KRON

BİLGİ GÜVENLİĞİ POLİTİKALARI

Information Security Policies

Alan	Değer	Alan	Değer
Belge No	302POL01	**Sürüm**	Rev 4.0
Hazırlayan	Operations Support & Delivery Director	**Hazırlanma Tarihi**	17.11.2017
Onaylayan	Genel Müdür	**Revize Tarihi**	01.06.2026
Gizlilik Sınıfı	İç Kullanım	**Standart**	ISO/IEC 27001:2022

ISO/IEC 27001:2022 · KVKK · GDPR Uyumlu

Bu belge KRON bünyesinde çalışan tüm personeli ve tedarikçi ilişkilerini kapsar.

İÇİNDEKİLER

Giriş ve Amaç

Bu belge, KRON bünyesinde bilgi sistemlerinin ve varlıklarının güvenliğinin sağlanması amacıyla uyulması zorunlu olan asgari güvenlik kurallarını ve politikalarını tanımlamaktadır. Politikalar; ISO/IEC 27001:2022 standardı, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve AB Genel Veri Koruma Tüzüğü (GDPR) ile uyumlu olacak şekilde hazırlanmıştır.

Temel Amaçlar

- Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini (CIA üçgeni) korumak
- Siber tehditlere (fidye yazılımı, kimlik avı, APT saldırıları, yapay zeka destekli saldırılar) karşı kurumsal direnci artırmak
- KVKK, GDPR ve sektörel yasal yükümlülüklere uyumu sağlamak
- İş sürekliliğini güvence altına almak ve olası ihlallerden kaynaklanan yasal ve itibar risklerini en aza indirmek
- Bulut ortamları, uzaktan çalışma ve mobil iş gücü dahil tüm dijital varlıkları kapsayan bütüncül bir güvenlik kültürü oluşturmak

Kapsam ve Bağlayıcılık

Bu belge; KRON'un tüm çalışanlarını, yöneticilerini, geçici personelini, danışmanlarını, tedarikçilerini ve kurum bilgi sistemlerine erişen üçüncü tarafları bağlayıcı niteliktedir. Politikalara aykırı davranış, disiplin prosedürleri ve gerektiğinde yasal işlemlere konu olabilir.

Revizyon	Bu belge yılda en az bir kez veya önemli bir teknolojik / yasal değişiklik sonrasında gözden geçirilir. Sorumlu birim: Bilgi Teknolojileri & BGYS Temsilcisi.

1. E-Posta Güvenliği Politikası

Kapsam: Kurumsal e-posta altyapısını kullanan tüm çalışanlar ve üçüncü taraflar	**ISO 27001:2022:** Madde 5.14 – Bilgi transferi; 8.23 – Web filtreleme

Kurumsal e-posta hesapları KRON kimliğini taşır ve yalnızca iş amaçlı kullanılır. Hesaplar gerektiğinde yetkili personel tarafından denetlenebilir.

Yasaklı Kullanımlar

- Taciz, ayrımcılık, ırkçılık, müstehcenlik veya siyasi propaganda içeren mesajların iletilmesi.
- Gizli kurumsal verilerin şifrelenmemiş e-posta ile kurum dışına iletilmesi.
- Çalıştırılabilir ek (.exe, .bat, .vbs vb.) içeren e-postaların açılması veya iletilmesi.
- Kimlik bilgisi talep eden e-postalara (phishing) yanıt verilmesi; bu tür mesajlar derhal silinmeli ve BT birimine raporlanmalıdır.
- Spam, zincir e-posta veya sahte gönderici adresli mesajların yönlendirilmesi.

Güvenlik Gereksinimleri

- E-posta altyapısında SPF, DKIM ve DMARC protokolleri etkinleştirilir; gelen/giden e-postalar bu standartlara göre doğrulanır.
- Tüm gelen/giden e-postalar anti-spam ve kötü amaçlı yazılım taramasına tabi tutulur; imza tabanları günde en az iki kez güncellenir.
- Hassas veri (KVKK kapsamındaki kişisel veri dahil) içeren e-postalar TLS şifrelemesi veya S/MIME ile iletilir.
- Kuruma ait e-posta hesabı hiçbir koşulda üçüncü kişilere kullandırılmaz; kimlik bilgileri paylaşılmaz.
- Kurum dışına gönderilen tüm iletilerin altında standart gizlilik ve sorumluluk notu yer alır.
- Ayrılan çalışanların e-posta hesapları çıkış günü devre dışı bırakılır; iş e-postaları belirlenen yöneticiye yönlendirilir (en fazla 30 gün).

2. Şifre ve Kimlik Doğrulama Politikası

Kapsam: Tüm kullanıcı ve sistem hesapları	**ISO 27001:2022:** Madde 5.17 – Kimlik doğrulama; 8.5 – Güvenli kimlik doğrulama

Güçlü parola yönetimi ve çok faktörlü kimlik doğrulama (MFA), hesap güvenliğinin temelini oluşturur.

Parola Gereksinimleri

- Minimum 12 karakter; büyük harf, küçük harf, rakam ve en az bir özel karakter içermelidir.
- Son 10 parola tekrar kullanılamaz.
- Kullanıcı parolaları en fazla 90 günde bir, sistem/servis hesabı parolaları 6 ayda bir yenilenir.
- Başarısız giriş denemesi 5'i geçtiğinde hesap otomatik kilitlenir; kilit açma BT yetkilisi onayı gerektirir.
- Parola yöneticisi kullanımı teşvik edilir; parolalar kağıda yazılamaz, e-posta ile iletilemez.

