MADDE 1. AMAÇ

1.1. Beta Enerji ve Teknoloji A.Ş. (bundan sonra "Şirket" olarak anılacaktır), bilgi güvenliğinin sağlanması, yönetilmesi, takip edilmesi, gözden geçirilmesi, sistemlerin bakımı ve sürekli geliştirilmesi için gereken mekanizmaları kurmayı ve iyileştirmeyi taahhüt eder. Bu doğrultuda, Şirket bünyesinde, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı referans alınarak, Kurumsal Bilgi Güvenliği Yönetim Sistemi uygulanır. Şirket, kurumsal olarak bilgi güvenliği ile ilgili uygulanabilir küresel standartları karşılamayı, bu konudaki her türlü mevzuat ve düzenlemelere yüzde yüz uymayı, Kurumsal Bilgi Güvenliği Yönetim Sistemimizi sürekli olarak iyileştirmeyi ve geliştirmeyi taahhüt eder. Bu politikanın amacı, Şirketin bilgi güvenliğinin kapsamını, ilkelerini, performans kriterleri ve hedefleriyle Kurumsal Bilgi Güvenliği Sistemi'nin takibi ve sürekli iyileştirmesi için gereken mekanizmaları tanımlamaktır.

MADDE 2. TANIMLAR

2.1. Bu bölümde politikada geçen özel terim ve kavramlar aşağıdaki şekilde kısaca açıklanmaktadır.

Şirket: Beta Enerji ve Teknoloji A.Ş.

Politika: Bilgi Güvenliği Politikası

Çalışan: Şirket yöneticilerini ve çalışanlarını ifade eder.

MADDE 3. KAPSAM

3.1. Bu politika;

a) Şirket Yönetim Kurulu üyelerini,
b) Şirket Çalışanlarını,
c) Mal ve hizmet alınan firmaları ve çalışanlarını,
d) Danışmanlar, avukatlar, müşavirler ve dış denetçiler de dâhil olmak üzere Şirket adına görev yapan kişi ve kuruluşlar ile ticari ilişki içinde olduğu müşterileri de dâhil olmak üzere diğer kişileri ("**İş Ortakları**")

kapsar.

Bilgi güvenliği politikasının uygulanmasından Şirket yönetimi ve tüm departman yöneticileri sorumludur. 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.

Şirket yönetimi bilgi güvenliği politikasının uygulanması, Kurumsal Bilgi Güvenliği Sisteminin kurulması ve geliştirilmesi gibi hususlarda IT departmanından destek alır.

MADDE 4. İLKE VE ESASLAR

4.1. Bilgi Güvenliği Taahhüdü

4.1.1. Şirket, müşteri ve paydaşlara sunulan ürün ve hizmetlerin güvenliğini sağlamaya büyük önem verir. Bilgi güvenliği politikasına uygun olarak tüm faaliyetlerini yürütmeyi taahhüt eder.

4.2. Yasalara ve Bilgi Güvenliği Standartlarına Uygunluk

4.2.1. Şirket ve çalışanları, bilgi güvenliği ile ilgili tüm yasal mevzuata ve düzenlemelere tam uyum sağlar.

4.3. Risk Yönetimi ve Bilgi Güvenliği Tedbirleri

4.3.1. Şirket, bilgi varlıklarının güvenliği, gizliliği, bütünlüğü, erişilebilirliği ve sürekliliğini sağlamak için sistematik risk yönetimini benimser ve gerekli tedbirleri alır.

4.4. Bilgi Güvenliği Farkındalığının Artırılması

4.4.1. Tüm çalışanlara teknik ve davranışsal yetkinlikleri geliştirici eğitimler verilir ve bu eğitimler mevzuat değişiklikleri ve güncel gelişmeler doğrultusunda sürekli olarak güncellenir.

4.5. Bilgi Güvenliği Politikaları ve Kontrolleri

4.5.1. Şirket, bilgi güvenliği politikalarına bağlı olarak alt prosedürler ve iç kontrol mekanizmaları oluşturulur, yayınlanır ve uygulanmaları denetlenir.

4.6. Bilgi Güvenliği Hedefleri ve Sürekli İyileştirme

4.6.1. Şirket, bilgi güvenliği hedeflerini belirler ve bu hedeflerin uyumluluğunu düzenli olarak ölçerek sürekli iyileştirme fırsatlarını değerlendirir.

