BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ, KAPSAM VE YASAL DAYANAK

1.1. Amaç

Bu politika, Ostim Endüstriyel Yatırımlar ve İşletme A.Ş.'nin ("Şirket") bilgi sistemleri kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik temel prensipleri, rolleri, sorumlulukları ve kontrolleri tanımlamaktadır.

1.2. Kapsam

Bu politika;

- Şirketin tüm bilgi sistemlerini
- Tüm bilgi varlıklarını (donanım, yazılım, veriler, belgeler)
- Tüm çalışanları, yöneticileri ve yönetim kurulu üyelerini
- Bilgi sistemlerine erişimi olan üçüncü tarafları
- Bulut hizmet sağlayıcılarını ve diğer dış hizmet sağlayıcılarını

kapsar.

1.3. Yasal Dayanak

Bu politika, Sermaye Piyasası Kurulu'nun VII128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Tebliği ve ilgili mevzuat hükümleri uyarınca hazırlanmıştır.

2. TANIMLAR

Bilgi Güvenliği: Bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması.

Bilgi Varlığı: Şirket için değer taşıyan her türlü bilgi, veri, donanım, yazılım ve sistem.

Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması.

Bütünlük: Bilginin doğruluğunun ve eksiksizliğinin korunması.

Erişilebilirlik: Bilginin ihtiyaç duyulduğunda yetkili kullanıcılar tarafından erişilebilir olması.

Kritik Bilgi Sistemi: Şirketin kritik iş süreçlerini ve faaliyetlerini destekleyen, kesintiye uğraması halinde önemli operasyonel, finansal veya itibar kayıplarına yol açabilecek sistemler.

Bilgi Güvenliği İhlali: Bilgi güvenliği politikalarının veya prosedürlerinin ihlal edilmesi veya bilgi varlıklarının gizliliğinin, bütünlüğünün veya erişilebilirliğinin tehlikeye girmesi.

3. TEMEL PRENSİPLER

3.1 Gizlilik (Confidentiality)

Bilgiye erişim, yalnızca yetkili kişilerle sınırlandırılır. Hassas bilgiler uygun şekilde sınıflandırılır ve korunur.

3.2 Bütünlük (Integrity)

Bilginin yetkisiz değişikliklerden korunması ve doğruluğunun sağlanması esastır.

3.3 Erişilebilirlik (Availability)

Bilgi sistemleri ve bilgiler, iş gereksinimleri doğrultusunda kesintisiz ve güvenilir şekilde erişilebilir olmalıdır.

3.4 Katmanlı Güvenlik

Ağ altyapısı, işletim sistemi ve uygulama seviyelerinde birden çok koruma katmanı uygulanır.

3.5 Görevler Ayrılığı

Bilgi sistemleri üzerinde hata, eksiklik veya kötüye kullanım risklerini azaltmak için görev ve sorumluluk alanları ayrılır.

3.6 En Az Yetki Prensibi

Kullanıcılara sadece görevlerini yerine getirmek için gerekli olan minimum yetkiler verilir.

3.7 Savunma Derinliği

Tek bir güvenlik kontrolüne güvenilmez; birden fazla güvenlik katmanı uygulanır.

4. ROL VE SORUMLULUKLAR

4.1 Yönetim Kurulu

Sorumluluklar:

- Bilgi Güvenliği Politikasını onaylar
- Bilgi güvenliği kontrollerinin etkin, yeterli ve uyumlu bir şekilde tesis edilmesi, değerlendirilmesi ve gözetiminden sorumludur
- Bilgi güvenliği ihlallerine ilişkin kritik raporları değerlendirir
- Bilgi güvenliği için gerekli kaynakları sağlar
- Yıllık bilgi güvenliği performans raporlarını değerlendirir

4.2 Üst Yönetim (Genel Müdür)

Sorumluluklar:

- Bilgi güvenliği politikalarını ve prosedürlerini hazırlar ve yönetim kuruluna sunar
- Bilgi Güvenliği Sorumlusunu görevlendirir
- Bilgi güvenliği politikalarının ve sorumlulukların yılda en az bir kez gözden geçirilmesini ve onaylanmasını sağlar
- Risk yönetimi sürecinin oluşturulmasını temin eder
- Bilgi güvenliği ihlallerinin takibini ve yılda en az bir kez değerlendirilmesini sağlar
- Personele bilgi güvenliği eğitimlerinin yılda en az bir kez verilmesini temin eder
- Görevler ayrılığı ilkesi çerçevesinde görevlendirmeler yapar
- Önemli kontrol eksikliklerini değerlendirir ve gerekli önlemleri alır

