

**PREDO SAĞLIK SAN. VE TİC.A. Ş. (Bundan böyle PREDO SAĞLIK olarak anılacaktır.)** Yönetimi, organizasyonun sorumluluğu altında bulunan bilgileri korumak için güvenlik önlemlerini yerine getirmenin önemini ve ihtiyacını vurgular. Çok gizli ve gizli şirket bilgisinin yetkilendirilmiş kullanıcıların kullanımına sunulması için gerekli önlemlerin alınmış olması şarttır. Teknik yollarla elde edilebilen güvenlik seviyesi sınırlıdır, dolayısıyla uygun yönetim, iş akışları ve prosedürler ile desteklenmelidir.

**PREDO SAĞLIK, bilgi** varlıklarının ve bilgi sistemlerinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasını, "Bilgi Güvenliği Yönetim Sistemi" olarak tanımlar. Bilgi varlıklarının korunmasına yönelik olarak her varlık üzerinde gizlilik, bütünlük ve erişilebilirlik değerlendirmesi yapılmaktadır.

Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olmasını ifade etmektedir. Bütünlük: Bilginin doğruluğunu ve tamlığını olumsuz etkileyecek değişikliklere karşı korunmasını ifade etmektedir. Erişilebilirlik: Bilginin yetkili kullanıcılar tarafından gerektiğinde erişilebilir olmasını ifade etmektedir.

Bilgilerin gizliliği, bütünlüğü ve erişilebilirliği, **PREDO SAĞLIK'IN** BGYS temel hedeflerinden birisidir. Hedeflenen BGYS sonuçlarına ulaşmak için **PREDO SAĞLIK** Yönetimi, ISO 27001 Bilgi Güvenliği Yönetim Standardına uyumlu olmayı sağlar. Şirketteki tüm iş birimleri ve ilgili taraflar, gerçekleştirdikleri faaliyetlerinde bu ilkelere dikkat edeceklerdir.

Tüm **PREDO SAĞLIK** personeli ve üçüncü taraf personel, her seviyeden, bilgi güvenliği sistem gereksinimlerini yerine getirmekte ve sistemin etkinliğini artırmak için faaliyetler yürütmektedir. **PREDO SAĞLIK** Bilgi varlıkları başta olmak üzere, Müşteriler, iş ortakları, paydaşlar, tedarikçiler veya diğer üçüncü kişilere ait bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini güvence altına almayı ve yetkisiz erişimden korumayı amaçlar.

**PREDO SAĞLIK** Yönetimi, Bilgi Güvenliği Yönetim Sistemi açısından sürekli iyileştirme ve iş sürekliliğinin sürdürülmesini ve yönetilmesini sağlar.

Bilgi Güvenliği Kapsamında oluşturulmuş kural ve süreçleri ihlal eden personel, paydaş ve üçüncü taraflar hakkında adli ve idari yasal takibat başlatılarak; işlem yapılabilir ve / veya ilgili sözleşmelerde yer alan yaptırımlarının bir ya da birden fazla hükmü uygulanabilir.