BİLGİ GÜVENLİĞİ POLİTİKASI

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No: YKS-BGP-01

Yayın Tarihi: 19.12.2025

Revizyon: 00

1. GİRİŞ VE AMAÇ

Yükselen Çelik A.Ş. (Şirket), bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı stratejik bir öncelik olarak kabul etmektedir. İşbu politika, SPK'nın VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği'ne tam uyum sağlamak, KVKK ile entegre çalışmak ve ISO 27001 prensiplerini esas alarak hazırlanmıştır. Bilgi güvenliği; bilginin yetkisiz erişim, değiştirilme, silinme veya açıklanmasından korunmasıdır. Şirketimiz, üretim, satış, finans ve yönetim süreçlerinde kullanılan tüm bilgi varlıklarının güvenliğini en üst düzeyde tutmayı taahhüt eder.

2. KAPSAM

Politika, Şirketimizin tüm bilgi işlem varlıklarını (Logo Muhasebe, Romsis ERP, QNAP sunucuları, NAR BULUT yedekleme, Fortigate firewall, ağ altyapısı, taşınabilir cihazlar, bulut sistemleri), süreçlerini, çalışanlarını, dış hizmet sağlayıcılarını (BC Bilişim Teknolojileri Eğitim Danışmanlık Yayıncılık Bilgisayar Hizmetleri San. Tic. Ltd. Şti.) ve üçüncü tarafları kapsar. Web sitesindeki KVKK Aydınlatma Metni ve Çerez Politikası bu politikanın tamamlayıcısıdır.

3. BİLGİ GÜVENLİĞİ TANIMI

- Gizlilik: Bilginin sadece yetkili kişilerce erişilebilir olması
- Bütünlük: Bilginin doğruluğu ve yetkisiz değiştirilememesi
- Erişilebilirlik: Yetkili kullanıcıların gerektiğinde bilgiye hızlı erişimi

4. YÖNETİMİN TAAHHÜDÜ VE SORUMLULUKLAR

- Yönetim Kurulu: Politikanın onaylanması, gözetimi ve yıllık inceleme (Tebliğ md.7)
- Genel Müdür: Kaynak tahsisi, risk kabulü, ihlal müdahale onayı
- Bilgi Güvenliği Sorumlusu: Politikanın günlük takibi, risk raporlaması, eğitim koordinasyonu, ihlal bildirimi (Tebliğ md.7/5 – en az 5 yıl tecrübe)
- Bilgi İşlem Ekibi: Teknik kontrollerin uygulanması, log takibi, yedekleme testleri
- Tüm Çalışanlar: Politika kurallarına uymak, ihlalleri bildirmek, yıllık eğitime katılmak
- Dış Hizmet Sağlayıcılar: BC Bilişim Teknolojileri Eğitim Danışmanlık Yayıncılık Bilgisayar Hizmetleri San. Tic. Ltd. Şti. ile imzalanan sözleşmede belirtilen gizlilik ve güvenlik taahhütlerine uymak

5. RİSK YÖNETİMİ

Yıllık risk analizi BC Bilişim Teknolojileri Eğitim Danışmanlık Yayıncılık Bilgisayar Hizmetleri San. Tic. Ltd. Şti. ile birlikte yapılır, üst yönetim onaylar (Tebliğ md.8). Riskler tanımlanır, değerlendirilir, azaltılır veya kabul edilir. Mevcut kontroller: YYS belgesi kapsamında risk değerlendirmeleri, dış firma raporları, firewall, antivirüs, erişim matrisleri.

6. BİLGİ VARLIK ENVANTERİ VE SINIFLANDIRMA

(Tebliğ md.10) Tüm varlıklar (donanım, yazılım, veri) envanterde tutulur.
Sınıflandırma:

- Gizli: Finansal veriler, müşteri sözleşmeleri, üretim planları
- Özel: Personel özlük dosyaları, iç yazışmalar
- Kamu: Web sitesi çerez bilgileri, genel tanıtım

Envanter Excel'de güvenlik sınıfı sütunuyla güncellenir ve yılda bir gözden geçirilir.

7. ERİŞİM KONTROLLERİ (Tebliğ md.11, md.16)

- Rol tabanlı erişim: "Erişim ve Kullanım Yetki Tablosu" (2 adet matris) ile yönetilir
- En az yetki prensibi, görevler ayrılığı
- Şifre politikası: 8+ karakter, büyük/küçük harf/rakam/özel karakter, 180 günde bir değişim
- İşten ayrılanların hesapları anında kapatılır
- Ağ erişimi: Fortigate firewall, VLAN ayrımı, çok faktörlü VPN

8. FİZİKSEL VE ÇEVRESEL GÜVENLİK (Tebliğ md.12)

- Sunucu odası kartlı giriş, kamera, UPS, jeneratör
- Temiz masa/temiz ekran politikası
- Taşınabilir cihazlar (dizüstü, USB) varlık sahibinin sorumluluğunda

9. AĞ VE SİSTEM GÜVENLİĞİ (Tebliğ md.13-14)

- Ağ Topolojisi diyagramı baz alınır
- Antivirüs merkezi yönetilir, güncellemeler zorunlu
- Kötü niyetli yazılım, phishing, spam koruması
- Loglar 1 yıl saklanır

10. İŞ SÜREKLİLİĞİ VE YEDEKLEME (Tebliğ md.27)

- Plan: "Kriz Yönetimi ve İş Sürekliliği Talimatı", "Felaket Kurtarma Merkezi Talimatı", "Bilgi Sistemleri Acil Durum Planlama Talimatı" bir bütündür
- Yedekleme: QNAP + NAR BULUT (günlük/haftalık/aylık)
- Yıllık geri yükleme testi zorunludur

11. İHLAL YÖNETİMİ (Tebliğ md.24)

- İhlal tespiti → 1 saat içinde Bilgi Güvenliği Sorumlusu'na bildirim
- Yatırımcıyı etkileyecek ihlallerde KAP bildirimi değerlendirilir
- İhlal kayıt altına alınır, kök neden analizi yapılır, tekrarlanmaması için önlem alınır

12. EĞİTİM VE FARKINDALIK (Tebliğ md.7/3-ç)

- Yılda en az 1 kez tüm personele verilir. Konular:
  - Güçlü şifre, phishing, temiz masa/ekran
  - Taşınabilir cihaz güvenliği, sosyal medya, bulut kullanımı
  - İhlal bildirim prosedürü

13. İNTERNET, E-POSTA, SOSYAL MEDYA, BULUT KULLANIMI

- Sadece iş amacı ile kullanım
- Kurum cihazlarında kişisel bulut (Dropbox, OneDrive vb.) yasaktır
- Sosyal medyada şirket dokümanı/fotoğraf paylaşımı yasaktır
- E-posta izlenebilir, spam filtresi zorunludur

14. GÖZDEN GEÇİRME VE GÜNCELLEME (Tebliğ md.6)

- Politika yılda en az 1 kez (Ocak ayı) gözden geçirilir
- Teknolojik değişim, risk analizi sonucu veya personel değişikliğinde revize edilir
- Güncellemeler web sitesinde yayımlanır, personele imza karşılığı duyurulur

15. YAPTIRIM

Politikaya aykırı davranışlar disiplin cezası ile sonuçlanır. Ağır ihlallerde hukuki işlem başlatılır.