BİLGİ GÜVENLİĞİ POLİTİKASI

ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi

AMAÇ

Bu politika; Nakitera Finansal Teknoloji Ve Yapay Zeka A.Ş. (bundan böyle "Nakitera" olarak anılacaktır) bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliği konusunda Şirket üst yönetiminin taahhütlerini ve uyulması gereken temel esasları, müşterilerimize, iş ortaklarımıza ve kamuoyuna açık bir şekilde ortaya koymak amacıyla hazırlanmıştır.

KAPSAM

Bu politika; Nakitera'nın tüm çalışanlarını, iş süreçlerini, bilgi sistemleri altyapısını, ağ ve bulut hizmetlerini, işlenen tüm müşteri ve kurumsal verileri, Nakitera adına faaliyet gösteren tedarikçileri ve iş ortaklarını kapsamaktadır. Politika, Nakitera tarafından yürütülen tüm ticari faaliyetler ve hizmet verilen tüm alan adları için geçerlidir.

GENEL ESASLAR

Nakitera üst yönetimi, bilgi güvenliğini kurumsal bir öncelik olarak kabul eder ve aşağıdaki temel taahhütleri verir:

- Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak.
- Çalışanların, iş ortaklarının ve müşterilerin bilgi varlıklarına güvenli erişimini sağlamak.
- Bilgi güvenliği risklerini sistematik olarak değerlendirmek ve yönetmek.
- Tabi olunan ulusal ve uluslararası mevzuata (başta 6698 sayılı KVKK ve 5651 sayılı Kanun olmak üzere), sözleşmeden doğan yükümlülüklere ve ISO/IEC 27001 standardına uyum sağlamak.
- Bilgi güvenliği farkındalığını artırmak için çalışanlara düzenli eğitim vermek.
- İş sürekliliğini tehdit eden olayların etkisini asgariye indirmek ve sürdürülebilir hizmet sağlamak.
- Bilgi Güvenliği Yönetim Sistemi'ni sürekli iyileştirmek.

Tüm Nakitera çalışanları ve paydaşları bu politikayı bilmek ve uygulamakla yükümlüdür. Politikaya aykırı davranışlar Nakitera disiplin süreçleri doğrultusunda değerlendirilir ve gerektiğinde hukuki süreçler başlatılabilir.

ONAYLAYANLAR

Hazırlayan	Kontrol Eden	Onaylayan
Bilgi Güvenliği Ekibi	Bilgi Güvenliği Komitesi	Genel Müdür

BİLGİ GÜVENLİĞİ POLİTİKASI STANDARTLARI

Nakitera Bilgi Güvenliği Yönetim Sistemi aşağıdaki temel süreçler üzerine inşa edilmiştir. Her bir sürecin uygulama detayları kurum içi prosedürlerle ayrıca yönetilir.

1. Veri Sınıflandırma Süreci

Nakitera bünyesinde üretilen, işlenen ve saklanan tüm veriler hassasiyet ve kritiklik seviyelerine göre "Gizli", "Kurum İçi" ve "Halka Açık" olmak üzere sınıflandırılır. Her veri sınıfı için uygun koruma, saklama, paylaşım ve imha kontrolleri uygulanır. Sınıflandırma, ilgili varlık sahibinin sorumluluğundadır ve düzenli aralıklarla gözden geçirilir.

2. BT Risk Belirleme ve Değerlendirme Süreci

Bilgi varlıkları üzerindeki tehditler ve zayıflıklar sistematik olarak belirlenir, risk analizi yapılır ve riskler kabul edilebilir seviyede tutulacak şekilde yönetilir. Risk değerlendirmesi ISO/IEC 27005 çerçevesine uygun olarak yılda en az bir kez ve önemli değişikliklerde tekrarlanır. Yüksek seviyeli riskler için Bilgi Güvenliği Komitesi tarafından azaltma, transfer, kaçınma veya kabul kararı verilir.

