# BİLGİ GÜVENLİĞİ POLİTİKASI

## 1. AMAÇ

Firmamız ve iştirakleri kurumsal ve kişisel bilgiyi değerli ve hayati bir varlık olarak kabul etmektedir. Bilgi; iş faaliyetlerimizin sürdürülebilmesi açısından kritik önem taşır ve uygun bir şekilde korunması gerekir. Firmamız kurumsal ve kişisel bilginin korunmasını, Bilgi Güvenliği Yönetim Sistemi (ISO 27001) de dahil olmak üzere uluslararası standartlar, yasa ve mevzuatlar çerçevesinde sağlamayı, mevcut ve oluşabilecek riskleri yöneterek bilgi güvenliğini sürekli olarak iyileştirmeyi, geliştirmeyi ve gözden geçirmeyi taahhüt eder.

## 2. KAPSAM

GÜRPİLSAN PLASTİK SAN. TİC. LTD. ŞTİ. 'nin bünyesinde tüm çalışanlara bu prosedür uygulanır. Bilgi Güvenliği Politikamız, tüm iş ortaklarımızla birlikte temel ilke ve değerlerimize dayanan, takım çalışması şeklinde yürüterek oluşturduğumuz standartları içerir.

## 3. SORUMLULUKLAR

Bu prosedürün uygulanmasından, Yönetim Temsilcisi sorumludur. Bu prosedürün uygulanması sonucu ortaya çıkan kayıtlar IK departmanında muhafaza edilir.

## 4. BİLGİ GÜVENLİĞİ POLİTİKASI

Gürpilsan Plastik ve çalışanları olarak, iş sürekliliğimize ve bilgi varlıklarımıza yönelik her türlü riski yönetmek amacıyla aşağıda belirtilen konuların yerine getirilmesini politika olarak benimsemiştir:

1. Bilgi güvenliği yönetim sistemimizin ISO 27001 başta olmak üzere diğer uluslararası standartların gereklerini yerine getirecek şekilde politika ve prosedürlerin belirlenmesi ve dokümante bilgilerinin hazırlanması ve güncelliğinin takip edilmesi,

2. Bilgi güvenliği yönetim sisteminin kurulması, sürdürülmesi ve iyileştirilmesi için kaynakların ayrılması,

3. Bilgi güvenliği yönetim sistemleriyle ilgili yasal mevzuat ve sözleşmelere uyulmasını temin etmek,

4. İş süreçlerine yönelik risklerin tanımlanması ve sistematik olarak yönetilmesi sağlamak,

5. Bilgi güvenliği ve iş sürekliliği yönetim sistemi farkındalığını artırmak amacıyla teknik ve davranışsal yetkinlikleri geliştirecek eğitimlerin gerçekleştirilmesi sağlamak,

6. Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, potansiyel kesintilerin önceden planlı uygulamalar ile engellenmesi.

7. Varlıkların gizlilik, bütünlük ve erişilebilirliklerini koruyarak kurumun güvenirliğini sürdürmek ve geliştirmek,

8. Kurumumuzun karşılaşacağı güvenlik ihlallerinin yönetilmesi ve gerekli durumlarda cezai yaptırımların uygulanmasını sağlamak,

9. Plansız kesintilerin en aza indirilmesi,

10. Bilgi güvenliği yönetim sistemi uygulamalarının etkinliğini sürdürmek için kişilerin yönlendirilmesi, desteklenmesi ve sürekli iyileştirmenin teşvik edilmesi,

11. Yönetim görevlerini yerine getiren personelin, kendi sorumluluk alanında liderliklerini ve işe verdikleri önemi göstermeleri için desteklenmesi,

Bilgi Güvenliği Politikalarımız ister tam zamanlı ister yarı zamanlı, daimî ya da sözleşmeli olsun, firma bilgilerini veya iş sistemlerini kullanan tüm personelimiz için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve bilgilerimize erişim gereği olan üçüncü şahıs hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine uyması, diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır