# ENERYA ENERJİ A.Ş.

**("ENERYA")**

# BİLGİ GÜVENLİĞİ POLİTİKASI

ENERYA bilişim sistemleri ve sistemlerde bulunan bilgi ve veri, günlük operasyonlar ve etkin hizmet sağlama için temel teşkil etmektedir. ENERYA gizliliğin korunması, bütünlüğün sürdürülmesi ve ENERYA bilişim sistemleri üzerinden saklanan, işlenen ve iletilen tüm bilginin erişilebilirliğini sağlamak için gerekli güvenlik politika, prosedür ve kontrollerini uygulamaktadır.

## 1. KAPSAM

Bilgi Güvenliği Politikasında yer alan güvenlik politikaları yazılım, donanım, saklama ve iletim ortamları ve bilgisayar ağları gibi ENERYA tarafından kullanılan bilgi, veri ve bilişim sistemlerini kapsayacak şekilde geliştirilir.

Bilgi Güvenliği Politikası ENERYA bilgi sistemine erişen ve/veya ENERYA bilişim sistemlerini kullanan kişiler (çalışanlar, sistem yöneticileri veya sorumluları, kullanıcılar, denetçiler, sözleşmeli çalışanlar, tedarikçiler, üçüncü partiler vb.) için geçerlidir.

## 2. AMAÇ

Bilgi Güvenliği Politikasının temel amaaçları aşağıdaki şekildedir:

- ENERYA bilişim sistemlerinde saklanan ve işlenen bilginin yetkisiz ifşasını engellemek (GİZLİLİK)
- Bilginin kazara ya da yetkisiz kişiler tarafından erişilebilir olmasını sağlamak (BÜTÜNLÜK)
- Bilginin gerek duyulduğunda yetkili kişiler tarafından erişilebilir olmasını sağlamak (ERİŞİLEBİLİRLİK)

ENERYA çalışanlarının mahremiyetine saygı göstermeyi amaçlar. Buna karşın, çalışanların gerçekleştirdiği işlemleri ve ENERYA bilişim sistemlerini kullanarak çalışanlar tarafından saklanan, işlenen, iletilen veya üzerinde çalışılan bilgiyi denetleme hakkını saklı tutmaktadır. Bilgi Güvenliği Politikası, ENERYA bilişim sistemlerinin, bilgi güvenliği yönetimi ile ilgili olan yasa ve yönetmelikler, kabul edilmiş iyi uygulamalar ve uluslararası standartlar ile uyumlu olmasını sağlamak için kılavuz niteliğini taşımaktadır.

## 3. BİLGİ GÜVENLİĞİ ORGANİZASYONU

Bilgi Güvenliği organişzasyon yapısı tanımlanır, gözden geçirilir ve gerekli hallerde güncellenir. Organizasyon yapısındaki rol ve sorumluluklar tanımlanırken, mümkün olan her durum için görevler ayrılığı ve en düşük erişim hakkı ilkeleri benimsenir. Bu yapı ile birlikte, birbiriyle uyuşmayan roller aynı kişiye atanmaz.

Her ne kadar bilgi güvenliği sisteminin belirlenmiş bir kapsamı olsa dahi, organizasyon dahilinde yürütülecek her türlü projede bu bilgi güvenliği politikası ve prosedürlerinde tariflenen temel prensipler çerçevesinde değerlendirmelerin yapılması esastır. Şirket bünyesinde bu prensiplerin değerlendirilmesi proje bazlı olarak ilgili proje sahibi birimin ve/veya proje yöneticisinin

sorumluluğunda olup, Bilgi Güvenliği Yöneticisi söz konusu gereksinimin duyurulması ve genel takibinden sorumlu olacaktır.

Projelerde değerlendirilmesi gerekebilecek bilgi güvenliği unsurları aşağıda belirtilmiştir:

- Projenin müşteri bilgileri ile ilgili gizlilik, bütünlük ve erişilebilirlik unsurlarını etkilediği durumlar
- Yeni bir sistem tedariği ya da geliştirilmesi gereken durumlar
- Mevcut sistemlerde önemli oranda değişiklik gerektiren durumlar (ör: veritabanı versiyon yükseltme, yeni bir modül ekleme)
- Sistemler üzerinde yetkilendirme seviyelerinde değişiklik ya da güncelleme gerektiren durumlar
- İlgili proje ekibinin ve/veya muhtemel tedarikçilerin Enerya sistemlerine uzaktan bağlantı kurması gerektiği durumlar
- Projenin iş sürekliliği ya da felaket kurtarma açısından mevcut bulunan mekanizmalarına temas ettiği durumlar
- Enerya fiziki tesislerindeki güvenlik önlemlerinin değişmesine neden olabilecek durumlar
- Projenin yürürlükteki yasa, mevzuat ya da yönetmeliklerden kaynaklı bilgi güvenliğine dokunan unsurlarının bulunması

Söz konusu unsurlar, proje bazlı olarak ve bu politika ve ilgili prosedürlerde tariflenen temel kurallar ışığında proje sahibi ve proje yöneticisinin yönlendirmesiyle uygun olduğu ölçüde dikkate alınır ve ilgili projelerin tasarım, analiz, vb. dokümanlarında kaydedilir.