Çok Faktörlü Kimlik Doğrulama (MFA)

- Tüm kritik sistemlere (VPN, e-posta, ERP, bulut platformları) erişimde MFA zorunludur.
- Yönetici (admin/root) hesapları için donanım güvenlik anahtarı (FIDO2/U2F) veya authenticator uygulaması tercih edilir.
- SMS tabanlı OTP yalnızca yedek faktör olarak kabul edilir; mümkün olan her durumda uygulama tabanlı TOTP kullanılır.

Ayrıcalıklı Erişim (PAM)

- Root/administrator hesapları günlük operasyonlarda kullanılmaz; ayrıcalıklı işlemler için zaman sınırlı oturum açma (just-in-time access) uygulanır.
- Sistem yöneticileri her sistem için farklı, benzersiz parolalar kullanır.
- Üçüncü taraf destek erişimleri geçici, kapsam sınırlı hesaplarla sağlanır; iş bitiminde derhal iptal edilir.

3. Uç Nokta Koruma (Anti-Malware / EDR) Politikası

Kapsam: Tüm masaüstü, dizüstü, sunucu ve mobil cihazlar	**ISO 27001:2022:** Madde 8.7 – Kötü amaçlı yazılımlara karşı koruma

KRON, geleneksel antivirüs çözümlerinin ötesinde, davranışsal analiz ve tehdit avcılığı (threat hunting) yetenekleri sunan EDR (Endpoint Detection & Response) çözümleri kullanır.

Gereksinimler

- Tüm uç noktalara onaylı EDR ajanı kurulur; kaldırılamaz veya devre dışı bırakılamaz.
- İmza tabanları ve tehdit istihbaratı beslemeleri günde en az iki kez otomatik güncellenir.
- Taşınabilir medya (USB, harici disk) kullanımı politika tabanlı olarak kısıtlanır; onaysız ortamlar otomatik engellenir.
- Fidye yazılımı (ransomware) koruması için kritik klasörler üzerinde yetkisiz şifreleme girişimleri otomatik durdurulur ve BT'ye uyarı gönderilir.
- Güvenlik uyarıları SIEM sistemine iletilir; kritik uyarılar 15 dakika içinde Olay Müdahale ekibine bildirilir.

4. İnternet Erişim ve Kullanım Politikası

Kapsam: Kurum ağından veya VPN üzerinden internete erişen tüm kullanıcılar	**ISO 27001:2022:** Madde 8.22 – Ağ ayrıştırma; 8.23 – Web filtreleme

İnternet erişimi iş amacıyla sağlanmaktadır. Tüm trafik güvenlik denetim katmanlarından geçirilir.

Teknik Kontroller

- Tüm çıkış trafiği Next-Gen Firewall (NGFW) ve Secure Web Gateway (SWG/CASB) üzerinden geçer.
- Kategori tabanlı içerik filtreleme uygulanır: kötü amaçlı, yasadışı, kumar, müstehcen ve iş dışı içerikler engellenir.
- DNS güvenliği (DNS-over-HTTPS / DNS filtreleme) ile C2 (komuta-kontrol) sunucularına erişim engellenir.
- SSL/TLS derin paket incelemesi (DPI) uygulanır; muafiyet listesi BT direktörü onayıyla yönetilir.
- P2P protokolleri ve yetkisiz uzaktan erişim araçları (TeamViewer, AnyDesk vb.) teknik olarak engellenir.
- Onaysız bulut depolama hizmetlerine (kişisel Google Drive, Dropbox vb.) kurumsal veri yüklenmesi engellenir.

Kullanıcı Yükümlülükleri

- Çalışma saatlerinde iş ile ilgisi olmayan sitelerde aşırı gezinmek yasaktır.
- Onaylı yazılım listesi dışındaki uygulamalar indirilip kurulamaz.
- Misafir kullanıcılar yalnızca "Misafir Wi-Fi" ağı üzerinden internete erişir; kurumsal ağa dahil edilemezler.

5. Sunucu ve Sistem Güvenlik Güçlendirme (Hardening) Politikası

Kapsam: Tüm fiziksel ve sanal sunucular, konteyner platformları	**ISO 27001:2022:** Madde 8.8 – Teknik açıkların yönetimi; 8.9 – Konfigürasyon yönetimi

Sunucular, CIS Benchmark veya eşdeğer sertleştirme kılavuzları esas alınarak yapılandırılır.

Konfigürasyon Standartları

- Kullanılmayan servisler, portlar ve protokoller devre dışı bırakılır (en az ayrıcalık prensibi).
- İşletim sistemi ve uygulama yamaları risk değerlendirmesine göre önceliklendirilir; kritik yamalar 72 saat, yüksek öncelikli yamalar 7 gün, orta öncelikli yamalar 30 gün içinde uygulanır.
- Tüm yönetimsel bağlantılar şifreli kanallar üzerinden yapılır (SSH, HTTPS, IPSec VPN); Telnet ve HTTP erişimi kapatılır.
- Sunucular fiziksel güvenliği sağlanmış, erişim denetim sistemine sahip sistem odalarında barındırılır.
- Uygulama/servis logları SIEM'e aktarılır; erişim kayıtları en az 1 yıl saklanır.
- Konteyner imajları güvenilir kayıt defterlerinden alınır; taramadan geçmeyen imajlar devreye alınmaz.

