



BİLGİ GÜVENLİĞİ YÖNETİM YAKLAŞIMI

Politika Onay Tarihi: 23.02.2021

BİLGİ GÜVENLİĞİ YÖNETİM POLİTİKASI

Enerjisa Enerji her türlü yöntemle topladığı ve işlediği, kendine ve paydaşlarına ait tüm bilgileri kritik varlıklar olarak kabul eder ve korunması için azami özen ve önem gösterir.

Bu doğrultuda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı referans alınarak, Enerjisa Enerji bünyesinde etkin bir şekilde Kurumsal Bilgi Güvenliği Yönetim Sistemi uygulanır.

Kurumsal bilgi güvenliğinin temel amacı, Enerjisa Enerji tarafından toplanan ve işlenen her tür bilginin gizlilik, bütünlük ve kullanılabilirliğinin sağlanmasıdır. Enerjisa Enerji'nin kurumsal faaliyetlerinin doğası gereği, oluşabilecek, Enerjisa ve paydaşlarını etkileyebilecek maddi ve manevi zararların önlenmesi, olduğu takdirde erken tespit edilmesi ve olası etkilerinin asgari düzeye indirilmesi konusunda gereken süreçlerin tasarlanması, işletilmesi, izlenmesi ve sürekli geliştirilerek önlem alınması kurumsal bilgi güvenliğinin ana hedefidir.

Pozisyonları veya görevlerinden bağımsız olarak tüm Enerjisa Enerji çalışanları ve ilgili üçüncü taraflar, Enerjisa Enerji'nin bilgi güvenliği ile ilgili uygulamalarına, politika ve prosedürlerine riayet eder. Kurumsal bilgi güvenliği politika ve prosedürlerinin ihlali disiplin cezası sonucunu doğurabilir ve ilgili mevzuat kapsamında cezai yaptırımlara neden olabilir.

Her birimin yöneticisi, kurumsal bilgi güvenliği politika ve prosedürlerine uyumun sağlanması için kendi sorumluluk alanlarında gerekli her türlü tedbiri almak ve iş faaliyetlerini kontrol etmekten birinci derece sorumludur.

Enerjisa Enerji, kurumsal olarak bilgi güvenliği ile ilgili uygulanabilir şartları karşılayacağını, Enerjisa Enerji'nin uymakla mükellef olduğu her türlü mevzuat, kanun, tebliğ ve benzeri düzenlemelere uyumluluğu sağlayacağını, sürdürdüğü Bilgi Güvenliği Yönetim Sistemi'ni sürekli olarak iyileştireceğini taahhüt eder.

BİLGİ GÜVENLİĞİ YÖNETİM YAKLAŞIMI

1.Kapsam

Enerjisa Enerji Bilgi Güvenliği Yönetim Yaklaşımının oluşturulmasında bilgi güvenliği politikası esas alınmıştır. Enerjisa Enerji Bilgi Güvenliği Yönetim Yaklaşımının kapsamı Enerjisa Enerji A.Ş.'yi, şirketin elektrik dağıtım şirketlerini (İstanbul Anadolu Yakası Elektrik Dağıtım A.Ş., Başkent Elektrik Dağıtım A.Ş., Toroslar Elektrik Dağıtım A.Ş.), görevli tedarik şirketlerini (Enerjisa İstanbul Anadolu Yakası Elektrik Perakende Satış A.Ş., Enerjisa Başkent Elektrik Perakende Satış A.Ş., Enerjisa Toroslar Elektrik Perakende Satış A.Ş.) ve Enerjisa Müşteri Çözümleri A.Ş.'yi (bundan böyle hepsi birlikte Enerjisa Enerji olarak anılacaktır) içermektedir.

2.Veri Güvenliği

- Enerjisa Enerji bünyesinde Bilgi Teknolojileri ve Dijital İş Yönetimi Bölüm Başkanlığı altında yer almakta olan Siber Güvenlik Grup Müdürlüğü; iş ihtiyaçları, yasalar ve yasal düzenlemelerle ilgili beklentileri karşılamak amacıyla tespit edilen bilgi güvenliği gerekliliklerini değerlendirir ve karşılar. Enerjisa Enerji yönetimi bilgi güvenliği gerekliliklerinin yerine getirilebilmesi için gerekli desteği ve atamaları gerçekleştirir.

