksel Mekânların Güvenliği	3.6.1.2	1	Güvenlik Biriminin Yeterliliği	A.11.1.1 Fiziksel güvenlik sınırı A.11.1.2 Fiziksel giriş kontrolleri A.18.2.1 Bilgi güvenliğinin bağımsız gözden geçirilmesi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Fiziksel Mekânların Güvenliği	3.6.1.3	1	Fiziksel Giriş ve Çıkış Kontrolleri	A.11.1.2 Fiziksel giriş kontrolleri
Fiziksel Mekânların Güvenliği	3.6.1.4	1	Dış Güvenlik Unsurlarının Kontrolü	A.11.1.4 Dış ve çevresel tehditlere karşı koruma
Fiziksel Mekânların Güvenliği	3.6.1.5	1	Ziyaretçi Giriş Çıkış Kontrolleri	A.11.1.2 Fiziksel giriş kontrolleri
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
Fiziksel Mekânların Güvenliği	3.6.1.7	1	Kablolama Güvenliği	A.11.2.3 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 A.11.2.2 Destekleyici altyapı hizmetleri
Fiziksel Mekânların Güvenliği	3.6.1.9	1	Kamera Sistemleri	A.9.2 Kullanıcı erişim yönetimi A.11.1 Güvenli alanlar A.11.2.1 Teçhizat yerleştirme ve koruma A.13.1.1 Ağ kontrolleri A.18.1.3 Kayıtların korunması
Fiziksel Mekânların Güvenliği	3.6.1.10	2	Çalışma Alanlarının Güvenliği	A.11.1 Güvenli alanlar
Fiziksel Mekânların Güvenliği	3.6.1.11	2	Destekleyici Altyapı Hizmetleri	A.11.2.2 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
Fiziksel Mekânların Güvenliği	3.6.1.13	3	Ziyaretçi Fiziksel Erişim Güvenliği	A.11.1.2 Fiziksel giriş kontrolleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Fiziksel Mekânların Güvenliği	3.6.1.14	3	Fiziksel Erişim Güvenliği	A. 11.1.2 Fiziksel giriş kontrolleri A.11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması A.11.1.5 Güvenli alanlarda çalışma
Fiziksel Mekânların Güvenliği	3.6.2.1	1	Sistem Odası/Veri Merkezi Güvenliği Politikası	A.5.1.1 Bilgi güvenliği politikaları A.11.1 Güvenli alanlar
Fiziksel Mekânların Güvenliği	3.6.2.2	1	Fiziksel Varlıkların Sistem Odası/Veri Merkezi Dışına Transferi	A.11.2.5 Varlıkların taşınması A.11.2.6 Teçhizat ve kuruluş dışındaki varlıkların güvenliği
Fiziksel Mekânların Güvenliği	3.6.2.3	1	Güvenli Alan Yetkilendirmesinin Yapılması	A.9.2 Kullanıcı erişim yönetimi A.11.1 Güvenli alanlar
Fiziksel Mekânların Güvenliği	3.6.2.4	1	Üçüncü Taraf Hizmetlerin Güvenliği	A.11.1.2 Fiziksel giriş kontrolleri
Fiziksel Mekânların Güvenliği	3.6.2.5	1	Ortam Koşullarının Kontrolü	A.11.1.4 Dış ve çevresel tehditlere karşı koruma A.11.2.2 Destekleyici altyapı hizmetleri A.13.1.1 Ağ kontrolleri
Fiziksel Mekânların Güvenliği	3.6.2.6	1	Kamera Sistemleri	A.9.2 Kullanıcı erişim yönetimi A.11.1 Güvenli alanlar A.11.2.1 Teçhizat yerleştirme ve koruma A.13.1.1 Ağ kontrolleri A.18.1.3 Kayıtların korunması
Fiziksel Mekânların Güvenliği	3.6.2.7	1	Destekleyici Altyapı Hizmetleri	A.11.2.2 Destekleyici altyapı hizmetleri A.11.2.4 Teçhizat bakımı
Fiziksel Mekânların Güvenliği	3.6.2.8	1	Dış ve Çevresel Tehditlere Karşı Koruma	A.11.1 Güvenli alanlar A.11.2.1 Teçhizat yerleştirme ve koruma A.11.2.2 Destekleyici altyapı hizmetleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Fiziksel Mekânların Güvenliği	3.6.2.9	1	Donanım Bakımı ve Güvenliği	A.11.2.1 Teçhizat yerleştirme ve koruma A.11.2.4 Teçhizat bakımı
Fiziksel Mekânların Güvenliği	3.6.2.10	1	Kablolama Güvenliği	A.11.2.3 Kablo güvenliği
Fiziksel Mekânların Güvenliği	3.6.2.11	1	Fiziksel Giriş Kontrolleri	A.11.1.2 Fiziksel giriş kontrolleri A.12.4 Kaydetme ve izleme
Fiziksel Mekânların Güvenliği	3.6.2.12	2	Ortam Koşullarının Gerçek Zamanlı İzlenmesi	A.11.1.4 Dış ve çevresel tehditlere karşı koruma A.11.2.2 Destekleyici altyapı hizmetleri
Fiziksel Mekânların Güvenliği	3.6.2.13	2	Siber Olay Tespitinde İz Kayıtlarının Kullanılması	A.12.4 Kaydetme ve izleme
Fiziksel Mekânların Güvenliği	3.6.2.14	3	Kontrollü Erişim Noktalarının Oluşturulması	A.11.1.2 Fiziksel giriş kontrolleri
Fiziksel Mekânların Güvenliği	3.6.2.15	3	İklimlendirme Kontrolü	A.11.2.2 Destekleyici altyapı hizmetleri A.11.2.4 Teçhizat bakımı
Fiziksel Mekânların Güvenliği	3.6.3.1	1	Sistem Odası/Veri Merkezi Cihaz Yerleşim Planı	A.8.1.1 Varlık envanteri
Fiziksel Mekânların Güvenliği	3.6.3.2	2	Gizlilik Seviyeli Bilgi İşleyen Cihazların TEMPEST Onayı	A.11.2.1 Teçhizat yerleştirme ve koruma A.8.1.1 Varlık envanteri
Fiziksel Mekânların Güvenliği	3.6.3.3	3	TEMPEST Tesisat Kurallarına Uyum	A.11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması A.11.2.1 Teçhizat yerleştirme ve koruma A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.1.2	1	Kişisel Veri Saklama ve İmha Politikasının Hazırlanması	A.5.1.1 Bilgi güvenliği politikaları A.18.1.4 Kişi tespit bilgisinin mahremiyeti 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 A.14.2.5 Güvenli sistem mühendisliği esasları A.14.2.6 Güvenli geliştirme ortamı
