

TEBLİĞ

Bankacılık Düzenleme ve Denetleme Kurumundan:

**BANKALARDA BİLGİ SİSTEMLERİ YÖNETİMİNDE ESAS ALINACAK
İLKELERE İLİŞKİN TEBLİĞ**

**BİRİNCİ KISIM
Başlangıç Hükümleri**

Amaç ve kapsam

MADDE 1 – (1) Bu Tebliğin amacı, bankaların, faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetiminde esas alınacak asgari usul ve esasları düzenlemektir.

Dayanak

MADDE 2 – (1) Bu Tebliğ, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 93 üncü maddesi ve 1/11/2006 tarihli ve 26333 sayılı Resmî Gazete’de yayımlanan Bankaların İç Sistemleri Hakkında Yönetmeliğin 11 inci maddesinin beşinci fıkrası ile 16 ncı maddesinin üçüncü fıkrası uyarınca düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 3 – (1) Bu Tebliğde yer alan;

- a) Akıllı kart: Üzerinde, bilginin kaydedilebildiği ve işlenebildiği çip barındıran kartı,
- b) ATM: Otomatik para çekme işleminin yanı sıra diğer bankacılık işlemlerinin tamamının veya bir bölümünün gerçekleştirilmesine imkân veren elektronik işlem cihazlarını,
- c) Banka: Kanunun 3 üncü maddesinde tanımlanan bankaları,
- ç) Bilgi sistemleri yönetimi: Bankaca gerçekleştirilen faaliyetlerin ve verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yürütülmesi; mevzuattan kaynaklanan yükümlülüklerinin yerine getirilmesi; muhasebe ve finansal raporlama sisteminden sağlanan bilgilerin bütünlüğünün, tutarlılığının, güvenilirliğinin, zamanında elde edilebilirliğinin ve gereken durumlarda gizliliğinin sağlanması amacıyla uygun bilgi sistemleri ortamının tesis edilmesine, bilgi sistemleri kaynaklarının verimli olarak kullanılmasına, söz konusu bilgi sistemlerinin kullanılmasından kaynaklanacak risklerin kontrolünün ve izlenmesinin sağlanmasına, bu amaçla gerekli sistemsel ve yönetsel önlemlerin alınmasına ilişkin faaliyetleri,
- d) Biyometrik: Bir kişinin diğer şahıslardan ayrılmasını sağlayan, bu kişiye ait ölçülebilir bir biyolojik veya davranışsal karakteristiğini,
- e) BSDHY: 16/5/2006 tarihli ve 26170 sayılı Resmî Gazete’de yayımlanan Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmeliği,
- f) COBIT: Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI) tarafından yayınlanmış olan Bilgi Teknolojilerine İlişkin Kontrol Hedefleri’nin (COBIT) güncel versiyonunu,
- g) Değişken parola: Kimlik doğrulamada kullanılan, belirli dönemlerde değiştirilmesi zorunlu kılınan gizli alfabetik ve/veya rakamsal karakterler dizisini,
- ğ) Denetim izi: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtları,
- h) Elektronik imza: 15/01/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanan elektronik imzayı,
- ı) Güvenlik duvarı: Farklı güvenlik hassasiyet düzeylerine sahip ağlar arasında kontrollü geçişe imkân tanıyan yazılım ya da donanım temelli çözümleri,
- i) İç Sistemler Yönetmeliği: 1/11/2006 tarihli ve 26333 sayılı Resmî Gazete’de yayımlanan Bankaların İç Sistemleri Hakkında Yönetmeliği,
- j) İnternet bankacılığı: Müşterilerin banka tarafından sunulan hizmetlere internet yoluyla ulaşmalarını ve yapmak istedikleri işlemleri gerçekleştirmelerini sağlayan bankacılık hizmeti dağıtım kanalını,
- k) İşlem doğrulama kodu: Kimlik doğrulama yöntemlerinden biriyle kendisini sisteme tanıtan bir kişinin gerçekleştirmek istediği bir işlem için, bu işlemi onaylayıp onaylamadığına dair sisteme tanıttığı kimliğe yöneltilen, bir kereye mahsus kullanılmak üzere yaratılmış belirli uzunlukta alfabetik ve/veya rakamsal karakter dizisinden oluşan kodu,
- l) Kanun: 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununu,
- m) Kimlik doğrulama: Bildirilen bir kimliğin gerçekten bildiren şahsa ait olduğuna dair güvence sağlayan mekanizmayı,
- n) Kontrol: Banka içerisinde bilgi teknolojileri süreçleriyle ilgili olarak gerçekleştirilen ve iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvenceyi oluşturma amacı güden politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,
- o) Oturum: Veri aktarımı, sunuşu veya gerçekleştirilecek finansal işlemler için taraflar arasında kurulan mantıksal bağı,

ö) Parola: Kimlik doğrulamada kullanılan, değiştirilmesi zorunlu kılınmayan gizli alfabetik ve/veya rakamsal karakterler dizisini,

p) Parolanın/değişken parolanın sıfırlanması: Bir kullanıcıya ait parolanın/değişken parolanın kullanım dışı kaldığı, unutulduğu, kullanıcı hesabının kilitlendiği ya da ilk defa parolanın/değişken parolanın atanmasının gerektiği gibi durumlarda, bir yardım masası vasıtasıyla ya da sistemsel bir takım sorgulardan geçerek, kullanıcıya kendi parolasını/değişken parolasını belirleme imkânının verilmesini veya rastgele oluşturulmuş bir alfabetik ve/veya rakamsal karakterler dizisinin yeni kullanıcı parolası/değişken parolası olarak atanarak, bu parolanın/değişken parolanın kullanıcıya iletilmesini,

r) Sızma testi: Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amaçlı gerçekleştirilen atakları,

s) Şifreleme açık anahtarı: Açık anahtarlı şifrelemede kullanılan, herkesin erişimine ve kullanımına açık olan, şifreleme gizli anahtarı ile matematiksel bağlantısı bulunan ve şifreleme gizli anahtarı ile atılan imzayı kontrol etmek, yapılan şifrelemeyi çözmek, ya da sadece şifreleme gizli anahtarının çözebileceği şekilde verinin şifrelenmesi için kullanılan şifreleme anahtarını,

