



BİLGİ GÜVENLİĞİ POLİTİKASI

D Yatırım Bankası A.Ş. olarak müşterilerimizin, çalışanlarımızın, iş ortaklarımızın ve diğer paydaşlarımızın bilgilerinin korunmasını kurumsal sorumluluğumuzun temel unsurlarından biri olarak görmekteyiz.

Bilgi güvenliği yaklaşımımız; bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasına, bankacılık hizmetlerinin güvenli ve kesintisiz şekilde sunulmasına ve bilgi güvenliği risklerinin etkin biçimde yönetilmesine dayanmaktadır.

Bilgi Güvenliği Yaklaşımımız

Bankamız, bilgi güvenliği faaliyetlerini başta bankacılık ve kişisel verilerin korunmasına ilişkin düzenlemeler olmak üzere yürürlükteki mevzuat, kurumsal politikalar ve risk yönetimi yaklaşımı doğrultusunda yürütmektedir.

Bilgi güvenliği; bilgi sistemlerinin yanı sıra çalışanları, iş süreçlerini, fiziksel ortamları, dijital kanalları ve destek hizmeti alınan kuruluşları kapsayan bütünsel bir yönetim anlayışıyla ele alınmaktadır.

Bu doğrultuda;

- Bilgi güvenliği riskleri düzenli olarak belirlenmekte, değerlendirilmekte ve izlenmektedir.
- Bilgi varlıklarının sahipliği, sınıflandırılması ve korunmasına ilişkin sorumluluklar tanımlanmaktadır.
- Risklerle uyumlu teknik ve idari güvenlik kontrolleri uygulanmaktadır.
- Değişen tehditler, teknolojik gelişmeler ve mevzuat gereklilikleri doğrultusunda güvenlik süreçleri güncellenmektedir.

Temel Bilgi Güvenliği İlkelerimiz

Bilgi güvenliği uygulamalarımız aşağıdaki temel ilkeler üzerine kuruludur:

- **Gizlilik:** Müşteri sırrı, banka sırrı, kişisel veri ve diğer hassas bilgilere yalnızca yetkilendirilmiş kişiler tarafından ve görev gereklilikleri çerçevesinde erişilmesi sağlanır.
- **Bütünlük:** Bilgilerin doğruluğunun, tamlığının ve güvenilirliğinin korunmasına; yetkisiz veya hatalı değişikliklerin önlenmesine yönelik kontroller uygulanır.
- **Erişilebilirlik:** Bilgi sistemlerinin ve hizmetlerin, yetkili kullanıcıların ihtiyaç duyduğu zamanda güvenli ve sürdürülebilir şekilde kullanılabilir olması hedeflenir.
- **İzlenebilirlik ve hesap verebilirlik:** Bilgi sistemleri üzerindeki önemli işlemlerin izlenebilir olması, sorumlulukların açıkça belirlenmesi ve gerekli kayıtların korunması esastır.

Bilgi Varlıklarının ve Verilerin Korunması

Bankamız, bilgi varlıklarını yaşam döngüsü boyunca uygun güvenlik kontrolleriyle korumaktadır. Bilgilerin oluşturulması, kullanılması, saklanması, aktarılması, yedeklenmesi ve güvenli şekilde imha edilmesi süreçlerinde bilgi güvenliği gereklilikleri gözetilmektedir.

Bu kapsamda;

- Bilgi varlıkları belirlenmekte, önem ve hassasiyet düzeylerine göre sınıflandırılmaktadır.
- Erişimler görev, sorumluluk ve bilmesi gereken prensibi doğrultusunda sınırlandırılmaktadır.
- Bilgilerin yetkisiz erişim, değişiklik, kayıp, ifşa veya kötüye kullanıma karşı korunmasına yönelik kontroller uygulanmaktadır.
- Yedekleme, kayıt yönetimi, değişiklik yönetimi, zafiyet ve güncelleme süreçleri kontrollü ve izlenebilir şekilde yürütülmektedir.

Kimlik ve Eriřim Güvenlięi

Bilgi sistemlerine erişim yetkileri, görevlerin gerektirdięi asgari yetki prensibi doęrultusunda yönetilmektedir. Kullanıcıların kimliklerinin doęrulanması, yetkilerin düzenli olarak gözden geçirilmesi ve görev deęiřiklięi veya işten ayrılma durumlarında zamanında güncellenmesi esastır. Kritik ve ayrıcalıklı erişimler için risk düzeyiyle uyumlu ilave güvenlik ve izleme kontrolleri uygulanmaktadır.

Siber Güvenlik ve Olay Yönetimi

Bankamız, siber tehditleri ve bilgi güvenlięi olaylarını önlemek, tespit etmek ve etkilerini azaltmak amacıyla gerekli izleme, koruma ve müdahale süreçlerini işletmektedir.