## 4. TEMEL ROL VE SORUMLULUKLAR

**Bilgi Güvenliği Yönlendirme Kurulu**

ENERYA nezdinde tüm birimlerin Bilgi Güvenliği ile ilişkili konularını tartışan ve çözen merkezi bir birim olarak görev alır. Kuruluş bünyesinde Bilgi Güvenliği politika ve prosedürlerinin uygulanmasından sorumludur. Bilgi Güvenliği ile ilişkili konularını tartışan ve genel bilgi güvenliği stratejisinin kuruluş bazında koordineli ilerlemesinden de yükümlüdür. Temel sorumlulukları:

- Stratejik hedeflerin, yeni yatırımların ve yapılanmaların bilgi güvenliğine olan etkisini değerlendirmek ve kuruluşu yönlendirmek.
- Merkezi olarak yürütülen ve bilgi güvenliğine yönelik aktivitelerin etkinliğini sorgulamak. Süreçlerin verimli işlemesi için gereken takibin yapılmasını sağlamak.
- Uygulanacak bilgi güvenliğine yönelik süreçleri ve kuralları onaylamak.
- Kuruluş nezdinde oluşturulan güvenlik kurullarının aktivitelerini ve toplantı tutanaklarını gözden geçirmek.
- Organizasyon içerisinde çalışanlara atanmış bilgi güvenliği sorumluluklarını gözden geçirmek ve onaylamak.
- İç denetim ve Bilgi Güvenliği Yöneticisinin raporladığı tüm bilgi güvenliği konularını gözden geçirmek ve değerlendirmek. Bilgi güvenliği denetim raporlarını gözden geçirmek ve düzeltici ve önleyici faaliyet planlarını takip etmek.
- Bilgi güvenliği konusundaki önemli gelişmeleri onaylamak.
- Bilgi sistemleri ya da altyapı ile ilişkili bilgi güvenliği olaylarını gözden geçirmek ve bir önleyici faaliyet planının gerçekleştirildiğini ve bu planının belirlenen gereksinimleri karşıladığını kontrol etmek.
- Bilgi Güvenliği Politikalarını ve Prosedürlerini ve oluşabilecek değişiklikleri gözden geçirmek ve onaylamak.

- Bilgi güvenliği politika ve prosedürlerindeki bilgi sistemlerindeki ya da altyapıdaki iş ile ilgili tüm istisnai durumları gözden geçirmek ve onaylamak.
- İlgili süreçlerdeki varlıkların, tehditlerden etkilenmemesi için yapılacak değişiklikleri onaylamak iş süreçleri
- üzerinde düşük risk oluşturan bilgi güvenliği politika ve prosedürlerine dair bulguları gözden geçirmek ve onaylamak; orta ve yüksek seviye risk bulguları içi oluşturulan risk tedavi planlarını değerlendirmek ve onaylamak

## 5. BİLGİ GÜVENLİĞİ İHLAL OLAY YÖNETİMİ

### 5.1 Bilgi Güvenliği Olaylarının ve Zayıflıkların Raporlanması

Olay, ENERYA'ya ait olan bilginin ya da bilişim sisteminin gizlilik, bütünlük veya erişilebilirliğinin zarar gördüğü durumun oluşmasıdır. Bu potansiyele sahip ve maddi anlamda çok büyük bir hasara sebep olabilecek istisnai durumlarda yönetimin de sürece dâhil olması gereklidir.

Güvenlik açıkları (bilişim sistemlerinin gizlilik, bütünlük ve erişilebilirliğinin zarar görmesi), bilgi güvenliği ihlaline sebebiyet veren yazılım hataları ve ENERYA'nın güvenlik politikalarının ve prosedürlerinin ihlal edilmesi de bir olay olarak kabul edilir.

Karşılaşılan olaylar, bu olayların zamanında çözülmesi ve gelecekte karşılaşılmaması için gerekli mercilere bildirilir ve önleyici aksiyonlar alınır. Bütün geçici personel ve üçüncü parti sağlayıcılarda bilgi güvenliği olayları prosedürü hakkında farkındalık yaratılılır (güvenlik ihlalleri, tehditler, zafiyetler ve arızaları). Bildirilen bütün olaylar kayıt altına alınır, analiz edilir ve önceden bildirilmiş kriterlere göre sınıflandırılır.

Bilişim sistemleri ve servislerini kullanan bütün çalışanlar, geçici personeller ve üçüncü parti sağlayıcılar güvenlik zayıflıkları ile karşılaştıklarında ya da şüphelendiklerinde bu durumu bildirirler.

### 5.2 Yetkililer ile İletişime Geçilmesi

İhtiyaç duyulması durumunda yetkili makamlardan uygun kişiler ile irtibata geçilir.

### 5.3 Bilgi Güvenliği Olaylarının Yönetimi ve İyileştirilmesi

Bilgi güvenliği olaylarına hızlı, etkin ve düzgün yanıt sağlanması için yönetim sorumlulukları ve gerekli prosedürler, oluşturulur. Bilgi güvenliği olaylarının sonucunda olayların tekrarını engelleyecek öğrenimleri sağlayan mekanizmalar oluşturulur. Olaylardan kaynaklanan etkinin derecesi ve maliyeti ölçülür ve izlenir. Bir kişi ya da ENERYA'nın bilgi güvenliği olaylarından kanuni bir işleme (sivil ya da cezai) tabi tutulması durumlarına karşı, olay ile ilgili kanıtlar kurallara uygun bir şekilde tutulup saklanır.

Bilgi güvenliği politika ve prosedürlerinin ihlali durumunda ENERYA çalışanları ENERYA Personel Yönetmeliği'nde yer alan disiplin hükümlerine tabidirler.