4.7. Yasal Düzenlemeler ve Sözleşmelere Uygunluk

4.7.1. Şirket ve çalışanları, bilgi güvenliği politikalarına ve Bilgi Güvenliği Yönetim Sistemi standartlarına uygun olarak yasal düzenlemelere, şirket taahhütlerine ve sözleşmelere tam uyum sağlar.

4.8. Bilgi Güvenliği Sisteminin Sürekli Geliştirilmesi

4.8.1. Bilgi Güvenliği Yönetim Sistemini sürekli iyileştirmek ve geliştirmek için gerekli mekanizmalar kurulur; yenilikler ve teknolojik gelişmeler takip edilerek sistemde güncellemeler ve geliştirmeler yapılır.

4.9. Bilgi Güvenliği Politikalarına Uyum ve Disiplin

4.9.1. Bilgi güvenliği politika ve prosedürlerinin ihlali disiplin cezası sonucunu doğurabilir ve ilgili mevzuat kapsamında cezai yaptırımlara neden olabilir.

MADDE 5. GÖREV VE SORUMLULUKLAR

5.1. Yönetim Kurulu

5.1.1. Politikada yer alan ilke ve esasların uygulanmasından ve bu ilke ve esaslara aykırı olan ihlal ve şüpheli durumlarda bildirim, inceleme ve yaptırım mekanizmalarının belirlenmesi ve işletmesinin üst gözetiminden Yönetim Kurulu ve ona bağlı olarak çalışan Denetim Komitesi sorumludur.

5.2. Dijital Dönüşüm ve Veri Analitiği Direktörlüğü

5.2.1. Dijital Dönüşüm ve Veri Analitiği Direktörlüğü, Politikada yer alan ilke ve esaslara aykırı olan ihlal ve şüpheli durumların tespiti halinde ilgili mevzuat hükümlerine uygun olarak, Disiplin Cezası ile sonuçlanabilecek durumlar hakkında objektif değerlendirmeler yapar.

5.2.2 Dijital Dönüşüm ve Veri Analitiği Direktörlüğü, Politikaya uygun davranmayan:

5.2.2.1. Çalışandan savunma almaya, soruşturma başlatmaya, iş sözleşmesini askıya almaya, iş sözleşmesini feshetmeye ve İş Kanunu ve yürürlükteki mevzuat uyarınca haklarını kullanma hak ve yetkisine sahiptir.

5.2.2.2. Uygun davranmayan danışman, avukat ve finansal uzmanlarından hizmet almayı durdurma ve hizmet sözleşmelerini sona erdirme hakkına sahiptir.

5.2.2.3. Uygun davranmayan iş ortakları ile arasındaki ticari iş ilişkilerini durdurma, askıya alma ve sona erdirme hak ve yetkisine sahiptir.

5.3. Çalışanlar

5.3.1. Çalışanlar, Genel Müdür tarafından belirlenen politikalara uyum sağlanması, iç ve dış mevzuata uyumlu çalışılması ve Politikaya aykırı bir davranış, tutum, işlem, eylem, karar, faaliyet ya da uygulama ile karşılaşılması durumunda Dijital Dönüşüm ve Veri Analitiği Direktörlüğü'ne bildirim yapılması ile sorumludur.

E-posta: etikhat@betaenerji.com
Adres: Hacı Sabancı Organize Sanayi Bölgesi Çanakkale Cd. No:11 / B Sarıçam ADANA / Türkiye

MADDE 6. YÜRÜRLÜK

6.1. İşbu Politika 04.04.2025 tarihli Yönetim Kurulu Kararıyla yürürlüğe konmuştur. İşbu Politika yeni bir duyuru yapılana kadar geçerli ve yürürlükte kalacaktır.

MADDE 7. GÖZDEN GEÇİRME

7.1. İşbu Politika yılda bir defa düzenli olarak, süreç veya teknik altyapı değişiklikleri ile ilgili kontroller temel alınarak Bilgi İşlem Yöneticisi tarafından gözden geçirilir. Gözden geçirilen ve güncellenen bu politika Yönetim Kurulu tarafından onaylanır.

MADDE 8. İLGİLİ POLİTİKA VE PROSEDÜRLER

Bilgi Güvenliği Prosedürü