4.3 Bilgi Güvenliği Sorumlusu

Nitelikler:

- Bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde yeterli teknik bilgiye sahip

- En az 5 yıl tecrübeye sahip
- Bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevi bulunmaz
- Üst yönetime bağlı çalışır

Sorumluluklar:

- Bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden ve takibinden sorumludur
- Bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hususunda üst yönetime düzenli raporlar sunar
- Bilgi güvenliği politikalarının ve prosedürlerinin hazırlanmasına ve güncellenmesine liderlik eder
- Bilgi güvenliği farkındalık eğitimlerini koordine eder
- Bilgi güvenliği ihlallerini yönetir ve raporlar
- Uzaktan erişim yetkilerini onaylar
- Güvenlik açıklarını ve tehditleri takip eder
- Bilgi varlıkları envanterinin güncelliğini kontrol eder
- Yıllık bilgi güvenliği değerlendirme raporunu hazırlar

4.4 Bilgi Sistemleri Yöneticisi

Sorumluluklar:

- Bilgi sistemlerinin güvenli bir şekilde kurulması, işletilmesi ve yönetilmesinden sorumludur
- Teknik güvenlik kontrollerinin uygulanmasını sağlar
- Sistem ve ağ altyapısının güvenliğini temin eder
- Yedekleme ve felaket kurtarma süreçlerini yönetir
- Güvenlik açıklarını tespit eder ve gerekli güncellemeleri yapar
- Denetim izlerini düzenli olarak gözden geçirir
- Kritik sistemlerin performans gözetimini sağlar

4.5 Bilgi Varlığı Sahipleri

Sorumluluklar:

- Sorumlu oldukları bilgi varlıklarının güvenlik sınıflandırmasını yapar
- Erişim yetkilerini yılda en az bir kez gözden geçirir
- Bilgi varlıklarına ilişkin güvenlik gereksinimlerini belirler
- Varlıklarına ilişkin güvenlik olaylarını bildirir

4.6 Tüm Çalışanlar

Sorumluluklar:

- Bu politika ve ilgili prosedürlere uygun hareket ederler
- Bilgi güvenliği farkındalık eğitimlerine katılırlar
- Şüpheli durumları ve güvenlik olaylarını derhal Bilgi Güvenliği Sorumlusuna bildirirler
- Güçlü şifreler kullanır ve parola güvenliği kurallarına uyarlar

- Kullanım prosedürlerine uygun hareket ederler
- İşten ayrılma durumunda tüm bilgi varlıklarını iade ederler

4.7 Dış Hizmet Sağlayıcılar

Sorumluluklar:

- Sözleşmelerde belirtilen güvenlik gereksinimlerine uyarlar
- Bilgi güvenliği olaylarını Şirkete derhal bildirirler
- Düzenli güvenlik raporları sunarlar
- Şirketin denetim ve gözetim faaliyetlerine destek verirler

5. BİLGİ GÜVENLİĞİ SÜREÇLERİ

5.1 Risk Yönetimi

5.1.1 Risk Değerlendirme Süreci

- Bilgi sistemlerine ilişkin potansiyel riskler düzenli olarak tespit edilir
- Risklerin etkileri ve olasılıkları değerlendirilir
- Risk azaltma stratejileri geliştirilir
- Risk kabul seviyeleri belirlenir
- Risk değerlendirmeleri yılda en az bir kez yapılır

5.1.2 Değerlendirilecek Risk Alanları

- Bilgi teknolojilerindeki hızlı gelişmelere uymamanın riskleri
- Öngörülemeyen hata ve hileli işlem riskleri
- Dış hizmet sağlayıcılara bağımlılık riskleri
- İş süreçlerinin bilgi sistemlerine bağımlılığı riskleri
- Denetim izleri ve veri güvenliği riskleri
- Siber güvenlik tehditleri (fidye yazılımı, veri sızıntısı, DDoS vb.)
- İç tehditler (yetkisiz erişim, veri hırsızlığı)
- Doğal afetler ve altyapı kesintileri

