BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Şirket Bilgi Güvenliği Politikası, tüm çalışanlara, tedarikçilere, iş ortaklarına ve paydaşlara Şirket'in bilgi güvenliği ihtiyacını, kapsamını, amaçlarını, hedeflerini, ilkelerini ve esaslarını ve bilgi güvenliği ile ilgili rol ve sorumlulukları bildirmek amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika, Şirket bünyesindeki veri ve bilgilerin; bilgi güvenliğinin kapsamını, hedeflerini, ilkelerini, yönetim desteğini, risk yönetimi çerçevesini, sürekliliğini, görev ve sorumlulukları, uyum gereksinimlerini ve ihlali durumunda uygulanacak yaptırımları kapsamaktadır.

3. ROLLER VE SORUMLULUKLAR

Bilgi Güvenliği Politikasının güncelliğinin ve sürekliliğinin sağlanmasından Bilgi Güvenliği Yönetim Temsilcisi sorumludur. Bilgi Güvenliği politikasında yapılacak güncellemeler, Bilgi Güvenliği Yönetim Temsilcisi tarafından dokümana yansıtılır.

İlgili tarafların bu kapsamdaki görev ve sorumlulukları Bilgi Güvenliği Rol ve Sorumluluklar Prosedürü'nde açıklanmıştır.

Tüm birim yöneticileri kendi sorumluluk alanlarına giren sistemlerin sürekli gözden geçirilmesi ve iyileştirmesinden, tüm çalışanlar güncel olan dokümanları kullanmak ve uygulamaktan sorumludur. Bu politika ile çerçevesi belirlenen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, bilgi güvenliği prosedürleri ile düzenlenir. Şirket çalışanları ve üçüncü taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

4. TANIMLAR

BGYS	**:** Bilgi Güvenliği Yönetim Sistemi
KYS	**:** Kalite Yönetim Sistemi
Şirket	**:** Innovate Teknoloji ve Güvenlik Sistemleri TİC. LTD. ŞTİ.
YS	**:** Yönetim sistemi

5. İLGİLİ DOKÜMANLAR / REFERANSLAR

- TS EN ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
- TS EN ISO 9001 Kalite Yönetim Sistemi Standardı
- Ana Doküman Listesi L.01
- PRO.02_Çalışma Düzeni ve Disiplin Prosedürü

6. BİLGİ GÜVENLİĞİ POLİTİKASI

Şirket, tabi olduğu ulusal, uluslararası ve sektörel düzenlemeler doğrultusunda; bilgi güvenliğini sağlamak, ilgili mevzuat ve standartlara uygunluğu sürdürmek ve kurumsal sorumluluklarını yerine getirmek amacıyla aşağıdaki esasları benimser.

- Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayacak altyapı ve kontrolleri uygular.
- Çalışanların bilgi güvenliği farkındalığını artırarak kurum kültürüne entegre eder.
- Kişisel verilerin mahremiyetini koruyacak teknik ve idari tedbirleri alır.
- Görevler ayrılığı prensibi çerçevesinde yetkilendirme ve onay mekanizmaları kurar.
- "Bilmesi gereken" ve "en az yetki" prensiplerine uygun erişim kontrolünü uygular.
- Dış tehditlere karşı ağ güvenliğini sağlar.
- Geliştirme, test ve üretim ortamlarını fiziksel ve mantıksal olarak ayırır.
- Katmanlı güvenlik mimarisi kurar ve sürekliliğini sağlar.
- Hizmetlerin doğrulanabilirliğini teknik yöntemlerle garanti altına alır.
- Şifreleme anahtarlarının güvenliğini temin eder.
- Mobil cihazlarda hassas verilerin güvenliğini sağlar.
- Bilgi güvenliği risklerini periyodik olarak değerlendirir ve aksiyon planları oluşturur.
- Bilgi güvenliği faaliyetlerini entegre bir yapıda yönetmek üzere organizasyon kurar.
- Bilgi varlıklarını tanımlar, sahipliklerini belirler ve risklerini yönetir.
- Bilgi güvenliği olaylarını tespit eder, raporlar ve tekrarını önleyici tedbirler alır.
- Fiziksel ve çevresel güvenlik önlemleriyle bilgiye erişimi kontrol altına alır.
- Sistemlerin edinim, geliştirme ve bakım süreçlerine güvenlik gerekliliklerini dahil eder.
- İş sürekliliği planları ile bilgiye kesintisiz erişimi güvence altına alır.
- Güncel teknolojileri takip ederek güvenlik kontrollerini sürekli iyileştirir.
- İç ve dış denetimlerle BGYS'nin etkinliğini izler, değerlendirir ve geliştirir.