ş) Şifreleme anahtarı: Şifreleme algoritmasının şifreleme ve şifre çözme amacıyla kullandığı karakter dizisini,

t) Şifreleme gizli anahtarı: Açık anahtarlı şifrelemede imza atma, şifreleme ve karşılığı olan şifreleme açık anahtarıyla şifrelenmiş veriyi çözmek için kullanılan, sadece sahibi tarafından bilinmesi ve kullanılması gereken anahtarı,

u) Tek kullanımlık parola: Kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele yaratılan alfabetik ve/veya rakamsal karakterler dizisini,

ü) Üst düzey yönetim: İç Sistemler Yönetmeliğinin 3 üncü maddesinde tanımlanan üst düzey yönetimi,

v) Üst yönetim: İç Sistemler Yönetmeliğinin 3 üncü maddesinde tanımlanan üst yönetimi,

y) Yama: Programlarda tespit edilen açıklıkları veya programın içeriğindeki hatalı bir fonksiyonu düzeltme amaçlı hazırlanan program eklentisini,

z) Yetkilendirme veritabanı: Müşteri ve kullanıcı erişim haklarının ve yetkilendirmeye ilişkin bilgilerin tutulduğu yapıyı ifade eder.

Bankalarda bilgi sistemleri yönetiminin önemi

MADDE 4 – (1) Banka, bilgi sistemlerinin yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele alır. Bankanın operasyonlarını istikrarlı, rekabetçi ve gelişen bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejinin iş hedefleri ile uyumlu olması sağlanır, bilgi sistemleri yönetimine ilişkin unsurlar yönetsel hiyerarşi içerisinde uygun yere yerleştirilir ve bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağı tahsis edilir.

(2) Banka, bilgi sistemlerinin yönetimine ilişkin politikalar, prosedürler ve süreçler tesis eder. Prosedürler ve süreçler ilgili iş alanında gerçekleşen değişiklikler veya teknolojik gelişmeler doğrultusunda gerekiyorsa yenilenmek üzere düzenli olarak gözden geçirilir.

(3) Bilgi sistemleri üzerinde tesis edilen yönetimin etkinliği; risk yönetimi, iç kontrol sistemi ve iç denetim kapsamında yürütülecek çalışmaların da katkısıyla sağlanır.

İKİNCİ KISIM

Bilgi Sistemlerine İlişkin Risk Yönetimi ve İç Kontrollerin Tesisi

BİRİNCİ BÖLÜM

Bilgi Sistemlerine İlişkin Risk Yönetimi

Bilgi sistemleri risk yönetimi

MADDE 5 – (1) Banka, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri ölçmek, izlemek, kontrol etmek ve raporlamak üzere gerekli önlemleri alır. Bilgi sistemlerine ilişkin risklerin yönetilmesi, bilgi sistemleri yönetiminin önemli bir bileşeni olarak ele alınır. Bilgi teknolojilerinin bankacılık faaliyetlerinde kullanılması nedeniyle oluşan risklerin temel kaynağı olarak kabul edilebilecek unsurlardan aşağıda sıralananlar banka tarafından göz önünde bulundurulur, risk yönetiminde değerlendirmeye katılır:

a) Bilgi teknolojilerindeki hızlı gelişmeler sebebiyle rekabetçi ortamda bu gelişmelere uymamanın olumsuz sonuçları ve bu gelişmelere uyma konusundaki zorluklar,

b) Bilgi sistemlerinin bilinenlerden farklı hatalara ve dolandırıcılıklara zemin hazırlayabilmesi,

c) Bilgi sistemlerinin bankacılık faaliyetlerinde kullanımının artmasına bağlı olarak yaygınlaşan destek hizmeti alımı, buna bağlı olarak operasyonlarda destek hizmeti kuruluşlarına bağımlılığın doğmuş olması,

ç) Bankanın iş sürekliliğinin önemli oranda bilgi sistemlerinin işlerliğine bağlı duruma gelmesi,

d) Bilgi sistemleri üzerinden gerçekleştirilen işlemlerin ve tutulan, aktarılan ve işlenen verilerin güvenliğinin sağlanmasının, müşteri tanınmanın, inkâr edilemezliğin ve işlem izlerine ilişkin kayıtların tutulmasının zorlaşmış olması.

(2) Banka, risk yönetim politika ve süreçlerini, bilgi teknolojilerinin kullanımına bağlı olarak gözden geçirip,

buradan kaynaklanacak risklerin yönetimini kapsayacak şekilde yeniler. Bilgi teknolojilerinden kaynaklanan risklerin operasyonel risk kapsamında değerlendirilmesinin yanısıra bu risklerin bankacılık faaliyetlerinden kaynaklanan diğer risklerin de bir çarpanı olabileceğinden, bilgi teknolojilerinden kaynaklanan riskleri de içeren bütünlük bir risk yönetim yaklaşımı tüm bankacılık faaliyetleri için benimsenir, bilgi teknolojilerinin takibi ve gözetimine ilişkin çalışmalarından edinilen verilerin bankanın bütünsel risk yönetim çerçevesinin bir parçası haline gelmesi sağlanır.

(3) Banka, belirleyeceği dönemlerde veya bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce planlanan değişiklikleri de göz önünde bulundurarak bilgi sistemlerine ilişkin risk analizlerini tekrarlar ve risk analizlerinin ne şekilde gerçekleştirileceğine ilişkin prosedürleri hazırlar.

(4) Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla geliştirilen politika ve prosedürlerin gerekleri, bankanın organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözetim ve takip gerçekleştirilir.