3. Bilgi Güvenliği Farkındalık Süreci

Tüm çalışanlar, işe başladıkları andan itibaren bilgi güvenliği farkındalık eğitimine tabi tutulur. Eğitimler yılda en az bir kez yenilenir; rol bazlı özel eğitimlerle desteklenir. Güncel tehditlere karşı hazırlıklı olmak için düzenli oltalama simülasyonları ve farkındalık kampanyaları düzenlenir.

4. Görevler Ayrılığı Prensibi

Yetki kötüye kullanımı ve hata riskini azaltmak için birbiriyle çelişen görevler farklı kişiler tarafından icra edilir. Sistem geliştirme ile üretim ortamına aktarım, işlem başlatma ile onaylama, hesap açma ile erişim denetleme gibi kritik fonksiyonlar ayrıştırılır. Bu ayrımın mümkün olmadığı durumlarda telafi edici kontroller (çift onay, bağımsız gözden geçirme, detaylı loglama) uygulanır.

5. Bilgi Güvenliği Komitesi

Bilgi Güvenliği Komitesi; bilgi güvenliği politikalarının yönlendirilmesi, kritik risklerin değerlendirilmesi ve sürekli iyileştirmeden sorumlu yönetim organıdır. Üst yönetim, bilgi teknolojileri, bilgi güvenliği, insan kaynakları, hukuk/uyum ve iç denetim temsilcilerinden oluşur. Komite düzenli aralıklarla toplanır; kritik olaylarda olağanüstü toplantı yapar. Kararları yazılı olarak kayıt altına alınır ve takip edilir.

ONAYLAYANLAR

Hazırlayan	Kontrol Eden	Onaylayan
Bilgi Güvenliği Ekibi	Bilgi Güvenliği Komitesi	Genel Müdür

6. Kullanıcı Kimlik ve Hesap Yönetimi Politikası

Nakitera sistemlerine erişim için kullanılan tüm kimlikler en az yetki (“least privilege”) ilkesi doğrultusunda tanımlanır. Her kullanıcı yalnızca kendi hesabını kullanır; parolalar güçlü ve gizli tutulur. Kurumsal servislerde çok faktörlü kimlik doğrulama (MFA) zorunludur. Kullanıcı hesapları ve yetkileri düzenli olarak gözden geçirilir; görevi değişen ya da işten ayrılan çalışanların erişim hakları zamanında güncellenir veya kaldırılır. Ayrıcalıklı (yönetici) hesaplar ek kontroller ve izleme altında yönetilir.

7. Fiziksel ve Çevresel Güvenlik

Nakitera tesisleri ve kritik altyapı alanları (sistem odası, ağ odası, veri merkezi), risk seviyelerine göre ayrılmış güvenlik bölgeleri olarak tasarlanır. Yetkilendirilmiş kart erişim sistemleri, kamera gözetimi ve ziyaretçi refakat kuralları uygulanır. Kritik altyapı alanları yangın algılama ve söndürme sistemleri, kesintisiz güç kaynakları ve çevresel sensörler ile korunur. Tüm BT ekipmanları envantere kaydedilir, kullanıcılara zimmetlenir ve kullanım ömrü dolan ortamlar güvenli yöntemlerle imha edilir.

8. Denetim İzleri Yönetimi

Nakitera bilgi sistemlerinde gerçekleştirilen kritik işlemler, kimlik doğrulama olayları, ayrıcalıklı erişimler, ağ trafiği ve güvenlik olayları merkezi bir log yönetim platformunda toplanır. Log kayıtları, 5651 sayılı Kanun, KVKK ve ilgili düzenleyici gereklilikler doğrultusunda saklanır; bütünlüğü koruyacak şekilde muhafaza edilir. Loglar düzenli olarak analiz edilir, anomaliler için korelasyon kuralları uygulanır ve yetkisiz erişim denemeleri zamanında tespit edilerek değerlendirilir.

