

GALATA WIND ENERJİ A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Galata Wind Enerji A.Ş. ("**Galata Wind**" ve/veya "**Şirket**") olarak, bilgi güvenliğini iş sürekliliği kapsamında stratejik bir öncelik olarak ele alıyor ve tüm faaliyetlerimizi kapsayacak biçimde "güvenilir, etkili ve uyumlu" bir bilgi yönetimi sistemi oluşturmayı taahhüt ediyoruz. Bu politika, şirketimizin iş sürekliliğini sağlamak, yasal ve düzenleyici gerekliliklere uymak, siber güvenlik tehditlerine karşı koruma sağlamak ve paydaş güvenliğini artırmak amacıyla oluşturulmuştur.

2. Kapsam

Bu Politika; Galata Wind'in tüm çalışanlarını, iş ortaklarını, tedarikçilerini, hizmet sağlayıcılarını ve şirket ağlarına erişen tüm tarafları kapsar. Galata Wind tarafından kullanılan, işlenen veya saklanan tüm bilgi varlıkları, sistemler ve dijital platformlar bu politikanın kapsamı içinde ele alınır.

3. Tanımlar ve Kavramlar

Bilgi güvenliği politikamızın çerçevesini bu politikanın ilgili taraflarının tamamı için netleştirmek adına, temel kavramlar aşağıda tanımlanmıştır:

Üst Yönetim: Galata Wind'in stratejik yönünü belirleyen, organizasyonun genel politika ve hedeflerinden sorumlu olan karar verici kadrodur. Üst yönetim, genellikle CEO (İcra Kurulu Başkanı), İcra Kurulu Üyeleri ve doğrudan CEO'ya bağlı çalışan yöneticilerden oluşur. Bilgi güvenliği özelinde, üst yönetim; bilgi güvenliği politikasının onaylanması, uygulanmasının gözetilmesi, gerekli kaynakların sağlanması, hedeflerin belirlenmesi ve sistematik iyileştirme süreçlerinin yürütülmesinden sorumlu olarak belirlenen yöneticileri de ifade eder.

Bilgi (Information): Galata Wind'in operasyonlarını, stratejik planlarını, finansal verilerini, müşteri ve tedarikçi bilgilerini, çalışan verilerini ve fikri mülkiyet haklarını içeren her türlü yazılı, sözlü, elektronik veya fiziksel ortamda bulunan ticari sır niteliğinde olup olmadığına bakılmaksızın veri ve dokümantasyonu kapsar

Bilgi Varlıkları (Information Assets): Şirketin ticari ve operasyonel süreçlerinde kullandığı her türlü veri, yazılım, sistem, ağ, donanım ve dokümantasyon bilgi varlığı olarak kabul edilir.

Bilgi Güvenliği (Information Security): Bilginin gizlilik, bütünlük ve erişilebilirlik prensipleri çerçevesinde korunmasını ifade eder. Bu yaklaşım, yetkisiz erişim, değişiklik, kayıp ve yok olma risklerine karşı güvenlik kontrollerini içerir.

Gizlilik (Confidentiality): Bilgilerin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlama prensibidir.

Bütünlük (Integrity): Bilginin doğruluğunu ve güvenilirliğini korumayı, yetkisiz değişiklikleri önlemeyi amaçlar.

GALATA WIND ENERJİ A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

Erişilebilirlik (Availability): Bilginin iş süreçlerinin gerektirdiği şekilde zamanında ve yetkili kişiler tarafından erişilebilir olmasını garanti eder.

Kurumsal Varlık Olarak Bilgi: Galata Wind, bilgiyi stratejik bir kurumsal varlık olarak görür ve şirketin başarısı ve iş sürekliliği için kritik bir unsur olarak değerlendirir. Bu nedenle, bilginin korunması yalnızca bir teknik gereklilik değil, aynı zamanda kurumsal risk yönetiminin bir parçasıdır.

4. Temel İlkeler

Bilgi güvenliği yönetim sistemimiz aşağıdaki amaç ve temel ilkeler doğrultusunda yönetilmektedir:

- **Gizlilik (Confidentiality):** Bilgilerin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlamak.
- **Bütünlük (Integrity):** Bilgilerin doğruluğunu ve güvenilirliğini korumak, yetkisiz değişiklikleri önlemek.
- **Erişilebilirlik (Accessibility):** Bilgilere yetkili kişiler tarafından gerektiğinde erişilebilmesini garanti altına almak.

5. Bilgi Güvenliği Yönetim Modeli

Galata Wind, bilgi güvenliğini **kurumsal risk yönetimi yaklaşımının ayrılmaz bir parçası** olarak ele alır. **Bilgi Güvenliği Yönetim Modeli**, Şirket'in iş sürekliliğini sağlamak, operasyonlarını güvenli bir şekilde yürütmek ve paydaşlarına güvenilir bir enerji altyapısı sunmak amacıyla oluşturulmuştur.