(5) Risk yönetimine ilişkin politikaların, prosedürlerin ve süreçlerin bilgi teknolojilerinin kullanımından kaynaklanan riskleri de kapsayacak şekilde düzenlenmesi çalışmalarında, bu Tebliğin 6 ila 19 uncu maddeleri arasında yer alan, bilgi sistemlerinin özel niteliklerinden kaynaklanan risk yönetim prensipleri göz önünde bulundurulur. Söz konusu prensipler, üst yönetim gözetimi, güvenlik kontrolleri ile yasal ve itibar riski yönetimi başlıkları kapsamında yapılması gerekenleri ifade eder. Bankanın, kendi risk profiline, operasyonel yapısına, kurumsal yönetim kültürüne ve ilgili diğer mevzuat ile çizilen çerçeveye uygun olarak bilgi sistemlerine ilişkin risk yönetim süreçlerini geliştirmesi ve bilgi teknolojilerinden kaynaklanan riskleri de bu kapsamda değerlendirmeye alması esastır.

Yönetim gözetimi

MADDE 6 – (1) Banka üst yönetimi bilgi sistemleri kullanımından kaynaklanan risklerin yönetilmesi için etkin bir gözetim yürütür. Bu amaçla üst yönetim tarafından değerlendirmeden geçirilmiş ve uygunluğu onaylanmış, bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesine yönelik, kapsamlı bir süreç üst düzey yönetim tarafından hazırlanır. Bu süreç sorumlulukların açıkça tanımlanması ile risklerin yönetilmesine ilişkin politikaların oluşturulması ve kontrollerin tesis edilmesi ve izlenmesi faaliyetlerini kapsar.

(2) Bilgi sistemleri üzerinde etkin ve yeterli iç kontrollerin tesis edilmesi yönetim kurulunun sorumluluğundadır.

(3) Banka risk profili ve stratejisi üzerinde önemli etkileri olacak yeni bilgi sistemi unsurlarının kullanıma alınmasına ilişkin projeler banka üst düzey yönetimi tarafından gözden geçirilir. Üst düzey yönetim, bilgi sistemleri unsurlarına ilişkin bu yeni projelerin getireceği riskleri yönetmek için gerekli uzmanlık düzeyinin banka bünyesinde bulunduğundan emin olmadan, çalışmalara onay vermez. Projelerin banka iç kaynaklarıyla veya destek hizmeti alımı yoluyla gerçekleştirilmesine bakılmaksızın üst düzey yönetim ve personel uzmanlığının, projeye ilişkin uygulamaların ve bunu destekleyen alt yapının gerektirdiği teknik detay ve karmaşıklık ile orantılı olması esastır. Bu yapıyı desteklemek üzere oluşturulacak yönetsel rol ve sorumluluklar açıkça belirlenir.

(4) Banka üst yönetimi, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder. Üst yönetim, aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

a) Bilgi güvenliği politikalarının ve tüm sorumlulukların belirli periyotlarla gözden geçirilmesi ve onay mekanizmasına tabi tutulması,

b) Bilgi kaynaklarına yönelik tehditlerin periyodik olarak değerlendirilmesi,

c) Bilgi güvenliği ihlaline ilişkin olayların izlenmesi ve periyodik olarak değerlendirilmesi,

ç) Bilgi güvenliği hususunda farkındalığı artıracak çalışmaların desteklenmesi.

(5) Bankanın bilgi güvenliği politikası, yönetim kurulunun onayından geçmeli ve tatbiki üst yönetim tarafından gözetilmelidir.

Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi

MADDE 7 – (1) Banka üst yönetimi, bilgi güvenliği politikası kapsamında, bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, güvenlik kontrol sürecini değerlendirmeye tabi tutar ve uygunluğunu onaylar. Banka üst yönetimi, bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak ve yedek olarak saklanmak üzere bulunan verilerin gizlilik, bütünlük ve ulaşılabilirliklerini sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarını gözetimi altında tutar.

(2) Güvenlik kontrol süreci ve bilgi güvenliği politikası vasıtasıyla sorumluluklar açıkça tanımlanmış şekilde kişilere atanır. Bu kapsamda güvenlik kontrol süreçlerinin oluşturulması, sürdürülmesi ve yönetilmesine ilişkin açık yönetsel sorumluluklar belirlenir.

(3) Bilgi güvenliğinin tesisi amacıyla uygulanacak kontroller asgari olarak aşağıdaki unsurları içerir:

a) Bilgi sistemleri ve içerdiği verilerin güvenliği konusunda gerekli kontrollerin ve yapıların oluşturulması çalışmaları kapsamında; risk değerlemesi yapılması, bilgi güvenliği politikası oluşturulması ve uygulanması, bilgi güvenliği testlerinin uygulanması, işlemlerin takip edilip raporlanması ve kontrollerin ve oluşturulan yapıların teknolojik gelişmelere göre güncellenmesi faaliyetlerini içeren bir süreç oluşturulur.

b) Banka personelinin güvenlik konusunda farkındalık kazanmaları banka tarafından sağlanır, bankanın güvenlik politikası kendilerine aktarılır, uyum konusunda yazılı taahhütleri alınır.

c) Bilgi sistemleri ve bilgi sistemleri üzerinde işlenen, iletilen, depolanan ve yedek olarak tutulan veriler güvenlik hassasiyet derecelerine göre sınıflanır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir.