Kişisel Verilerin Güvenliği	4.1.1.4	1	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	A.9.1.1 Erişim kontrol politikası A.9.4.1 Bilgiye erişimin kısıtlanması A.13.2.1 Bilgi transfer politikaları ve prosedürleri
Kişisel Verilerin Güvenliği	4.1.1.5	1	Kişisel Verilerin Güvensiz Ortamlarda Saklanmaması	A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi A.18.1.3 Kayıtların korunması
Kişisel Verilerin Güvenliği	4.1.1.6	1	Kişisel Veri Üzerinde Girdi/Çıktı Denetimi Yapılması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği esasları A.14.2.8 Sistem güvenlik testi
Kişisel Verilerin Güvenliği	4.1.1.7	1	Kişisel Verinin Gizli Alanlarda Saklanmaması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği esasları A.14.2.8 Sistem güvenlik testi A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.1.8	1	Hata Mesajlarında Mahremiyetin Korunması	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği esasları A.14.2.8 Sistem güvenlik testi A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kişisel Verilerin Güvenliği	4.1.1.9	1	Özel Nitelikli Kişisel Verinin Saklanması	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika A.18.1.3 Kayıtların korunması A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması A.18.1.5 Kriptografik kontrollerin düzenlenmesi
Kişisel Verilerin Güvenliği	4.1.1.10	1	Geçici Olarak Tutulan Kişisel Verinin Yok Edilmesi	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği esasları A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.1.11	2	Veri Tabanı Tasarımı	A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi A.14.2.1 Güvenli geliştirme politikası
Kişisel Verilerin Güvenliği	4.1.2.1	1	Erişimlerin Kayıt Altına Alınması	A.9.4.2 Güvenli oturum açma prosedürleri A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.2.2	1	Erişim Kayıtlarının Arşivlenmesi	A.12.3.1 Bilgi yedekleme A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.2.3	1	Erişim Kayıtlarının Güvenliğinin Sağlanması	A.12.4.2 Kayıt bilgisinin korunması
Kişisel Verilerin Güvenliği	4.1.2.4	1	Erişim Kayıtlarının Aktarımı	A.13.2.1 Bilgi transfer politikaları ve prosedürleri
Kişisel Verilerin Güvenliği	4.1.2.5	2	Yetkisiz Erişimlerin Tespiti	A.9.4.1 Bilgiye erişimin kısıtlanması A.12.4.2 Kayıt bilgisinin korunması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kişisel Verilerin Güvenliği	4.1.2.6	3	Erişim Kayıtlarında Özel Nitelikli Kişisel Veri Bulundurulmaması	A.12.4.1 Olay kaydetme A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.3.1	1	Yetkilendirme Mekanizmasının Kullanılması	A.9.2 Kullanıcı erişim yönetimi A.9.4.1 Bilgiye erişimin kısıtlanması A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.3.2	1	Kimlik Doğrulama Mekanizmasının Kullanılması	A.9.1 Erişim kontrolünün iş gereklilikleri A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.3.3	1	Erişimin Sınırlandırılması	A.9.1.1 Erişim kontrol politikası A.9.4.1 Bilgiye erişimin kısıtlanması A.9.4.2 Güvenli oturum açma prosedürleri
Kişisel Verilerin Güvenliği	4.1.3.4	1	Erişim Denetim Politikalarının Oluşturulması	A.5.1.1 Bilgi güvenliği politikaları A.9.1.1 Erişim kontrol politikası
Kişisel Verilerin Güvenliği	4.1.3.5	2	Çok Faktörlü Kimlik Doğrulama Mekanizmasının Kullanılması	A.9.4.2 Güvenli oturum açma prosedürleri
Kişisel Verilerin Güvenliği	4.1.3.6	2	Dış Sistemler / Uygulamalar Arası Veri Akışı için Erişimlerin Doğrulanması	A.9.4.1 Bilgiye erişimin kısıtlanması A.12.4.1 Olay kaydetme A.13.2.1 Bilgi transfer politikaları ve prosedürleri
Kişisel Verilerin Güvenliği	4.1.3.7	3	Alt Bileşenler Arasında Veri Akışı için Erişimlerin Doğrulanması	A.9.4.1 Bilgiye erişimin kısıtlanması A.13.2.1 Bilgi transfer politikaları ve prosedürleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kişisel Verilerin Güvenliği	4.1.4.1	1	İletişimin Şifrelenmesi	A.10.1 Kriptografik kontroller A.13.1 Ağ güvenliği yönetimi A.13.2.1 Bilgi transfer politikaları ve prosedürleri
Kişisel Verilerin Güvenliği	4.1.4.2	2	Verinin Maskelenmesi	A.18.1.3 Kayıtların korunması A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.4.3	2	Verinin Bütünlüğünün Korunması	A.9.2 Kullanıcı erişim yönetimi A.10.1 Kriptografik kontroller
Kişisel Verilerin Güvenliği	4.1.4.4	3	Sistemin Alt Bileşenleri Arasındaki İletişimin Şifreli Yapılması	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika A.13.1.2 Ağ hizmetlerinin güvenliği A.13.2.1 Bilgi transfer politikaları ve prosedürleri A.14.1.3 Uygulama hizmet işlemlerinin korunması
Kişisel Verilerin Güvenliği	4.1.5.1	1	Sistem Yedeklerinin Yetkili Kullanıcılar Tarafından Alınması	A.9.1.1 Erişim kontrol politikası A.9.4.1 Bilgiye erişimin kısıtlanması A.12.3.1 Bilgi Yedekleme A.12.4.1 Olay Kaydetme
Kişisel Verilerin Güvenliği	4.1.5.2	1	Kişisel Verilerin Silinmesi	A.8.3.2 Ortamın yok edilmesi A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı
