BİLGİ GÜVENLİĞİ POLİTİKASI

Amaç

Bilgi güvenliği politikası, İBB veri ortamının bütünlüğü ve erişilebilirliğini sağlamak için gerekli olan teknik kontrol ve güvenlik yapılandırmalarının İBB tarafından gerçekleştirilmesini açıklar. Bu politika, bütün kurum çalışanları ve üçüncü parti tarafların bilmekle yükümlü olduğu ve kullanıcıların takip etmesi gereken aksiyon ve yaptırımları tanımlayan merkezi bir dokümandır. Bu politika dahilinde kabul edilebilir kullanım politikası, teknolojik ekipmanlar, e-posta, internet bağlantısı ve gelecekteki teknoloji kaynakları ve bilgi/veri işleme aktarılmaktadır.

Politika dahilinde tanımlanan gereksinim ve yaptırımlar bütün İBB fikri mülkiyet, ağ altyapısı, veri tabanları, dış medya, şifreleme, yazılı rapor, film, slayt, model, kablosuz ağ, iletişim, görüşme ve bilgi/veri iletiminin yapılabildiği bütün donanım, yazılım ve veri taşıma mekanizmalarına uygulanır. İBB'nin bütün lokasyonlarında çalışan tüm çalışan ve üçüncü parti şirket çalışanlarını bağlayıcıdır.

Kapsam

Bu doküman, bilgi/veri üreten, saklayan, taşıyan ve erişen İBB personel veya sistemleri için gerekli olan ortak güvenlik gereksinimlerini tanımlar. Ayrıca, İBB ile ilişkisi olan bütün üçüncü parti şirketler, iştirakler ve diğer sözleşmeleri çalışanlar için de geçerlidir ve uygulanabilir. İhlal durumunda ilgili yaptırımlar uygulanacaktır. Bu doküman İBB etki alanına veya ağına, herhangi bir lokasyonda kablolu/kablosuz şekilde bağlanan bütün cihazlar için geçerlidir.

Uygulanabilir Regülasyonlar/Standartlar

Aşağıdaki liste İBB'nin uyduğu/takip ettiği çeşitli kurum ve kuruluşları göstermektedir.

- 6698 sayılı Kişisel Verileri Koruma Kanunu (KVKK)
- Avrupa Birliği GDPR
- Türk Devleti/Hükümeti ve ilgili bakanlık tebliğleri
- ISO 27001 BGYS Standardı
- PCI DSS Standardı