7. BİLGİ GÜVENLİĞİ HEDEFLERİ VE AMAÇLARI

Bilgi Güvenliği Politikası, şirket çalışanlarına, tedarikçilerine, temsilcilerine, iş ortaklarına ve paydaşlarına şirketin güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini artırmak ve bu şekilde şirkette oluşabilecek riskleri minimuma indirmek, şirketin güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, teknik güvenlik kontrollerini uygulamak, şirketin temel ve destekleyici iş faaliyetlerinin minimum kesinti ile devam etmesini sağlamak amacıyla şirketin tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını iç ve dış kasıtlı veya kasıtsız tehditlere karşı korumayı hedefler.

8. BİLGİ GÜVENLİĞİ ORGANİZASYONU

Şirket yönetimi bilgi güvenliği organizasyonunu şirket bünyesinde oluşturur. Bu kapsamda şirkette güvenlik politikalarının bütünsel bir yaklaşım oluşturulması, sürdürülmesi ve yönetilmesine ilişkin çalışmalar Bilgi Güvenliği Yönetim Süreci kapsamında yürütülür. Şirketin güvenlik kontrol süreçlerini koordine edecek, yönetecek rol ve sorumluluklar Bilgi Güvenliği Rol ve Sorumluluklar Prosedürü kapsamında belirlenir.

9. RİSK YÖNETİM ÇERÇEVESİ

Şirketin bilgi güvenliğine ilişkin risk değerlendirme yaklaşımı Bilgi Güvenliği Yönetim Temsilcisi tarafından belirlenir ve Bilgi Güvenliği Yönetim Süreci kapsamında tanımlanır. Bilgi güvenliği risk değerlendirme yaklaşımı ile şirketin bilgi güvenliği risklerinin hangi yöntemler ile belirleneceği, risk seviyelerinin nasıl hesaplanacağı ve risklerin nasıl değerlendirileceği belirlenir. Bilgi varlıklarıyla ilgili oluşabilecek risklerin tanımlanması, derecelendirilmesi, işlenmesi ve gözden geçirilmesi çalışmaları belirlenen risk değerlendirme yaklaşımına uygun olarak gerçekleştirilir

Risk değerlendirme çalışması sonucunda, riskleri azaltmaya yönelik aksiyonları da içeren "Bilgi Sistemleri Risk Değerlendirme Raporu" oluşturulur.

10. POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Bu politikanın ihlali halinde, Çalışma Düzeni ve Disiplin Prosedürü gereğince; uyarma, kınama, maaş kesintisi, yasal otoriterelere bildirim ve sözleşme feshi yaptırımlarından biri ya da birden fazlası uygulanabilir.

11. GÖZDEN GEÇİRME, YAYINLAMA VE DENETİM, RAPORLAMA

Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika Genel Müdür tarafından onaylanır. Onaylanan politika kurumun tüm çalışanlarının eriştiği ortak dosya sunucusu üzerinde yer alan "BGYS" klasöründe yayınlanır.

Bu prosedür, güvenlik anlayışı ile hizmet sunulması faaliyetleri kapsamında Kalite Yönetim Temsilcisi sorumluğunda yılda en az (1) bir defa denetlenir.

Doküman Revizyon Bilgileri		
Yapılan Değişiklik	**Tarih**	**Revizyon No:**
Bilgi Güvenliği Politikası Oluşturulması	25.05.2025	01.0