EVRENCİK RÜZGAR ENERJİSİNDEN ELEKTRİK ÜRETİM A.Ş.

Doküman No: BGYS.PL.00

Doküman Adı: BGYS Politikası

İlk Yayın Tarihi: 10.01.2023

HİZMETE ÖZEL

** Sadece kurum çalışanlarının görebileceği, kurum dışı kişilerin görmemesi gereken dokümanlar bu sınıfta yer alır.*

*** Elektronik Nüsha, Çıktısı Kontrolsüz Dokumandır.*

ISO REFERANSLARI

ISO27001 Referans Madde Numarası
5.1 - Liderlik ve bağlılık
5.2 - Politika
A.5.1.1 - Bilgi güvenliği için politikalar
A.5.1.2 - Bilgi güvenliği için politikaların gözden geçirilmesi

REVİZYON KAYITLARI

Sıra No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Hazırlayan	Onaylayan

İçindekiler

1. Amaç

Bu doküman, Kuruluştaki ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kapsamındaki tüm bilgi varlıklarının güvenliğinin sağlanması, BGYS'nin kurulması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi için yönetimin desteğinin belirtildiği, BGYS'nin politika ve prosedürlerine uygun davranılmaması sonucunda oluşacak yaptırımların tanımlanması amacıyla oluşturulmuş, kapsam dahilindeki tüm personelin gereğini yerine getirmesi gereken üst seviye bir dokümandır.

2. Kapsam

Evrencik Rüzgar Enerjisinden Elektrik Üretim A.Ş. Kapsamı "Bilgi Güvenliği Kapsamı" dokümanında belirtilmiştir.

3. Kısaltmalar ve Tanımlar

Kuruluş: Evrencik Rüzgar Enerjisinden Elektrik Üretim A.Ş.

BGYS: Bilgi Güvenliği Yönetim Sistemi

Politika: Bir şirket, Kuruluş veya kişinin görüş, felsefe, amaç ve tutumunun belirli şekilde ifadesini, bu görüş, felsefe veya amaç doğrultusunda bir hareket planını içeren doküman tipidir.

4. Sorumluluk ve Yetki

Görev	Roller
Dokümanın Hazırlanması:	BGYS Yönetim Temsilcisi
Dokümanın Onaylanması:	İşletme Müdürü
Dokümanın Yayınlanması:	BGYS Yönetim Temsilcisi
Dokümanın Revizyonu:	BGYS Yönetim Temsilcisi
Dokümanın Uygulanması:	Tüm Çalışanlar

5. Bilgi Güvenliği Politikası

Bilgi varlıklarımızın gizliliğini, bütünlüğünü ve erişilebilirliğini temin etmek için politikalar oluşturulmuştur.
Varlıkların Kabul edilebilir Kullanımı Politikası, Mobil Cihaz Kullanım Politikası, Uzaktan Erişim ve Çalışma Politikası, Erişim Kontrol Politikası, Parola Politikası, Temiz Masa Temiz Ekran Politikası, Tedarikçi İlişkileri Yönetim Politikası, Kriptografi Politikası olarak oluşturulmuş ve paylaşılmıştır.
BGYS politikaları özet politikamız;

Evrencik Rüzgar Enerjisinden Elektrik Üretim A.Ş. , Bilgi Güvenliği Yönetim Standardı doğrultusunda;

- Kendisi ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişim sağlamayı,
- Bilginin kullanılabilirliğini, bütünlüğünü ve gizliliğini korumayı,
- Kendisinin ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi,
- Kurumun güvenilirliğini ve marka imajını korumayı,
- Bilgi güvenliği ihlali durumunda gerekli görülen yaptırımları uygulamayı,
- Tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, ilgili mevzuat ve standart gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimleri sağlamayı,
- İş/Hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmayı ve işin sürekliliği ve sürdürülebilirliğini sağlamayı,
- Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi,
- Bilgi güvenliği farkındalığını arttırmak amacıyla yetkinlikleri geliştirecek eğitimleri sağlamayı,

taahhüt eder.

ÜST YÖNETİM

Ayrıca BGYS kapsamında oluşturulan diğer alt politikalarda ve prosedürlerde de uyulması gereken kurallar tanımlanmıştır.

8.1. Genel Esaslar

a) Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. Kuruluş çalışanları ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.
b) Bu kural ve prosedürlerin, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.
c) Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001:2013 " Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği Yönetim Sistemleri - Gereksinimler (Information technology - Security techniques - Information Security Management Systems - Requirements) standardını temel alarak yapılandırılır ve işletilir.
d) Kuruluş tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça Kuruluşa aittir.

