BİLGİ SİSTEMLERİ YÖNETİM POLİTİKASI

1. AMAÇ, KAPSAM VE YASAL DAYANAK

1.1. Amaç

Bu politika, Ostim Endüstriyel Yatırımlar ve İşletme A.Ş.'nin ("Şirket") bilgi sistemlerinin yönetimine ilişkin kontrol, politika, prosedür ve süreçlerin yazılı hale getirilmesi, düzenli gözden geçirilmesi, güncellenmesi ve yönetim kurulu tarafından onaylanarak ilgililere duyurulmasını temin etmek amacıyla hazırlanmıştır.

1.2. Kapsam

Bu politika, Şirketin tüm bilgi sistemlerinin (donanım, yazılım, ağ, veri, uygulamalar ve ilgili hizmetler) yaşam döngüsü boyunca yönetimine ilişkin süreçleri, kontrolleri ve sorumlulukları kapsar.

1.3. Yasal Dayanak

Bu politika, Sermaye Piyasası Kurulu'nun VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Tebliği, ilgili mevzuat hükümleri ve Şirket iç düzenlemeleri uyarınca hazırlanmıştır.

2. TEMEL İLKELER

2.1. Bilgi sistemleri yönetimi, iş stratejileri ve hedefleri ile uyumlu şekilde yürütülür.

2.2. Bilgi sistemleri yaşam döngüsü boyunca etkin kontroller tesis edilir.

2.3. Tüm politika, prosedür ve süreçler yazılı hale getirilir, düzenli gözden geçirilir ve güncellenir.

2.4. Bilgi sistemleri yönetiminde görev ve sorumluluklar açıkça tanımlanır ve görevler ayrılığı ilkesi uygulanır.

2.5. Değişiklik yönetimi, risk yönetimi ve uyumluluk süreçleri entegre edilir.

3. ROL VE SORUMLULUKLAR

3.1. Yönetim Kurulu

- Bilgi sistemleri yönetim politikalarının ve önemli stratejik kararların nihai onayı.
- Bilgi sistemleri yönetim performansının genel gözetimi.

3.2. Üst Yönetim (Genel Müdür)

- Bilgi sistemleri yönetim politikalarını hazırlatır ve yönetim kuruluna sunar.
- Bilgi sistemleri yönetim süreçlerinin etkinliğinden sorumludur.
- Görevler ayrılığı ilkesi çerçevesinde görevlendirmeler yapar.
- Politika ve prosedürlerin düzenli gözden geçirilmesini ve onaylanmasını sağlar.

3.3. Bilgi Sistemleri Yöneticisi

- Bilgi sistemlerinin güvenli, verimli ve kesintisiz işletilmesinden sorumludur.
- Teknik politika ve prosedürlerin hazırlanmasını koordine eder.

- Sistem performans, kapasite ve kullanılabilirlik yönetimini sağlar.
- Değişiklik, yedekleme ve felaket kurtarma süreçlerini yönetir.
- İç ve dış denetimlere destek verir.

3.4. Bilgi Güvenliği Sorumlusu

- Bilgi sistemleri güvenlik kontrollerinin uygulanmasını ve izlenmesini sağlar.
- Güvenlik risk değerlendirmelerine katılır.
- Güvenlik olaylarına müdahale süreçlerini koordine eder.
- Üst yönetime güvenlik durum raporları sunar.

3.5. Sistem ve Ağ Yöneticileri

- Günlük operasyon, izleme, bakım ve sorun giderme faaliyetlerini yürütür.
- Teknik dokümantasyonu güncel tutar.
- Yetkili değişiklikleri uygular.

3.6. Süreç Sahipleri / Kullanıcı Departmanlar

- İş gereksinimlerini tanımlar ve sistem ihtiyaçlarını iletir.
- Kullanıcı kabul testlerine katılır.
- Sistem kullanımına ilişkin uyumluluktan sorumludur.

4. POLİTİKA, PROSEDÜR VE SÜREÇ YÖNETİMİ

4.1. Bilgi sistemleri yönetimine ilişkin tüm politika, prosedür ve süreçler yazılı hale getirilir.

4.2. Bu dokümanlar en az yılda bir defa gözden geçirilir.

4.3. Gözden geçirme, aşağıdaki durumlarda da gerçekleştirilir:

- İş süreçlerinde önemli değişiklikler,
- Teknolojik gelişmeler,
- Yasal değişiklikler,
- Güvenlik olayları veya denetim bulguları.

4.4. Güncellemeler, üst yönetim tarafından onaylanır.

4.5. Onaylanan dokümanlar, ilgili tüm personele ve üçüncü taraflara (gerektiğinde) duyurulur.

5. DEĞİŞİKLİK YÖNETİMİ

5.1. Tüm bilgi sistemlerinde yapılacak değişiklikler (donanım, yazılım, yapılandırma, ağ vb.) resmi bir değişiklik yönetim sürecinden geçer.

5.2. Değişiklik talepleri kayıt altına alınır, risk değerlendirmesi yapılır, test edilir ve onaylanır.

5.3. Acil değişiklikler için hızlandırılmış prosedürler tanımlanır ve sonrasında dokümante edilir.

5.4. Tüm değişikliklerin geri alınabilir olması esastır.

6. KAPASİTE VE PERFORMANS YÖNETİMİ

6.1. Bilgi sistemleri kapasite ihtiyaçları düzenli olarak izlenir ve planlanır.

6.2. Performans metrikleri (kullanılabilirlik, yanıt süresi, hata oranları vb.) tanımlanır ve takip edilir.

6.3. Kritik sistemler için performans eşik değerleri belirlenir; aşımlar otomatik bildirilir.

7. TEDARİKÇİ VE HİZMET YÖNETİMİ

7.1. Bilgi sistemleri ile ilgili dış hizmet alımlarında, hizmet sağlayıcılar güvenlik ve performans kriterlerine göre değerlendirilir.

7.2. Hizmet seviyesi anlaşmaları (SLA) yapılır ve düzenli izlenir.

7.3. Tedarikçi sözleşmelerinde gizlilik, veri koruma ve denetim maddeleri bulunur.

8. YAŞAM DÖNGÜSÜ YÖNETİMİ

8.1. Bilgi sistemleri bileşenleri için planlama, edinme, kurulum, işletme, bakım ve emeklilik aşamaları tanımlanır.

8.2. Yazılım lisans yönetimi etkin şekilde yürütülür.

8.3. Donanım ve yazılım envanteri güncel tutulur.

9. DOKÜMANTASYON VE RAPORLAMA

9.1. Aşağıdaki dokümanlar hazırlanır ve güncel tutulur:

- Sistem mimari diyagramları,
- Ağ topolojisi haritaları,
- Yapılandırma kayıtları,
- Operasyon el kitapları,
- Kurtarma prosedürleri.

9.2. Bilgi sistemleri performansı, olayları ve riskleri hakkında düzenli raporlar üst yönetime sunulur.

9.3. Yılda en az bir kez, bilgi sistemleri yönetim süreçlerinin etkinliğine ilişkin kapsamlı bir değerlendirme raporu hazırlanır.

10. UYUMLULUK VE İÇ KONTROL

10.1. Bilgi sistemleri süreç ve kontrollerinin etkinliği, yeterliliği ve mevzuata uygunluğu sürekli izlenir.

10.2. Tespit edilen önemli kontrol eksiklikleri ve alınan önlemler yılda en az bir kez üst yönetime raporlanır.

10.3. İç denetim ve bağımsız denetim (gerektiğinde) bulguları zamanında ele alınır.

11. EĞİTİM VE FARKINDALIK

11.1. Bilgi sistemleri personeline rol ve sorumluluklarına uygun teknik eğitimler verilir.

11.2. Sistem kullanıcılarına, kabul edilebilir kullanım politikaları ve temel güvenlik kuralları konusunda farkındalık eğitimleri sağlanır.

12. İLGİLİ DOKÜMANLAR

- Bilgi Güvenliği Politikası
- Bilgi Sistemleri Süreklilik Politikası
- Olay Yönetimi Politikası
- Erişim Kontrol Prosedürü
- Değişiklik Yönetim Prosedürü
- Yedekleme ve Geri Yükleme Prosedürü
- Bilgi Varlıkları Envanter ve Sınıflandırma Prosedürü

13. YÜRÜRLÜK VE GÜNCELLEME

13.1. Bu politika, yönetim kurulu onayı ile yürürlüğe girer.

13.2. Politika, yılda en az bir kez veya ihtiyaç halinde gözden geçirilir ve gerekli güncellemeler yapılır.

13.3. Güncellemeler, üst yönetim tarafından onaylanarak ilgili taraflara duyurulur.

REVİZYON GEÇMİŞİ

Versiyon	Tarih	Değişiklik Açıklaması	Hazırlayan
1.0	27.11.2025	İlk Hazırlık	

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