Güvenlik Açığı Yönetimi

- Tüm sunucular aylık periyodik güvenlik açığı taramasına (vulnerability scanning) tabi tutulur.
- CVSS ≥ 7.0 skorlu açıklar kritik olarak sınıflandırılır ve acil yama sürecine alınır.

6. Ağ Cihazları Güvenlik Politikası

Kapsam: Router, switch, firewall, WAP ve diğer ağ altyapı cihazları	**ISO 27001:2022:** Madde 8.20 – Ağ güvenliği; 8.21 – Ağ hizmetleri güvenliği

Temel Gereksinimler

- Tüm ağ cihazları ve IP/MAC adresleri güncel envanter kayıtlarında tutulur; kayıt dışı cihaz ağa bağlanamaz (NAC uygulaması).
- Varsayılan servisler (Telnet, HTTP, SNMP v1/v2) kapatılır; güvenli alternatifler (SSH v2, HTTPS, SNMP v3) kullanılır.
- Enable ve yönetim parolaları kriptografik hash ile saklanır; varsayılan parolalar kesinlikle değiştirilir.
- Yazılım ve firmware güncellemeleri önce test ortamında doğrulanır; değişiklik bakım pencerelerinde (maintenance window) uygulanır.
- Tüm cihazlarda NTP ile senkronize zaman damgası ve merkezi log iletimi (Syslog/SIEM) zorunludur.
- Yetkisiz erişim girişimlerini caydırmak amacıyla tüm cihazlarda yasal uyarı banner'ı görüntülenir.
- Ağ bölümlendirme (segmentation) uygulanır: üretim, test, yönetim ve misafir ağları birbirinden izole edilir.

7. Ağ Yönetimi Politikası

Kapsam: Tüm kurumsal ağ altyapısı	**ISO 27001:2022:** Madde 8.20 – Ağ güvenliği; 8.22 – Ağ ayrıştırma

- Ağın iş sürekliliği için yedekli bağlantı (redundancy) ve yük dengeleme (load balancing) uygulanır.
- VLAN segmentasyonu ile ağ trafiği kullanıcı rolü ve risk seviyesine göre ayrıştırılır.
- NGFW ile kaynak/hedef tabanlı trafik kontrolü sağlanır; varsayılan kural "hepsini reddet" (deny-all) ilkesidir.
- Ağ trafik anomalileri IDS/IPS ve NDR (Network Detection & Response) araçlarıyla izlenir.
- Ağ diyagramları, IP planı ve konfigürasyon yedekleri güncel tutulur; yetkisiz erişime karşı korunur.
- Tüm ağ işlemleri SIEM üzerinde takip edilir; şüpheli trafik paternleri otomatik uyarı tetikler.
- BGP/OSPF gibi dinamik yönlendirme protokolleri kimlik doğrulama ile güvenli hale getirilir.
- Firewall kural seti çeyrek yılda bir gözden geçirilir; gereksiz kurallar kaldırılır.

8. Uzaktan Erişim Politikası

Kapsam: VPN, RDP ve diğer uzaktan bağlantı yöntemleriyle erişen tüm kullanıcılar	**ISO 27001:2022:** Madde 8.20 – Ağ güvenliği; 5.17 – Kimlik doğrulama

Uzaktan erişim, sıfır güven (Zero Trust) mimarisi ilkeleri doğrultusunda yönetilir: "asla güvenme, her zaman doğrula."

VPN ve Erişim Gereksinimleri

- Kurumsal ağa uzaktan erişim yalnızca onaylı VPN çözümü (IKEv2/IPSec veya WireGuard tabanlı) üzerinden sağlanır.
- Tüm uzaktan erişimde MFA zorunludur; basit parola doğrulaması yeterli değildir.
- Cihaz uyumluluk kontrolü (device compliance check) uygulanır: güncel OS yaması, aktif EDR, disk şifreleme (BitLocker/FileVault) olmayan cihazlar bağlanamaz.
- Split tunneling yalnızca onaylı trafik türleri için izin verilir; varsayılan yapılandırma tam tüneldir (full tunnel).
- Uzaktan erişim oturumları eş zamanlı bağlantı sayısı ve oturum süresi bakımından sınırlandırılır.
- İlişkisi kesilen veya görev değişikliği olan kullanıcıların VPN hesapları ayrılış günü kapatılır.

Üçüncü Taraf Erişimi

- Üçüncü taraf erişimi BT direktörü onayıyla, kapsam ve süre sınırlı hesaplarla sağlanır.
- Dış erişim oturumları kaydedilir ve düzenli olarak incelenir.

9. Kablosuz Ağ Güvenliği Politikası

Kapsam: Kurumsal kablosuz ağ altyapısı ve bağlanan tüm cihazlar	**ISO 27001:2022:** Madde 8.20 – Ağ güvenliği

- Kurumsal Wi-Fi ağı WPA3-Enterprise (802.1X/EAP-TLS) ile korunur; WEP ve WPA/WPA2-Personal kullanımı yasaktır.
- Erişim noktaları (AP) üretici güvenlik önerilerine uygun şekilde sertleştirilir; yönetim arayüzü yalnızca yönetim VLAN'ından erişilebilir.
- Firmware güncellemeleri aylık periyotlarda kontrol edilir ve uygulanır.
- Kablosuz ağ kapsamı fiziksel sınırları aşmayacak şekilde güç ve anten yönlendirmesiyle optimize edilir.
- Yetkisiz erişim noktaları (rogue AP) tespiti için kablosuz saldırı tespit sistemi (WIDS) çalıştırılır.
- Misafir ağı kurumsal ağdan izole edilmiş ayrı SSID üzerinde sunulur; misafir trafiği internet erişimiyle sınırlıdır.
- Kablosuz ağ üzerinden kurumsal kaynaklara erişimde VPN tüneli zorunludur.

