HEDEF
YATIRIM BANKASI

BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Hedef Yatırım Bankası A.Ş. (“Banka”) Bilgi Güvenliği Politikası’nın (“Politika”) amacı, Banka bilgi varlıklarının güvenliğinin sağlanması, bilgi varlıklarına yönelik kasıtlı veya kasıtsız her türlü tehdidin belirlenmesi ve bu tehditlerin oluşturabileceği risklerin yönetilebilmesidir.

2. KAPSAM

Politika, Bankanın ortam ve formata bakılmaksızın saklanan, iletişim halindeki ve işlenen fiziksel ve elektronik tüm bilgi ve verilerini kapsar. Politika, Bankanın tüm çalışanlarına, yüklenicilere, tedarikçilere ve Banka ile çalışan üçüncü kişilere uygulanır.

Bilgi sistemleri vasıtasıyla üretilen bilgi, hizmet ve üretim süreçleri ile kullanılan tüm bilgi teknoloji donanımları, yazılımları, işletim sistemleri, bilgi saklama ortamları, iletişim ağları ve dokümantasyon ile bu sistemlere etkileşimde bulunan diğer tüm sistemler bu Politika kapsamındadır.

3. TANIMLAR

Bilgi: Banka için değeri olan ve basılı veya elektronik ortamlarda saklanabilen, posta ve elektronik imkanlar kullanılarak gönderilebilen ve korunması gereken varlık

Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunması

BGK: Bilgi Güvenliği Komitesi

BGYS: Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Olayı: Olası bir bilgi güvenliği politikası açığı, uygulanmış kontrollerin başarısızlığı ya da güvenlikle ilgili olabilecek önceden bilinmeyen bir durumu belirten bir sistem, hizmet ya da ağ durumunun ortaya çıkışı, bilgi güvenliği politikaların bilerek ya da bilmeyerek ihlal edilmesi

Bilgi Varlığı: Banka için değeri olan ve işin yapılması için kullanılan her türlü veri ve bu verileri işleyen ya da kullanan her türlü yazılım, donanım, servis, süreç ...vb varlıklar

Bilginin Bütünlüğü: Bilginin güncel olması, doğruluğunun ve tamlığının korunması ve sadece yetkili kişiler tarafından değiştirilmesi

Bilginin Erişilebilirliği: Bilginin ihtiyaç duyulduğunda erişilebilir olması; yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olması

Bilginin Gizliliği: Bilgiye sadece yetkili kişiler tarafından erişilebilmesi; bilgiye yetkisiz kişiler, varlıklar ya da süreçler tarafından erişilememesi veya kullanılamaması

Hassas Veri: BDDK tarafından yayımlanan “Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hakkında Yönetmelik”de tamımlanan “Hassas Veri”

Kurumsal SOME: Banka bünyesinde oluşturulan, bilgi güvenliği olaylarına müdahale etmekle sorumlu, çeşitli birimlerden çalışanların katılımıyla oluşturulmuş siber olaylara müdahale ekibi

Risk: Bilgi varlıklarına yönelik tehditlerin oluşturabileceği potansiyel kayıplar

Sektörel SOME: USOM mevzuatı kapsamında sektörler bazında kurulan SOME organizasyonları

USOM: Ulusal Siber Olaylara Müdahale Merkezi

Üçüncü Taraflar: ISP ve diğer servis sağlayıcılar, telekom operatörleri, destek ve servis elemanları, müşteriler, danışmanlar, denetçiler, stajyerler ve diğer geçici çalışanlar, temizlik ve yemek şirketi elemanları ve benzeri

4. İLKE VE ESASLAR

Banka, bu Politikaya uyumu sağlamak ve sürdürmek, kanunlara ve yasal düzenlemelere, sözleşmelerden doğan yükümlülüklere ve iş ihtiyaçlarına uygun şekilde bilgi güvenliğini sağlamak üzere ulusal ve uluslararası bilgi güvenliği standartlarını esas alır.

