Trasta ESG Danışmanlık A.Ş.

Bilgi Güvenliği ve Siber Güvenlik Politikası

1.Amaç ve Kapsam

Trasta ESG'nin varlıklarını, müşteri verilerini ve bilgi sistemlerini siber tehditlere karşı korumak için açık ve kapsamlı bir çerçeve oluşturmaktır. Politika bilgi güvenliği ve siber güvenlik gereksinimlerini, önemini ve uygulamasını tanımlama amacıyla yürürlüğe girer. Siber tehditlere karşı güvenli ve dirençli bir altyapı oluşturulması ve sürdürülmesi, kurum ve müşteri bilgilerinin güvenliğinin sağlanması, müşteri güveninin korunması konularında kararlılığını özetlemektedir.

Bu politika, bilgi sistemleri süreçleri ve altyapısını, tüm çalışanları, üçüncü parti tedarikçileri, danışmanları, kurum sistemlerine, verilerine veya teknoloji kaynaklarına erişimi olan tüm paydaşları kapsar. Dış hizmet ve tedarikçilerden alınacak hizmetlerin şirket açısından doğuracağı güvenlik risklerinin değerlendirilmesi ve yönetilmesi süreçlerinde, dış hizmet alınan taraflar sorumludur.

2. Uygulama İlkeleri

Gizlilik: Şirketin iş süreçlerinde yer alan tüm bilgilere yalnızca yetkili kişiler erişebilir, yetkisiz kişilerle paylaşılması yasaktır.

Bütünlük: Tüm veri ve sistemler yanlışlıkla veya kasıtlı olarak değiştirilemez; veri bütünlüğü korunur, veri kaybı ve bozulması önlenir.

Kimlik Doğrulama ve Yetkilendirme: Kullanıcılar yalnızca kendilerine tanımlanan erişim haklarına sahiptir ve kimlik doğrulama süreçlerine uygun hareket eder.

Eğitim ve Farkındalık: Tüm çalışanlara bilgi güvenliği ve siber güvenlik farkındalık eğitimleri düzenli olarak verilir; güvenlik açıkları ve tehditler hakkında bilgilendirme yapılır.

3. Güvenlik Politikaları

Erişim Kontrolü: Kullanıcılar, yalnızca iş fonksiyonlarını yerine getirmek için gerekli olan bilgi ve sistemlere erişim sağlayabilir.

Veri Şifreleme: Hassas veriler, iletim sırasında ve depolandığında şifrelenmelidir.

Şifre Yönetimi: Güçlü şifre politikaları uygulanmalı ve düzenli olarak güncellenmelidir.

Güvenlik Duvarı ve Antivirüs Yazılımları: Tüm sistemler güncel güvenlik duvarı ve antivirüs yazılımları ile korunmalıdır.

Fiziksel Güvenlik: Fiziksel erişim kontrolleri uygulanmalı ve tüm bilgi işlem cihazları uygun şekilde korunmalıdır.

3. Sorumluluklar

Yönetim, bilgi güvenliği ve siber güvenlik alanında gerekli kaynakların temin edilmesi ve güvenlik politikalarının etkin bir şekilde uygulanmasını denetlemekle sorumludur. Bu bağlamda, şirketin güvenlik standartlarını belirler ve bu standartlara uyumun sağlanıp sağlanmadığını sürekli olarak gözlemler. Birim yöneticileri ise kendi departmanlarında güvenlik politikalarının doğru şekilde hayata geçirilmesinden, güvenlik risklerinin doğru bir biçimde değerlendirilmesinden ve çalışanlarının bu konuda düzenli olarak bilgilendirilmesinden sorumludur. Tüm çalışanlar, şirketin belirlediği bilgi güvenliği ve siber güvenlik politikalarına uymak zorundadır; ayrıca herhangi bir güvenlik tehdidi ya da ihlali durumunda derhal raporlama yükümlülüğü taşırlar. Bu güvenlik politikalarına uymayan çalışanlar için disiplin süreçleri uygulanabilir. Teknolojik altyapının güvenliği, sistemlerin güncel tutulması, ağ güvenliği sağlanması ve siber saldırılara karşı alınacak önlemler ve ihlallerin etkisimin minimize edilmesi ise IT departmanının sorumluluğundadır. Şirketle iş birliği yapan üçüncü taraflar, belirlenen güvenlik önlemlerine uymakla yükümlüdür ve şirketle yaptıkları sözleşmeler çerçevesinde güvenlik sorumluluklarını yerine getirmelidirler.

4. Yürürlük

Bu politika, şirket yönetimi tarafından onaylandığı tarihten itibaren yürürlüğe girer ve tüm çalışanlar için bağlayıcıdır. Bu politika, siber tehditlerin evrimi ve düzenleyici gereksinimlerin değişimi ışığında yıllık olarak gözden geçirilecek ve gerektiğinde güncellenecektir. Politikanın uygulama sürecindeki her türlü değişiklik, şirketin güvenlik ihtiyaçlarına göre belirlenecektir.