Kişisel Verilerin Güvenliği	4.1.5.3	1	Kişisel Verilerin Yok Edilmesi	A.8.3.2 Ortamın yok edilmesi A.5.1.1 Bilgi güvenliği politikaları A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.5.4	1	Kişisel Verilerin Anonim Hale Getirilmesi	A.5.1.1 Bilgi güvenliği politikaları A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kişisel Verilerin Güvenliği	4.1.5.5	1	Kişisel Veri Barındıran Yedeklerin Güvenliğinin Sağlanması	A.12.3.1 Bilgi Yedekleme A.12.4.1 Olay Kaydetme
Kişisel Verilerin Güvenliği	4.1.5.6	2	Kişisel Veri Barındıran Yedeklerin Yok Edilmesi	A.8.3.2 Ortamın yok edilmesi A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı
Kişisel Verilerin Güvenliği	4.1.6.1	1	Aydınlatmanın Doğru Zamanda Yapılması	A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.6.2	1	Aydınlatmanın Yerine Getirildiğinin İspat Edilmesi	A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama A.18.1.4 Kişi tespit bilgisinin mahremiyeti 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 A.12.4.1 Olay Kaydetme
Kişisel Verilerin Güvenliği	4.1.7.1	1	Açık Rıza Unsurlarının Belirlenmesi	A.18.1 Yasal ve sözleşmeye tabi gereksinimlere uyum A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması
Kişisel Verilerin Güvenliği	4.1.7.2	1	Açık Rızanın Kayıt Altına Alınması	A.12.4.1 Olay Kaydetme A.18.1.3 Kayıtların korunması
Kişisel Verilerin Güvenliği	4.1.7.3	1	Açık Rıza Durumunun Sorgulanması	A.9.4.1 Bilgiye erişimin kısıtlanması A.12.4.1 Olay Kaydetme
Kişisel Verilerin Güvenliği	4.1.7.4	3	Uygulama Üzerinden Açık Rıza Alınması	A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi
Kişisel Verilerin Güvenliği	4.1.7.5	3	Açık Rıza Metninin Güncellenmesi	A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama A.18.1.3 Kayıtların korunması

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
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
Kişisel Verilerin Güvenliği	4.1.7.7	3	Islak İmzalı Açık Rıza Metninin Saklanması	A.18.1.3 Kayıtların korunması
Kişisel Verilerin Güvenliği	4.1.8.1	1	İlgili Kişinin Başvuru Hakkının Yönetilmesi	A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama
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
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
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 A.18.1.3 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
Anlık Mesajlaşma Güvenliği	4.2.1.1	1	Mesajlaşma Uygulaması Seçimi	A.13.2.3 Elektronik mesajlaşma
Anlık Mesajlaşma Güvenliği	4.2.1.2	1	İletim Ortamı Güvenliği	A.10.1 Kriptografik kontroller
Anlık Mesajlaşma Güvenliği	4.2.1.3	1	Gizlilik Dereceli Veri Paylaşımı	A.13.2.1 Bilgi transfer politikaları ve prosedürleri
Anlık Mesajlaşma Güvenliği	4.2.1.4	1	Çoklu Cihaz Kullanımı	A.9.4.1 Bilgiye erişimin kısıtlanması A.9.4.2 Güvenli oturum açma prosedürleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.14.1.3 Uygulama hizmet işlemlerinin korunması
Anlık Mesajlaşma Güvenliği	4.2.1.6	2	Şifreleme Anahtarlarının Saklanması	A.10.1.2 Anahtar yönetimi A.18.1.3 Kayıtların korunması
Anlık Mesajlaşma Güvenliği	4.2.1.7	2	Yönetim Arayüzüne Erişim	A.9.4.1 Bilgiye erişimin kısıtlanması A.12.4.1 Olay Kaydetme
Anlık Mesajlaşma Güvenliği	4.2.1.8	3	Cihaz Üzerindeki Verinin Şifrelenmesi	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika A.18.1.3 Kayıtların korunması
Anlık Mesajlaşma Güvenliği	4.2.1.9	3	Kritik Haberleşmenin Güvenliği	A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama
Bulut Bilişim Güvenliği	4.3.1.1	1	Bulut Hizmeti Kullanımı	A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği A.15.2 Tedarikçi hizmet sağlama yönetimi A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama
Bulut Bilişim Güvenliği	4.3.1.2	1	Hizmet Kapsamı ile Rol ve Sorumlulukların Belirlenmesi	A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Bulut Bilişim Güvenliği	4.3.1.3	1	Veri İletimi Güvenliği	A.14.1.3 Uygulama hizmet işlemlerinin korunması A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Bulut Bilişim Güvenliği	4.3.1.4	1	Kaynakların İzole Edilmesi	A.9.1 Erişim kontrolünün iş gereklilikleri A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Bulut Bilişim Güvenliği	4.3.1.5	1	İmajların İmha Edilmesi	A.8.3.2 Ortamın yok edilmesi A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Bulut Bilişim Güvenliği	4.3.1.6	1	Sanal Makineye Ait Belleklerin İmhası	A.8.3.2 Ortamın yok edilmesi A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Bulut Bilişim Güvenliği	4.3.1.7	1	Bulut Ortamı Güvenliği	A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği A.15.2 Tedarikçi hizmet sağlama yönetimi