ç) Bilgi sistemlerinin güvenilirliğinin ve tutarlılığının düzenli olarak incelenmesini sağlayacak süreçler tesis edilir. Bu çerçevede güvenlik ile ilgili hükümlerin gereklerinin yerine getirilmesi hususunda herhangi bir icrai görevi bulunmayan bağımsız ekiplere düzenli aralıklarla sızma testleri yaptırılır. Güvenlik alanındaki güncel gelişmeler ve yeni açıklar takip edilir, gerekli yazılım güncellemeleri yapılır, gerekli yamalar uygulanır.

d) Banka, kendi kurumsal ağı dışındaki ağlarla iletişimde bulunduğu hallerde bu dış ağlardan gelebilecek tehditler için gerekli ağ kontrol güvenlik sistemlerini tesis eder.

e) Banka, dış ağdan iç ağına yapılacak erişimleri kontrol altında tutmak, ayrıca, iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere, gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan bir veya birden fazla güvenlik duvarını kullanır.

f) Bilgi sistemleri güvenliğine ilişkin hükümlerin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda bilgi sistemleri yöneticisine rapor veren, yeterli teknik bilgi ve tecrübeye sahip bir bilgi sistemleri güvenliği sorumlusu atanır.

Bilgi sistemlerine ilişkin destek hizmeti alımı sürecinin yönetimi

MADDE 8 – (1) Banka üst yönetimi, bilgi sistemleri kapsamında alınacak destek hizmetlerine ilişkin olarak, söz konusu hizmetin destek hizmeti alımı yoluyla gerçekleştirilmesinin banka açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve destek hizmeti kuruluşu ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak yeterli bir gözetim mekanizması tesis eder. Tesis edilecek gözetim mekanizması ile asgari olarak;

a) Bilgi sistemleri alt yapısına ilişkin destek hizmeti alınımının doğuracağı risklerin tüm yönleriyle değerlendirilmesi,

b) Destek hizmeti kuruluşunun seçiminde gerekli özenin gösterilmesi,

c) Destek hizmeti alımı kapsamındaki tüm sistem ve süreçlerin bankanın kendi risk yönetimi, güvenlik ve müşteri mahremiyeti politikalarına uygun olması,

ç) Destek hizmeti kapsamında banka verilerinin destek hizmeti kuruluşuna aktarılmasının gerekli olduğu durumlarda, destek hizmeti kuruluşunun güvenlik konusundaki prensip ve uygulamalarının en az bankanın uyguladıkları düzeyde olması,

d) Destek hizmeti alımı kapsamındaki faaliyetlerin banka bünyesinde gerçekleştirilmesi durumunda hangi denetimlere tabi tutulması öngörülüyorsa, herhangi bir kapsam daraltılmasına gidilmeden aynı denetimlere tabi tutulması, faaliyetin destek hizmeti alımı yoluyla gerçekleştirilmesi nedeniyle ek denetim ihtiyacı duyuluyorsa bunların da gerçekleştirilmesi,

e) Destek hizmeti alımına ilişkin hususların banka iş süreklilik planı göz önünde bulundurularak düzenlenmesi ve gerekli önlemlerin alınması, destek hizmeti kuruluşunun bu kapsamdaki yükümlülüklerinin sözleşme ile netleştirilmesi,

temin edilir.

(2) Destek hizmeti alınımının, planlananın dışında sonlanması durumlarına ilişkin risklerin yönetilmesine uygun bir çıkış stratejisi belirlenir.

(3) Destek hizmeti alınımına ilişkin koşul, kapsam ve her türlü diğer tanımlama, ilgili destek hizmeti kuruluşunca da imzalanmış olacak şekilde sözleşmeye bağlanır. Sözleşme, asgari olarak aşağıdaki hususları içerir;

a) Hizmet seviyelerine ilişkin tanımlamalar,

b) Hizmetin sonlanma koşulları,

c) Bankaya ait iş süreklilik planının sektöre uğramasını engelleyecek şekilde destek hizmeti kuruluşunun alması gereken önlemlere ilişkin hükümler,

ç) Bankanın güvenlik politikası dâhilinde hassasiyet arz eden konulara ilişkin gereklilikler,

d) Sözleşme kapsamında üretilecek olan ürünün sahipliğini, fikri mülkiyet haklarını da göz önünde bulundurularak düzenleyen hükümler,

e) Sözleşmede destek hizmeti kuruluşları için yükümlülük teşkil eden hükümlerin, alt yüklenici kuruluşlar ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler,

f) Destek hizmeti alınımının, planlananın dışında sonlanmasından kaynaklanacak risklerin yönetilmesine ilişkin hükümler,

g) Bankanın tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde destek hizmeti kuruluşları için de uygulanmasını sağlayacak hükümler.

(4) Banka, güvenlik politikasının tanımladığı ilkeler doğrultusunda, destek hizmeti alımından kaynaklanan riskleri kontrol altında tutmak üzere gerekli organizasyonel değişiklikleri yapar, idari prosedürler tanımlar ve bu kapsamda alınacak önlemleri ilgili tüm diğer bölümlerin günlük işlemlerine ve sistemlerine entegre eder, alınan destek hizmetine ilişkin olarak, destek hizmeti kuruluşuyla ilişkileri yürütecek, yeterli bilgi ve tecrübeye sahip bir sorumlu atar.

(5) Destek hizmeti kuruluşlarına verilen erişim hakkı tipleri özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılır; buna göre, eğer gerekiyorsa ek kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim tipi, erişilen verinin değeri, destek hizmeti kuruluşu tarafından yürütülmekte olan kontroller ve bu erişimin banka bilgilerinin güvenliği üzerindeki etkileri dikkate alınır.

(6) Banka üst yönetimi, destek hizmeti alımı yoluyla gerçekleştirilen servisler için; servisin erişilebilirliğini, performansını, kalitesini, bu servis kapsamında gerçekleşen güvenlik ihlali olayları ile destek hizmeti kuruluşunun

güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu yakından takip eder.

(7) Bu maddede yer alan hükümler, bilgi sistemlerine ilişkin destek hizmeti alımlarında, 1/11/2006 tarihli ve 26333 sayılı Resmî Gazete’de yayımlanan Bankaların Destek Hizmeti Almalarına ve Bu Hizmeti Verecek Kuruluşların Yetkilendirilmesine İlişkin Yönetmelik’te belirtilen hükümler aynen geçerli olmak kaydıyla, ilave hükümler olarak değerlendirilir.

