BİLGİ SİSTEMLERİ GÜVENLİK POLİTİKASI

TTL Tütün süreçlerinin tamamında sahip olduğu kurumsal bilgiyi değerli kabul eder. Bu kapsamda bilgi varlıklarının güvenliği için ilgili uluslararası standartlar ile yasal mevzuatların ve düzenlemelerin gerektirdiği zorunlulukları yerine getirmeyi ve ihtiyaç duyulacak kaynakları sağlamayı taahhüt eder.

Hedefimiz şirketimizin temsil ettiği güvenilirlik imajının istikrarlılığını sağlamak, iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, kurumsal bilginin gizlilik, bütünlük, erişilebilirlik ile ilgili mevcut ve ortaya çıkabilecek olası risklerin etkilerini en aza indirmek ve fırsatları değerlendirerek uluslararası seviyede sektörde yeniliklere öncülük etmektir. Bu hedefe ulaşmak için Bilgi Güvenliği Yönetim Temsilcisi ve BGYS Ekibi tarafından çalışmaların etkin şekilde sürdürülmesi konusunda üst yönetim, sistemin gerektirdiği uygulanabilir tüm şartların karşılanması ve aşağıdaki başlıklar ile ilgili tam desteğini sunmaktadır.

- Mevcut ve olası risklerin değerlendirilmesi, sürekli iyileştirme çalışmalarının yürütülmesi, gerekli aksiyonların planlanması, zamanında gerçekleştirilmesi ve bu süreçler ile ilgili takiplerin yapılması için gerekli genel ve özel sorumlulukları atamak.
- Şirket stratejisi ve bilgi güvenliği hedeflerine uygun şekilde süreçlerde bilgi güvenliği ile ilgili tüm faaliyetlere kılavuzluk edecek özel durumlar ve değişiklikleri doğru şekilde yönetebilmek için gerekli alt politikaların ve dokümantasyonun oluşturulmasını, gözden geçirilmesini ve paylaşılmasını sağlamak.
- Bilginin yaşam döngüsü boyunca gizlilik, bütünlük ve erişilebilirliğini korumak için ihtiyaç duyulan altyapıyı sağlamak.
- Fiziksel ve çevresel güvenlik ile ilgili gereklilikler doğrultusunda ihtiyaç duyulan altyapının ve kuralların uygulanmasını sağlamak.
- Kullanılan sistem ve donanımları teknolojik gelişmelere paralel olarak yenilemek.
- Çalışanların görev ve sorumluluklarına uygun olarak, belirlenen bilgiye erişebilmeleri için sistem ve donanım gereksinimlerini belirlemek, karşılamak ve bilgiye erişimin sadece yetkili kişilerce yapılabilmesi için gerekli güvenlik tedbirlerinin alınmasını sağlamak.
- Yetki aşımı, kaynakların kötüye kullanımı ve dışarıdan şirket bilgi sistemine yapılabilecek fiziksel ve sanal saldırıları izlemek**,** olay kayıtlarını tutmak ve gerekli aksiyonları almak
- Çalışanlarının bilgi güvenliği ile ilgili yükümlülüklerinin farkına varması amaçlanarak yetki aşımı durumunda oluşabilecek zararlar ve uygulanacak cezaları tanımlamak.
- Müşteriler, çalışanlar, tedarikçiler, iş ortakları ve diğer üçüncü taraflara ait bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak.
  Çalışanların ve ilgili diğer tarafların bilgi güvenliği ile ilgili farkındalığını artırmak, kullanıcı prosedürlerini öğrenmek için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimlerin planlanması, gerçekleştirilmesi ve oluşacak acil ihtiyaçlar doğrultusunda bilgilendirmelerin yapılmasını sağlamak.