Bulut Bilişim Güvenliği	4.3.1.8	1	Sanal Makineye Ait Disk Bölgelerinin İmhası	A.8.3.2 Ortamın yok edilmesi A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Bulut Bilişim Güvenliği	4.3.1.9	1	İş Sürekliliğinin Sağlanması	A.12.3 Yedekleme A.15.2 Tedarikçi hizmet sağlama yönetimi A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları
Bulut Bilişim Güvenliği	4.3.1.10	1	Erişim Yetkilerinin Yönetiminin Sağlanması	A.9.2 Kullanıcı erişim yönetimi A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Bulut Bilişim Güvenliği	4.3.1.11	1	Hizmetin Sonlandırılması Hususları	A.8.3.2 Ortamın yok edilmesi A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Bulut Bilişim Güvenliği	4.3.1.12	2	Güvenli Veri Depolama Politikasının Uygulanması	A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği
Bulut Bilişim Güvenliği	4.3.1.13	2	Bulut Ortamı İşlem Kayıtlarının Tutulması	A.12.4.1 Olay Kaydetme A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği A.18.1.3 Kayıtların korunması
Bulut Bilişim Güvenliği	4.3.1.14	3	Kaynakların Fiziksel Olarak İzole Edilmesi	A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği A.15.2 Tedarikçi hizmet sağlama yönetimi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kripto Uygulamaları Güvenliği	4.4.1.1	1	Kriptografik Algoritma Tipinin Seçilmesi	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.1.2	1	Kripto Uygulama, Cihaz ve Sistemlerin Kriptografik Algoritma Güvenliği	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.1.3	1	Standart Kriptografik Algoritmaları İçeren Kripto Modüllerinin Güvenliği	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.1.4	3	Milli Kriptografik Algoritmaların Gerçeklendiği Kripto Cihazlarının Tedariki	A.10.1 Kriptografik kontroller A.18.1.5 Kriptografik kontrollerin düzenlenmesi
Kripto Uygulamaları Güvenliği	4.4.2.1	1	Kriptografik Anahtara İlişkin Güvenlik Gereksinimleri Analizi	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.2	1	Kriptografik Anahtarların Üretilmesi	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.3	1	Anahtar Üretim ve Dağıtım Cihazlarına Erişim	A.9.2 Kullanıcı erişim yönetimi A.10.1 Kriptografik kontroller A.11.1.2 Fiziksel giriş kontrolleri A.12.4 Kaydetme ve izleme
Kripto Uygulamaları Güvenliği	4.4.2.4	1	Güvenli Yedekleme	A.10.1 Kriptografik kontroller A.11.1.2 Fiziksel giriş kontrolleri A.12.4 Kaydetme ve izleme
Kripto Uygulamaları Güvenliği	4.4.2.5	1	Kriptografik Anahtarlara Erişim Kontrolü	A.9.2 Kullanıcı erişim yönetimi A.10.1 Kriptografik kontroller A.12.4 Kaydetme ve izleme
Kripto Uygulamaları Güvenliği	4.4.2.6	1	Kriptografik Anahtarların Revize Edilmesi	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.7	1	Güvenli Anahtar Ulaştırma / İletimi	A.10.1 Kriptografik kontroller

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.10.1 Kriptografik kontroller A.12.4 Kaydetme ve izleme
Kripto Uygulamaları Güvenliği	4.4.2.9	1	Anahtar Üretim Ortamlarına Güvenli Erişim	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.10	1	İz Kayıtlarının Oluşturulması	A.12.4 Kaydetme ve izleme A.16.1.7 Kanıt toplama
Kripto Uygulamaları Güvenliği	4.4.2.11	1	Kriptografik Anahtarların İptal Edilmesi/Güvenli Yok Edilmesi	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.12	1	Kriptografik Anahtar Sorumlusu Zimmet Tutanağının Hazırlanması	A.8.1.2 Varlıkların sahipliği A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.13	1	Kriptografik Anahtar Yetkilendirme	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.14	1	Anahtarların Üretim Yerinden Sonra Kopyalanamaması ve Çoğaltılamaması	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.15	1	Anahtarlara Açık Metin Olarak Erişilmemesi	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.16	1	İhlal Raporlama	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.17	1	Yedek Anahtar	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.18	1	Anahtar Üretim ve Yönetim Sistemi Testi	A.10.1 Kriptografik kontroller A.18.1.5 Kriptografik kontrollerin düzenlenmesi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kripto Uygulamaları Güvenliği	4.4.2.19	2	Güvenli Anahtar Saklama	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.20	3	Anahtar Taşıma Cihazlarında Yapılan Tüm Anahtar İşlemlerinin Kaydının Tutulması	A.10.1 Kriptografik kontroller A.12.4 Kaydetme ve izleme
Kripto Uygulamaları Güvenliği	4.4.2.21	3	Anahtar Taşıma Cihazlarında Bulunan Anahtarın Onaylı Kriptografik Yöntemlerle Şifreli Olarak Tutulması	A.10.1 Kriptografik kontroller
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
Kripto Uygulamaları Güvenliği	4.4.2.23	3	Kripto Güvenlik Belgesi Kontrolü	A.9.2 Kullanıcı erişim yönetimi A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.24	3	Anahtar Kimliği	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.25	3	Anahtar Sayımı	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.2.26	3	Anahtar Üretim ve Yönetim Sistemi Testi	A.10.1 Kriptografik kontroller A.18.1.5 Kriptografik kontrollerin düzenlenmesi