Kimlik doğrulama

MADDE 9 – (1) Bilgi sistemleri üzerinden gerçekleşen işlemler için uygun bir kimlik doğrulama mekanizması kurulur. Hangi kimlik doğrulama tekniklerinin kullanılacağına, üst düzey yönetim tarafından yapılacak risk değerlendirmesi sonucuna göre karar verilir. Risk değerlendirmesi, bilgi sistemleri üzerinden gerçekleştirilmesi planlanan işlemlerin türü (tipi, niteliği, varsa doğuracağı finansal ve finansal olmayan etkilerinin büyüklüğü gibi), işleme konu verinin hassaslık derecesi ve kimlik doğrulama tekniğinin kullanım kolaylığı da göz önünde bulundurularak gerçekleştirilir.

(2) Uygulanacak kimlik doğrulama mekanizması, müşterilerin ve personelin bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde tesis edilir. Kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek gerekli önlemler alınır.

(3) Bilgi sistemlerine erişim için kullanılan kimlik doğrulama verilerinin tutulduğu veritabanlarının güvenliğini sağlamaya yönelik gerekli önlemler alınır. Bu amaçla alınacak önlemler asgari olarak kimlik doğrulama verilerinin veritabanlarında şifreli olarak muhafaza edilmesi, yapılacak her türlü kontrolsüz değişikliği algılayacak sistemlerin kurulması, yeterli denetim izlerinin tutulması ve bu denetim izlerinin güvenliğinin sağlanması hususlarını içerir. Ayrıca bu veriler kimlik doğrulama amacıyla aktarılırken şifrelenir ve verilerin aktarımı sırasında gizliliğinin sağlanmasına yönelik önlemler alınır.

İnkâr edilemezlik ve sorumluluk atama

MADDE 10 – (1) Banka, bilgi sistemleri dâhilinde gerçekleşen ve kapsamını kendisinin belirleyeceği kritik işlemler için, inkâr edilemezlik ve sorumluluk atama imkânlarını içeren teknikler kullanır.

Görevler ayrılığı prensibi

MADDE 11 – (1) Bilgi sistemlerine ilişkin sistem, veritabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görevler ve sorumluluklar ayrılığı prensibi uygulanır, atanan görevler ve sorumluluklar görevler ayrılığı prensibine göre periyodik olarak gözden geçirilir ve gerekiyorsa güncellenir. Süreçler ve sistemler, kritik bir işlemin tek bir personel veya destek hizmeti kuruluşu tarafından girilmesi, yetkilendirilmesi ve tamamlanmasına imkân vermeyecek şekilde tasarlanır.

(2) Etkin bir görevler ayrılığı ortamının tesis edilebilmesi için banka verileri üzerinde etkileri olabilecek süreçleri yürütecek personele, kendilerine atanan görevler göz önünde bulundurularak, sadece bu görevleri yerine getirmelerine yetecek kadar yetkinin verilmesi temin edilir.

(3) Görevlerin tam manasıyla ve uygun şekilde ayrıştırılmasının mümkün olmadığı durumlarda, bu durumdan kaynaklanabilecek hata ve suiistimalleri önlemeye yönelik risk azaltıcı veya telafi edici kontroller tesis edilir.

(4) Bilgi sistemlerine ilişkin fonksiyonların gerçekleştirilmesinde görevler ayrılığı ilkesinin gereklerini sağlamak için tesis edilen kontrollerin aşılabilirliğini tespit etmek üzere testler yapılır.

Yetkilendirme

MADDE 12 – (1) Banka, bilgi sistemlerine ilişkin veritabanlarına, uygulamalara ve sistemlere erişim için uygun bir yetkilendirme ve erişim kontrolü tesis eder. Bu çerçevede bilgi sistemlerinde gerçekleşen faaliyetlere müdahil kullanıcı, taraf ve sistemlere uygun yetkilendirme düzeyi ve erişim hakkı atanır. Yetkilendirme düzeyi ve erişim haklarının atanmasında ilgili unsurun görev ve sorumlulukları göz önünde bulundurularak, gerekli olacak en düşük yetkinin atanması ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınır. Böylelikle sistemlere, servislere ve verilere sadece gerekli yetkiye sahip kullanıcı, taraf ve sistemlerin erişimi mümkün kılınır. Atanacak yetkiler görevler ayrılığı prensibinin tanımladığı ilkeler ile tutarlı olmalıdır.

(2) Yetkilendirme ve erişim hakkı tahsisi mekanizması, hiçbir kullanıcı, taraf ya da sistemin kendi yetkilendirme düzeyini ve erişim haklarını önceden tanımlanmış düzeylerin üzerine çıkartmasına izin vermeyecek şekilde tesis edilir.

(3) Bilgi sistemleri dâhilinde gerçekleşen kritik faaliyetlerin güncel ve geçerli yetkilendirme veritabanları üzerinden gerçekleştirilmesi temin edilir. Tüm kullanıcı, taraf ve sistemlere atanmış olan yetkiler ve erişim hakları periyodik olarak güncel durumla uyumlulukları açısından değerlendirilmeye tabi tutulur. Yetkilendirme veritabanlarının güvenliği sağlanır ve yapılacak her türlü kontrolsüz değişikliği algılayacak mekanizmalar kurulur. Yetkilendirme veritabanlarına yetkisiz erişim teşebbüsleri kayıt altına alınır ve düzenli olarak gözden geçirilir.

(4) Bilgi sistemleri dâhilinde gerçekleşen kritik faaliyetlere ilişkin yetkilendirme veritabanları da dâhil olmak üzere her türlü veritabanı, uygulama ve sistemde meydana gelecek değişiklik, ekleme ve silmenin, kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş yetkili kullanıcılar tarafından yapılması sağlanır. Bu kapsamdaki her türlü işlem için banka bünyesinde etkin bir değişiklik yönetimi tesis edilir, yeterli denetim izi tutulur ve tutulan denetim izlerinin düzenli olarak gözden geçirilmesi sağlanır.

(5) Bilgi sistemleri dâhilinde gerçekleşen kritik faaliyetlere ilişkin yetkilendirme veritabanlarının güvenilirliğini yitirmesi durumunda, ilgili veritabanları güncel ve güvenilir duruma getirilene kadar kullanılmaz,

güvenilir olmayan veritabanları üzerinden yetkilendirme ve erişim hakkı tahsisi işlemleri gerçekleştirilmez.

(6) Ayrıcalıklı yetkilere sahip kullanıcı ve sistem hesapları için ek denetim izleri tutulur ve periyodik olarak gözden geçirilir.

(7) Ayrıcalıklı yetkilere sahip kullanıcılar, yetkilerinin başka kişilerce kullanımının önlenmesinin önemi konusunda yeterli düzeyde bilinçlendirilir.

(8) Acil durumlar için, yetkili personele ulaşılamaması nedeniyle geçici olarak gerçekleştirilen yetkilendirmelerde, bu yetkilendirme süresince gerçekleştirilecek işlemlerin yeterli düzeyde takibine izin verecek şekilde detaylı denetim izlerinin tutulması sağlanır.

(9) Bilgi sistemleri alt yapısına yönelik yetkisiz fiziksel ve mantıksal erişimleri engelleyecek kontroller ve gözetim süreçleri tesis edilir.

İşlemlerin, kayıtların ve verilerin bütünlüğü

MADDE 13 – (1) Banka, bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli tedbirleri alarak bunların doğruluğunu, tamlığını ve güvenilirliğini temin eder. Bütünlüğü sağlamaya yönelik tedbirler verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsayacak şekilde tesis edilir. Destek hizmeti kuruluşları nezdinde gerçekleşen işlemler için de aynı yaklaşım gösterilir.

(2) Bilgi sistemlerine ilişkin işlemlerin doğruluğu ve güvenilirliği asgari olarak, yapılmak istenen işleme ait anahtar öneme sahip bilgilerin işlemin başlangıcından tamamlanışına kadar doğruluğunu yitirmemesini ve yapılmak istenen işlemin kendinden beklenen sonucu yerine getirmesini; tamlığı ise asgari olarak bütün işlemlerin hata üretmeden gerçekleşmesini ve mükerrer olamamasını gerektirir.

(3) Banka, bilgi sistemlerine ilişkin işlemlerde ve kayıtlarda meydana gelebilecek olası bozulmaları saptayacak teknikleri kullanır.

Denetim izlerinin oluşturulması

MADDE 14 – (1) Bilgi sistemleri üzerindeki riskler, sistemlerin boyutu ve faaliyetlerin karmaşıklığı göz önünde bulundurularak bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizması tesis edilir. Bu sayede, bilgi sistemleri dâhilinde gerçekleşen ve bankacılık faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemlere ilişkin denetim izlerinin yeterli detayda ve açıklıkta tutulması temin edilir. Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır. Kayıt sisteminin her türlü yetkisiz sistemsel ve kullanıcı müdahalesine karşı korunmasına yönelik önlemler alınır. Bankacılık faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemler için asgari olarak;

- a) Bu kapsamdaki işlemlere ilişkin yetkisiz erişim teşebbüslerine,
 - b) İşlemi gerçekleştiren uygulamaya,
 - c) İşlemi gerçekleştiren kişinin kimliğine,
 - ç) Yapılan işlemlerin zamanına,
- ilişkin bilgileri içeren denetim izleri tutulur.

(2) Kapsamı birinci fıkrada tanımlanmış olan denetim izleri asgari 3 yıl boyunca banka nezdinde saklanır. Ayrıca, bankacılık faaliyetlerine ait kayıtlarda değişikliğe sebep olmasalar bile, Kanunun 73 üncü maddesine göre sır kapsamında olan bilgilerin sorgulanmasına ilişkin işlemlere ait denetim izleri, Kanunun aynı maddesindeki hükümlere aykırı olarak bu bilgilerin ifşası durumunda sorumluların tespitini sağlayacak nitelikte, asgari 1 yıl boyunca banka nezdinde saklanır. Denetim izlerinin, yeterli güvenlik düzeyine sahip ortamlarda korunması ve yedeklerinin alınması suretiyle, yaşanacak olası felaketler sonrasında da öngörülen süre için erişilebilir olmaları temin edilir.

(3) Banka, müşterilerini ve personelini, aktivitelerinin kaydının tutulduğu hususunda haberdar eder.

(4) Banka, kayıt sisteminin düzenli olarak gözden geçirilmesine ve kayıtların değerlendirilmesine, olağanüstü durumların üst yönetime raporlanmasına ilişkin süreçleri tesis eder.

(5) Denetim izlerinin tutulması, mevzuatın diğer hükümleri gereği bankanın belgeleri saklamasına ilişkin yükümlülüklerini değiştirmez.

(6) Bilgi sistemleri faaliyetleri kapsamında destek hizmeti alınıyor olması durumunda banka, destek hizmeti kuruluşu tarafından tutulan denetim izlerinin kendi standartlarına uygunluğunu ve bu denetim izlerine erişilebilirliğini temin eder.

(7) Bu maddede bilgi ve belge tutulmasına ilişkin yer alan hükümler, diğer mevzuatın bilgi ve belge saklama ile ilgili hükümleri aynen saklı kalmak koşuluyla uygulanır.

