KONRUT TARIM A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ VE KAPSAM

Konfrut Tarım A.Ş. ve bağlı ortaklıkları ("Konfrut" veya "Şirket"), kurumsal bilgiyi ve iş süreçlerinin sürekliliğini en değerli varlıklarından biri olarak kabul eder. Bu politikanın amacı; Şirket'in itibarını, güvenilirliğini ve bilgi varlıklarını korumak; Sermaye Piyasası Kurulu'nun VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği ile uyumu sağlamak ve kurumsal bilginin Gizlilik, Bütünlük ve Erişilebilirliğini temin etmektir.

Bu politika; Şirket bilgilerini veya bilgi sistemlerini kullanan tüm çalışanları (daimi, süreli, stajyer), Yönetim Kurulu üyelerini, tedarikçileri ve üçüncü taraf hizmet sağlayıcılarını kapsar.

2. YÖNETİMİN TAAHHÜDÜ VE ONAY

Bu politika, Sermaye Piyasası Kanunu ve ilgili mevzuat gereğince Konfrut Tarım A.Ş. Yönetim Kurulu tarafından onaylanmıştır.

Yönetim Kurulu ve Üst Yönetim, aşağıda belirtilen hususların yerine getirilmesini taahhüt eder:

- Bilgi güvenliği stratejisinin iş hedefleriyle uyumlu olmasını sağlamak,
- Bilgi varlıklarına yönelik riskleri tespit etmek ve risk yönetim sürecini işletmek,
- Bilgi güvenliği ihlallerini takip etmek ve gerekli kaynakları (finansman, personel) tahsis etmek,
- Yasal mevzuata (SPK, KVKK, TTK vb.) tam uyum sağlamak,
- Bilgi güvenliği farkındalığını artırmak amacıyla çalışanlara düzenli eğitimler verilmesini sağlamak.

3. GÖREV VE SORUMLULUKLAR

3.1. YÖNETİM KURULU

Bilgi güvenliği stratejisinin belirlenmesi, politikanın onaylanması ve uygulanmasının izlenmesinden sorumludur. Bilgi Güvenliği Sorumlusu'nu belirler.

3.2. BİLGİ GÜVENLİĞİ SORUMLUSU

Tebliğ hükümleri uyarınca atanan/görevlendirilen Bilgi Güvenliği Sorumlusu; politikanın uygulanmasını takip eder, risk analizlerini koordine eder, güvenlik ihlallerini inceler ve doğrudan Üst Yönetime raporlama yapar.

Bilgi Güvenliği Sorumlusu'nun bilgi sistemleri operasyonlarına ilişkin icracı görevi bulunmaz.

3.3. ÇALIŞANLAR

Konumları ne olursa olsun tüm çalışanlar; şirket bilgilerinin gizliliğini korumaktan, kendilerine tahsis edilen erişim yetkilerini (kullanıcı adı, parola vb.) başkalarıyla paylaşmamaktan ve şüpheli durumları derhal raporlamaktan sorumludur.

4. TEMEL BİLGİ GÜVENLİĞİ İLKELERİ

4.1. VARLIK YÖNETİMİ VE SINIFLANDIRMA

Şirket, sahip olduğu bilgi varlıklarının (donanım, yazılım, veri) envanterini çıkarır. Varlıklar önem derecelerine göre sınıflandırılır ve buna uygun güvenlik önlemleri alınır.

4.2. RİSK YÖNETİMİ

Bilgi sistemlerine yönelik risk analizi yılda en az bir kez gerçekleştirilir. Tespit edilen riskler için kabul edilebilir seviyeler belirlenir ve risk azaltıcı önlemler Üst Yönetim onayı ile hayata geçirilir.

4.3. ERİŞİM KONTROLÜ

Erişim yetkileri "bilmesi gereken" ve "en az yetki" prensibine göre verilir. Uzaktan erişimlerde (VPN vb.) ve kritik sistemlerde çok faktörlü kimlik doğrulama (MFA) kullanımı esastır.

4.4. KAYIT VE İZLEME (LOGLAMA)

Bilgi sistemleri üzerinde gerçekleşen kritik işlemler, yetkilendirme değişiklikleri ve güvenlik ihlali teşebbüslerine ilişkin denetim izleri (log kayıtları) bütünlüğü bozulmayacak şekilde kayıt altına alınır ve yasal saklama süreleri boyunca (en az 5 yıl) güvenli ortamda saklanır.

4.5. DIŞ KAYNAK KULLANIMI

Bilgi sistemleri konusunda dışarıdan hizmet alınan firmalarla yapılan sözleşmelere; gizlilik, veri güvenliği ve hizmet seviyesi şartları eklenir.

4.6. FİZİKSEL VE ÇEVRESEL GÜVENLİK

Kritik bilgi sistemlerinin barındırıldığı alanlara (sistem odaları vb.) yetkisiz fiziksel erişim engellenir. Bu alanlar yangın, sel, elektrik kesintisi gibi çevresel tehditlere karşı korunur ve giriş-çıkışlar kayıt altına alınır.

5. POLİTİKANIN GÖZDEN GEÇİRİLMESİ

Bu politika; iş ihtiyaçları, teknolojik değişiklikler, yasal düzenlemeler ve risk ortamındaki değişimler doğrultusunda yılda en az bir defa gözden geçirilir ve gerektiğinde Yönetim Kurulu onayı ile güncellenir.

6. İHLALLER VE YAPTIRIMLAR

Bilgi Güvenliği Politikası'nın ihlali, Şirket'in ticari ve itibar kaybına uğramasına neden olabileceğinden ciddiyetle ele alınır. İhlaller; Şirket İnsan Kaynakları Uygulamaları ve Disiplin Prosedürleri çerçevesinde değerlendirilir. İhlalin boyutuna göre iş akdinin feshine ve yasal (cezai/hukuki) işlemlerin başlatılmasına gidebilecek seviyede yaptırımlar uygulanabilir.