BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK POLİTİKASI

QNB Finansbank'ta bilgi güvenliğinin amacı QNB Finansbank'ın varlıklarını, müşteri verilerini ve bilgi sistemlerini siber tehditlere karşı korumak için açık ve kapsamlı bir çerçeve oluşturmaktır. Bankanın bilgi güvenliği ve siber güvenlik gereksinimlerini, önemini ve uygulamasını tanımlama amacıyla yürütülen bilgi güvenliği yönetimi aktiviteleri için formal bir metodoloji oluşturmaktır. Siber tehditlere karşı güvenli ve dirençli bir altyapı oluşturulması ve sürdürülmesi, banka ve müşteri bilgilerinin güvenliğinin sağlanması, müşteri güveninin korunması konularında kararlılığını özetlemektedir.

Bu politika, QNB Finansbank bilgi varlıklarını, bilgi sistemleri süreçleri ve altyapısını, tüm çalışanları, üçüncü parti tedarikçileri, danışmanları, banka sistemlerine, verilerine veya teknoloji kaynaklarına erişimi olan tüm paydaşları kapsar.

Bilgi; kurum ve kuruluşların faaliyetlerini gerçekleştirmesi için gerekli olan, çeşitli ortamlarda bulunabilen değerli bir kaynaktır. QNB Finansbank edinilen, saklanan, taşınan tüm bilgilerin uygun koşullarda korunmasını hedeflemektedir.

QNB Finansbank'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.

QNB Finansbank'ta 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 gereksinimlerine uygun, BS 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. Yönetim kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlüdür. Bu sorumluluk kapsamında yönetim kurulu, banka genelinde uygulanmasını gözetmekle yükümlü olduğu bir bilgi güvenliği yönetim sistemi tesis eder. Bilgi güvenliği yönetim sistemi ulusal veya uluslararası standartları referans alır. Bankanın genel siber güvenlik stratejisinin oluşturulması, yeterli kaynakların sağlanması ve siber güvenlik önlemlerinin etkinliğinin düzenli olarak gözden geçirilmesi sağlanır. Bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesi sağlanır ve gelişen yeni teknolojileri de göz önünde bulundurarak bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesi için etkin bir gözetim faaliyeti yürütülür.

Banka genelinde bilgi güvenliği yönetim sisteminin nasıl uygulanacağı bilgi güvenliği ve siber güvenlik politikası, prosedürleri ve süreç dokümanları ile düzenlenir. Bilgi sistemlerine ilişkin kabul edilebilir kullanım standartları belirlenir.

Banka, bilgi varlıklarının güvenlik gereksinimlerine uygun kontroller tesis etmek için bu varlıkları sınıflandırarak detaylı bir varlık envanteri hazırlar. Her bir varlığın tanımlı ve onaylı bir güvenlik sınıfına ve erişim kısıtlamasına sahip olması sağlanır. Bilgi varlıklarının kötüye

kullanım ve zarara karşı uygun şekilde korunması, varlıkların gizlilik bütünlük ve erişilebilirliğini etkileyen güvenlik ihlalleriyle ilişkili risklere karşı korunması sağlanır.

Verilerin güvenlik sınıfına göre sınıflandırılması ve etiketlenmesi sağlanır. Verilerin güvenlik sınıfına göre taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu ortamlarda, tutulduğu ortamın kâğıt veya elektronik ortam olmasından bağımsız olarak gizliliğini sağlayacak önlemler alınır. Verilerin paylaşım koşulları belirlenir. Hassas verilerin farklı güvenlik seviyesine sahip ortamlar arasında iletiminde uçtan uca güvenli iletişimin kullanılması ve bu verilerin şifrelenmiş bir şekilde saklanması esastır. Veri gizliliğini sağlamada kullanılacak şifreleme teknikleri için güncel durum itibarıyla güvenilirliğini yitirmemiş ve günün teknolojisine uygun algoritmalar kullanılır. Veri barındıran ortamların, medya ya da cihazların içerdikleri verilerin gizlilik derecesine uygun imha politikaları, koşulları belirlenir ve güvenli bir şekilde imhası sağlanır. Bilginin sahibi, bilgi varlıklarının sınıflandırılması, erişim yetkisi verilmesi, bilginin ne zaman ve nasıl güncellenmesi, silinmesi, imhası, transferi konularında nihai sorumluluğu ve yetkisi bulunan iş birimi temsilcileridir.

