

1. AMAÇ

Çates Elektrik Üretim A.Ş. ("ÇATES") için, bilişim sistemleri ve bu sistemlerdeki işlenen kurumsal veriler, günlük operasyonların ve temel hizmetlerin sürekliliği kritik öneme sahiptir. ÇATES bilgi sistemlerinin ve bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin sağlanması, korunması, sürdürülmesi ve yönetilmesini amaçlar. Bu kapsamda, Bilgi Güvenliği yönetimi kapsamında tabi olduğu ulusal, sektörel ve yasal düzenlemeler ile ilgili mevzuat, standart ve yönetmeliklere uyumun sağlanmasını ve bu gerekliliklerin sistematik bir yaklaşımla uygulanmasını amaçlar.

2. KAPSAM

Bu politika, ÇATES bünyesindeki tüm çalışanları, kurumsal verilere erişen üçüncü tarafları ve bilginin işlendiği tüm bilişim sistemleri ile fiziksel ortamları kapsar.

3. SORUMLULUKLAR

ÇATES'in bilgi güvenliği stratejisini ve yol haritasını belirleyen bu politika, ÇATES Üst Yönetimi tarafından hazırlanmış olup, ÇATES Yönetim Kurulu tarafından onaylanmıştır.

ÇATES Yönetim Kurulu, kurum genelinde etkin bir Bilgi Güvenliği Yönetim Çerçevesinin oluşturulması ve sürdürülmesini gözetir. Bilgi Güvenliği Yönetim Sistemi'nin uygulanması ve sürekli iyileştirilmesi için gerekli kaynakları sağlayacağını taahhüt eder.

ÇATES Yönetim Kurulu, Şirketin tabi olduğu mevzuat ve düzenlemelere uyumu sağlamak amacıyla yeterli teknik bilgi ve tecrübeye sahip, operasyonel bilgi teknolojileri faaliyetlerinden bağımsız olarak görev yapan bir Bilgi Sistemleri Güvenliği Sorumlusunu atamıştır. Bilgi Güvenliği Sorumlusu doğrudan Yönetim Kuruluna raporlama yapar ve bilgi güvenliği yönetişimi kapsamında gözetim ve koordinasyon görevlerini yerine getirir.

Bilgi güvenliği faaliyetleri; kurumun stratejik hedefleri, risk yönetimi yaklaşımı ve yürürlükteki mevzuat gereklilikleri ile uyumlu şekilde planlanır ve uygulanır.

3.1. ÇALIŞANLAR

Pozisyonları veya görevlerinden bağımsız olarak tüm ÇATES çalışanları, sorumlu oldukları iş süreçlerinde bilgi güvenliği politikası, prosedür ve talimatlarına uymakla yükümlüdür.

ÇATES, çalışanların mahremiyetine saygı gösterir, ancak gerekli durumlarda bilişim sistemleri üzerindeki işlemleri denetleme hakkını saklı tutar.

3.2. ÜÇÜNCÜ PARTİLER

ÇATES'e mal ve hizmet sağlayan üçüncü partiler ve çalışanlarının uyması gereken Bilgi Güvenliği kuralları sözleşmelerle belirlenir. Bu kapsamda Tedarikçilerin, bilgi güvenliği kuralları başta olmak üzere üçüncü taraflarla ilişkileri düzenleyen ÇATES Politika ve Prosedürleri'ne uygun hareket etmesi esastır.

4. GENEL İLKELER

ÇATES, kurumsal sürdürülebilirliğin temel unsurlarından biri olarak gördüğü Bilgi Güvenliği Politikasında aşağıdaki ilkeleri esas almaktadır;

- Yasal Gereksinimlere Uygunluk
- Bilgi Güvenliği Sistemlerinin Sürekli İyileştirilmesi
- Varlık Yönetimi ve Risk Değerlendirme Süreci
- Verinin Korunması ve Yedekleme
- Fiziksel ve Çevresel Güvenlik
- Bilgi Sistemleri İş Sürekliliği
- Operasyon ve Değişiklik Yönetimi
- Erişim Kontrolü
- Dış Kaynaklı Bilgi Sistemleri Hizmetlerinde Bilgi Güvenliği Gereksinimlerinin Belirlenmesi
- Bilgi Güvenliği Tehditlerinin İzlenmesi ve Yanıtlanması
- Bilgi Güvenliği İhlal Olayı ve Olay Bildirimi Süreci
- Bilgi Güvenliği Farkındalık Programı
- Kabul Edilebilir Kullanım
- Temiz Masa Temiz Ekran

Politika yılda en az bir defa gözden geçirilir ve gerekli hallerde güncellenir. Politika'nın güncel versiyonu çalışanlara ilan edilir. Şirket kurumsal web sitesinde yayımlanır.