10. İş Sürekliliği ve Olay Müdahale Politikası

Kapsam: Tüm kritik iş süreçleri ve bilgi sistemleri	**ISO 27001:2022:** Madde 5.29 – İş sürekliliği; 5.26 – Güvenlik olaylarına müdahale

KRON, olası siber saldırı, felaket senaryosu veya sistem arızası durumlarında iş sürekliliğini sağlamak için BCP (İş Sürekliliği Planı) ve DRP (Felaket Kurtarma Planı) yürütür.

Olay Sınıflandırması

Müdahale Prosedürü

- Olay fark edildiğinde çalışan derhal bilgi işlem birimine ve BGYS Temsilcisi'ne bildirim yapar.
- Kritik/yüksek olaylar için Olay Müdahale Ekibi (CSIRT) 1 saat içinde toplanır.
- KVKK ve GDPR kapsamındaki kişisel veri ihlalleri, tespit tarihinden itibaren 72 saat içinde ilgili düzenleyici otoriteye bildirilir.
- Tüm olaylar kayıt altına alınır; kapanış sonrasında kök neden analizi (RCA) ve öğrenilen dersler raporu hazırlanır.
- BCP/DRP tatbikatları yılda en az bir kez gerçekleştirilir; sonuçlar plan revizyonunda kullanılır.

11. Erişim Yönetimi ve Yetkilendirme Politikası

Kapsam: Tüm bilgi sistemi kullanıcıları ve hesap yönetimi süreçleri	**ISO 27001:2022:** Madde 5.15 – Erişim kontrolü; 5.18 – Erişim hakları

KRON, erişim yönetiminde "en az ayrıcalık" (least privilege) ve "görevler ayrılığı" (segregation of duties) prensiplerini uygular.

Kullanıcı Yaşam Döngüsü Yönetimi

- Yeni çalışan erişimi, onaylı "Kullanıcı Oluşturma Formu" ile İK ve BT birimi işbirliğiyle sağlanır.
- Rol tabanlı erişim kontrolü (RBAC) uygulanır; bireysel kullanıcılara özel izin yerine role dayalı yetkilendirme tercih edilir.
- Erişim hakları çeyrek yılda bir gözden geçirilir (access review); görev değişikliği veya ayrılma durumunda anında güncellenir.
- Ayrılan çalışanların tüm hesapları ve erişim anahtarları (API key dahil) işten ayrılış günü içinde iptal edilir.

İzleme ve Denetim

- Başarılı ve başarısız oturum açma girişimleri merkezi log sisteminde (SIEM) tutulur; anormal davranışlar UEBA tarafından tespit edilir.
- Her kullanıcı yalnızca kendisine ait hesapla sisteme girer; hesap paylaşımı kesinlikle yasaktır.
- Sistemlere erişim kayıtları KVKK gereği 2 yıl, ISO 27001 gereği en az 1 yıl saklanır.

12. Veri Tabanı Güvenliği Politikası

Kapsam: Tüm veritabanı sistemleri ve yöneticileri	**ISO 27001:2022:** Madde 8.31 – Geliştirme, test ve üretim ayrımı; 8.34 – Denetim günlükleri

- Veritabanı sistemleri envanteri ve her sistem için sorumlu DBA tanımlanmıştır.
- Veritabanına yalnızca yetkili uygulamalar ve kullanıcılar erişir; doğrudan sorgu erişimi üretim ortamında kısıtlıdır.
- Hassas veriler (kişisel veri, ödeme bilgisi) veritabanı seviyesinde AES-256 ile şifrelenir.
- Root/DBA parolası çift kontrol (dual control) ile yönetilir ve fiziksel kasada saklanır.
- FTP, Telnet gibi açık metin bağlantı protokolleri kapatılmıştır; yalnızca SSL/TLS şifreli bağlantılar kabul edilir.
- Tüm veritabanı sorguları ve ayrıcalıklı işlemler loglanır; loglar yetkisiz değişime karşı korunur.
- Yamalar ve güncellemeler değişiklik yönetimi süreci (bkz. Politika 13) çerçevesinde uygulanır.
- Üretim veritabanına doğrudan DML/DDL müdahalesi değişiklik talep formu ve BT direktörü onayı gerektirir.
- SQL injection ve diğer veritabanı saldırılarına karşı DAM (Database Activity Monitoring) çözümü kullanılır.

13. Değişim Yönetimi Politikası

Kapsam: Tüm bilgi sistemi değişiklikleri ve ilgili personel	**ISO 27001:2022:** Madde 8.32 – Değişim yönetimi

Bilgi sistemlerine yapılacak her türlü değişiklik, güvenlik ve sürekliliği koruyacak şekilde planlanır, test edilir ve onaylanır.

Süreç Adımları

- Değişiklik talebi (RFC – Request for Change) standart form ile hazırlanır; etkilenen sistemler ve geri dönüş planı belirtilir.
- Değişiklik, BT Değişiklik Danışma Kurulu (CAB) ve BT direktörü tarafından riske göre sınıflandırılır ve onaylanır.
- Yüksek/kritik değişiklikler önce test/staging ortamında doğrulanır; canlıya aktarım bakım penceresinde gerçekleştirilir.
- Değişiklik öncesi ve sonrasında sistem/uygulama kontrol listeleri uygulanır; sonuçlar kayıt altına alınır.
- Acil değişiklikler (emergency change) güvenlik olayı sırasında hızlandırılmış onay süreciyle işlenir; retrospektif onay 24 saat içinde alınır.
- Yazılım sürüm kontrolü zorunludur; CI/CD hattında güvenlik taraması (SAST/DAST) entegre edilir.