Siber güvenlik faaliyetleri kapsamında;

- Bilgi sistemleri ve güvenlik olayları risk temelli bir yaklaşımla izlenmekte ve deęerlendirilmektedir.
- Tespit edilen olaylar önem ve etki düzeylerine göre sınıflandırılmakta, yetkilendirilmiş ekipler tarafından yönetilmektedir.
- Olayın sınırlandırılması, etkisinin giderilmesi ve hizmetlerin güvenli şekilde normale döndürülmesine yönelik çalışmalar yürütölmektedir.
- Önemli olaylar için kök neden ve etki analizleri gerçekleştirilmekte, tekrarın önlenmesine yönelik düzeltici ve iyileřtirici önlemler alınmaktadır.
- Yürürlükteki yükümlölükler doęrultusunda ilgili otoriteler ve sektörel yapılarla gerekli bildirim ve koordinasyon süreçleri yürütölmektedir.

Kişisel Verilerin ve Gizli Bilgilerin Korunması

Bankamız, kişisel verileri ve gizli nitelikteki bilgileri yalnızca belirli, açık ve meşru amaçlar doęrultusunda; yürürlükteki mevzuata ve kurumsal düzenlemelere uygun şekilde işlemekte ve korumaktadır.

Bu bilgilere erişim görev gereklilikleriyle sınırlandırılmakta; yetkisiz erişim, açıklama, deęiřtirme veya kayba karşı uygun teknik ve idari tedbirler uygulanmaktadır.

Üçüncü Taraf ve Destek Hizmeti Güvenlięi

Bankamız adına hizmet sunan kuruluşların bilgi güvenlięi riskleri, hizmet ilişkisinin nitelięi ve kapsamı doęrultusunda deęerlendirilmektedir.

Bu kapsamda;

- Bilgi güvenlięi ve gizlilik yükümlölükleri sözleşmelerde tanımlanmaktadır.
- Hizmet sağlayıcıların güvenlik, süreklilik ve olay bildirim sorumlulukları takip edilmektedir.
- Hizmet ilişkileri boyunca risk deęerlendirme, kontrol ve gözden geçirme faaliyetleri yürütölmektedir.

İş Süreklilięi ve Operasyonel Dayanıklılık

Bilgi güvenlięi, iş süreklilięi ve acil durum yönetimi süreçleri birbiriyle koordineli şekilde yürütölmektedir. Bankamız, kritik hizmetlerin olası kesintiler karşısında kabul edilebilir süreler içerisinde sürdürölebilmesini veya yeniden devreye alınmasını hedeflemektedir.

Bu doęrultuda;

- Kritik süreçler, bilgi sistemleri ve baęımlılıklar düzenli olarak deęerlendirilmektedir.
- İş süreklilięi, acil durum ve bilgi sistemleri kurtarma planları oluřturulmakta ve güncel tutulmaktadır.
- Planlar belirli aralıklarla test edilmekte, test ve tatbikat sonuçlarına göre iyileřtirilmektedir.
- Destek hizmeti alınan kuruluşların süreklilik yükümlölükleri de ilgili süreçler kapsamında deęerlendirilmektedir.

Çalışan Farkındalığı ve Sorumluluğu

Bilgi güvenliğinin yalnızca teknolojik tedbirlerle değil, çalışanların bilinçli ve sorumlu davranışlarıyla sağlanabileceği anlayışı benimsenmektedir.

Çalışanlara; bilgi güvenliği, kişisel veri güvenliği, sosyal mühendislik, ortalama saldırıları ve güvenli teknoloji kullanımı konularında düzenli eğitim ve farkındalık çalışmaları uygulanmaktadır. Çalışanların gizlilik ve bilgi güvenliği yükümlülüklerine görevleri süresince ve görevlerinin sona ermesinden sonra da uymaları esastır.

Uyum, Güvence ve Sürekli İyileştirme

Bilgi güvenliği yönetimi yaşayan ve sürekli gelişen bir süreç olarak ele alınmaktadır. Bu nedenle bilgi güvenliği uygulamalarımız düzenli olarak gözden geçirilmekte; risk değerlendirmeleri, güvenlik testleri, kontrol faaliyetleri ve denetim sonuçları doğrultusunda geliştirilmektedir.

Politika, süreç ve kontroller; bilgi sistemlerinde veya iş süreçlerinde meydana gelen değişiklikler, yeni tehditler, yaşanan olaylar ve mevzuat değişiklikleri dikkate alınarak güncellenmektedir.

Güvenlik Bildirimleri

Bilgi güvenliğini etkileyebileceği düşünülen şüpheli durumlar, sahte veya yanıltıcı iletişimler ve olası güvenlik açıkları Bankamızın resmî iletişim kanalları aracılığıyla bildirilebilir. Bildirimler yetkili birimler tarafından gizlilik içinde değerlendirilir ve gerekli incelemeler gerçekleştirilir.

Kamuoyu Taahhüdümüz

D Yatırım Bankası A.Ş. olarak müşterilerimizin ve tüm paydaşlarımızın bilgilerinin korunmasını temel sorumluluklarımızdan biri olarak görmek; güvenli, sürdürülebilir ve kesintisiz bankacılık hizmeti sunma hedefimiz doğrultusunda bilgi güvenliği uygulamalarımızı sürekli geliştirmekteyiz. Bu politika, Bankamızın kamuya açık bilgi güvenliği yaklaşımını açıklamak ve kamuoyunu bilgilendirmek amacıyla yayımlanmıştır.