- Enerjisa Enerji ilgili yasal mevzuatlar çerçevesinde müşteri bilgilerinin gizliliğini ve güvenliğini en üst seviyede sağlamak konusunda gerekli tedbirleri almakta ve bu doğrultuda şirket politikaların belirlediği tedbir ve aksiyonları uygulamaktadır.
- Enerjisa Enerji’de verinin en büyük değerlerden biri olması sebebiyle verinin gizliliği, bütünlüğü ve erişilebilirliği büyük önemi haizdir. Verinin tutulduğu, iletiği depolandığı her noktada verinin güvenliğini tesis etmek için gerekli kontroller uygulanır ve verilerin sadece iş amacı doğrultusunda gerekli kişiler tarafından erişilebilirliği sağlanır.
- Enerjisa Enerji web sitesinde bulunan bilgi, materyal ve bunların düzenlenmesi konusundaki telif hakları, Enerjisa Enerji’ye aittir. Enerjisa Enerji web sitesinde yer alan üçüncü şahıslara ait materyaller dışında kalan bilgi ve materyallere dair tüm telif hakları, tescilli marka, patent, entelektüel ve diğer mülkiyet hakları Enerjisa Enerji’da saklıdır.
- Bilgi güvenliği yönetim sistemi, tanımlı bir risk yönetim yaklaşımı ile en iyi uygulamalara dayanan temel kuralların belirlendiği bilgi güvenliği politikaları, prosedürleri, talimatları ve diğer dokümantasyon ile sağlanmaktadır. İlgili dokümantasyon, tüm Enerjisa Enerji çalışanlarının erişebileceği şekilde şirket Doküman Yönetim Sistemi üzerinde paylaşılmıştır. Bilgi güvenliği dokümantasyonunun amacı, bilgi güvenliği risklerinin yönetilmesi ve verinin yeterli seviyede güvenliğinin sağlanmasıdır. Tüm Enerjisa Enerji personeli, sorumlusu oldukları iş süreçleri ve bilgi varlıklarında bu politikalarda yazan kuralların uygulanmasından sorumludur.

3. Kişisel Verilerin Korunması Kanunu (KVKK)

- Enerjisa Enerji faaliyetlerini gerçekleştirebilmek ve hizmetlerinin kesintisiz ilerleyebilmesini sağlamak adına, Genel Müdürlük, bölge ofisleri, müşteriler, bayiler, internet sitesi, çağrı merkezi gibi kanallardan; sözlü, yazılı ya da elektronik ortam üzerinden müşterinin rızası ile (Kişisel Verilerin Korunması Kanunu (KVKK) 5. Maddesi kapsamındaki istisnalar hariç) temin edebildiği kişisel verileri, Veri Sorumlusu sıfatıyla, hukuka uygun bir biçimde işlemektedir.
- İş birimleri tarafından gerekli çalışmaların yapılması amacıyla işlenen kişisel veriler, Enerjisa Enerji’nin kullandığı elektronik sistemler ve fiziksel ortamlarda güvenle saklanır.
- Veri sahipleri söz konusu veri işleme faaliyetleri hakkında çeşitli kanallarımız aracılığıyla, işleme amaçları, alınan güvenlik önlemleri, veri sahibinin hakları ve başvuru kanalları hakkında aydınlatma metinleri ile bilgilendirilmektedir. Hukuka uygun bir veri işlemenin sağlanması için bu açıklamanın veri sahibine veri işlenmeden önce yapılması ve KVKK uyarınca istisna kapsamında değilse açık rızasının alınması gerekmektedir.
- Enerjisa Enerji, kişisel verilerin gizliliğini ve güvenliğini korumaya önem verir. Bu doğrultuda, kişisel verilerin korunmasına yönelik politika ve prosedürleri oluşturur, günceller ve kişisel verileri yetkisiz erişim, zarar, kayıp veya ifşaya karşı korumak için ilgili mevzuatla uyumlu, gerekli ve uygun teknik ve idari güvenlik önlemleri alır.
- Enerjisa web sitesi üzerinden ürün ve hizmet satışı/başvurusu için talep edilen veya Enerjisa Enerji sisteminde var olan ve müşterilere ait her türlü kişisel bilgi, müşteri rızası olmadan 3. kişilerle hiçbir şekilde paylaşılmamaktadır (KVKK’nın 5. Maddesi uyarınca rıza gerektirmeyen veri

transferleri hariç). KVKK'nın 5. Maddesi uyarınca rıza gerekip gerekmediğine ilişkin incelemeyi Hukuk Regülasyon ekibi tarafından yerine getirilmektedir.