Bilgi Güvenliği politikasının oluşturulması ve uygulanması faaliyetlerinin Yönetim Kurulu adına gerçekleştirilmesi, güvenlik önlemlerinin etkinliğinin değerlendirilmesi ve izlenmesi, bilgi güvenliği risklerinin kabul edilebilir seviyeye indirmek amacıyla gerekli yönlendirmelerin yapılması amacıyla Bilgi Güvenliği Komitesi kurulur.

Bilgi Güvenliği Komitesinin koordinasyonunu sağlaması, BGYS kapsamında oluşturulan politika ve prosedürlerinin yönetilmesi, Banka içinde bilgi güvenliği bakış açısı ile bilgi varlıklarının sınıflandırılması, gerekli güvenlik önlemlerinin alınması ve aldırılması ve bilgi güvenliği faaliyetlerine ilişkin yönetim kuruluna rapor sunulması Bilgi Güvenliği ve Kalite Direktörlüğü sorumluluğundadır. Bilgi Güvenliği ve Kalite Direktörü Banka'nın bilgi güvenliği sorumlusudur.

Yasal otoriteler ile, siber olaylar ve dolandırıcılık faaliyetlerine ilişkin iletişimi sağlamak amacıyla bir irtibat görevlisi atanır ve ilgili otoriter kurumlar bilgilendirilir.

Banka bilgi varlıklarını etkileyecek, her tülü siber olaylara karşı önlem alacak, müdahale planlarının etkinliğini test edecek, Sektörel SOME ve USOM ile koordineli çalışacak bir Kurumsal SOME ekibi kurulur.

Mevzuat, yönetmelik ve sözleşmelerde önemli değişiklikler veya yeni tehdit ve zafiyetlerin ortaya çıkması durumlarında, risklerin kabul edilebilir seviyeye indirilmesi için alınmış olan önlemler gözden geçirilir ve gerektiğinde yeni önlemler alınır.

Bu Politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar BGYS prosedürleri ile düzenlenir.

Sistemler, erişilen uygulama ve cihazlar sadece Bankanın işlerinin yürütülmesi için kullanılır, iş dışı amaçlarla kullanılamaz. Tüm kaynaklar yetkili çalışanlar tarafından güvenlik veya bakım amaçlı düzenli veya düzenli olmayan aralıklarla izlenir. Dış ve iç kaynaklarlar da zafiyetleri tespit etmek amacıyla sızma testleri ve zafiyet tarama çalışmaları gerçekleştirilir.

Kişisel verilerin güvenliği için yasal düzenlemeler, yönetmelik veya mevzuata uyum sağlayacak önlemler alınır.

Hassas verinin yetkisiz erişime maruz kalmaması için bilgi sınıflandırması ile uyumlu şekilde şifreleme teknikleri kullanılır.

Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur. Bilgi varlıkları sahipleri atanır, sınıflandırılır ve sınıflandırmalarına uygun güvenlik ihtiyaçları ve kullanım kuralları belirlenir. Bilgi varlıklarına erişen ve bilgi varlıklarını kullanan şirket çalışanları ve üçüncü tarafların tanımlanabilir, hesap verebilir ve izlenebilir olması için gerekli güvenlik önlemleri alınır.

Banka bilgilerinin, sadece iş ihtiyaçları doğrultusunda yetkilendirilmesi, sadece yetki verilen amaçlarla kullanılması sağlanır. Bilgi varlıklarına erişim sadece yetkili kişilere, önceden belirlenmiş olan yetki ve sorumlulukları dahilinde görevlerini yerine getirmeye imkân verecek şekilde minimum seviyede ve görevler ayrılığı ilkesi de göz önünde bulundurularak verilir.

Banka bilgi varlıklarının korunması amacıyla, belirli zaman aralıklarında risk değerlendirme çalışmaları gerçekleştirilir ve bu doğrultuda gereken aksiyonlar alınarak riskler yönetilir.

Bilgi güvenliği olaylarının ve zayıflıklarının raporlanması için gerekli altyapı oluşturulur. Olay kayıtları tutulur ve gerekli düzeltici ve iyileştirici faaliyetler uygulanır.

