BİLGİ GÜVENLİĞİ POLİTİKASI

Türkiye Kalkınma ve Yatırım Bankası A.Ş. ("TKYB", "Bankamız") bilgi güvenliği ve kişisel veri güvenliği hedef ve stratejileri doğrultusunda iç ve dış hususlarını, iç ve dış hususları ile ilgili bilgi güvenliği ve kişisel veri güvenliği ihtiyaç ve beklentilerini, ihtiyaç ve beklentilere yönelik ara yüzler ve bağımlılıklarını tanımlamayı hedeflemekte; bu doğrultuda bilişim sistemlerinin işletimi ve yönetimi süreçlerinde ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı ve ISO/IEC 27701:2019 Kişisel Veri Yönetim Sistemi Standardını referans alarak kurmuş olduğu Bilgi Güvenliği Yönetim Sisteminin ve Kişisel Veri Yönetim Sisteminin işletimini sağlamaktadır.

Tabi olunan mevzuat kapsamında yasal gereksinimler, düzenleyici kararlar, sözleşmeden doğan şartlar, risk değerlendirme ve işleme sonuçları dikkate alınarak TKYB Üst Yönetimi, Bilgi Güvenliği Yönetim Sisteminin ve Kişisel Veri Yönetim Sisteminin kurulumu, uygulanması, işletimi, izlenmesi ve sürekli iyileştirilmesi için gerekli çalışmaları yapacağını ve Bilgi Güvenliği Politikası'na hem iç hem de dış paydaşlar tarafından uyum sağlanacağının teminatını taahhüt etmektedir. Bankamız faaliyetleri kapsamında vizyon, misyon ve stratejileri ile eş doğrultuda Bilgi Güvenliği Politikası ve tüm gereksinimlere uyumun teminatı, Bilgi Güvenliği Yönetim Sisteminin ve Kişisel Veri Yönetim Sisteminin sürekliliği ve sürdürülebilirliğinin sağlanması kapsamında önem arz etmektedir.

Bankamız Üst Yönetimi, etkin bir Bilgi Güvenliği Yönetim Sisteminin ve Kişisel Veri Yönetim Sisteminin sağlanması amacıyla gerekli tüm teknik ve idari kaynakların teminatını sağlamakta; bilgi ve kişisel veri içeren varlıkların risklerini ve kabul edilebilirlik seviyelerini, planlanmış iç denetimler ve sürekli denetim faaliyetleri kapsamında iç kontrol aktiviteleri ile kontrol altına almaktadır. Tüm iç ve dış paydaşların bilgi ve kişisel veri güvenliği farkındalığı ve gerekliliklerini yerine getirmeye yönelik çalışmalar gerçekleştirilmekte; Bilgi Güvenliği Yönetim Sistemi ve Kişisel Veri Yönetim Sistemi kapsamında belirlenen tüm risk ve fırsatlar için hedeflerin tanımlanması ve ulaşılması çalışmaları yerine getirilmektedir.

Bankamız, bilgi varlıkları ve kişisel verilerin işlenmesi kapsamında temin edilmesi, kayıt altına alınması, arşivlenmesi, duyurulması, sözleşmeli taraflar ile paylaşılması, sınıflandırılması faaliyetlerinde verinin gizliliği, bütünlüğü ve erişilebilir olması konularında özen göstermektedir. Bankamız kaynakları ile üretilen, müşterilerimizden veya tedarikçilerimizden edinilen ve resmi kurumlar aracılığı ile temin edilen bilginin gizliliği, bütünlüğü ve erişilebilirliği sağlanmakta; Bilgi Güvenliği Yönetim Sistemi ve Kişisel Veri Yönetim Sistemi kapsamında gerçekleştirilen fırsat ve risk değerlendirme çalışmaları bilginin üç boyutu dikkate alınarak gerçekleştirilmektedir.

Bankamız Üst Yönetimi;

- Bilgi Güvenliği Politikası ve bilgi güvenliği amaçlarının oluşturulmasını ve kuruluşun stratejik yönü ile uyumlu olmasının temin edilmesini,
- Bilgi Güvenliği Yönetim Sisteminin ve Kişisel Veri Yönetim Sisteminin şartlarının kuruluşun süreçleri ile bütünleştirilmesinin temin edilmesini,
- Bilgi Güvenliği Yönetim Sistemi ve Kişisel Veri Yönetim Sistemi için gerekli olan kaynakların erişilebilirliğinin temin edilmesini,
- Etkin bilgi güvenliği ve kişisel veri yönetiminin ve Bilgi Güvenliği Yönetim Sistemi ve Kişisel Veri Yönetim Sistemi şartlarına uyum sağlamanın öneminin duyurulmasını,
- Bilgi Güvenliği Yönetim Sisteminin ve Kişisel Veri Yönetim Sisteminin hedeflenen çıktılarının başarılmasının temin edilmesini,

- Bilgi Güvenliği Yönetim Sisteminin ve Kişisel Veri Yönetim Sisteminin etkinliğine katkı sağlamaları için kişilerin yönlendirilmesi ve desteklenmesini,
- Sürekli iyileştirmenin desteklenmesini,
- Gizlilik, bütünlük ve erişilebilirlik boyutlarının bilgi varlıkları ve kişisel verilerin doğru işleme faaliyetlerini,
- Bilgi kapsamında gerçek kişilerden edinilen kişisel verilerin güvenliğinin ilgili mevzuat ve Bilgi Güvenliği Yönetim Sistemi ve Kişisel Veri Yönetim Sistemi gereklilikleri doğrultusunda korunmasını,
- Bilgi Güvenliği Yönetim Sisteminin ve Kişisel Veri Yönetim Sisteminin sürekliliği ve sürdürülebilir olmasının sağlanması için gerekli kaynakları tahsis etmeyi

taahhüt eder.

CEO