14. Bilgi Sistemleri Yedekleme Politikası

Kapsam: Tüm kritik sistemler, uygulamalar ve veri depoları	**ISO 27001:2022:** Madde 8.13 – Bilgilerin yedeklenmesi

Yedekleme Gereksinimleri

- Kritik veriler için RPO (Kurtarma Noktası Hedefi) ≤ 4 saat, RTO (Kurtarma Süresi Hedefi) ≤ 8 saat hedeflenir.
- Yedeklemeler 3-2-1 kuralına göre yönetilir: 3 kopya, 2 farklı ortam, 1 offsite/bulut yedek.
- Yedekler şifreli (AES-256) olarak saklanır; şifreleme anahtarları yedek veriden ayrı konumda tutulur.
- Fidye yazılımı koruması için son yedekler değişmez (immutable) depolama alanında tutulur.
- Yedekleme başarısızlıkları otomatik uyarıyla BT ekibine bildirilir ve 4 saat içinde giderilir.

Test ve Doğrulama

- Yedek kurtarma testleri aylık periyotlarda gerçekleştirilir; sonuçlar kayıt altına alınır.
- Tam sistem kurtarma tatbikatı (tam DR testi) yılda bir kez yapılır.
- Yedekleme ortamlarının fiziksel ve mantıksal erişim kontrolü sağlanır; yetkisiz erişim loglanır.

15. Temiz Ekran ve Temiz Masa Politikası

Kapsam: Tüm çalışma alanları ve bilgisayar kullanan personel	**ISO 27001:2022:** Madde 7.7 – Temiz masa/ekran politikası

- Bilgisayar ekranı, 3 dakika hareketsizlik sonrası otomatik kilitlenir ve kilit açmak için kimlik doğrulama gerekir.
- Çalışanlar bilgisayarları başından ayrılmadan önce manuel olarak kilitlemekle yükümlüdür (Windows: Win+L, Mac: Ctrl+Cmd+Q).
- Çalışma masasında gizlilik sınıfı taşıyan belge, not veya kartlar mesai bitiminde kilitli dolaba kaldırılır.
- Yazıcı ve fotokopi cihazından alınan çıktılar gözetimsiz bırakılmaz; gizli çıktılar imha makinesinde imha edilir.
- Ekran yerleşimi, yetkisiz kişilerin ekran içeriğini göremeyeceği şekilde düzenlenir; gerektiğinde gizlilik filtresi kullanılır.
- Şifre politikası ve güvenlik farkındalığı çalışanlara oryantasyon eğitiminde aktarılır; yıllık güvenlik farkındalık eğitimi zorunludur.

16. Bulut Güvenliği Politikası

Kapsam: Tüm SaaS, IaaS ve PaaS bulut hizmetleri	**ISO 27001:2022:** Madde 5.23 – Bulut hizmetlerinin kullanımında bilgi güvenliği

Bu politika, ISO 27017 (Bulut Güvenliği) ve ISO 27018 (Bulutta Kişisel Veri) standartlarını referans alır.

Bulut Hizmet Yönetimi

- Bulut hizmetleri güvenlik risk değerlendirmesinden geçtikten sonra BT direktörü onayıyla devreye alınır; onaysız "shadow IT" kullanımı yasaktır.
- CASB (Cloud Access Security Broker) çözümü ile onaysız bulut kullanımı tespit edilir ve engellenir.
- Veri sınıflandırma politikasına göre "Gizli" ve "Çok Gizli" veriler yalnızca onaylı, KVKK/GDPR uyumlu bulut sağlayıcılarında saklanabilir.
- Bulut kaynaklarına erişimde MFA zorunludur; ayrıcalıklı kimlikler için PAM çözümü entegre edilir.
- Yanlış yapılandırma riskleri için bulut güvenlik durum yönetimi (CSPM) aracı sürekli çalıştırılır.
- Bulut sağlayıcısı ile imzalanan SLA ve DPA (Veri İşleme Sözleşmesi) güncel tutulur; KVKK kapsamındaki yurt dışı aktarım gereksinimleri karşılanır.

17. Kişisel Veri Koruma Politikası (KVKK / GDPR)

Kapsam: Kişisel veri işleyen tüm süreçler ve çalışanlar	**ISO 27001:2022:** Madde 5.34 – Gizlilik ve kişisel bilgilerin korunması

6698 sayılı KVKK ve AB GDPR kapsamında kişisel veriler yalnızca belirli, açık ve meşru amaçlarla işlenir.

Temel İlkeler

- Veri minimizasyonu: yalnızca işleme amacı için gerekli veriler toplanır.
- Amaç sınırlılığı: toplanan veriler belirlenen amaç dışında kullanılamaz.
- Saklama sınırlılığı: yasal süreler bittikten sonra kişisel veriler güvenli yöntemle imha edilir.
- Veri güvenliği: teknik (şifreleme, erişim kontrolü) ve idari (eğitim, politika) tedbirler alınır.

Haklar ve Yükümlülükler

- İlgili kişilerin KVKK madde 11 kapsamındaki hakları (erişim, düzeltme, silme vb.) için resmi başvuru kanalı tanımlanmıştır; talepler 30 gün içinde yanıtlanır.
- Kişisel veri ihlali tespitinden itibaren 72 saat içinde Kişisel Verileri Koruma Kurumu'na ve ihlalden etkilenen veri sahiplerine bildirim yapılır.
- Veri envanteri (VERBİS) ve etki değerlendirmesi (DPIA) düzenli olarak güncellenir.
- Tüm kişisel veri işleme faaliyetleri Veri İşleme Kaydı'nda (RoPA) belgelenir.

18. Yapay Zeka ve Üretken YZ Kullanım Politikası

Kapsam: Yapay zeka araçlarını kullanan tüm çalışanlar	**ISO 27001:2022:** Madde 5.14 – Bilgi transferi; 5.36 – Politikaya uyum

Yapay zeka araçları (ChatGPT, Copilot, Gemini vb.) iş verimliliğini artırmak için kullanılabilir; ancak bilgi güvenliği riskleri dikkate alınmalıdır.

Kullanım Kuralları

- Gizli, çok gizli veya kişisel veri niteliğindeki bilgiler halka açık yapay zeka platformlarına girilemez.
- Kurumsal verilerin üçüncü taraf YZ modelleri için eğitim verisi olarak kullanılması yasaklanmıştır; bu özelliği kapatmayan uygulamalar kurum bilgisayarında kullanılamaz.
- Yapay zeka tarafından üretilen kod, doküman veya içerik yayınlanmadan önce insan denetiminden geçirilir.
- Onaylı kurumsal YZ araçları (Microsoft 365 Copilot gibi) BT direktörü onayıyla devreye alınır; risk değerlendirmesi yapılır.
- YZ destekli sosyal mühendislik saldırılarına (deepfake, hedefli phishing) karşı çalışan farkındalık eğitimleri düzenlenir.

19. Roller ve Sorumluluklar

Bu bölüm, bilgi güvenliği süreçlerinin etkin biçimde işletilebilmesi için gerekli rolleri ve bu rollere ait sorumlulukları tanımlamaktadır. Tanımlanan her rol; ilgili politikaların uygulanmasından, denetiminden ve sürdürülebilirliğinden sorumludur.

Üst Yönetim

- Bilgi güvenliği yönetim sistemini (BGYS) onaylamak, gerekli kaynakları tahsis etmek ve kurumsal destek sağlamak.
- Bilgi güvenliği politikasını ve hedeflerini onaylamak; bu hedeflerin kurumsal stratejiyle uyumunu gözetmek.
- Yıllık BGYS gözden geçirme toplantılarına katılmak ve kararları onaylamak.
- Güvenlik ihlali veya kriz durumlarında nihai karar mercii olarak hareket etmek.

BGYS Temsilcisi

- Bilgi Güvenliği Yönetim Sistemi'nin kurulumu, işletimi ve sürekli iyileştirilmesini koordine etmek.
- Bilgi güvenliği politikalarının güncellenmesini, duyurulmasını ve uygulanmasını sağlamak.
- İç denetimleri planlamak ve sonuçlarını üst yönetime raporlamak.
- KVKK/GDPR uyum faaliyetlerini yürütmek; veri ihlali bildirimlerini ilgili otoritelere yapmak.
- Güvenlik farkındalık eğitimlerini planlamak ve yürütmek.

BT Direktörü / Operations Support & Delivery Director

- Teknik güvenlik altyapısının (firewall, SIEM, EDR, VPN vb.) tasarımından ve işletiminden sorumlu olmak.
- Güvenlik politikalarının teknik gerekliliklerini belirlemek ve uygulatmak.
- Değişiklik yönetimi, yedekleme ve olay müdahale süreçlerini yönetmek.
- Üçüncü taraf erişimlerini ve tedarikçi güvenlik gereksinimlerini denetlemek.
- Sistem yöneticilerinin ve BT personelinin teknik faaliyetlerini gözetmek.

Sistem ve Uygulama Yöneticileri

- Sorumlu oldukları sistemlerin güvenlik konfigürasyonlarını politika standartlarına uygun tutmak.
- Yama ve güncelleme yönetimini tanımlanan süreler içinde gerçekleştirmek.
- Kullanıcı hesaplarını ve erişim haklarını yönetmek; ihlalleri raporlamak.
- Sistem loglarını SIEM'e iletmek ve periyodik olarak incelemek.

Tüm Çalışanlar

- Bu belgede yer alan tüm politikalara uymak.
- Şüpheli güvenlik olaylarını derhal BT birimine ve BGYS Temsilcisi'ne bildirmek.
- Yıllık zorunlu bilgi güvenliği farkındalık eğitimini tamamlamak.
- Kurumsal bilgi varlıklarını yalnızca iş amaçlı ve yetkili sistemler üzerinden kullanmak.

Tedarikçiler ve Üçüncü Taraflar

- Kurum sistemlerine erişim öncesinde bilgi güvenliği politikasını kabul etmek ve imzalamak.
- Erişim kapsamı dışına çıkmamak; kendilerine tahsis edilen hesapları başkasıyla paylaşmamak.

- Sözleşme süresi sonunda tüm erişimlerini ve kurumsal verilerini iade etmek veya imha etmek.

20. Görev Tanımları

Bu bölüm, bilgi güvenliği yönetimiyle doğrudan ilişkili kilit rollerin görev tanımlarını detaylandırmaktadır. Tanımlar, ISO/IEC 27001:2022 Madde 5.3 kapsamında yetki ve sorumlulukların atanması ilkesi doğrultusunda hazırlanmıştır.