İlgili mevzuatlara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli kontrol süreçleri tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri gerçekleştirilir ve sonuçları takip edilerek raporlanır.

Dış hizmet alımlarının yönetimi kapsamında Banka Bilgi Güvenliği politika ve standartlarına uyum göz önünde bulundurulur.

Yaşanacak herhangi bir olumsuzluk karşısında faaliyetlerin ve paydaşlara olan sorumlulukların aksamaması ve banka servislerinin kesintiye uğramaması adına İş Sürekliliği Politikalarında belirlenen ilke ve esaslara uyum gözetilir. Bu kapsamda, Yedekleme ve Acil Durum Merkezi ortamları oluşturulur ve ihtiyaç duyulduğunda çalışır durumda olması sağlanır.

Bilgi güvenliği farkındalık programı hazırlanarak bu kapsamda gerekli eğitim, anket ve bülten çalışmaları yapılır. Farkındalık programı ile, Banka bilgi güvenliği politika ve stan-

dartlarının çalışanlar tarafından bilinmesi, sahiplenilmesi ve faaliyetlerinin Politika ile uyumunun sağlanması amaçlanır.

Bu Politikaya uymayan durumlar, Bilgi Güvenliği ve Kalite direktörlüğü çalışanlarına yönlendirilir. Bilgi Güvenliği ve Kalite direktörlüğü çalışanları, ilgili durumları ve istisna taleplerini Bilgi Güvenliği Komitesi'ne sunar. Bilgi Güvenliği Komitesi istisna taleplerini kabul ya da reddetmeye yetkilidir.

Banka içinde kullanılan ve lisans gerektiren her türlü yazılım lisanslı olmalıdır. Kullanıcılar ve bilgi teknolojileri çalışanları, kullanılan her türlü ürün ve diğer materyallerin telif haklarına uymakla yükümlüdür.

Bilgi varlıklarının değeri, gizlilik seviyesi, kaybolma ve çalınma tehlikesi ve tekrar elde etme kolaylığıyla uyumlu olarak fiziki ve mantıksal erişim güvenliği mekanizmaları kullanılarak bilgi varlıkları korunur. Bilgi varlıklarının Banka dışına çıkarılması durumlarında, içinde bulunduğu güvenlik sınıfına uygun koruma kuralları geçerlidir.

Bilgi varlığının bütünlüğü yetkisiz değişikliklere karşı korunur. Bilgi varlığının iş süreçleri tarafından ihtiyaç duyulduğunda erişilebilir olması için bilgi güvenliği ile ilgili gereksinimler de göz önüne alınarak gerekli önlemler alınır.

Veri merkezleri, sunucuların bağlı bulunduğu odalar, kablo dolapları, Acil Durum Merkezi gibi önemli merkezlerin fiziki güvenliği sağlanır. Bu tip yerlere sadece yetki verilen kişilerin erişebilmesini sağlayacak süreçler oluşturularak uygulanır.

Bankanın ağlarına yapılacak iç ve dış bağlantıların, ağ üzerinde iletilen verilerin bütünlüğüne ve ağın kendisine herhangi bir zarar vermeden yapılması gerekir. Üçüncü taraflar, kendilerine ait herhangi bir cihazı Banka ağına bağlayamazlar. Üçüncü tarafların Banka ağından bilgi talepleri ancak Bankadaki muhatap direktörlük yöneticisinin ve Bilgi Güvenliği ve Kalite biriminin tespit ettiği yöntemle ve onayı alındıktan sonra karşılanır.

Politikaya uyum için gerekli standartlarla beraber sistemlerin iş amaçlı kullanımı, gizlilik, elverişlilik, bütünlük, arşiv, imha, erişim güvenliği, ağ güvenliği, güvenlik ihlali, yazılım lisansları ve telif hakları gibi hususlar BGYS prosedürlerinde detaylandırılmıştır.