Bu model, bilgi güvenliği politikalarının belirlenmesi, uygulanması, sürekli iyileştirilmesi ve tüm organizasyon genelinde benimsenmesi süreçlerini kapsar. Şirketimiz, bilgi güvenliğini yalnızca teknik bir konu olarak değil, iş stratejimizin temel unsurlarından biri olarak görmektedir.

Bilgi Güvenliği Yönetim Modelimiz aşağıdaki temel unsurlar üzerine kuruludur:

Liderlik ve Taahhüt: Üst yönetimin bilgi güvenliği konusundaki sorumluluğunu ve desteğini içerir.

Risk Yönetimi: Bilgi varlıklarına yönelik tehditlerin belirlenmesi ve kontrol mekanizmalarının uygulanmasının şirketin risk yönetimine entegre edilerek yönetilmesidir.

Bilgi Güvenliği Kültürü: Çalışanlar, iş ortakları ve tedarikçilerin bilgi güvenliği farkındalığının artırılmasıdır.

GALATA WIND ENERJİ A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

Bilgi Güvenliği Ekibi: Galata Wind'in bilgi varlıklarını korumak, siber tehditlere karşı önlem almak, bilgi güvenliği sistemlerini yönetmek ve sürekli iyileştirmekle görevli olan teknik ve yönetsel ekiptir.

Sürekli İyileştirme: Sistematik denetimler ve gözden geçirmeler ile bilgi güvenliği uygulamalarının geliştirilmesidir.

5.1. Liderlik ve Taahhüt

Galata Wind'in üst yönetimi, bilgi güvenliği politikalarının oluşturulması, uygulanması ve sürekli iyileştirilmesi konusunda **aktif bir liderlik sergiler. Bilgi güvenliği, yalnızca Bilgi Teknolojileri departmanları tarafından yönetilen teknik bir detay değil, kurumsal yönetim ve sürdürülebilir iş stratejisi açısından kritik bir konu olarak değerlendirilir.**

Şirketimizin bilgi güvenliği konusundaki liderlik ve taahhüt anlayışı, aşağıdaki ilkeler doğrultusunda şekillenir:

5.1.1. Stratejik Öncelik Olarak Bilgi Güvenliği

- Galata Wind Yönetim Kurulu, **bilgi güvenliğini iş sürekliliğinin ve operasyonel verimliliğin temel unsurlarından biri olarak ele alır.**
- Bilgi güvenliği, **yenilenebilir enerji altyapısının ve dijital operasyonların kesintisiz çalışmasını sağlamak için kritik bir unsur** olarak görülür.
- Siber güvenlik tehditlerine karşı proaktif yaklaşımlar geliştirilerek, şirketin enerji üretim süreçlerine yönelik olası saldırılar minimize edilir.
- Bilgi güvenliği yatırımları, **şirketin genel risk yönetimi ve sürdürülebilirlik politikalarıyla entegre edilir.**

5.1. 2. Kaynak ve Destek Sağlama

- Bilgi güvenliğini desteklemek için **finansal, teknik ve insan kaynağı tahsis edilir.**
- Galata Wind Yönetim ve İcra Kurulu, bilgi güvenliği politikalarının uygulanabilirliğini sağlamak için ilgili bölümlerle koordineli çalışır.
- **Bilgi güvenliği ekipleri, üst yönetim tarafından yetkilendirilerek gerekli kaynaklara erişimleri sağlanır.**
- **Üst Yönetim teknolojik altyapının** güncellenmesi, veri koruma sistemlerinin geliştirilmesi ve çalışanlara yönelik güvenlik eğitimlerinin düzenlenmesi için gerekli desteği verir.

5.1. 3. Şirket Kültüründe Bilgi Güvenliği Farkındalığı

- **Bilgi güvenliği kültürünü güçlendirmek amacıyla** üst yönetim tarafından Şirketin her birimi ile düzenli iletişim kurulur, istek ve hedefler iletilir.
- Çalışanların bilgi güvenliği farkındalığını artırmaya yönelik **eğitimler ve bilinçlendirme kampanyaları teşvik edilir.**

GALATA WIND ENERJİ A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

- Her çalışanın **bilgi güvenliğinden bireysel olarak sorumlu olduğu vurgulanır.**
- **İcra Kurulu Üyeleri ve departman yöneticileri**, ekiplerine bilgi güvenliği standartlarına uygun çalışma kültürünü önemsediklerini belirten hedefler koyar.