BGYS Temsilcisi – Görev Tanımı

- Unvan: Bilgi Güvenliği Yönetim Sistemi Temsilcisi
- Bağlı Olduğu Birim: Üst Yönetim
- Temel Sorumluluklar: BGYS'nin kurulması, dokümante edilmesi, işletilmesi ve sürekli iyileştirilmesi; iç ve dış denetimlerin koordinasyonu; yönetim gözden geçirme toplantılarının hazırlığı ve raporlanması; yasal uyum takibi (KVKK, GDPR, sektörel mevzuat).
- Gerekli Yetkinlikler: ISO 27001 Lead Auditor/Implementer sertifikası veya eşdeğeri; bilgi güvenliği yönetimi konusunda en az 3 yıl deneyim.

BT Direktörü – Görev Tanımı

- Unvan: Operations Support & Delivery Director / BT Direktörü
- Bağlı Olduğu Birim: Genel Müdürlük
- Temel Sorumluluklar: Bilgi güvenliği altyapısının teknik tasarımı ve yönetimi; güvenlik politikalarının teknik gereksinimlerinin belirlenmesi; olay müdahale ekibinin (CSIRT) liderliği; BT güvenlik bütçesinin planlanması; değişiklik yönetimi süreçlerinin onaylanması.
- Gerekli Yetkinlikler: Bilgi teknolojileri veya siber güvenlik alanında lisans diploması; CISSP, CISM veya eşdeğer sertifika; en az 5 yıl BT yönetim deneyimi.

Sistem Yöneticisi – Görev Tanımı

- Unvan: Sistem Yöneticisi / Network & Security Administrator
- Bağlı Olduğu Birim: BT Direktörü
- Temel Sorumluluklar: Sunucu, ağ cihazı ve güvenlik sistemlerinin kurulumu, konfigürasyonu ve izlenmesi; yama ve güncelleme yönetimi; kullanıcı hesapları ve erişim kontrolü yönetimi; yedekleme süreçlerinin yürütülmesi; güvenlik uyarılarının takibi ve ilk müdahale.
- Gerekli Yetkinlikler: Ağ ve sistem yönetimi alanında teknik sertifika (CCNA, MCSA vb.); siber güvenlik temelleri bilgisi.

Son Kullanıcı – Yükümlülükler

- Kullanıcılar, kendilerine tahsis edilen hesap, cihaz ve uygulamaların güvenliğinden birincil derecede sorumludur.
- Güvenlik politikalarına aykırı bir durum tespit ettiklerinde derhal BT birimine bildirim yaparlar.
- Yıllık zorunlu farkındalık eğitimini tamamlar ve alındı belgesi imzalarlar.
- Görev değişikliği veya işten ayrılma durumunda tüm kurumsal varlıkları (donanım, erişim bilgileri, belgeler) eksiksiz iade ederler.

21. Bilgi Güvenliği Hedefleri

KRON'un bilgi güvenliği hedefleri; ölçülebilir, zaman sınırlı ve kurumsal stratejik hedeflerle uyumlu biçimde aşağıda tanımlanmıştır. Hedefler yılda en az bir kez BGYS gözden geçirme toplantısında değerlendirilir ve gerektiğinde güncellenir.

Stratejik Hedefler

- Gizlilik (Confidentiality): Bilgi varlıklarına yalnızca yetkili kişilerin erişimini sağlamak. Hedef: Yetkisiz erişim kaynaklı veri ihlali sayısını yılda sıfırda tutmak.
- Bütünlük (Integrity): Bilginin yetkisiz değiştirilmesini, silinmesini veya bozulmasını önlemek. Hedef: Bütünlük ihlali tespit oranını %100 düzeyinde tutmak.
- Erişilebilirlik (Availability): Kritik sistemlerin ve hizmetlerin iş gereksinimleri doğrultusunda kesintisiz çalışmasını sağlamak. Hedef: Kritik sistemler için yıllık %99,5 hizmet sürekliliği.

Operasyonel Hedefler ve KPI'lar

- Güvenlik Açığı Yönetimi: Kritik (CVSS ≥ 9.0) açıkların %100'ünü 24 saat, yüksek (CVSS 7.0–8.9) açıkların %100'ünü 7 gün içinde kapatmak.
- Yama Yönetimi: İşletim sistemi ve uygulama yamalarının aylık %95 ve üzeri uygulama oranına ulaşmak.
- Farkındalık Eğitimi: Tüm çalışanların yıllık güvenlik farkındalık eğitimini %100 tamamlaması; kimlik avı simülasyon testlerinde tıklama oranını %5'in altında tutmak.
- Olay Müdahale: P1 ve P2 güvenlik olaylarında ortalama tespit süresini (MTTD) 15 dakikanın altında, müdahale süresini (MTTR) 4 saatin altında tutmak.
- Erişim Kontrolü: Çeyrek yıllık erişim gözden geçirme tamamlanma oranını %100 düzeyinde sürdürmek; gereksiz yetkileri 5 iş günü içinde iptal etmek.
- Yedekleme ve Kurtarma: Aylık yedek kurtarma testlerinin %100'ünü başarıyla tamamlamak; RPO ≤ 4 saat, RTO ≤ 8 saat hedeflerine uymak.
- Uyumluluk: ISO/IEC 27001:2022 ve KVKK denetimlerinde uygunsuzluk bulgu sayısını yıldan yıla azaltmak; majör uygunsuzluk sıfırda tutmak.

