Bilgi Güvenliği Politikası

İçerisinde bulunduğumuz bilişim ve dijital dönüşüm çağında toplumsal ve ekonomik gelişmelere bilgi yön vermektedir. Bu durum, kurumların tüm paydaşlar nezdindeki güvenilirliğinin sürdürülmesi, itibarın korunması ve faaliyetlerinin kesintisiz, kayıpsız yürütülmesi açısından bilgi güvenliğinin önemini ortaya koymaktadır.

Türkiye İş Bankası, sunduğu tüm ürün ve hizmetlerde bilgi güvenliğini en yüksek seviyede sağlamayı; müşterilerimizin, çalışanlarımızın, iş ortaklarımızın ve diğer paydaşlarımızın güvenini korumayı öncelikli hedefi olarak kabul etmektedir. Bu doğrultuda, kurumsal bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini güvence altına almak amacıyla uluslararası kabul görmüş ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardına uygun bir yönetim sistemi oluşturmayı ve sürekliliğini sağlamayı stratejik hedef olarak benimsemektedir.

Bilgi güvenliği yaklaşımımız, yalnızca teknolojik önlemlerle sınırlı kalmamakta; süreçler, çalışanlar, fiziksel ortamlar ve dış hizmet sağlayıcılar dahil olmak üzere tüm unsurlar dikkate alınarak bütüncül bir şekilde ele alınmaktadır. Bankamız, bilgiye yetkisiz erişimin engellenmesini (gizlilik), bilginin doğruluğunun ve bütünlüğünün korunmasını (bütünlük) ve bilginin yalnızca yetkili kişiler tarafından ihtiyaç duyulduğunda ulaşılabilir olmasını (erişilebilirlik) temel unsur olarak kabul etmektedir. Bilgi varlıklarına yönelik iç ve dış tehditler sistematik bir şekilde analiz edilmekte; tanımlanan riskler, uluslararası standartlarla uyumlu biçimde değerlendirilerek uygun kontrollerle yönetilmektedir.

Tüm faaliyetlerimiz, yasal yükümlülüklere ve ulusal/uluslararası düzenlemelere azami uyum hedefi çerçevesinde sürdürülmektedir. Bilgi güvenliği gerekliliklerinin sağlanması, yalnızca bilgi teknolojileri ekiplerinin değil, kurum faaliyetlerinde rol alan her bir bireyin ve süreç sahibinin sorumluluğunda bulunmaktadır. Bu doğrultuda, kurumsal politikalar ve etkin organizasyonel yapı aracılığıyla gerekli yönlendirmeler yapılmakta; farkındalık artırıcı eğitim ve bilinçlendirme faaliyetleriyle bu sorumluluğun kurumsal kültürün bir parçası haline getirilmesi sağlanmaktadır.

Bilgi güvenliği olaylarının önlenmesi, tespiti, müdahalesi ve benzeri durumlar için etkin bir olay yönetim süreci yürütülmekte; bu olaylardan edinilen deneyimler sistemin sürekli iyileştirilmesi amacıyla kullanılmaktadır. Ayrıca, iş sürekliliği ve felaket kurtarma planları oluşturularak bilgi sistemlerine yönelik kesintilerin etkisi en aza indirilmektedir. Kurum adına hizmet sunan üçüncü taraflar ve tedarikçiler de bilgi güvenliği yönetimi kapsamına dâhil edilmekte; gerekli güvenlik şartları sözleşmeler ve denetimler yoluyla güvence altına alınmaktadır.

Bilgi Güvenliği Yönetim Sistemi'mizin etkinliği; iç denetimler, yönetim gözden geçirme toplantıları, ölçüm faaliyetleri ve paydaş geri bildirimleriyle düzenli olarak izlenmekte ve değerlendirilmektedir. Sürekli iyileştirme yaklaşımı doğrultusunda sistem performansı devamlı olarak artırılmakta, yeni risk ve ihtiyaçlara karşı proaktif önlemler geliştirilmektedir. Politika yılda en az bir kez gözden geçirilerek güncellenmekte ve kurumsal web sitesi üzerinden kamuoyu ile paylaşılmaktadır.

Bankamız, ISO/IEC 27001 standardına uygun olarak oluşturulan BGYS ile bilgi güvenliği risklerini yönetmeyi, yasal yükümlülüklere uyum sağlamayı, bilgi güvenliğini kurumsal kültürün bir parçası haline getirmeyi ve müşterilerine güvenli bir hizmet sunmayı taahhüt eder.