5.2 Varlık Yönetimi

5.2.1 Envanter Yönetimi

- Tüm bilgi varlıkları belirlenir ve envantere kaydedilir
- Envanter sürekli güncel tutulur
- Varlık Yönetimi Prosedürüne uygun hareket edilir

5.2.2 Sınıflandırma

- Bilgi varlıkları güvenlik sınıflarına ayrılır
- Her sınıf için uygun koruma önlemleri belirlenir
- Bilgi Varlıkları Sınıflandırma Prosedürü uygulanır

5.2.3 Kullanım Prosedürleri

- Bilgi varlıklarının uygun kullanımına ilişkin prosedürler geliştirilir
- Prosedürler yazılı hale getirilir ve personele duyurulur
- Kötüye kullanım durumları takip edilir

5.3 Erişim Kontrolü

5.3.1 Rol Tabanlı Erişim

- Erişim yönetiminde rol tabanlı erişim kontrolü uygulanır
- Kullanıcı hesapları ve yetkiler düzenli gözden geçirilir
- Gereksiz yetkiler iptal edilir

5.3.2 Kimlik Doğrulama

- Bilgi varlığının güvenlik sınıfına uygun kimlik doğrulama yöntemleri kullanılır
- Kritik sistemler için çok faktörlü kimlik doğrulama uygulanır
- Uzaktan erişimde çok faktörlü kimlik doğrulama zorunludur

5.3.3 Yetkilendirme Süreci

- Kullanıcı hesabı açma ve yetkilendirme işlemleri onay sürecine bağlanır
- Erişim haklarına ilişkin tüm işlemlerin denetim izleri tutulur
- Yetkiler yılda en az bir kez ilgili bilgi varlığının sorumlusu tarafından gözden geçirilir

5.4 Görevler Ayrılığı

- Ayrılması gereken görev ve sorumluluklar belirlenir
- Görevler ayrılığı matrisi oluşturulur ve yılda en az bir kez gözden geçirilir
- Çakışan yetkilerin verilmesi engellenir
- İstisna durumlar belgelenir ve onaylanır

5.5 İzleme ve Denetim

5.5.1 Denetim İzleri

Aşağıdaki işlemlere ilişkin denetim izleri tutulur:

- Kritik bilgi sistemlerine ilişkin kayıt değişiklikleri
- Hassas verilere erişim, sorgulama, görüntüleme, kopyalama ve değiştirme işlemleri
- Erişim yetkilerinin verilmesi, değiştirilmesi ve geri alınması
- Yetkisiz erişim teşebbüsleri
- Sistem yönetici işlemleri
- Başarısız oturum açma denemeleri

5.5.2 İzleme Faaliyetleri

- Denetim izleri düzenli olarak gözden geçirilir
- Olağandışı aktiviteler tespit edilir ve araştırılır
- Kritik sistemler sürekli gözetim altında tutulur
- Performans eşik değerleri belirlenir ve aşımlar otomatik bildirilir

5.6 Olay Yönetimi

5.6.1 Olay Tespit ve Bildirimi

- Bilgi güvenliği olayları derhal tespit edilir ve bildirilir
- Olay Yönetimi Politikası ve Prosedürüne uygun hareket edilir
- Olay müdahale planı uygulanır

5.6.2 Olay Analizi

- Bilgi güvenliği ihlalleri takip edilir
- İhlaller yılda en az bir kez değerlendirilir
- Kök neden analizleri yapılır
- İyileştirme aksiyonları alınır

5.7 Eğitim ve Farkındalık

5.7.1 Periyodik Eğitimler

- Tüm personele bilgi güvenliği eğitimleri yılda en az bir kez verilir
- Eğitimler rol ve sorumluluklara uygun şekilde tasarlanır
- Eğitim konuları: güvenlik gereksinimleri, riskler, güncel tehditler, politika ve prosedürler

5.7.2 Farkındalık Faaliyetleri

- Düzenli güvenlik bültenleri yayınlanır
- Güvenlik hatırlatmaları yapılır
- Oltalama (Phishing) simülasyonları düzenlenir