Hedef Takip ve Raporlama

- KPI'lar aylık BT güvenlik raporu ile BGYS Temsilcisi tarafından izlenir.
- Çeyrek yıllık güvenlik durum raporu BT Direktörü aracılığıyla üst yönetime sunulur.
- Yıllık BGYS gözden geçirme toplantısında hedef gerçekleşme oranları analiz edilerek bir sonraki dönem hedefleri belirlenir.

22. Risk Yönetimi

Bu bölüm, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçleri tanımlamaktadır. Risk yönetimi süreci ISO/IEC 27001:2022 Madde 6.1 ve ISO/IEC 27005 standardı esas alınarak tasarlanmıştır.

Risk Yönetimi Metodolojisi

- KRON, niteliksel ve niceliksel karma bir risk değerlendirme metodolojisi benimser. Riskler; olasılık (1-5) ve etki (1-5) eksenlerinde değerlendirilerek Risk Skoru = Olasılık x Etki formülüyle hesaplanır.
- Risk seviyeleri: Düşük (1-4), Orta (5-9), Yüksek (10-16), Kritik (17-25) olarak sınıflandırılır.
- Değerlendirme kapsamı; bilgi varlık envanteri, tehdit kataloğu ve mevcut kontrolleri içerir.

Risk Değerlendirme Süreci

- 1. Bağlamın Belirlenmesi: Değerlendirme kapsamı, varlık sahipleri ve kabul kriterleri tanımlanır.
- 2. Varlık Envanteri: Bilgi varlıkları (donanım, yazılım, veri, personel, süreç) gizlilik/bütünlük/erişilebilirlik açısından sınıflandırılır.
- 3. Tehdit ve Açık Analizi: Her varlık için tehdit senaryoları (siber saldırı, doğal afet, insan hatası vb.) ve mevcut açıklar belirlenir.
- 4. Risk Hesaplama: Olasılık ve etki değerlendirmesi yapılarak risk skoru hesaplanır.
- 5. Risk İşleme: Her risk için işleme seçeneği belirlenir (kabul, azaltma, transfer, kaçınma).
- 6. Kalıntı Risk Onayı: İşleme sonrası kalan kalıntı risk, BT Direktörü veya üst yönetim tarafından onaylanır.

Risk Kabul Kriterleri

- Düşük Risk (1-4): Mevcut kontroller yeterli kabul edilir; izlemeye devam edilir.
- Orta Risk (5-9): Risk azaltma planı hazırlanır; 90 gün içinde iyileştirme başlatılır.
- Yüksek Risk (10-16): Öncelikli aksiyon gerektirir; BT Direktörü onayı ile 30 gün içinde azaltma planı uygulamaya alınır.
- Kritik Risk (17-25): Derhal müdahale gerektirir; üst yönetim bilgilendirilir ve 7 gün içinde aksiyon alınır.

Risk İşleme Seçenekleri

- Azaltma (Threat): Riski kabul edilebilir seviyeye indirmek için teknik veya idari kontroller uygulanır. Bu politikadaki güvenlik kontrolleri (bkz. Bölüm 1-18) öncelikli azaltma araçlarıdır.
- Transfer (Transfer): Risk, siber güvenlik sigortası veya sözleşmesel düzenlemelerle üçüncü tarafa aktarılır.
- Kaçınma (Avoid): Riski doğuran faaliyet veya süreç sonlandırılır ya da değiştirilir.
- Kabul (Accept): Kalıntı risk, tanımlı kabul kriterlerinin altında ise BT Direktörü onayıyla kabul edilir; izlemeye devam edilir.

Risk Gözden Geçirme ve İzleme

- Risk değerlendirmesi yılda en az bir kez veya önemli organizasyonel/teknolojik değişikliklerde yenilenir.
- Risk kayıt defteri (risk register) BGYS Temsilcisi tarafından sürekli güncellenir.
- Yüksek ve kritik riskler aylık BGYS toplantısında, tüm riskler yıllık gözden geçirme toplantısında ele alınır.
- Risk yönetimi çıktıları; denetim, uyumluluk ve iş sürekliliği planlaması ile entegre edilir.

Ekler ve Referanslar

Referans Standartlar ve Mevzuat

Kaynak	Açıklama
ISO/IEC 27001:2022	Bilgi Güvenliği Yönetim Sistemi Gereksinimleri
ISO/IEC 27002:2022	Bilgi Güvenliği Kontrolleri Kılavuzu
ISO/IEC 27017:2015	Bulut Hizmetleri için Güvenlik Kontrolleri
ISO/IEC 27018:2019	Bulutta Kişisel Veri Koruma
6698 Sayılı KVKK	Kişisel Verilerin Korunması Kanunu (Türkiye)
AB GDPR (2016/679)	Genel Veri Koruma Tüzüğü
NIST CSF 2.0	Siber Güvenlik Çerçevesi
CIS Controls v8	Kritik Güvenlik Kontrolleri

Belge Revizyon Geçmişi

Sürüm	Tarih	Değişiklik Özeti	Hazırlayan
Rev 1.0	17.11.2017	İlk yayın	BT Direktörü
Rev 2.0	—	Güncelleme ve kapsam genişletme	BT Direktörü
Rev 4.0	**01.06.2026**	ISO 27001:2022 uyumu, bulut/YZ/KVKK politikaları eklendi	Hakan OTAL Operations Support & Delivery Director

İletişim Bilgi güvenliği sorularınız veya olay bildirimleriniz için: bgys@krontech.com