ENPARA BANK A.Ş

BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK POLİTİKASI

Bu politikanın amacı Enpara Bank varlıklarını, müşteri verilerini ve bilgi sistemlerini siber tehditlere karşı korumak için açık ve kapsamlı bir çerçeve oluşturmaktır. Bu politika, Enpara Bank bilgi varlıklarını, bilgi sistemleri süreçleri ve altyapısını, tüm çalışanları, üçüncü parti tedarikçileri, danışmanları, banka sistemlerine, verilerine veya teknoloji kaynaklarına erişimi olan tüm paydaşları kapsar.

Enpara Bank'ta bilgi güvenliği; iş sürekliliğini sağlamak, finansal ve operasyonel kayıpları en aza indirmek amacıyla bilgi varlıklarının tehditlere karşı korunması olarak tanımlanır. Bilgi güvenliği ile saklanan, işlenen veya iletilen her türlü bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması hedeflenir.

Enpara Bank bilgi güvenliği ve siber güvenlik; risk bazlı bir yaklaşımla yönetilmekte ve uluslararası bilgi güvenliği standartlarına göre planlanmakta, uygulanmakta ve gözden geçirilmektedir. Risk yönetimi yaklaşımı; bilgi güvenliği ve siber güvenlik risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini ve gerekli önlemlerin alınmasını içerir. Banka, bilgi güvenliği ve siber güvenlik risklerini, mevzuat ve ISO 27001 gereksinimlerine uygun, bilgi sistemleri stratejisine ve iş için kabul edilebilir bir tolerans düzeyinde bankanın kurumsal risk yönetimi çerçevesine uygun olarak, bütünleşik bir risk yönetim metodolojisi ile yönetir.

Banka bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk yönetim kuruluna aittir. Tüm çalışanlar ve tedarikçiler, ülkemizdeki yasal mevzuatlar, ilgili yasa ve yönetmeliklere, bankacılık kanunlarına, BDDK yönetmeliklerine ve bu politikaya uymakla yükümlüdür. Bu amaçla banka bilgi sistemlerini kullanan, yöneten ve bilgi kaynaklarına erişen herkes;

✓ Bilgi varlıklarının gizlilik, bütünlük ve kullanılabilirliğini korumak,

✓ Bilgi güvenliği ve siber güvenlik politika, standart, prosedür ve talimatlarını bilmek ve uygulamak,

✓ BT kaynaklarını yasalara, politikalara ve iş amaçlarına uygun kullanmak,

✓ Müşteri bilgilerinin gizliliğini ve mahremiyetini sağlamak

✓ Temiz masa ve ekran politikasını benimsemek ve uygulamak,

✓ Bilgiyi sadece yetkili kişiler ile paylaşmak,

✓ Tahmin edilmesi zor şifreler kullanmak ve gizliliğini sağlamak

✓ Bilginin uygun şekilde yedeklenmesini ve iş sürekliliğini sağlamak,

✓ Bilgi sınıflandırması yapmak ve gerekli kontrollerin uygulanmasını sağlamak,

✓ Bilgi güvenliği ihlal olaylarını ve potansiyel zayıflıkları raporlamak zorundadır.

Tüm çalışanlar, dış hizmet sağlayıcılar ve müşteriler için bilgi güvenliği ve siber güvenlik farkındalık seviyesini artırmak için kapsamlı bir bilgi güvenliği farkındalığı eğitim programı oluşturulur ve uygulanır.

Bilgi güvenliği politikamızda yer alan amaç ve hedefleri destekleyen çalışmalar, yıl içinde takip edilir ve raporlanır. Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi sağlanır, sürekli iyileştirmeye yönelik çalışmalar yönetim tarafından gözden geçirilir.