5.1. 4. Sorumluluk ve Hesap Verebilirlik

- Üst yönetim, bilgi güvenliği uygulamalarının etkinliğini değerlendirmek ve iyileştirme alanlarını belirlemek amacıyla **düzenli gözden geçirme toplantıları** yapar.
- **Bilgi güvenliğiyle doğrudan bağlantılı konuların yönetimi** konusunda hesap verebilirlik mekanizmaları oluşturulur.
- Üst yönetim, **bilgi güvenliği ihlallerine karşı sıfır tolerans yaklaşımı** benimseyerek, gerekli disiplin süreçlerini takip eder.

5.1. 5. Yasal Süreçler ve Uyum

- Galata Wind, **ISO 27001, KVKK, GDPR (General Data Protection Regulation) ve sektörel düzenlemelere tam uyum sağlamayı taahhüt eder.**
- Bilgi güvenliği süreçleri, **CSRD'nin dijital risk yönetimi beklentileriyle** uyumlu şekilde yönetilir.
- Galata Wind, yasal gereklilikleri takip etmek ve en iyi uygulamaları takip ederek uygulayabilmek amacıyla **dış denetim ve sertifikasyon süreçlerine katılımı teşvik eder.**

5.1.6. Sürekli İyileştirme ve Yenilikçilik

- Bilgi güvenliği sistemlerinin etkinliğini artırmak için **veriye dayalı analizler ve performans ölçümleri yapılır.**
- **Siber Tehdit istihbaratı ve yeni teknolojiler takip edilerek** bilgi güvenliği politikaları sürekli güncellenir.
- **Dijital dönüşüm süreçlerinde güvenlik ilkeleri ön planda tutulur** ve yenilikçi çözümler entegrasyon sürecine dahil edilir.

6. Sorumluluklar

Galata Wind'de bilgi güvenliği, yalnızca bir departmanın veya BT ekibinin sorumluluğunda değil, tüm şirket çalışanlarının ve yöneticilerinin ortak sorumluluğudur.

Üst yönetim, bilgi güvenliği stratejilerini oluşturmak, yönlendirmek ve kaynak sağlamakla yükümlüdür; Bilgi Güvenliği Ekibi bu stratejilerin uygulanmasını, risk değerlendirmelerinin yapılmasını ve güvenlik kontrollerinin sürekli iyileştirilmesini yönetir.

Çalışanlar, bilgi varlıklarının korunması için güvenlik politikalarına uymak, farkındalık eğitimlerine katılmak ve şüpheli faaliyetleri rapor etmekle yükümlüdür.

GALATA WIND ENERJİ A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

Bilgi güvenliği süreçlerinin etkinliğini sağlamak için iç denetimler düzenli olarak gerçekleştirilir. Üçüncü taraf hizmet sağlayıcılar ve iş ortakları da belirlenen güvenlik gerekliliklerine uyum sağlamakla yükümlüdür.

7. Yürürlük

Bu Politika/...../2025 tarih ve 2025/..... sayılı Galata Wind Enerji A.Ş. Yönetim Kurulu kararı ile onaylanmıştır. Gerekli durumlarda yeniden gözden geçirilir ve güncellenir.

8. Ek Prosedürler

Bu politika, Galata Wind'in bilgi güvenliği yönetimi için genel çerçeveyi belirler. Ancak, uygulamaya yönelik detaylar ve operasyonel gereklilikler, ilgili prosedürlerde tanımlanmıştır. Çalışanlar, yükleniciler ve üçüncü taraflar, bilgi güvenliği süreçlerine tam uyum sağlamak için aşağıdaki prosedürlere uygun hareket etmelidir. Güncel prosedürlere Galata Wind intranet sistemi veya Bilgi Güvenliği Departmanı aracılığıyla erişilebilir.

1. Bilgi Güvenliği Risk Yönetimi Prosedürü

2. Erişim Kontrol Prosedürü

3. Veri Sınıflandırma ve Koruma Prosedürü

4. Şifre Yönetimi ve Kimlik Doğrulama Prosedürü

5. Fiziksel Güvenlik ve Veri Merkezi Erişim Prosedürü

6. Bilgi Güvenliği Olay Yönetimi ve İhlal Bildirimi Prosedürü

7. İş Sürekliliği ve Felaket Kurtarma Prosedürü (Disaster Recovery Plan - DRP)

8. Tedarikçi ve Üçüncü Taraf Güvenliği Prosedürü

9. Çalışan Bilgi Güvenliği Farkındalık ve Eğitim Prosedürü

10. Siber Tehdit İstihbaratı ve Proaktif Güvenlik Önlemleri Prosedürü

11. Bulut Güvenliği Prosedürü