- Enerjisa Enerji müşterilerinin web sitesi üzerinden girmiş oldukları bilgilere 3. tarafların erişimi engellenmiştir. Müşterilerin kişisel bilgilerinin gizliliğini korumak amacıyla Enerjisa Enerji sistem ve erişim alt yapısı en güvenilir seviyede tutularak gerekli önlemler alınmıştır.
- Kullanım amacı sonlanan ve yasal saklama süresi sona eren kişisel veriler, KVKK'nın 7. maddesi uyarınca Enerjisa Enerji tarafından silinmekte, yok edilmekte veya anonim hale getirilmektedir.
- Enerjisa Enerji, gerekli gördüğü durumlarda farklı kuruluşlardan destek hizmeti almakta ve ilgili kuruluşların Enerjisa Enerji'nin gizlilik standartlarına ve şartlarına uygun hareket etmesini sağlamaktadır. Enerjisa Enerji, sözleşme düzenlediği veri işleyenlerin bilgi güvenliğine en az kendisi kadar önem verdiklerinden ve müşterek sorumluluğun bilinciyle hareket ettiklerinden emin olmakta ve bunu sözleşmesel olarak da güvenceye almaktadır. Veri işleyenler, mevzuattaki tanım ile paralel olarak yalnız Enerjisa Enerji'nin talimatları doğrultusunda, Enerjisa Enerji ile akdedilmiş sözleşme çerçevesinde kalmak suretiyle ve mevzuata uygun olarak kişisel verileri işler.
- KVKK'nın 11. Maddesi kapsamında kişisel verileri işlenen gerçek kişilerin hakları düzenlenmektedir ve bu madde uyarınca veri sahipleri Enerjisa Enerji üzerinde aşağıdaki haklara sahiptir:
 - i. Kişisel verilerin işlenip işlenmediğini öğrenme,
 - ii. Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
 - iii. Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
 - iv. Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
 - v. Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,
 - vi. KVKK'nın 7. Maddesinde öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme,
 - vii. Gerçekleştirilen işlemlerin (eksik ve yanlış bilgilerin düzeltilmesi talebi, kişisel verilerin silinmesi veya yok edilmesi talebi) kişisel verilerin aktarıldığı üçüncü taraflara bildirilmesini isteme,
 - viii. İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
 - ix. Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme.

Veri sahipleri tarafından bu madde kapsamında yapılan başvurular, sistem kayıtları ve müşteri belgeleri incelenerek yasal süresi içinde cevaplandırılır.

Enerjisa Enerji bu yasal uyarıda yer alan koşulları ve hükümleri, önceden bir ihbara gerek kalmaksızın değiştirme ve güncelleme hakkına sahiptir.

4.Bilgi Güvenliđi Olay Yönetimi

Enerjisa Enerji bünyesinde Siber Güvenlik Grup Müdürlüğü içerisinde Siber Olaylara Müdahale Ekibi bulunmaktadır. Enerjisa Enerji iş süreçlerinin normal çalışma düzenini bozucu, bilişim veya endüstriyel kontrol sistemlerinin bir kısmına veya tamamına negatif olarak etki eden yazılım, donanım ve insan kaynaklı her türlü durum bilgi güvenliđi olayı olarak tanımlanmaktadır. Zararlı yazılımlar, ortalama (phishing) saldırıları, yetkisiz erişimler, siber ataklar, verinin dışarı çıkartılması gibi süreçler bilgi güvenliđi olay yönetim süreci kapsamında incelenmektedir. Bilişim güvenliđi endüstrisi içerisinde başarılı olduđu kabul edilen izleme ve tespit araçları kullanılarak Enerjisa Enerji'nin uygulama, sistem ve erişim bileşenleri sürekli olarak izlenmektedir. Bu izleme kapsamında karşılaşılan olayların değerlendirilmesi, aksiyon alınması ve dođru şekilde kapatılması sağlanmaktadır.

Siber Güvenlik Grup Müdürlüğü tarafından dünyadaki teknolojik gelişmeler ve zafiyetler siber istihbarat servisleri üzerinden takip edilmektedir. Yılda bir kez bağımsız ekiplerce sızma testleri gerçekleştirilmekte, güvenli uygulama geliştirme hayat döngüsü işletilerek Enerjisa Enerji'ya ait uygulama ve servislerin güvenliđi sağlanmakta, ek olarak zafiyet taramaları, kaynak kod analizleri ve olgunluk değerlendirmeleri yapılmaktadır. Bu çalışmalar sonrası tespit edilen eksiklikler Siber Güvenlik Grup Müdürlüğü personeline incelenmekte, takip edilmekte ve aksiyonlar alınarak kapatılmaktadır.

