KKTC MERKEZ BANKASI

BİLGİ GÜVENLİĞİ POLİTİKASI GENELGESİ

(Genelge No: 2015/02)

Mart-2015

BANKACILIK DÜZENLEME VE GÖZETİM MÜDÜRLÜĞÜ

İçindekiler

BİLGİ GÜVENLİĞİ POLİTİKASI GENELGESİ

(Genelge No: 2015/02)

Giriş

İşbu Genelge, 39/2001 Sayılı Bankalar Yasasının 15'inci maddesinin (3)'üncü fıkrası altında 18 Aralık 2014 tarih ve 258 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren "Bankalarda İç Denetim, Risk Yönetimi, İç Kontrol ve Yönetim Sistemleri Tebliği'nin" 11'inci maddesinin (3)'üncü fıkrası (E) bendi (b) alt bendi uyarınca düzenlenmiş olup, Bankamız Yönetim Kurulunun 30 Mart 2015 tarih ve 902 sayılı kararı ile onaylanmıştır. 2015/02 sayılı Genelge 8 Nisan 2015 tarihinde yürürlüğe girer.

1 Amaç

Bilgi güvenliğini etkin bir şekilde sağlamak amacıyla uygulanan kurallar ve metotlar, bankanın tehdit ve açıklarını analiz ederek, risklerini farkına varmasından, teknik güvenlik çözümlerini sisteme entegre etmesine, sözleşmelerde bilgi güvenliğini de ele alan düzenlemeler yapmasından, kullanıcıların bilgi güvenliği farkındalığını arttırmaya kadar çok çeşitli alanlarda uygulanabilir. Bu metotlardan en önemlisi, bankanın bilgi güvenliği hedefini ve bu hedefe ulaşmak için uygulanacak kural ve metotların çerçevesini çizen bilgi güvenliği politikalarının oluşturulması ve uygulanmasıdır.

Bu dokümanın amacı ISO/IEC 27001 standardına uygun olarak bankaların Bilgi Güvenliği Politikası oluşturması ve bu politikanın uygulanması ile ilgili usul ve esaslar açıklamaktır.

2 Bilgi Güvenliği Politikaları

Bilgi güvenliği politikaları, bir bankanın değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür.

Bu kural ve uygulamaları tanımlayan politikalar çeşitli seviyelerde yazılabilir. Politikalar, genel bir Bilgi Güvenliği Politikası ve belirli alanlara ait politikalardan (Erişim Kontrol Politikası, Bilgisayar Ağları Güvenlik Politikası, Sistem Erişim ve Doğrulama Politikası, Sistem Yönetim ve İşletim Politikası vb.) oluşur ve uygulamaları tanımlayan prosedür ve talimatlarla tamamlanır.

Her seviyedeki politikanın tek bir dokümanda bulunması yerine, en üst seviyede temel ilkeleri barındıran bir Bilgi Güvenliği Politikasının oluşturulması ve bu dokümanla diğer ayrıntılı politikaların ilişkilendirilmesi gerekmektedir.

Bilgi güvenliği politikası, bu politikalar doğrultusunda uygulanacak prosedürlerin amaçlarını tanımlayan en üst düzey doküman olmalıdır.

3 Bilgi Güvenliği Politikasının Bileşenleri

Bilgi Güvenliği Politikası, bankanın bilgi güvenliği ihtiyacını ve bilgi güvenliği kavramını bankanın bilgi kaynaklarını kullanan her kişiye anlatma amacıyla hazırlanmalıdır. Bankanın bilgi güvenliği ihtiyacı ile ilgili iş gerekleri ve yasal zorunluluklar bu dokümanda net bir biçimde ortaya konmalıdır.

Bilgi güvenliği politikası, banka yönetiminin bilgi güvenliğine dair sözünü ve desteğini göstermeli ve bilgi güvenliğinin, bankanın belirlemiş olduğu misyonuna ulaşabilmesindeki destekleyici rolünü tanımlamalıdır.

Bilgi Güvenliği Politikasında asgari aşağıdaki hususlar yer almalıdır:

a. Bilgi güvenliğinin tanımı, genel kapsamı ve hedefi,

b. Bilgi güvenliğinin banka için önemi, bilgi güvenliği sağlanmasının amacı ve bilgi güvenliği ilkeleri, bu amaç ve ilkeler için yönetim desteği,

c. Kontrol hedefleri ve kontrollerin seçimi için risk değerlendirmesi ve risk yönetimini de içeren bir çerçevenin ortaya konulması,

d. Güvenlik politikaları, ilkeleri, standartları ve uyum gereksinimlerinin özet bir açıklaması,

e. Bilgi güvenliği ile ilgili tüm görev ve sorumlulukların tanımı,

f. Diğer ayrıntılı politikalar ve belirli bilgi sistemleri için prosedürler veya kullanıcıların uyması gereken kurallar gibi politikayı destekleyen dokümanlara atıflar.

3.1 Bilgi Güvenliğinin Tanımı

Bilgi güvenliği politikası bankanın geneline hitap etmektedir. Banka içinde farklı görevlerde birçok çalışan olduğundan dolayı bilgi güvenliği kavramı bazı çalışanlar için yabancı veya yeni bir kavram olabilir. Bilgi güvenliği dendiğinde herkes tarafından aynı kavramın anlaşılmasını sağlamak için, politikada bilgi güvenliğinin açık ve anlaşılır bir tanımının bulunması gereklidir.

3.2 Bilgi Güvenliği İhtiyacı ve Bilgi Güvenliği Kapsamı

Bankanın bilgiye, dolayısıyla bilgi güvenliğine olan bağımlılığını vurgulayan bir ifadeden oluşmalıdır. Bir bankada neden bilgi güvenliği politikasına ihtiyaç duyulduğu sorusunun temelini oluşturmalıdır.

