BİLGİ GÜVENLİĞİ POLİTİKASI

Biotrend Çevre ve Enerji Yatırımları A.Ş. bilgi güvenliği kapsamında gizlilik açısından farklı seviyelerde hassasiyete sahip bilgiler hakkında kurumsal farkındalığı artırmak, farklı hassasiyet seviyelerine sahip bilgiler için uygulanması önerilen mantıksal, fiziksel ve idari kontrolleri belirlemek ve uygulamak; taşınabilir ortamlarda bulunan verilerin saklanma ve imha kurallarını tanımlamak amaçlı bilgi sınıflandırma kılavuzu oluşturulmuştur.

Bilgi Güvenliği ile ilgili uygulamaların gerçekleşmesi, gözden geçirilmesi ve sürekli iyileştirilmesi için aşağıdaki hususları taahhüt ederiz.

- Risk kabul kriterlerini ve riskleri belirlemek, kontrolleri geliştirmek ve uygulamak.
- Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki bilginin gizlilik, bütünlük ve erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi için bilgi güvenliği risk değerlendirme sürecinin uygulanmasını sağlamak, risk sahiplerini belirlemek.
- Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki bilginin gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik çerçeveyi tanımlamak.
- Şirket olarak, kişisel verilerin korunması ve gizliliğini sağlamak, KVKK (Kişisel Verilerin Korunması Kanunu) başta olmak üzere ulusal ve uluslararası mevzuatlara uygun olarak kişisel verilerin işlenmesi, saklanması ve imhası konularında titizlikle hareket etmek.
- Bilgi güvenliği yönetim sistemimizi, kişisel verilerin bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için gerekli tüm teknik ve idari tedbirleri içerecek şekilde detaylandırmak, bu kapsamda, veri sahiplerinin haklarını koruyacak şeffaf süreçler geliştirmek ve bu süreçleri düzenli olarak gözden geçirip iyileştirmek.
- Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek.
- Tabi olduğu ulusal veya sektörel düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.
- Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak.
- Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak.
- Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.
- Kurum itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak.
- Şirket olarak, teknolojik süreçlerimizde ve bilgi güvenliği uygulamalarımızda çevresel sürdürülebilirlik ve iklim değişikliği ile mücadele bilincini entegre etmek.
- Bilgi güvenliği yönetim sistemi kapsamında, enerji tüketimini azaltacak, karbon ayak izimizi minimize edecek ve doğal kaynakları koruyacak çözümleri önceliklendirmek, bu bağlamda, çevresel etkiyi azaltma ve iklim değişikliğiyle mücadele etmek ve böylece hem bilgi güvenliğini sağlamak hem de çevresel sorumluluklarımızı yerine getirmek.