Veri gizliliği

MADDE 15 – (1) Banka, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemleri alır. Alınacak önlemler, gizliliği sağlanmaya çalışılan işlem ve verilerin gizlilik derecesine uygun olmalı, gerekli yerlerde ek kontroller tesis edilmelidir. Bu çerçevede yapılan çalışmalar, sırların saklanmasına ilişkin mevzuat yükümlülüklerini karşılayacak nitelikte olmak zorundadır. Gizliliği sağlamak üzere yapılacak çalışmalar asgari olarak;

a) Değer ve risk analizi gerçekleştirilerek, verilerin hassasiyetine uygun tedbirlerin alınmasının temin edilmesi, bu değerlendirme sırasında bankanın ağ ve sistem yapısının, operasyonlarının, genişliğinin ve çeşitliliğinin göz önünde bulundurulması,

b) Verilere, görevler ayrılığı ilkesi göz önünde bulundurularak tanımlanmış kişilerce, kişilerin sorumluluğu

gereği kendileri için öngörülen yetkiler çerçevesinde, uygun bir kimlik doğrulama süreci sonrasında ulaşımın temin edilmesi,

c) Veri gizliliğini sağlamada kullanılacak şifreleme teknikleri için güncel durum itibarıyla güvenilirliği ve sağlamlığı ispatlanmış algoritmaların baz alınması, ilgili algoritmalar için kullanılacak şifreleme anahtarlarının geçerli olacağı ve kullanılabileceği zaman zarfında kırılmayacak şekilde uzun seçilmesi,

ç) Geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılabilirliğinin engellenmesi, verinin ve operasyonun kritiklik düzeyine göre anahtarların değiştirilme sıklıklarının belirlenmesi,

d) Şifreleme anahtarlarının güvenli bir şekilde oluşturulması, müşteri ve personel kullanımına sunulması ve saklanması,

e) Gizlilik arz eden bankacılık verilerine erişimlerin kayıt altına alınması ve bu kayıtların yetkisiz erişim ve müdahalelere karşı korunması,

f) Destek hizmeti alımı kapsamında destek hizmeti kuruluşlarının, bankacılık verilerine erişiminin söz konusu olduğu durumlar için bu madde altında söz edilen hususlar ile bankanın bilgi güvenliği standartlarına uyumlu davranmasının sağlanması

hususlarını içerir.

Müşterilerin bilgilendirilmesi

MADDE 16 – (1) Banka tarafından sunulan elektronik bankacılık/alternatif dağıtım kanalları (internet, telefon, televizyon, WAP/GPRS, Kiosk, ATM vb.) hizmetlerinden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir. Buna ek olarak bankanın söz konusu hizmetlere ilişkin risklerin etkisini azaltmaya yönelik benimsediği güvenlik prensipleri ve bu risklerden korunmak için kullanılması gereken yöntemler müşterinin dikkatine sunulur.

(2) Bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı müşterilerin yaşayabileceği sorunların takip edilebileceği ve müşterilerin şikâyetlerini ulaşturmalarına imkân tanıyacak mekanizmalar oluşturulur. Ulaşan şikâyet ve uyarılar değerlendirilerek, banka itibarını zedeleyici aksaklıkları giderici çalışmalar yapılır.

Müşteri bilgilerinin mahremiyeti

MADDE 17 – (1) Banka, faaliyetlerinin ifası sırasında bilgi sistemleri aracılığıyla edindiği veya sakladığı müşteri bilgilerinin mahremiyetini sağlamaya yönelik politika ve prosedürleri oluşturur, yazılı hale getirir, ilgili tüm birimlere iletir ve bunların gerektirdiği tedbirleri alır,

(2) Birinci fıkra kapsamındaki müşteri bilgileri, yasalarla açıkça yetkili kılınan merciler dışındaki taraflarla, ancak paylaşım sınırları açıkça belirtilmek ve müşterilerin yazılı rızaları alınmak kaydıyla paylaşılabilir. Müşterilere bilgilerini söz konusu taraflarla paylaşıp paylaşmama konusunda seçenek sunulmalı ve müşterinin böyle bir seçeneğinin bulunduğu dair mutlaka bilgilendirilmesi sağlanmalıdır.

Bilgi sistemlerine ilişkin iş sürekliliği ve kurtarma planı

MADDE 18 – (1) Bilgi sistemlerinde yaşanabilecek problemler nedeniyle faaliyetlerin kesintiye uğramasını önlemek üzere yönetim kurulu tarafından onaylanmış bilgi sistemlerine ilişkin bir iş süreklilik ve kurtarma planı hazırlanır. Bu kapsamda banka uygun bir yedekleme altyapısı tesis eder, performans takip teknikleri kullanır, kapasite planlaması yapar, ağ altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif kanallar oluşturur. Hazırlanan plan, acil ve beklenmedik durum planı ile uyumlu olacak şekilde düzenlenir. Planın bankanın hedefleri ve öncelikleriyle uyumlu, güncel ve yeterli olması esastır. Plan, yaşanabilecek problemler için alternatif kurtarma prosedürlerini de içerecek şekilde düzenlenir. Planda görevler, roller ve riskler açık ve net olarak tanımlanır. Plana ilişkin olarak tüm personel bilgilendirilir, görev ve sorumlulukları konusunda eğitilir.

(2) Bilgi sistemlerine ilişkin iş süreklilik ve kurtarma planı hazırlanırken; iş etki analizi, risk değerlendirmesi, risk azaltma ve risk izleme faaliyetleri gerçekleştirilir.

(3) Mevcut planın etkinliğini ve güncelliğini temin etmek üzere düzenli olarak testler yapılır ve test sonuçları üst yönetime raporlanır.

(4) Bilgi sistemlerine ilişkin iş süreklilik ve kurtarma planı periyodik olarak güncellenmenin yanında bunları etkileyecek değişikliklerden sonra da gözden geçirilir ve güncellenir.

