

## BİLGİ GÜVENLİĞİ POLİTİKASI

Erkurt Holding Bilgi Güvenliği Politikasının amacı, otomotiv ve beyaz eşya sektörlerine hizmet veren Erkurt Holding ve grup şirketlerinin üretim süreçleri başta olmak üzere, tüm iş süreçlerinin sürekliliğini ve faaliyetlerine ilişkin bilgilerin güvenliğini sağlamak, bilgiye yönelik potansiyel tehditlerin etkisini azaltarak bilgi güvenliği ihlallerini engellemek ve hasar riskini minimum seviyede tutmaktır.

Bilgi Güvenliği Yönetim Sistemi'nin holding ve grup şirketleri içinde ISO/IEC 27001 standardına uyumlu olması, Erkurt Holding ve grup şirketleri bünyesindeki tüm bilgi varlıklarını kapsamaktadır. Tüm lokasyonlardaki çalışanlar, lokasyon içi ve dışı tedarikçiler ve yükleniciler bu politikaya bağlı prosedürlere uygun şekilde çalışmakla yükümlüdür.

Yönetim Kurulu olarak, müşterilerimizin ihtiyaç ve beklentilerini karşılayıp tam bir müşteri memnuniyeti yaratmayı, yasal ve ilgili tarafların uygulanabilir şartları için yapacağı uygulamaların tüm süreçler içinde uçtan uca tanımlı olduğu, dijital olarak izlenebilir bir yapıda olması amacıyla Bilgi Güvenliği Yönetim Sistemi'nin geliştirilmesi ve sürekli iyileştirilmesinden hareket ederek uyumu taahhüt ederiz.

Bu amaçtan yola çıkılarak Erkurt Holding ve grup şirketlerinin bilgi varlıklarını iç ve dış, kasıtlı veya kasıtsız tehditlere karşı koruma amacına yönelik olarak önceliklerimiz ve hedeflerimiz:

- Şirketin güvenilirliğini ve kurumsal itibarını koruyarak veri bütünlüğünü, erişilebilirliğini ve gizliliğini sağlamak,
- Bilgi güvenliği farkındalığını artırmak amacıyla tüm çalışanlarımıza teknik ve davranışsal yetkinliklerini geliştirecek eğitimler vermek,
- Bilgi varlıklarının ve iş süreçlerinin tanımlanarak bunlara yönelik risk değerlendirmelerinin sistematik olarak yönetimini sağlamak ve sürekli iyileştirmeyi etkin kılmak,
- Bilgi güvenliğiyle ilgili tüm yasal mevzuat ve sözleşmelere uymak,
- Müşterilerimiz, iş ortaklarımız, tedarikçilerimiz, sivil toplum örgütleri, kamu kurum ve kuruluşları ile yapılan sözleşmelerin ilgili mevzuata uygunluğunu temin etmek,
- Kurumun temel ve destekleyici iş faaliyetlerinin en az kesintiyle devam etmesini sağlamak ve olağanüstü durumlarda acil durum eylem planını hayata geçirmek,
- Kurumsal uygulamaları, verileri, iletişim ağını ve ekipmanlarını kayıplara, yetkisiz kullanıma ve suistimallere karşı koruma altına almak,
- Tüm kullanıcıların Bilgi Güvenliği Politikası ve ilgili destekleyici prosedürler ile talimatlara bütünüyle uymalarını ve farkında olmalarını sağlamak,
- Bilgi güvenliği ihlali olduğunda, söz konusu ihlalin tespit, raporlama ve kayıt altına alınmasına yönelik aksiyonları hayata geçirerek, ivedi bir şekilde bilgi güvenliğini sağlamaktır.