

Şirketimiz, geçtiği tüm ilişkilerde hizmetlerin güvenlik ve kesintisiz hali için bilgi güvenliği, kişisel veri güvenliği ve iş sürekliliğine özel dikkat göstermektedir. Aşağıda yer alan prensipler çerçevesinde amacımız, müşteri ve iş ortaklarının güvenliğini sağlamaktır:

- Bilgi varlıklarımızın gizliliği, bütünlüğü ve erişilebilirliğini korumak amacıyla gerekli teknik ve idari tedbirler alınır. Bu tedbirler, BDDK'nın "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" ve TCMB'nin "Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Kullanılan Bilgi Sistemleri Hakkında Tebliğ" kapsamında belirlenen güvenlik önlemlerini içermektedir.
- Bilgi güvenliği tehditlerini en aza indirmek amacıyla düzenli risk değerlendirmeleri yapılır ve alınacak önlemler bu değerlendirmeler ışığında güncellenir. Risk değerlendirmeleri ve güvenlik önlemleri, BDDK'nın "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" ve TCMB'nin "Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Kullanılan Bilgi Sistemleri Hakkında Tebliğ" doğrultusunda gerçekleştirilir.
- Bilgi sistemlerimize erişim, yalnızca yetkilendirilen kişilerce sağlanır ve erişim hareketleri kaydedilir. Erişim kayıtları, düzenleyici otoritelerin belirlediği süre boyunca saklanır ve düzenli olarak gözden geçirilir.
- Kişisel veriler yasal mevzuatlar kapsamında (KVKK, GDPR vb.) korunmaktadır. Ayrıca, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu ile 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamındaki veri koruma yükümlülükleri de yerine getirilmektedir.
- Kişisel verilerin toplanması, işlenmesi, saklanması ve imhasında veri güvenliği sağlık güvencesi süreçlerinde gerekli tüm tedbirler alınmaktadır.
- Kişisel verileriniz sadece belirlenen amaçlar için kullanılır ve yetkisiz erişimlere karşı korunmaktadır.
- Hizmetlerimizin kesintisiz bir şekilde devamını sağlamak için iş sürekliliği planlarımız devreye alınır ve buna göre olası acil durum ve felaket senaryoları oluşturulmaktadır. İş sürekliliği planları, BDDK'nın "Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik" kapsamındaki gereklilikleri karşılamaktadır.
- Bir felaket durumunda kritik iş süreçleri kesintiye uğramadan kurtarılabilmesi için düzenli yedeklemeler ve testler ile felaket kurtarma planlarımız periyodik olarak test edilir.

- Çalışanlar, bilgi güvenliği ve veri koruma konusunda sürekli eğitimlerle bilinçlendirilmektedir. Bilgi güvenliği kültürünü yaygınlaştırmak amacıyla düzenli farkındalık programları ve tatbikatlar düzenlenmektedir.
- Şirketimiz, tüm bilgi güvenliği ve veri koruma süreçlerinde ulusal ve uluslararası yasal düzenlemelere ve standartlara tam uyum sağlamaktadır. Bu kapsamda, PCI DSS (Ödeme Kartları Endüstrisi Veri Güvenliği Standardı) gerekliliklerine de uyum sağlanmaktadır.
- Politika ve prosedürlerimiz, düzenli olarak denetlenmekte ve gelişen teknoloji ve mevzuatlar doğrultusunda güncellenmektedir.
- Sürekli iyileştirme. Bilgi güvenliği, kişisel veri güvenliği ve iş sürekliliği uygulamalarımız, sürekli iyileştirme anlayışı ile periyodik olarak gözden geçirilir. Yeni tehditlere karşı proaktif yaklaşımlar benimsenerek güvenlik politikalarımız güncellenir.
- Tedarikçilerimiz ve iş ortaklarımızla bilgi güvenliği ve veri koruma gereksinimlerini içeren iş birlikleri yapılır.
- Bilgi güvenliği gereklilikleri üçüncü tarafların uygulamaları periyodik olarak denetlenir.
- Şirketimiz bu politikaya uygun hareket etmeyi kabul eder ve hizmetlerimizi güvenli bir şekilde sürdürürüz. Müşteri hizmetlerimiz bu politika gerekliliklerine göre bilgi güvenliği ve iş sürekliliği. Müşteri gizliliği ve güvenliği birinci önceliğimizdir.
- Şirketimiz, TCMB'nin "Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik" kapsamında belirlenen güvenlik önlemlerini uygulamaktadır.
- Kritik sistemlerimiz ve verilerin bulunduğu ortamlar için güçlü şifreleme yöntemleri kullanılmakta ve düzenli olarak güncellenmektedir.
- Güvenlik olayları ve ihlalleri için bir olay müdahale planı bulunmaktadır. Bu plan, yasal raporlama gerekliliklerini de içermektedir.
- Mobil uygulamalar ve internet bankacılığı hizmetleri için düzenleyici otoritelerin belirlediği güvenlik önlemleri uygulanmaktadır.
- Düzenli olarak bağımsız güvenlik denetimleri ve penetrasyon testleri gerçekleştirilmekte ve sonuçlarına göre gerekli iyileştirmeler yapılmaktadır.