9. Bilgi Güvenliği Olay Yönetimi

Nakitera, bilgi güvenliği olaylarının zamanında tespit edilmesi, kayıt altına alınması, analiz edilmesi ve en az zararla çözüme kavuşturulması için tanımlı bir olay yönetimi sürecine sahiptir. Çalışanlar, şüpheli her durumu derhal Bilgi Güvenliği Ekibi'ne bildirmekle yükümlüdür. Olaylar etki seviyelerine göre önceliklendirilir, kanıtlar standartlara uygun toplanır ve kök neden analizi ile tekrarların önlenmesi için iyileştirme aksiyonları tanımlanır. Kişisel veri ihlalleri mevzuatın gerektirdiği süreler içinde yetkili kurum ve ilgili kişilere bildirilir.

ONAYLAYANLAR

Hazırlayan	Kontrol Eden	Onaylayan
Bilgi Güvenliği Ekibi	Bilgi Güvenliği Komitesi	Genel Müdür

10. E-Posta Kullanım Esasları

Kurumsal e-posta, Nakitera'nın bilgi varlığıdır ve iş amaçlı kullanılır. Kullanıcılar; yasadışı, taciz edici veya zararlı içerik göndermekten, sahte ve zincir e-posta iletmekten ve kurumsal adresleri kişisel sitelere üyelikte kullanmaktan kaçınır. Hassas veriler yalnızca şifreli kanallar üzerinden paylaşılır. Tüm giden ve gelen e-postalar antivirüs, anti-spam ve anti-phishing filtreleri ile denetlenir. SPF, DKIM ve DMARC gibi e-posta kimlik doğrulama mekanizmaları Nakitera alan adlarında etkin tutulur.

11. İnternet Kullanım Esasları

Nakitera ağları üzerinden internet erişimi; içerik denetimi yapan güvenlik çözümleri aracılığıyla, yasalara ve kurum kültürüne uygun şekilde sağlanır. Zararlı ve uygunsuz sitelere erişim engellenir. Güvenlik kontrollerini atlatmayı amaçlayan yöntemlerin kullanımı, telif hakkı ihlal eden içeriklerin indirilmesi ve kurumsal hesap bilgilerinin internet üzerinde paylaşılması yasaktır. 5651 sayılı Kanun kapsamında internet erişim kayıtları mevzuatın öngördüğü süre boyunca saklanır.

12. Kullanıcı Bilgisayarları ve Taşınabilir Aygıtlar Kullanım Standartları

Nakitera tarafından tahsis edilen bilgisayarlar, dizüstüler, mobil cihazlar ve taşınabilir depolama aygıtları iş amaçlı kullanım için verilmiştir ve ilgili kullanıcıya zimmetlenir. Tüm cihazlarda kurumsal güvenlik yazılımları (antivirüs/EDR) aktif ve güncel tutulur; diskler şifrelenir; ekran kilidi ve parola koruması zorunludur. Uzaktan çalışma yalnızca onaylı cihazlar ve kurumsal VPN üzerinden, çok faktörlü kimlik doğrulama ile gerçekleştirilir. Cihaz kaybı ya da çalınması durumunda derhal Bilgi Güvenliği Ekibi'ne bildirim yapılır ve uzaktan silme uygulanabilir. Temiz masa ve temiz ekran prensipleri tüm çalışma ortamlarında geçerlidir.

Referans Standart ve Mevzuat

Bu politika; ISO/IEC 27001:2022, ISO/IEC 27002:2022, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), 5651 sayılı İnternet Kanunu ve ilgili sektörel düzenlemelerle uyumlu olarak hazırlanmış ve yayımlanmıştır.

ONAYLAYANLAR

Hazırlayan	Kontrol Eden	Onaylayan
Bilgi Güvenliği Ekibi	Bilgi Güvenliği Komitesi	Genel Müdür