Banka, bilgi varlıklarına olan erişimlerin, görevler ayrılığı ve en az yetki prensibine göre belirlenmiş, kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrolleri uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesini sağlamakla yükümlüdür. Bilgi sistemlerine ait kimlik doğrulama ve erişim yönetimi politikaları ve standartları belirlenir.

Banka, bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli tedbirleri alarak bunların doğruluğunu, tamlığını ve güvenilirliğini temin eder. Proje yönetiminde güvenlik gereksinimlerinin proje yaşam döngüsünde belirlenmesi ve karşılanması sağlanır. Yasal gereksinimler, kimlik doğrulama, yetkilendirme, erişim kontrolleri, onay mekanizmaları, şifreleme, iz kaydı gibi güvenlik ve gizlilik gereksinimleri, bütünlük ve erişilebilirlik ihtiyaçlarına ait detay gereksinimler tanımlanır.

Banka, bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması tesis eder. İz kayıtlarının oluşturulması, detayı ve içeriği, saklanma süresi, erişim koşulları, takibi ve yedeklenmesi koşulları riskler ve yasal gereksinimler doğrultusunda belirlenir. Tesis edilecek iz kayıt mekanizmasının, yaşanan bilgi güvenliği ve siber güvenlik olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte olması sağlanır.

Kurumsal mimari içerisinde bankanın siber güvenlik çözümleri ve gereksinimlerini özetleyen ve siber güvenlik yeteneklerinin geliştirilmesine yönelik tasarım ilkelerini ele alan siber güvenlik mimarisi tanımlanır. Oluşturulan güvenlik stratejisi doğrultusunda gelişmiş ve güncel tehditlere karşı koruma sağlamak için son teknoloji ürünü güvenlik araçlarına ve teknolojilerine yatırım yapılır. Banka gerek kendi kurumsal ağı gerek dış ağlardan gelebilecek tehditler için gerekli ağ güvenlik kontrol sistemlerini tesis eder. Güvenlik önlemlerinin tesis edilmesinde çok katmanlı güvenlik mimarisi esas alınır. İşletim sistemi, veritabanı, uygulamalar ve ağ cihazları için güvenlik konfigürasyon yönetimi sağlanır. Bankanın BS altyapısı ve süreçlerindeki potansiyel güvenlik açıklarını ve tehditleri tespit etmek, hızlı ve etkin bir şekilde gidermek için etkin bir zafiyet ve tehdit yönetim süreci, yama yönetimi süreci tesis edilir. Kapsamlı ve düzenli risk değerlendirmesi, sızma testleri ve güvenlik taramaları yapılır.

Banka, siber olayların tespiti, ele alınması, takibi ve raporlanması, bankacılık faaliyetlerini en az etkileyecek şekilde ve mümkün olan en kısa sürede BS hizmetlerini normal işleyişine

döndürmek üzere olayın çözüme kavuşturulmasına yönelik etkin bir siber olay yönetimi ve siber olaylara müdahale süreci oluşturur.

Dış hizmet ve tedarikçilerden alınacak hizmetlerin banka açısından doğuracağı güvenlik risklerinin değerlendirilmesi ve yönetilmesi için yeterli bir gözetim mekanizması tesis edilir.

Banka tesisleri, veri merkezi, kritik bilgi sistemleri ve varlıkları, dış ve çevresel tehditlere karşı, yetkisiz erişim ve müdahaleyi önlemek için yasal gereksinimler doğrultusunda fiziksel güvenlik kontrolleri oluşturulur, ilgili politika ve standartlar belirlenir.