8.2. Temel BGYS Prensipleri

a) Çalışanlar ve üçüncü taraflarla yapılan sözleşme/iş sözleşmelerinde kuruluşun gizlilik ihtiyaçlarını güvence altına almayı amaçlayan sır saklama taahhütleri bulunur.
b) Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilerek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir.
c) Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.
d) Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.
e) İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.

f) Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.
g) Kuruluşa ait bilgi varlıkları için kuruluş içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
h) Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
i) Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.
j) Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
k) Bilgi güvenliği ihlal olayları ve zayıflıklarının raporlanması için gerekli altyapı oluşturulur. İhlal olay kayıtları tutulur, gerekli düzeltici önleyici faaliyetler uygulanır ve düzenlenen farkındalık eğitimleri vasıtasıyla güvenlik olaylarından öğrenme sağlanır.
l) Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
m) Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.
n) Yönetimin Gözden Geçirmesi toplantıları “Yönetimin Gözden Geçirmesi Prosedürü” ne göre yapılır.

8.3. Uyulması Gereken Kabul Edilebilir Kullanım Kuralları

Uyulması gereken kurallar BGYS Kapsamında hazırlanan politika ve prosedürlerde belirtilmiştir. Tüm kurallar esas olarak “Varlıkların Kabul Edilebilir Kullanımı Politikası” dokümanında yer almaktadır. BGYS kapsamı dâhilinde yer alan tüm çalışanlar ve 3. Taraflar belirtilen kurallara uymak zorundadır.

6. Yaptırım

Kuruluşta BGYS politika ve prosedürlerine uyulmadığının tespit edilmesi halinde, bu ihlalden sorumlu olan çalışan ya da 3. taraf için geçerli olan usul, esas ve sözleşmelerde geçen ilgili maddelerde belirlenen yaptırımlar uygulanır. Cezai yaptırımlarda öncelik hukuki, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere aittir. Tüm cezai şartlar “Yasal Gereksinimlere Uyum ve Kontrol Prosedürü” ‘nde yer almaktadır.

7. Yönetimin Taahhüdü

Kuruluşun belirlediği hedef ve politikaları gerçekleştirmek için Kuruluş, Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001:2013’de belirtilen gereksinimleri yerine getirecek şekilde kurarak yürütür.

Kuruluş Üst Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder. Bu taahhüdün sonucu olarak, Kuruluş genelinde bilgi güvenliği farkındalık programları düzenler ve alt yapı yatırımlarını sürdürür.

BGYS Yönetim temsilcisi değiştiğinde veya işten ayrıldığında, Kuruluşun Üst Yönetimi tarafından doküman revize edilerek atama tekrar yapılır.

Kuruluş Üst Yönetimi, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturulmasından sorumludur.

8. Üçüncü tarafların yönetimi

Kuruluş çalışanı olmayıp bilgi sistemleri kaynaklarına erişim sağlayan her türlü kişi 3. Taraf olarak kabul edilir. 3. Tarafların uyması gereken kurallar ve yönetim şekli BGYS kapsamlı dokümanlarda 3. Taraf olarak ayrıca belirtilmiştir. 3. Taraf tanımına uyan her türlü kişi ya da Kuruluşla yapılacak geçici ya da sürekli çalışma sözleşmelerin imzalanması ile düzenli olarak takip edilir. Sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları hazırlanıp Kuruluşlarla Kurumsal gizlilik sözleşmesi, 3. Taraf çalışanlarıyla bireysel gizlilik sözleşmesi yapılır. Gerektiği takdirde üçüncü taraf çalışanlarının politikaya uyması için süre tahsis edilir.

9. Bilgi Güvenliği Politika Dokümanı Güncellenmesi ve Gözden Geçirilmesi

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden Yönetim Temsilcisi sorumludur. Bilgi Güvenliği Politikası Dokümanı, en az yılda bir kez gözden geçirilir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilir ve herhangi bir değişiklik gerekiyorsa versiyon değişimi olarak kayıt altına alınır ve her versiyon onaylatılır. Her versiyon değişikliği ortak klasör üzerinden yayımlanır ve yönetim temsilcisi tarafından kapsamdaki tüm kullanıcılara duyurulur.

Gözden geçirmelerde;

a) Politikanın etkinliği, kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenir.
b) Politikanın güncelliği, teknolojik değişimlerin etkisi vasıtasıyla gözlemlenir.
c) Bilgi Güvenliği Politikası organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından gözlemlenir.
d) Politika, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilir.

10. İlgili Dokümanlar

13.1. İç Kaynaklı Dokümanlar

Risk Analizi ve Risk İşleme Planı
Risk Yönetim Prosedürü
Varlıkların Kabul Edilebilir Kullanımı Politikası
Yönetimin Gözden Geçirmesi Prosedürü
Yasal Gereksinimlere Uyum ve Kontrol Prosedürü
İş Sürekliliği Planı

Roller, Sorumluluklar Ve İletişim Dokümanı

13.2. Dış Kaynaklı Dokümanlar

- TS ISO/IEC 27001:2013 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği Yönetim Sistemleri

Evrencik Rüzgar Enerjisinden Elektrik Üretim A.Ş. olarak, “Bilgi Güvenliği Politikası” ‘nın kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederiz.

Yönetim Temsilcisi İşletme Müdürü