6. TEKNİK GÜVENLİK KONTROLLERİ

6.1 Ağ Güvenliği

6.1.1 Katmanlı Güvenlik

- Ağ altyapısı, işletim sistemi ve uygulama seviyelerinde koruma katmanları uygulanır
- Güvenlik duvarları (firewall) kullanılır
- Sızma tespit ve önleme sistemleri (IDS/IPS) devreye alınır
- Ağ segmentasyonu yapılır

6.1.2 Ağ Topolojisi

- Kurumsal ağın fiziksel ve mantıksal topolojisi yazılı hale getirilir
- Topoloji güncel tutulur ve güvenli saklanır
- Tüm alt ağlar, güvenlik cihazları, erişim noktaları ve bağlantı yolları dahil edilir

6.1.3 Uzaktan Erişim

- Uzaktan erişimde çok faktörlü kimlik doğrulama kullanılır
- Uzaktan erişim yetkilendirmeleri Bilgi Güvenliği Sorumlusunun onayı ile yapılır
- Yalnızca güncel işletim sistemi ve uygulamalara sahip cihazlardan erişime izin verilir
- Uzaktan erişim denetim izleri tutulur
- VPN kullanımı zorunludur

6.2 Sistem Güvenliği

6.2.1 Güvenlik Yamaları

- İşletim sistemleri ve uygulamalar düzenli olarak güncellenir
- Kritik güvenlik yamaları yayınlandığında ivedilikle uygulanır
- Yama yönetim süreci uygulanır

6.2.2 Kötü Amaçlı Yazılım Koruması

- Tüm sistemlerde güncel antivirüs/antimalware çözümleri kullanılır
- Gerçek zamanlı tarama aktiftir
- Tanımlar otomatik güncellenir

6.2.3 Sistem Sıkılaştırma

- Gereksiz servisler ve portlar kapatılır
- Güvenlik yapılandırmaları uygulanır
- Varsayılan parolalar değiştirilir

6.3 Veri Güvenliği

6.3.1 Şifreleme

- Hassas veriler hem depolama hem de iletim sırasında şifrelenir
- Güçlü şifreleme algoritmaları kullanılır
- Şifreleme anahtarları güvenli bir şekilde yönetilir

6.3.2 Veri Yedekleme

- Kritik veriler düzenli olarak yedeklenir
- Yedekler güvenli bir şekilde saklanır
- Yedekleme ve geri yükleme testleri düzenli yapılır
- İkincil sistem yurt içinde bulundurulur

6.3.3 Veri İmhası

- Artık ihtiyaç duyulmayan veriler güvenli bir şekilde imha edilir
- Veri imha prosedürlerine uyulur

6.4 Fiziksel Güvenlik

6.4.1 Veri Merkezi Güvenliği

- Kritik bilgi sistemlerinin bulunduğu veri merkezleri fiziksel olarak korunur
- Yetkisiz fiziksel erişim engellenir
- Çevresel koşullar (sıcaklık, nem) izlenir
- Yangın söndürme sistemleri kurulur
- Kesintisiz güç kaynağı (UPS) kullanılır

6.4.2 Erişim Kontrolü

- Güvenli alanlara erişim kayıt altına alınır
- Ziyaretçiler gözetim altında tutulur
- Erişim kartları veya biyometrik sistemler kullanılır

6.5 Bulut Hizmetleri Güvenliği

- Bulut hizmeti alımı ve kullanımı dışarıdan hizmet alımı olarak değerlendirilir
- Bulut hizmet sağlayıcıları güvenlik gereksinimlerine göre değerlendirilir
- Sözleşmelerde güvenlik maddeleri yer alır
- Düzenli güvenlik denetimleri yapılır

7. İŞ SÜREKLİLİĞİ

7.1 İş Sürekliliği Planlaması

- Kritik iş süreçlerini destekleyen bilgi sistemlerinin sürekliliği sağlanır
- Bilgi Sistemleri Süreklilik Planı, İş Sürekliliği Planının bir parçası olarak hazırlanır
- İş Sürekliliği & Bilgi Sistemleri Süreklilik Politikası uygulanır

7.2 Yedeklilik

- Kritik sistemler için yedeklilik sağlanır
- İkincil sistemler yurt içinde bulundurulur
- İkincil sistem yeri, birincil sistemle aynı risklere maruz kalmayacak şekilde seçilir
- Düzenli felaket kurtarma testleri yapılır

