Smart Güneş Teknolojileri Bilgi Güvenliği Politikası

Smart Güneş Teknolojileri (Smart)olarak, sahip olduğumuz teknolojinin, bilgi birikimimizin ve şirket prestijimizin korunmasının yanı sıra iş operasyonlarımızın devam edebilmesi için bilgi güvenliğinin hem stratejik hem de operasyonel açıdan büyük önem taşıdığının bilincindeyiz. Şirketimiz tarafından elde edilen veya kullanılan bilgi varlıkları, ürün ve hizmetlerimizin geliştirilmesinin ve mükemmelleştirilmesinin temel taşlarıdır. Bu nedenle, bilgi güvenliği tehditlerini gözeterek, kuruluşumuzun bilgi varlıklarını ve sunduğumuz hizmetleri koruyacak, riskler ile alınacak önlemler arasında dengeli bir Bilgi Güvenliği Yönetim Sistemi'nin uygulanması amaçlanmaktadır.

Bu çerçevede Bilgi Güvenliği alanında benimsediğimiz temel ilkeler şunlardır:

• Smart'ın bilgi varlıklarına yalnızca yetkilendirilmiş kişilerin erişiminin mümkün olması, erişilen verinin doğruluğunun ve beklenen süre içinde kullanılabilir olmasının garanti edilmesi,

• Bilişim sistemlerinin yönetiminde, Smart iş süreçleri ve amaçlarına hizmet edecek şekilde bilgi güvenliği ve iş standardizasyonunun sağlanması,

• Çalışanların, iş ortaklarının ve üçüncü tarafların bilgi güvenliği konusunda farkındalıklarının artırılması,

• Smart bünyesinde oluşturulan Bilgi Güvenliği Yönetim Sistemimizin bilgi güvenliği risklerini azaltmaya odaklı bir bakış açısıyla işletilmesi ve sürekli olarak iyileştirilmesi, geliştirilmesi,

• Smart'ın uymakla yükümlü olduğu ulusal ve uluslararası düzenlemelerin yanı sıra ilgili yasal mevzuatın gerekliliklerinin yerine getirilmesi, anlaşmalardan doğan sorumlulukların karşılanması ve kurumsal sorumlulukların gerektirdiği bilgi güvenliği ihtiyaçlarının karşılanması,

• Kişisel verilerin, Avrupa ve Türkiye'deki Kişisel Verilerin Korunması mevzuatına (GDPR ve KVKK) uygun bir şekilde işlenmesi, saklanması, aktarılması ve ilgili bireylerle hukuki ilişkinin sonlanması durumunda da sürecin mevzuata uygun şekilde yönetilmesi,

• Smart bünyesindeki temel ve destekleyici iş faaliyetlerinin kabul edilebilir kesinti süreleri içerisinde sürdürülmesinin temin edilmesi,

• Bilgi güvenliği ihlali olaylarının oluşma ihtimalinin minimize edilmesine yönelik önlemlerin alınması ve ihlal durumunda paydaşlarımızın (çalışanlar, tüketiciler, hissedarlar vb.) olumsuz etkilerden mümkün olan en az derecede etkilenmesini sağlamak için gerekli aksiyonların alınması, güvenlik ihlaline sebep olan kişiler hakkında gerekli yaptırımların icra edilmesi

Bu politika doğrultusunda, bilgi güvenliği ilkelerimize bağlı kalacağımızı, TS ISO/IEC 27001 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi kuracağımızı, bu sistemi işleteceğimizi ve sürdüreceğimizi, gerekli kaynakları ayıracağımızı, Bilgi Güvenliği Yönetim Sistemi'nin etkinliğini değerlendirerek sürekli iyileştirme, geliştime sağlayacağımızı ve bu yaklaşımı tüm ilgili taraflara ileteceğimizi taahhüt ediyoruz.

İşbu Bilgi Güvenliği Politikalası, ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, tüm bilgileri veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden

bağımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve Smart bilgilerine erişim gereği olan üçüncü şahıs hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır.