BİLGİ GÜVENLİĞİ POLİTİKASI

BİLGİ GÜVENLİĞİ POLİTİKASI

Zorlu Holding Bilgi Güvenliği Yönetim Sistemi (BGYS), bilginin gizliliği, bütünlüğü ve erişilebilirliğini; varlık ve risk yönetimi süreçlerini uygulayarak muhafaza etmek ve ilgili taraflara risklerin doğru bir şekilde yönetildiğine dair güvence vermek için kurulmuştur.

Zorlu Holding, bilgi güvenliği süreçlerini TS ISO/IEC 27001:2022, SPK Bilgi Sistemleri Yönetimi Tebliği, CB DDO Bilgi ve İletişim Güvenliği Rehberi, EPDK Siber Yetkinlik Modeli ve PCI DSS standartlarına uygun olarak işletir. Bilgi Güvenliği Yönetim Sistemi'nin uygulanması ve sürekli iyileştirilmesi için tüm grup hizmetleri çerçevesinde gerekli kaynakları kullanacağını taahhüt eder.

Bu politika Zorlu Holding Üst Yönetimi tarafından hazırlanmış olup, Yönetim Kurulu tarafından onaylanmıştır. Teknoloji ve Dijital İş Geliştirme Grubu Başkanlığı, Bilgi Güvenliği Politikası ve ilgili politikalara uyumun sağlanmasından birinci derecede sorumludur.

Bilgi güvenliğini sistematik olarak yönetebilmek adına belirlenen ana hedefler aşağıdaki gibidir:

- Bilgi Güvenliği Yönetim Sistemi kapsamında, kurumsal bilgi varlıklarının ve tüm ilgili taraflardan emanet edilen bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak,
- Bilginin Gizlilik, Bütünlük, Erişilebilirlik ile ilgili ortaya çıkabilecek risklerini değerlendirmek ve bu risklerin etkilerini en aza indirmek,
- Bilgi güvenliği ile ilgili tüm yasal mevzuat ve üçüncü taraflar (iş ortakları, müşteriler, tedarikçiler vb.) ile yapılan sözleşmelere uymak,
- Zorlu Holding'in tabi olduğu tüm kanunlara, yönetmeliklere ve tebliğlere uyum sağlamak,
- Zorlu Holding bünyesinde sürdürülen yönetim sistemleri dahilinde yayınlanan tüm politikalara ve prosedürlere bağlı kalmak,
- Yönetim Sisteminin gerekliliklerini karşılamak ve etkin bir şekilde işletmek üzere çalışanların yetkinliğini artıracak gerekli kaynakları ayırmak ve eğitim programları planlamak,
- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçmek, geçilemediği durumda hedeflenen kurtarma süresi içerisinde tekrar çalışabilir hale gelmek,
- Tüm personelin ve iş ortaklarının yönetim sistemlerine katılımını ve uyumunu sağlamak için bilinçlendirici ve yönlendirici faaliyetler planlamak,
- Yönetim Sisteminin yürütülmesi için kullanılan süreç ve faaliyetlerin sürekli iyileştirilmesi amacıyla düzenli gözden geçirmeler gerçekleştirmek,
- Bilgi güvenliği kontrollerini zorunlu tutan konulara ilişkin politikalar ve prosedürler hazırlamak, bu politikalara ve prosedürlere uyumluluğu gözden geçirmek, geliştirilmesi ve iyileştirilmesi için kontroller yapmak,
- Tüm çalışma yöntem ve esaslarının bilgi güvenliği süreçleriyle uyumlu ve dengeli olmasını sağlamaktır.
- Bilgi Güvenliği ve Siber Güvenlik riskleri ile tehditleri sürekli izlenmekte, tespit edilen olaylara hızlı ve etkili şekilde müdahale edilmekte olup kapsamlı bir yönetim modeli uygulanmaktadır.

Zorlu Holding Bilgi Güvenliği Politikaları ve Prosedürleri; tam veya yarı zamanlı, sözleşmeli veya daimî, şirket bilgilerini ve/veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve elzemdir. Bu sınıflandırmalara girmeyen üçüncü taraf hizmet sağlayıcıları; bilgi güvenliği politikasının ve bilgi güvenliği prosedürlerinin genel ilkelerine bağlı hizmet vermesi zorunludur.