ALTINAY SAVUNMA TEKNOLOJİLERİ A.Ş

BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Bu politikanın amacı; Sermaye Piyasası Kurulu'nun Seri VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği'nin 6'ncı maddesi uyarınca, Şirketimiz faaliyetleri kapsamında kullanılan bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin olarak; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilirliğinin sağlanmasına yönelik ilke ve esasları belirlemektir.

2. Kapsam

Bu politika;

- Elektronik ortamda veya fiziksel olarak tutulan tüm verileri,
- Bilgi sistemlerini, uygulamaları, donanımları ve ağ altyapısını,
- Şirket çalışanlarını ve Şirket adına bilgiye erişimi bulunan üçüncü tarafları kapsar.

3. Dayanak

Bu politika;

- Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10),
- İlgili diğer SPK düzenlemeleri ve yürürlükteki mevzuat çerçevesinde hazırlanmıştır.

4. Tanımlar

- Bilgi: Şirket faaliyetleri kapsamında üretilen, işlenen veya saklanan her türlü veri.
- Bilgi Sistemleri (BS): Bilginin işlendiği, saklandığı ve iletildiği tüm yazılım, donanım ve ağ altyapıları.
- Yetkilendirme: Kullanıcıların görev tanımları doğrultusunda bilgiye erişiminin sınırlandırılması.

5. Temel Bilgi Güvenliği İlkeleri

5.1 Gizlilik

Bilgi, yalnızca yetkili kişiler tarafından erişilebilir olacak şekilde korunur.

- Kullanıcı erişimleri görev ve sorumluluklara göre belirlenir.
- Gizli nitelikteki bilgiler üçüncü kişilerle mevzuat ve sözleşmeler çerçevesinde paylaşılır.

5.2 Bütünlük

- Bilginin doğruluğu, tamlığı ve güncelliği korunur.
- Yetkisiz değişikliklerin önlenmesi için erişim kontrolleri uygulanır.
- Bilgilerde yapılan değişiklikler izlenebilir ve kayıt altına alınabilir şekilde yönetilir.

5.3 Erişilebilirlik

- Bilgi ve bilgi sistemleri, yetkili kullanıcılar için ihtiyaç duyulduğunda erişilebilir durumda tutulur.
- Sistem sürekliliğini sağlamak amacıyla yedekleme ve kurtarma önlemleri alınır.
- Kritik verilerin kaybını önlemek için düzenli yedekleme yapılır.

6. Bilgi Güvenliği Organizasyonu

6.1 Yönetim Kurulu

Yönetim Kurulu;

- Bilgi sistemleri yönetimine ilişkin politika ve stratejileri onaylar,

- Bilgi sistemleri kaynaklı riskleri ve siber tehditleri gözetir,
- Kritik sistemlere ilişkin iş sürekliliği ve olağanüstü durum kurtarma süreçlerini izler,
- Gerekli organizasyonel yapı, kaynak ve yatırımların tesis edilmesini sağlar,
- Bilgi sistemleri riskleri, iş sürekliliği test sonuçları ve önemli bilgi güvenliği olaylarına ilişkin raporları yılda en az bir kez değerlendirir,
- Gerekli gördüğü hâllerde bilgi sistemleri risklerine ilişkin özel rapor talep edebilir.

6.2 Üst Yönetim

Üst Yönetim;

- Politika'nın uygulanmasını sağlar,
- Bilgi sistemleri performansı ve risklerine ilişkin raporları düzenli olarak Yönetim Kurulu'na sunar,
- Risk yönetimi fonksiyonları ile koordinasyonu temin eder.

6.3 Bilgi Güvenliği Sorumlusu

Bilgi Güvenliği Sorumlusu;

- Bilgi sistemlerinin güvenli, kesintisiz ve mevzuata uyumlu şekilde işletilmesinden sorumludur,
- Sistem kontrollerini tesis eder, dokümante eder ve etkinliğini izler,
- Bilgi sistemleri riskleri ve güvenlik önlemlerinin etkinliği hakkında üst yönetime raporlama yapar,
- En az 5 yıl bilgi sistemleri güvenliği, yönetişimi, iç kontrol veya denetim alanlarında tecrübeye sahiptir,
- Günlük operasyonel işleyişe dâhil değildir ve doğrudan üst yönetime bağlı çalışır.

6.4 Risk Yönetimi

- Bilgi sistemlerine ilişkin risk ve kontrolleri değerlendirir.
- Bulguları üst yönetime ve gerekli hallerde Yönetim Kurulu'na raporlar.

7. Erişim ve Yetkilendirme Kontrolleri

- Bilgi sistemlerine erişim kişiye özel kullanıcı adı ve parola ile sağlanır.
- Parolalar gizli tutulur, üçüncü kişilerle paylaşılmaz.
- İşten ayrılan personelin erişim yetkileri derhal kaldırılır.

8. Fiziksel ve Çevresel Güvenlik

- Bilgi sistemlerini barındıran donanımlar yetkisiz erişime karşı korunur.
- Fiziksel evraklar kilitli alanlarda muhafaza edilir.

9. Bilgi Güvenliği İhlalleri

- Bilgi güvenliği ihlali şüphesi derhal yönetime bildirilir.
- İhlalin etkileri değerlendirilir ve gerekli düzeltici önlemler alınır.
- Önemli ihlaller mevzuat çerçevesinde raporlanır.

10. Üçüncü Taraflar

- Bilgi sistemlerine erişimi olan üçüncü taraflarla gizlilik hükümleri içeren sözleşmeler yapılır.
- Dış hizmet sağlayıcıların bilgi güvenliği yükümlülükleri izlenir.

11. Eğitim ve Farkındalık

- Çalışanlar bilgi güvenliği konusunda bilgilendirilir.
- Bilgi güvenliği farkındalığının artırılması amaçlanır.

12. Politikanın Gözden Geçirilmesi

Politika; en az yılda bir kez veya mevzuat ve organizasyonel değişiklikler doğrultusunda gözden geçirilir, iş ihtiyaçları ile değişen tehdit ve risklere göre güncellenir.

13. Yürürlük

Bu politika Yönetim Kurulu'nun 31.12.2025 tarihli kararı ile aynı tarihte yürürlüğe girer.