Banka, sunmakta olduğu elektronik bankacılık hizmetleri kapsamında gerçekleştirilen işlemlerde hem banka hem de müşteri için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanır. Kimlik doğrulama ve işlem güvenliği politikaları belirlenir ve uygulanır. Elektronik bankacılık hizmetlerine ilişkin tehditler ve siber güvenlik risklerine ilişkin uygun güvenlik önlemleri alınır, teknolojik çözümler kullanılır, güvenlik açıklarını giderecek gerekli yamalar ve güncellemeler müşteri kullanımına sunulur. Bankanın elektronik bankacılık hizmetlerine ilişkin risklerin etkisini azaltmaya yönelik benimsediği güvenlik prensipleri ve bu risklerden korunmak için kullanılması gereken yöntemler müşterinin dikkatine sunulur.

Bilgi Teknolojileri Genel Müdür Yardımcılığı, bilgi sahiplerinin tanımladığı güvenlik gereksinimlerine uygun olarak bilginin ve üzerinde bulunduğu ortamların yönetiminden ve korunmasından sorumludur.

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 farkındalık seviyesini arttırıcı faaliyetlerin desteklenmesi ve bilgiyi korumak için gerekli kaynakların sağlanması üst yönetimin sorumluluğundadır. Banka genelinde bilgi güvenliği ve siber güvenlik farkındalık seviyesini artırmak için kapsamlı bir bilgi güvenliği farkındalığı eğitim programı oluşturulur ve uygulanır.

Banka içerisinde bilgi güvenliği ve siber güvenliğin sağlanması için kontrollerin gözetimi, güvenlik ihlali durumunda disiplin süreci ile gerekli yaptırımın uygulanması üst yönetim sorumluluğundadır.

“Bilgi Güvenliği ve Siber Güvenlik Komitesi”, bilgi güvenliği ve siber güvenlik politikasının oluşturulması ve bilgi güvenliği yönetiminin uygulanması faaliyetlerinin üst yönetim adına

BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK POLİTİKASI

gözetimi için bilgi güvenliği ve siber güvenlik çalışmalarına yönlendirme ve koordinasyonu sağlar. Komite, bilgi güvenliği ve siber güvenlik stratejisi, politikalar, programlar, güvenlik risk yönetimi süreci, temel risk göstergelerini (KRI'lar) ve temel performans göstergelerini (KPI'lar) izler, gözden geçirir ve yürütülen faaliyetlere ilişkin yılda en az bir defa yönetim kuruluna rapor sunar.

Bilgi güvenliği ve siber güvenlik uygulamalarımızın grup siber güvenlik politikaları ile uyumlu olması zorunludur ve grup genelinde güvenli ve dirençli bir dijital ortamın sürdürülmesine yönelik ortak vizyona olan bağlılığımızın altını çizmektedir. Tüm grup ve iştirakler genelinde proaktif önlemler uygulanarak, güvenlik ortamı sürekli izlenerek ve siber güvenliğe duyarlı bir kültür teşvik edilerek, siber tehditlere karşı dirençli kalma ve bankamızın güvenlik yeteneklerine güven oluşturma hedeflenir. Bu yaklaşım dijital varlıklarımızın, müşteri verilerimizin ve kritik sistemlerimizin korunmasında tutarlılık, iş birliği ve kolektif güç sağlar.

Bilgi güvenliği ve siber güvenlik politikasına uyum, banka içerisinde Teftiş Kurulu tarafından denetlenir ve üst yönetime raporlanır. Politikanın ihlal edilmesi durumunda, Teftiş Kurulu tarafından sorumlular hakkında soruşturma ve inceleme başlatılır, disiplin kurulu kararlarına göre yaptırımlar uygulanır.

Bu politika, Yönetim Kurulu tarafından periyodik olarak en az yılda 1 (bir) kez gözden geçirilir. Kanun ve yönetmeliklerdeki değişiklikler, önemli bilgi güvenliği vakaları, yeni kritik güvenlik açıkları, önemli altyapı değişikliklerinin bir sonucu olarak bilgi güvenliği gereksinimlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Güncellenen politika onaylanarak uygun kitleye sunulmak üzere elektronik ortamda yayınlanır.