7.3 Kurtarma Hedefleri

- Kurtarma Süresi Hedefi (RTO) ve Kurtarma Noktası Hedefi (RPO) belirlenir
- Kritik sistemler için öncelik sıralaması yapılır

- Kurtarma prosedürleri dokümante edilir

8. DIŞ HİZMET YÖNETİMİ

8.1 Tedarikçi Değerlendirmesi

- Dış hizmet sağlayıcılar güvenlik yetenekleri açısından değerlendirilir
- Güvenlik gereksinimleri sözleşmelere dahil edilir
- Hizmet seviyesi anlaşmaları (SLA) yapılır

8.2 Sürekli Gözetim

- Dış hizmet sağlayıcıların performansı düzenli izlenir
- Güvenlik raporları talep edilir
- Denetim hakları sözleşmelerde yer alır
- Kritik dış hizmetler için bağımlılık analizi yapılır

8.3 Üçüncü Taraf Erişimi

- Üçüncü tarafların bilgi sistemlerine erişimi kontrol altında tutulur
- Gizlilik anlaşmaları (NDA) imzalanır
- Erişimler düzenli gözden geçirilir ve gerektiğinde iptal edilir

9. UYUM VE DEĞERLENDİRME

9.1 İç Kontrol

- Bilgi sistemleri süreçleri ve kontrollerinin etkinlik, yeterlilik ve uyumluluğu sürekli takip edilir
- Önemli kontrol eksiklikleri tespit edilir
- Yapılan çalışmalar yılda en az bir kez üst yönetime raporlanır

9.2 Uyumluluk Denetimi

- Politika ve prosedürlere uyum düzenli olarak değerlendirilir
- İç denetim faaliyetleri yürütülür
- Uyumsuzluklar tespit edilir ve düzeltilir

9.3 Politika Güncellemeleri

- Bu politika yılda en az bir defa gözden geçirilir
- İş ihtiyaçları, değişen tehdit ve risklere göre güncellenir
- Mevzuat değişiklikleri takip edilir ve politikaya yansıtılır
- Güncellemeler yönetim kurulu tarafından onaylanır

9.4 Raporlama

Yönetim Kuruluna Raporlama:

- Yıllık bilgi güvenliği değerlendirme raporu
- Önemli güvenlik olayları ve ihlaller
- Önemli kontrol eksiklikleri
- Risk değerlendirme sonuçları

Üst Yönetime Raporlama:

- Aylık güvenlik durum raporu
- Güvenlik olayları ve müdahale faaliyetleri

- Risk yönetimi güncellemeleri
- Uyumluluk durumu

10. YAPTIRIMLAR

10.1 İhlal Durumları

Bu politikanın ihlali durumunda:

- Disiplin işlemleri başlatılabilir
- İş sözleşmesi feshedilebilir
- Hukuki süreçler başlatılabilir
- İlgili kurumlar bilgilendirilebilir

10.2 Değerlendirme

- İhlaller dokümante edilir
- Kök neden analizleri yapılır
- İyileştirme aksiyonları alınır
- İhlal istatistikleri tutulur

11. DUYURU VE YÜRÜRLÜK

11.1 Duyuru

- Bu politika Yönetim Kurulu tarafından onaylanır
- Üst yönetim tarafından tüm personele ve ilgili diğer taraflara duyurulur
- Personel, politikayı okuduğunu ve anladığını imza ile teyit eder
- Politika Şirket içi sistemlerde erişilebilir hale getirilir

11.2 Yürürlük

Bu politika, Yönetim Kurulu onayını takiben yürürlüğe girer.

12. İLGİLİ DOKÜMANLAR

- Bilgi Sistemleri Süreklilik Politikası
- Olay Yönetimi Politikası
- Bilgi Varlıkları Yönetimi & Sınıflandırma Politikası
- Erişim Kontrolü Prosedürü
- Yedekleme ve Geri Yükleme Prosedürü
- Olay Müdahale Prosedürü
- Uzaktan Erişim Prosedürü
- Dışardan Hizmet Alımı Prosedürü
- Veri Sınıflandırma Prosedürü
- Rol ve Sorumluluklar Matrisi

Bu politika, SPK'nın VII128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Tebliği uyarınca hazırlanmış Yönetim Kurulu'nun 16.12.2025 tarihli toplantısında kabul edilmiştir.