Bilgi güvenliği kapsamı ile bankada hangi yönetimsel birimlerin ve aktivitelerin bilgi güvenliği yapısı içinde değerlendirileceği belirtilmelidir.

3.3 Bilgi Güvenliği Hedefleri

Bilgi güvenliği hedefleri, bilgi güvenliğinin yönetimi ile ulaşılacak amaç hakkında okuyucuyu bilgilendirmek için özet olarak tanımlanmalıdır. Bu hedefler bankanın iş gerekleri ve stratejileri ile ilişkilendirilmelidir.

3.4 Risk Yönetim Çerçevesi

Banka, bankanın bilgi güvenliği risklerini nasıl yönettiğine dair bir çerçeve ortaya koymalıdır. Bankanın bilgi güvenliğini sağlamak için uygulayacağı kontroller ve bu kontrollerin hangi risklerle ilintili olarak uyguladığını ortaya koyduğu bir metodolojisi bulunmalıdır.

3.5 Yönetimin Bilgi Güvenliği Sağlama Sözü ve Politika Dokümanının Onayı

Banka yönetiminin, bankada bilgi güvenliğini sağlama niyeti, politikada bulunması gereken en önemli ifadedir. Yönetim, bu söz ile bilgi güvenliği amaçlarına ulaşma konusunda kararlılığını ve bu iş için gereken desteği sağlayacağını ifade ederken, banka çalışanlarının bilgi güvenliğine önem vermesini de sağlamalıdır. Onay imzası, bankada bilgi güvenliğinin sağlanmasının desteklendiğini gösterir ve bankadaki en yüksek makam tarafından imzalanmalıdır.

3.6 Bilgi Güvenliği İlkeleri

Bilgi güvenliği ilkeleri, bankadaki bilgi güvenliği ile ilgili genel kuralları koymalı ve bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlamalıdır.

3.7 Roller/Görevler ve Sorumluluklar

Bu kısım, bankada bilgi güvenliği ile ilgili, tam olarak ne beklendiğini anlatır. Görev ve sorumluluklar, bankanın bilgi kaynaklarını kullanan tüm tarafların sorumluluklarını ve bilgi güvenliğinin her alanını kapsamalıdır.

3.8 Politikanın İhlali ve Yaptırımlar

Bir kullanıcının politikaya uymadığı ve politikayı ihlal ettiği durumlarda o kullanıcıya yaptırım uygulanabileceğini belirten ifadedir. Bankanın genel disiplin politikasıyla ilişkilendirilmelidir.

3.9 Atıflar (Diğer Politika, Prosedür, Talimat ve Yönetmeliklere Atıflar)

Bilgi güvenliği politikası tek başına bir doküman değildir. Bilgi güvenliği amaçlarının gerçekleşmesi için hazırlanan başka ilgili politikalar, prosedürler, talimat ve yönetmeliklerle desteklenmelidir.

Ayrıca, yasa, mevzuat vb. ile belirtilmiş, bankanın uygulaması gereken belirli kontrol ve önlemler varsa, bu kontrol ve önlemlere politikada referans verilmelidir.

3.10 Bilgi Güvenliği Politikası Gözden Geçirme Kuralları

Bankada bilgi güvenliğinin sağlanması için, uygulamaya konulan kurallar ve alınan önlemlerin uygulanabilirlik ve etkinlik açılarından kontrol edilmesi ve gerekli gözden geçirme ve güncellemelerin yapılması gerekmektedir. Politika düzenli olarak en az yılda bir defa gözden geçirilmelidir. Politika ile ilgili gözden geçirme, geliştirme ve değerlendirmelerin kimin tarafından, hangi aralıklarla yapılacağı belirlenmeli ve dokümanda yer almalıdır.

Bunun dışında, bilgi güvenliği uygulama süreçlerindeki değişiklikler, ortaya çıkabilecek yeni yasal düzenlemeler ve teknik değişikliklere göre de politikanın düzenlenmesi gerekmektedir.

Her iki durumda da, yapılan gözden geçirme ve güncellemelerin kayıtlarının tutulması ve geliştirilen politikanın Banka Yönetimi tarafından tekrar onaylanıp, yürürlüğe konması gerekmektedir. Dokümanda politikanın gözden geçirme ve yayınlanma tarihleri bulunmalıdır.

3.11 Bilgi Güvenliği Politikasına Erişim

Bilgi Güvenliği Politikası bankada bilgi güvenliğine yön veren temel doküman olduğundan dolayı bankanın tüm paydaşları tarafından kolayca erişilebilen ve bilinen bir doküman olmalıdır. Banka Yönetimi, bunu sağlamak için gereken tedbirleri almalı, çalışanlarının bankadaki bilgi güvenliği varlıklarının korunmasındaki sorumluluklarını bilmeleri ve anımsayabilmeleri amacıyla çalışanlara yönelik olarak bilgilendirme ve farkındalık eğitimleri düzenlemelidir.

Bilgi güvenliği politikasının banka çalışanları tarafından uygulanması beklendiğinden dolayı tüm kullanıcılar tarafından anlaşılabilir ve net olmalıdır.

4 Bilgi Güvenliği Politikasının Merkez Bankasına İletilmesi

Banka Yönetimi, Bilgi Güvenliği Politikasını yönetim kurulunda onaylandıktan sonra, yedi iş günü içinde Merkez Bankasına hem elektronik ortamda hem de matbu olarak bildirilmelidir. Politika her değiştirildiğinde aynı süreç tekrarlanmalıdır.