BİLGİ GÜVENLİĞİ POLİTİKASI

Bu politikanın uygulanması ile Angst Pfister Gelişmiş Teknik Çözümler A.Ş. Üst Yönetimi, küresel pazarda hem Titreşim Önleyici hem de sızdırmazlık ürünleri için önde gelen bir üretici, tasarım ortağı ve çözüm sağlayıcısı olma vizyonu ile gerçekleştirdiği iş süreçlerinin sürekliliğini sağlamak amacıyla Bilgi Güvenliği Yönetim Sistemi kapsamındaki hizmetlerin güvenilirliğini, sürekliliğini ve sürdürülebilirliğinin gerekleri olan aşağıdaki temel ilkeleri yerine getirmeyi taahhüt ve beyan eder.

- Bilgi varlıklarının bilerek veya bilmeyerek yetkisiz kullanımı, değiştirilmesi, açıklanması ve hasara uğratılması önlenecektir.
- Müşterilerden alınacak bilgiler; bilgi güvenliği temel ilkeleri doğrultusunda yetkisiz erişeme karşı korunacaktır.
- Müşterilerine ait iş maksadıyla toplanan bilgiler sadece bu maksatla kullanılacak ve hiçbir şekilde üçüncü şahıslarla paylaşmayacaktır.
- Müşterilerine ilişkin iş gereksinimlerini yasal mevzuat gerekliliklerine uygun alt yapı, süreç ve personel ile yapılması için gerekli kaynaklar sağlanacaktır.
- Angst Pfister Gelişmiş Teknik Çözümler A.Ş. 'nin Bilgi güvenliği kapsamı dâhilindeki, kurumsal ve kişisel bilgilerin ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.
- "Bilmesi gereken" prensibine uygun erişim kontrolü sağlanacak ve bilgi yetkisiz erişime karşı korunacaktır.
- Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeylere indirilecektir.
- Bilgi; bilginin elektronik iletişimi, üçüncü taraflarla paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak her durumda korunacaktır.
- Bilgi varlıkları, gizlilik dereceleri ile tanımlanacak ve çalışanlar tarafından gizlilik tedbirlerinin uygulanması ile gizliliği ve bütünlüğü sağlanacaktır.
- T.C. yasaları, yönetmelikler, genelgeler, müşteri sözleşmeleri ve işin gerektirdiği yasal mevzuat ile belirlenmiş gereksinimler karşılanacak, bunlar ile uyumlu çalışma sağlanacaktır.
- Müşterilere sağlanan hizmetlerin; büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla, iş sürekliliği yönetimi uygulanacak ve iş sürekliliği yönetim planı oluşturulacaktır. İş sürekliliği planının sürekliliği sağlanacak ve test edilecektir.
- Personelin bilgi güvenliği farkındalığını arttıracak ve sistemin işleyişine katkıda bulunmasını teşvik edecek eğitimler düzenli olarak kurum çalışanlarına ve yeni işe giren çalışanlara sağlanacaktır.
- Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlâlleri rapor edilecek; tekrar etmesini engelleyici önlemler alınacaktır.
- Personelin çalışma alanlarında, "Temiz Ekran / Temiz Masa" prensiplerine uygun olarak, "Açık" özellikteki bilgiler dışında bilgilerin, başkalarınca görülmesine imkân verilmeyecek şekilde önlemler alınacaktır.

REV. NO : 00 **ERAY ULUGÜL**

YAYIN TARİHİ : 23.08.2016 **GENEL MÜDÜR**