1. AMAÇ

Bu dokümanın amacı, şirketin bilgi sistemlerinin; **güvenli, sürdürülebilir, izlenebilir ve Sermaye Piyasası Kurulu (SPK) düzenlemelerine tam uyumlu** şekilde yönetilmesini sağlamak üzere bilgi sistemleri yönetim stratejisinin esaslarını belirlemektir.

2. KAPSAM

- Bilgi teknolojileri altyapısını,
- Uygulama, veri tabanı, ağ ve sunucu sistemlerini,
- Bulut hizmetlerini,
- Bilgi varlıklarını,
- Bilgi sistemleri süreçlerinde yer alan çalışanlar ve üçüncü tarafları kapsar.

3. MEVZUAT VE DAYANAKLAR

- SPK VII-128.9 Bilgi Sistemleri Yönetimi Tebliği
- SPK III-62.2 Bilgi Sistemleri Bağımsız Denetim Tebliği
- SPK İlke Kararları (i-SPK.62.1 ve i-SPK.128.20)
- 6698 sayılı KVKK
- ISO 27001 ve ISO 22301 standartları (rehber niteliğinde)

4. YÖNETİŞİM VE ORGANİZASYON YAPISI

- Bilgi sistemleri faaliyetleri üst yönetimin gözetim ve sorumluluğunda yürütülür.
- Yetki ve sorumluluklar yazılı olarak tanımlanır.
- Görevlerin ayrılığı ilkesi esas alınır.
- Kritik görevler için yedekli organizasyon yapısı oluşturulur.

5. BİLGİ SİSTEMLERİ MİMARİSİ

- Birincil ve ikincil sistemler tanımlanır.
- Kritik sistemler için yüksek erişilebilirlik sağlanır.
- Bulut hizmetleri kullanılması halinde hizmet sağlayıcı risk değerlendirmesi yapılır.
- Bilgi sistemleri bağımsız denetim kapsamına girilmesi durumunda birincil sistemlerin **yurtiçinde konumlandırılması** sağlanır.

6. BİLGİ GÜVENLİĞİ VE ERİŞİM YÖNETİMİ

- Erişimler rol ve yetki bazlı olarak tanımlanır.
- Yetkiler periyodik olarak gözden geçirilir.
- Güçlü parola ve çok faktörlü kimlik doğrulama uygulanır.
- Sistem logları tutulur ve izlenir.

7. RİSK YÖNETİMİ

- Bilgi sistemlerine ilişkin riskler düzenli olarak değerlendirilir.
- Kritik riskler için aksiyon planları oluşturulur.
- Üçüncü taraf hizmet sağlayıcı riskleri ayrıca analiz edilir.

8. İŞ SÜREKLİLİĞİ VE FELAKET KURTARMA

- Kritik sistemler için iş sürekliliği planları hazırlanır.
- Yedekleme ve geri dönüş testleri düzenli olarak yapılır.
- Felaket kurtarma senaryoları dokümante edilir.

9. GÜVENLİK TESTLERİ VE SIZMA TESTLERİ

- Bilgi sistemlerine yönelik sızma testleri periyodik olarak gerçekleştirilir.
- 01.04.2024 sonrası sızma testleri, SPK Bilgi Sistemleri Bağımsız Denetim Lisansına sahip kişiler tarafından yapılır.
- Bulgular için düzeltici faaliyetler takip edilir.

HAZIRLAYAN	ONAYLAYAN
İÇ DENETÇİ	YÖNETİM TEMSİLCİSİ

10. DENETİM VE İZLEME

- Bilgi sistemleri kontrolleri sürekli izlenir.
- İç ve bağımsız denetim bulguları değerlendirilir.
- Aksiyon planları üst yönetime raporlanır.

11. EĞİTİM VE FARKINDALIK

- Çalışanlara düzenli bilgi güvenliği farkındalık eğitimleri verilir.
- Yeni personel için oryantasyon sürecinde bilgilendirme yapılır.

12. YÜRÜRLÜK VE GÜNCELLEME

Bu doküman Yönetim Kurulu onayı ile yürürlüğe girer. Mevzuat değişiklikleri doğrultusunda ve en az yılda bir kez gözden geçirilir.

HAZIRLAYAN	ONAYLAYAN
İÇ DENETÇİ	YÖNETİM TEMSİLCİSİ