Kripto Uygulamaları Güvenliği	4.4.3.1	1	Güvensiz Ağlar Üzerinden Güvenli Haberleşme	A.9.1 Erişim kontrolünün iş gereklilikleri A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.3.2	1	Envanter Yönetimi	A.8.1.1 Varlık envanteri A.9.2 Kullanıcı erişim yönetimi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kripto Uygulamaları Güvenliği	4.4.3.3	1	Güvenlik Değerlendirme ve Onay Durumu Yönetimi	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.3.4	2	Kripto Protokollerinin En Güncel ve Güvenilir Versiyonlarının Kullanımı	A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.3.5	2	Envanter Yönetim Araçları ile Kriptografik Ürünlerin Yönetimi ve İzlenmesi	A.9.2 Kullanıcı erişim yönetimi A.10.1 Kriptografik kontroller
Kripto Uygulamaları Güvenliği	4.4.3.6	3	Kripto Cihazları TEMPEST Laboratuvar Onayı	A.10.1 Kriptografik kontroller A.12.6.1 Teknik açıklıkların yönetimi
Kripto Uygulamaları Güvenliği	4.4.3.7	3	Kripto Cihazları Kripto Analiz Laboratuvar Onayı	A.10.1 Kriptografik kontroller A.18.1.5 Kriptografik kontrollerin düzenlenmesi
Kripto Uygulamaları Güvenliği	4.4.3.8	3	Kripto Cihazları COMSEC Laboratuvar Onayı	A.10.1 Kriptografik kontroller A.18.1.5 Kriptografik kontrollerin düzenlenmesi
Kritik Altyapılar Güvenliği	4.5.1	-	Aşağıda listelenen rehber ana başlıklarında yer alan tedbirler uygulanır: • Ağ ve Sistem Güvenliği • Uygulama ve Veri Güvenliği • Taşınabilir Cihaz ve Ortam Güvenliği • Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği • Personel Güvenliği • Fiziksel Mekânların Güvenliği	-

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kritik Altyapılar Güvenliği	4.5.2.1	1	Cihaz Konfigürasyonları	A.14.2.5 Güvenli sistem mühendisliği esasları
Kritik Altyapılar Güvenliği	4.5.2.2	1	Ağ Erişim Kontrolü	A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.9.2 Kullanıcı erişim yönetimi
Kritik Altyapılar Güvenliği	4.5.2.3	1	Ağ Segmentasyonu	A.13.1.3 Ağlarda ayrım
Kritik Altyapılar Güvenliği	4.5.2.4	1	Kimlik Doğrulama	A.9.1 Erişim kontrolünün iş gereklilikleri A.9.2 Kullanıcı erişim yönetimi
Kritik Altyapılar Güvenliği	4.5.2.5	1	Erişim Yönetimi	A.6.2.2 Uzaktan çalışma A.13.1.1 Ağ kontrolleri
Kritik Altyapılar Güvenliği	4.5.2.6	1	Fiziksel Erişim Güvenliği	A.11 Fiziksel ve çevresel güvenlik
Kritik Altyapılar Güvenliği	4.5.2.7	1	Sistem Sürekliliğinin Sağlanması	A.17.2 Yedek fazlalıklar
Kritik Altyapılar Güvenliği	4.5.2.8	1	Veri Manipülasyonunun Engellenmesi	A.14.1.3 Uygulama hizmet işlemlerinin korunması
Kritik Altyapılar Güvenliği	4.5.2.9	1	Kullanıcı Erişim Yönetimi	A.6.2.2 Uzaktan çalışma A.9.2 Kullanıcı erişim yönetimi
Kritik Altyapılar Güvenliği	4.5.2.10	1	SSL/TLS Korumalı İletişim	A.13.1.2 Ağ hizmetlerinin güvenliği A.14.1.3 Uygulama hizmet işlemlerinin korunması
Kritik Altyapılar Güvenliği	4.5.2.11	1	GPS İletişim ve Senkronizasyonunun Güvenliği	-
Kritik Altyapılar Güvenliği	4.5.2.12	1	Ekipman Güvenliğinin Sağlanması	A.13.1.2 Ağ hizmetlerinin güvenliği

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kritik Altyapılar Güvenliği	4.5.2.13	1	Tehdit İstihbaratı Yönetimi	A.6.1.4 Özel ilgi grupları ile iletişim
Kritik Altyapılar Güvenliği	4.5.2.14	1	Otoritelerle İletişim	A.6.1.3 Otoritelerle iletişim
Kritik Altyapılar Güvenliği	4.5.2.15	2	Veri İletimi	A.13.2.1 Bilgi transfer politikaları ve prosedürleri A.13.2.2 Bilgi transferindeki anlaşmalar
Kritik Altyapılar Güvenliği	4.5.3.1	1	Hizmet Güvenliği ve Sürekliliği	A.17.1 Bilgi güvenliği sürekliliği
Kritik Altyapılar Güvenliği	4.5.3.2	1	Üçüncü Taraflara İlişkin Güvenlik Gereksinimleri	A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme
Kritik Altyapılar Güvenliği	4.5.3.3	1	Altyapı Servislerinin Güvenliği	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2 Geliştirme ve destek süreçlerinde güvenlik
Kritik Altyapılar Güvenliği	4.5.3.4	1	Sahtecilik İşlemlerini Tespit ve Önleme	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.18.1.3 Kayıtların korunması
Kritik Altyapılar Güvenliği	4.5.3.5	1	Sinyalleşme Trafiğinin Güvenliği	A.13.1 Ağ güvenliği yönetimi
Kritik Altyapılar Güvenliği	4.5.3.6	1	Güvenilir İletişimin Tesisi	A.13.1 Ağ güvenliği yönetimi
Kritik Altyapılar Güvenliği	4.5.3.7	1	Sıkılaştırma Faaliyetleri	A.12.1 İşletim prosedürleri ve sorumlulukları
Kritik Altyapılar Güvenliği	4.5.3.8	1	Ekipman Arızalarının İzlenmesi	A.11.2.1 Teçhizat yerleştirme ve koruma A.11.2.2 Destekleyici altyapı hizmetleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Kritik Altyapılar Güvenliği	4.5.3.9	1	Ekipman Güvenliğinin Sağlanması	A.11.1 Güvenli alanlar A.11.2 Teçhizat