Uyulması gereken kabul edilebilir kullanım kuralları, BGYS kapsamında hazırlanan prosedürlerde belirtilmiştir. BGYS kapsamı dahilinde yer alan tüm çalışanlar ve üçüncü taraflar kurallara uymakla yükümlüdür. Banka adına uygulama ve sistem geliştiren dış hizmet firmaları kendi iç süreçlerinde Bankanın bilgi güvenliği politika ve prosedürlerine uygun süreçler işletmekle yükümlüdür. Bankanın talep edeceği her türlü bilgi ve belgeyi sağlamakla ve tesis edeceği ek önlemlere uymakla yükümlüdür.

Banka içinde geliştirilen tüm projelerde bilgi güvenliği esasları göz önünde bulundurulur İşe alım, görev değişikliği,işten ayrılma ve diğer insan kaynakları süreçlerine yönelik bilgi güvenliği kontrolleri belirlenir ve uygulanır.

Uzaktan çalışma esasları için teknik ve fiziksel koruma önlemleri kurumsal riskler göz önünde bulundurularak oluşturulur. Üçüncü taraflara verilecek her türlü bağlantı yetkisi öncesi risk değerlendirmesi yapılır ve gerekli önlemler alınarak yetki verilir. Uzak bağlantı yetkileri düzenli olarak gözden geçirilir ve gerekli düzenlemeler yapılır.

Yasal düzenlemeler ve güvenlik önlemleri gerekliliği olarak iz kayıtları saklanır ve düzenli olarak incelenir. Bankacılık faaliyetleri kapsamında gerçekleştirilen işlemler için inkar edilemezliği ve sorumluluk atamayı mümkün kılacak yeterli ve etkin bir denetim izi tutma mekanizması tesis edilir.

Kötü niyetli yazılımlardan korunmak için teknik açıklıkların kontrolü, yama yönetimi, zararlı yazılım tespit ürünlerinin kullanımı yanında kullanıcıların duyarlılığı da koruma sisteminin bir parçası kabul edilir.

Kullanıcılara, görev ve sorumluluklarına uygun roller ve profiller aracılığı ile yetki verilir ve sistemler üzerindeki yetkiler dokümante edilir. Ayrıcalıklı yetkilere sahip kullanıcılar için ek güvenlik önlemleri uygulanır. Sistemlere erişimler için kullanılan kimlik doğrulama anahtarlarının birden çok kişi tarafından kullanılmayacak şekilde bir kişiye atanması esastır. Bilgi varlıklarına ve kritik mekanlarına yetkisiz erişimleri, çalınmayı ve fiziksel zararı engelleyici kontroller oluşturulur.

Bilgi sistemleri hizmetlerinin güvenli ve kesintisiz sunulabilmesi için iletişim ağı üzerinde gerekli kontroller tesis edilir.

Bilgi Güvenliği Politika ve prosedürlerinde belirtilen önlemlerin gerek teknik gerekse iş ihtiyacı açısından uygulanamadığı durumlar ayrıca dokümante edilerek gerekli onaylar alınır.

5. SORUMLULUKLAR

Politika'nın oluşturulmasından, yayımlanmasından, güncel ve işler tutulmasından ve uygulamasının izlenmesinden Bilgi Güvenliği Komitesi sorumludur.

Tüm Banka çalışanları ve üçüncü taraflar bu Politika ve BGYS prosedürlerini bilmek ve çalışmalarını bu düzenlemelere uygun şekilde yürütmekle yükümlüdür. Bütün çalışanlar ve üçüncü taraflar işlerini bu Politika ile uyum içinde gerçekleştireceklerini anlamalı ve yazılı olarak bunu onaylamalıdırlar. Politikaya aykırı faaliyetler ile Banka bilgilerinin gizliliğini, bütünlüğünü veya elverişliliğini tehlikeye düşürecek davranışlar, İş Kanunu ve Banka iç düzenlemeleri hükümleri uyarınca değerlendirilir.

6. YÜRÜRLÜK

Politika, Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girer. Politika, yılda en az bir kez ya da sistem yapısını veya risk değerlendirmesini etkileyecek önemli bir değişiklik olması durumunda gözden geçirilir ve gerekli görülmesi halinde güncellenir.

HEDEF

YATIRIM BANKASI