Enerjisa Enerji personelinin veya ilişkili olabilecek dışkaynak / danışman personellerinin bilgi güvenliđi olayı ile veya olaya sebebiyet verebilecek bir zafiyet ile karşılaşması durumunda bildirimlerini hangi kanallardan yapacağı hakkında gerekli bilgilendirmeler yapılmıştır ve belirli aralıklarla hatırlatmalar da sağlanmaktadır. Bildirimler sonrası alınacak aksiyonlar için süreç dokümanı periyodik olarak gözden geçirilmekte ve uygulanmaktadır. Ayrıca, tedarikçiler ile imzalanan Bilgi Güvenliđi Taahhütname dokümanı içerisinde de bilgi güvenliđi olayının fark edilmesi durumunda Enerjisa Enerji ile iletişime geçmeleri gerektiđi madde olarak da eklenmiştir.

5.Bilgi Güvenliđi Farkındalıđı

Enerjisa Enerji bünyesinde verinin ve veri güvenliđinin büyük önem arz etmesi sebebiyle bilgi güvenliđi farkındalıđının artırılması amacıyla eğitimler gerçekleştirilmektedir. Enerjisa Enerji bünyesinde farkındalıđın artırılabilmesi ve kurum içerisinde bütünsel bir yaklaşım sergilenebilmesi amacıyla eğitimlerin tamamlanma oranı üst yönetim tarafından takip edilmektedir.

Yıl içinde belirli aralıklarla Siber Güvenlik Grup Müdürlüğü tarafından ortalama (phishing) saldırıları örnekleri yapılarak sonuçlar değerlendirilmekte ve üst yönetime raporlanmaktadır. İki haftada bir bütün personele Siber Güvenlik Bülteni hazırlanıp gönderilmekte ve dünyadan siber güvenlik haberleri paylaşılmaktadır. Yine iki haftada bir farkındalık e-eğitimi personel ile paylaşılmaktadır. Farkındalık kapsamında temiz masa – temiz ekran politikaları uygulanmakta, ofis içi poster ve afişlerle politikalar hatırlatılmaktadır.

Her personelin bilgi güvenliđi taahhütnamesini imzalaması sağlanmakta ve bilgi güvenliđi hususlarının bütün personelin sorumluluđu olduđu bildirilmektedir.

6.Lisanslar ve Sertifikalar

Enerjisa Enerji ana şirketi ve dağıtım ve perakende tüzel kişiliklerinin bilgi güvenliđi ve sistemleri alanında sahip olduđu lisans ve sertifikalar aşağıdaki gibidir.

- Enerjisa Enerji (ana şirket, dağıtım ve perakende tüzel kişilikleri) ISO27001 Bilgi Güvenliđi Yönetim Sistemi Standardına sahiptir.

- Enerjisa dağıtım ve perakende tzel kiřilikleri ISO20000 Bilgi Teknolojileri Hizmet Ynetimi Standardı lisansına sahiptir.
- Enerjisa perakende tzel kiřilikleri ise ISO22301 İř Sreklilięi Ynetim Sistemi sertifikasına sahiptir.

Ek olarak Enerji Piyasası Dzenleme Kurulu dolayısıyla tabi olunan Elektrik Lisans Ynetmelięi, EKS Biliřim Gvenlięi Ynetmelięi, Elektrik Daęıtım ve Satıř Çaęrı Merkezi Hizmet Kalite Standartlarına İliřkin Usul ve Esaslar, EKS Gvenlik Analiz ve Test Usul ve Esasları'na uygunluklar ile Cumhurbaşkanlıęı Dijital Dnřm Ofisi Bilgi ve İletiřim Gvenlięi Rehberi uyumlulukları dzenli olarak Siber Gvenlik Grup Mdrlęnce kontrol edilmektedir.

7.nc Taraf Bilgi Gvenlięi

Enerjisa Enerji tarafından saęlanan hizmetlerin devamlılıęını ve kalitesini saęlamak amacıyla nc taraf firmalarla alıřılması durumunda szleřmelerde gizlilik maddelerine yer verilmektedir. nc taraflarla szleřmede yer alan iř gereęi veri paylařımı yapılacak olması durumunda sadece gerektięi kadar veri paylařımı yapılmaktadır. Verilerin gvenli aktarımına iliřkin onay sreleri de devreye alınır ve iřin gerektirdięinden daha fazla verinin aktarılmamasını saęlar. Sistemlerde bu tr verilerin korunması iin sistemlerde ve uygulamalarda uluslararası standartlara uygun gvenlik nlemleri alınmaktadır. Yıllık plan doęrultusunda belirlenen kriterlere gre kritik tedarikilerin bilgi gvenlięi kapsamında deęerlendirmeleri yapılır. Deęerlendirmelere ait sonularda grlen eksikliklerin kapatılmasına dair aksiyonlar Siber Gvenlik Grup Mdrlę tarafından takip edilmektedir.