Kritik Altyapılar Güvenliği	4.5.3.10	1	Tehdit İstihbaratı Yönetimi	A.6.1.4 Özel ilgi grupları ile iletişim
Kritik Altyapılar Güvenliği	4.5.3.11	1	Otoritelerle İletişim	A.6.1.3 Otoritelerle iletişim
Kritik Altyapılar Güvenliği	4.5.3.12	1	Arayan Hat Bilgisi Kullanımı	A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama
Kritik Altyapılar Güvenliği	4.5.3.13	1	İnternet Değişim Noktası	A.13.1 Ağ güvenliği yönetimi
Kritik Altyapılar Güvenliği	4.5.3.14	3	Kritik Haberleşme Güvenliği	A.13.1 Ağ güvenliği yönetimi A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama A.18.1.5 Kriptografik kontrollerin düzenlenmesi
Yeni Geliştirmeler ve Tedarik	4.6.1.1	1	Politika ve Prosedürlerin Tanımlanması	A.8.1.1 Varlık envanteri A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği A.15.2 Tedarikçi hizmet sağlama yönetimi
Yeni Geliştirmeler ve Tedarik	4.6.1.2	1	Yazılım Varlık Envanterine Kayıt Edilmemiş Yazılımların Yönetimi	A.8.2.3 Varlıkların kullanımı
Yeni Geliştirmeler ve Tedarik	4.6.1.3	1	Donanım Varlık Envanterine Kayıt Edilmemiş Donanımların Yönetimi	A.8.2.3 Varlıkların 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

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Yeni Geliştirmeler ve Tedarik	4.6.1.5	2	Alt Yüklenici Yönetimi	A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği A.15.2 Tedarikçi hizmet sağlama yönetimi
Yeni Geliştirmeler ve Tedarik	4.6.1.6	2	Fonksiyonel ve Fonksiyonel Olmayan Testlerin Yapılması	A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri A.14.2 Geliştirme ve destek süreçlerinde güvenlik
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.1	1	Kurulum Güvenliği	A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.2	1	Servis Güvenliği	A.9.1 Erişim kontrolünün iş gereklilikleri A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.3	1	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.4	1	Şifreli Haberleşen Servislerin Kullanılması	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.5	1	Parola Politikasının Belirlenmesi	A.9.4.3 Parola yönetim sistemi
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.6	1	Son Kullanıcı Bilgisayarlarında Ağ Erişiminin Kısıtlanması	A.9.1 Erişim kontrolünün iş gereklilikleri
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 A.12.5 İşletimsel yazılımın kontrolü

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.13.1.2 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 A.13.1.2 Ağ hizmetlerinin güvenliği
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.10	1	Yerel Güvenlik Duvarı Ayarlarının Yapılması	13.1.2 Ağ hizmetlerinin güvenliği
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.11	1	Sunucularda Zaman Senkronizasyonunun Sağlanması	A.12.4.4 Saat senkronizasyonu
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.12	1	Güvenli Süreç (Process) İşleme Ayarlarının Yapılması	A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.13	2	Kullanılmayan Uygulamaların Kaldırılması	A.12.1.3 Kapasite yönetimi A.13.1.1 Ağ kontrolleri
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.14	2	Merkezi Güncelleme Sunucusu	A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.15	2	IPv6 Pasif Hale Getirilmesi	A.9.1.2 Ağlara ve ağ hizmetlerine erişim
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.16	2	Sistem İz Kayıtlarının Aktif Edilmesi	A.12.4.1 Olay kaydetme A.12.4.3 Yönetici ve operatör kayıtları
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.17	2	Sistem İz Kayıtlarının Merkezi Bir Sunucuda Toplanması	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.18	2	Merkezi Kimlik Yönetimi Servisinin Kullanılması	A.9.2.2 Kullanıcı erişimine izin verme
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.19	3	Sunucularda Çalışan Servislerin Takibi	A.12.4.1 Olay kaydetme
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.20	3	Bilgisayar Tabanlı Saldırı Tespit ve Engelleme Sistemlerinin Kullanılması	A.12.4.1 Olay kaydetme A.12.6.1 Teknik açıklıkların yönetimi
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.21	3	Disk Kotalarının Belirlenmesi	-
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.1.22	3	Disk Seviyesinde Şifreleme Yapılması	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.2.1	1	Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi	-
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.2.2	1	Yetkili Kullanıcı Hesap Yönetimi	A.9.2 Kullanıcı erişim yönetimi A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.2.3	2	Dosya Sistemi Güvenli Erişim Düzenlemeleri	A.9.4.1 Bilgiye erişimin kısıtlanması A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.2.4	2	Güvenli Disk Bölümlendirme	-
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.2.5	2	Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi	-

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.2.6	2	Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması	A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.2.7	2	Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması	A.9.4.2 Güvenli oturum açma prosedürleri
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.2.8	3	Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi	A.9.4 Sistem ve uygulama erişim kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.1	1	Kullanıcı Haklarının Kısıtlanması	A.9.1 Erişim kontrolünün iş gereklilikleri A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.2	1	Otomatik Güncellemenin Aktif Olması	A.12.5 İşletimsel yazılımın kontrolü
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.3	1	SMB Protokolü Güvenliği	A.9.1 Erişim kontrolünün iş gereklilikleri
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.4	1	Yerel Yönetici Hesapları Yönetimi	A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.5	1	Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.6	1	Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.7	2	Kullanılmayan Hesapların Devre Dışı Bırakılması	A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.8	2	Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	A.9.2 Kullanıcı erişim yönetimi
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.9	2	Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	A.9.2 Kullanıcı erişim yönetimi
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.10	2	Aktif Dizin Sorguları Güvenliği	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.11	2	Yönetici Hesaplarının İzlenmesi	A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi A.12.4.1 Olay kaydetme A.12.4.3 Yönetici ve operatör kayıtları
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.12	2	Güvenli Yönetici İş İstasyonu Kullanımı	-
İşletim Sistemi Sıkılaştırma Tedbirleri	5.1.3.13	2	Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	A.9.1 Erişim kontrolünün iş gereklilikleri A.9.2 Kullanıcı erişim yönetimi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.1	1	Güncelleme ve Yama Yönetimi	A.12.5 İşletimsel yazılımın kontrolü A.12.6 Teknik açıklık yönetimi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.2	1	Veri Tabanı Parametrelerinin Güvenli Yapılandırılması	A.12.5 İşletimsel yazılımın kontrolü A.14.2.5 Güvenli sistem mühendisliği prensipleri

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.3	1	Varsayılan Hesap ve Parolaların Kullanılmaması	A.5.1.1 Bilgi güvenliği politikaları A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.4	1	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	A.9.4.3 Parola yönetim sistemi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.5	1	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	A.6.2.2 Uzaktan çalışma A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1 Ağ güvenliği yönetimi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.6	1	Kullanılmayan Hesapların Kapatılması	A.9.2 Kullanıcı erişim yönetimi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.7	1	Anonim Hesapların Bulunmaması	A.9.2 Kullanıcı erişim yönetimi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.8	1	Veri Tabanı Rol ve Yetkilerinin Kısıtlanması	A.9.1 Erişim kontrolünün iş gereklilikleri A.9.2 Kullanıcı erişim yönetimi
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 A.9.2 Kullanıcı erişim yönetimi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.10	1	Komut/Sorgu Geçmişi Kayıtlarının Güvenliğinin Sağlanması	A.18.1.3 Kayıtların korunması
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.11	1	Yedeklerin Güvenliğinin Sağlanması	A.9.2 Kullanıcı erişim yönetimi A.12.3 Yedekleme
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.12	1	Adanmış Sunucu Kullanılması	A.12.5 İşletimsel yazılımın kontrolü

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.13	1	Kurulum Dosyalarının Güvenilir Kaynaklardan Temin Edilmesi	A.12.5 İşletimsel yazılımın kontrolü
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.14	1	Örnek Verilerin Silinmesi	A.12.5 İşletimsel yazılımın kontrolü
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
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.16	2	Veri Tabanında Tablo ve Nesne Düzeyinde Yetkilendirme Yapılması	A.9.1 Erişim kontrolünün iş gereklilikleri
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
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 A.13.1 Ağ güvenliği yönetimi
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.19	2	Merkezi Kimlik Doğrulama Sisteminin Kullanılması	A.9.2.2 Kullanıcı erişimine izin verme
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 A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Veri Tabanı Sıkılaştırma Tedbirleri	5.2.1.21	3	Veri Tabanı Sunucusu ile İstemci Arasındaki İletişimin Şifreli Olması	A.13.1 Ağ güvenliği yönetimi
Sunucu Sıkılaştırma Tedbirleri	5.3.1.1	1	Güncel Web Sunucu Yazılımlarının Kullanılması	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.2	1	WebDAV Desteğinin Kaldırılması	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.3	1	Web Sunucusu Kullanıcı Yönetimi	A.9.2 Kullanıcı erişim yönetimi A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.4	1	Web Sunucusunun Bilgi İfşalarını Önleyecek Şekilde Yapılandırılması	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.5	1	Desteklenen HTTP Metotlarının Kısıtlanması	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.6	1	Dizin Listelemenin Pasif Hale Getirilmesi	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.7	1	Debug Modunun Kapalı Olması	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.8	1	İstek Limitlerinin Tanımlanması	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.9	1	İz Kayıtlarının Alınması	A.12.4.1 Olay kaydetme A.12.4.3 Yönetici ve operatör kayıtları
Sunucu Sıkılaştırma Tedbirleri	5.3.1.10	1	Yazma İzni Olan Dizinlerin Kısıtlanması	A.9.2 Kullanıcı erişim yönetimi A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.11	1	SSL/TLS Kullanımı	A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
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 A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.13	1	Kullanılmayan Modüllerin Kaldırılması	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.14	1	Açık Portların Kısıtlanması	A.9.1 Erişim kontrolünün iş gereklilikleri A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.1.15	1	Kaynak Kullanım Optimizasyonu	A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması A.14.2.5 Güvenli sistem mühendisliği esasları
Sunucu Sıkılaştırma Tedbirleri	5.3.1.16	1	Sunucunun Korumalı ve Ayrıştırılmış Şekilde Kurulumu	A.9.1.2 Ağlara ve ağ hizmetlerine erişim A.13.1.3 Ağlarda ayrım
Sunucu Sıkılaştırma Tedbirleri	5.3.1.17	1	Sunucuda Koruyucu HTTP Başlıklarının Kullanımı	A.14.2.5 Güvenli sistem mühendisliği esasları
Sunucu Sıkılaştırma Tedbirleri	5.3.1.18	1	Sunucunun Özel Anahtarının (Private Key) Korunması	A.10.1 Kriptografik kontroller
Sunucu Sıkılaştırma Tedbirleri	5.3.1.19	2	İz Kayıtlarının Merkezi Kayıt Sistemine Gönderilmesi	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
Sunucu Sıkılaştırma Tedbirleri	5.3.1.20	2	Sunucuya IP Adresi Üzerinden Erişimlerin Engellenmesi	A.9.1 Erişim kontrolünün iş gereklilikleri
Sunucu Sıkılaştırma Tedbirleri	5.3.2.1	1	Güncel Sanallaştırma Yazılımının Kullanılması	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.2.2	1	Konteynerların /Sanal Makinelerin Çalıştığı Ana Makine Üzerinde Sıkılaştırmaların Yapılması	A.12.5 İşletimsel yazılımın kontrolü

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Sunucu Sıkılaştırma Tedbirleri	5.3.2.3	1	Sanal Makineler Arasında Zaman Senkronizasyonunun Sağlanması	A.12.4.4 Saat senkronizasyonu
Sunucu Sıkılaştırma Tedbirleri	5.3.2.4	1	Sanallaştırma Yazılımı Güvenlik Duvarının Aktif Olması	A.13.1.2 Ağ hizmetlerinin güvenliği
Sunucu Sıkılaştırma Tedbirleri	5.3.2.5	1	Mantıksal Birim Numarası (LUN) Maskelemesi Yapılması	A.14.2.1 Güvenli geliştirme politikası
Sunucu Sıkılaştırma Tedbirleri	5.3.2.6	1	Sanallaştırma Ünitesi Üzerinden Konsol Erişimlerinin Kısıtlanması	A.9.1 Erişim kontrolünün iş gereklilikleri A.9.2 Kullanıcı erişim yönetimi
Sunucu Sıkılaştırma Tedbirleri	5.3.2.7	1	Sanallaştırma Ünitesinde Kullanıcı Yetkilendirme	A.9.1 Erişim kontrolünün iş gereklilikleri A.9.2 Kullanıcı erişim yönetimi
Sunucu Sıkılaştırma Tedbirleri	5.3.2.8	1	Gereksiz Hizmetlerin ve Kullanılmayan Donanımların Kaldırılması	A.12.1.3 Kapasite yönetimi A.13.1.1 Ağ kontrolleri
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 A.9.2 Kullanıcı erişim yönetimi
Sunucu Sıkılaştırma Tedbirleri	5.3.2.10	2	Sanallaştırma Yazılımının Merkezi Olarak Güncellenmesi	A.12.5 İşletimsel yazılımın kontrolü
Sunucu Sıkılaştırma Tedbirleri	5.3.2.11	2	Sanal Makineler için İz Kayıtlarının Yönetilmesi	A.12.4.1 Olay kaydetme A.12.4.2 Kayıt bilgisinin korunması A.12.4.3 Yönetici ve operatör kayıtları
Sunucu Sıkılaştırma Tedbirleri	5.3.2.12	2	Sanal Makinelerin Güvenli İmhası	A.8.3.2 Ortamın yok edilmesi

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ				TS ISO/IEC 27001:2017
Varlık Grubu Ana Başlığı	Tedbir No	Tedbir Seviyesi	Tedbir Adı	
Sunucu Sıkılaştırma Tedbirleri	5.3.2.13	2	Hipervizörler Tarafından Sunulan Bellek Paylaşımı Özelliklerinin Kullanımı	-
Sunucu Sıkılaştırma Tedbirleri	5.3.2.14	2	Sunucu Yedeklerinin Alınması	A.12.3 Yedekleme
Sunucu Sıkılaştırma Tedbirleri	5.3.2.15	3	Disk ve İmajların Şifreli Olarak Saklanması	A.10.1 Kriptografik kontroller