(5) İç Sistemler Yönetmeliğinin 13 üncü maddesinin beşinci fıkrasında yer alan hüküm uyarınca veri yedekleme merkezi kurulurken, riskleri asgari seviyeye indirmek üzere yer seçiminde gerekli dikkat gösterilir. Gerçek sistem ile yedekleme merkezinin aynı risklere karşı hassas olmaması öncelikli hedef olarak alınır.

(6) Banka, bilgi sistemleri varlıklarının ve tutulan verilerin kritikliğini değerlendirerek olası kesintilerin etkilerini analiz eder. Bu etki analizinin sonuçlarına göre her bir servis için kabul edilebilir kesinti süreleri belirleyerek, bu kesinti süresi içerisinde servisin tekrar erişime açılabilmesine imkân tanıyacak kurtarma prosedürleri geliştirir ve buna göre gerekli önlemleri alır.

(7) Banka, bilgi sistemleri alt yapısının kapasitesinin ölçeklenebilirliğini, genel piyasa dinamikleri ve planlanmış müşteri kazanma oranı ışığında analiz eder. İşlem hacmi tahminleri doğrultusunda gerçekleştirilecek stres testleri ile alt yapının dayanıklılığı periyodik olarak test edilir.

(8) Bilgi sistemlerine ilişkin iş süreklilik ve kurtarma planı geliştirilirken eğer varsa ilgili destek hizmeti kuruluşları da dikkate alınır, testlere destek hizmeti kuruluşları da dâhil edilerek önlemlerin etkinliği kontrol edilir.

Acil ve beklenmedik durum planı

MADDE 19 – (1) Banka, bilgi sistemlerine ilişkin beklenmedik olayları yönetmek ve bunların etkilerini en

aza indirmek üzere, İç Sistemler Yönetmeliğinin 13 üncü maddesinde düzenlenen acil ve beklenmedik durum planı çerçevesinde gerekli önlemleri alır.

(2) Birinci fıkra kapsamında yapılacak çalışmalarla riskin olasılığı ve etkisi göz önünde bulundurularak, öngörülen senaryolar için, faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci tesis edilir.

(3) Banka, bilgi sistemlerine ilişkin beklenmedik olayları erken haber almayı sağlayacak mekanizmaları tesis eder.

(4) Acil ve beklenmedik durum planı kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulmayı sağlama, hasarı tespit etme, olayın potansiyel boyutunu ve etkisini gösterme, yetkili yönetim birimine ulaştırılmasını sağlama ve etkilenen müşterileri tespit etme süreçleri ele alınır.

(5) Acil ve beklenmedik durum planı, bankanın, müşterileri ve yayın organları ile hangi iletişim yöntemlerinin kullanılacağına da belirtildiği bir haberleşme stratejisini içerir. Söz konusu strateji ile banka müşterileri ve yayın organlarının zamanında ve doğru haber alması temin edilir.

(6) Banka, bilgi sistemlerine ilişkin gerçekleşecek her türlü beklenmedik olay için, olayın sonradan incelenmesine imkân tanıyacak, adli incelemede kullanılacak nitelikte kayıtları ve bilgileri toplayan bir mekanizma tesis eder. Tutulacak kayıtlar uğranılan parasal kaybı belirlemeyi sağlayacak bilgileri de içerir.

İKİNCİ BÖLÜM

Bilgi Sistemlerine İlişkin İç Kontrollerin Tesisi ve Takibi

Bilgi sistemleri kontrolleri

MADDE 20 – (1) Banka, varlıklarının korunmasını, faaliyetlerinin etkin ve verimli bir şekilde Kanuna ve ilgili diğer mevzuata, banka içi politika ve kurallara ve bankacılık teamüllerine uygun olarak yürütülmesini, muhasebe ve finansal raporlama sistemlerinin güvenilirliğini, bütünlüğünü ve bilgilerin zamanında elde edilebilirliğini sağlamak üzere İç Sistemler Yönetmeliğinin 16 ncı maddesinin üçüncü fıkrasında ifade edilen bilgi sistemlerine ilişkin kontrolleri, bu Tebliğin 21 inci ve 22 nci maddelerinde yer alan hükümler doğrultusunda tesis eder ve 23 üncü maddesinde yer alan hükümler doğrultusunda takip eder.

Uygulama kontrolleri

MADDE 21 – (1) Uygulama kontrolleri, bilgi sistemleri içerisinde yer alan ve bankacılık faaliyetlerini yürütmek veya desteklemek için kullanılan finansal verilerin tanımlanması, üretilmesi, kullanılması, bütünlük ve güvenilirliğinin sağlanması, verilere erişimin yetkilendirilmesi gibi tüm iş süreçlerinde kullanılması gereken iç kontrolleri kapsar.

(2) Uygulama kontrolleri, bankanın iş süreçlerinin kontrolünü ifade eden iş döngüsü kontrolleri içerisinde yer alan, bilgisayar destekli ve manüel yordamlarla gerçekleştirilen özelleşmiş kontrollerdir.

(3) Uygulama kontrolleri asgari düzeyde aşağıdaki unsurları içerir;

a) Veri oluşturma/yetkilendirme kontrolleri:

1) Veri hazırlama prosedürleri: Girdi form tasarımları, hataların ve eksikliklerin en aza indirilmesine yardım eder. Veri oluşturma sürecinde kullanılan hata ele alma prosedürleri, hataların ve düzensizliklerin tespit edilmesini, raporlanmasını ve düzeltilmesini temin eder.

2) Kaynak belge yetkilendirme prosedürleri: Yetkilendirilmiş personel, yetkilerine uygun bir biçimde kaynak belgeleri hazırlar. Kaynak belgelerin oluşturulması ve onaylanması konusunda görevler ayrılığı prensibine göre hareket edilir.

3) Kaynak belge verilerinin toplanması: Yetkilendirilmiş kaynak belgelerin bütünlüğünü ve doğruluğunu, hesap verilebilirliğini ve zamanında iletimini temin eden prosedürler bulunmalıdır.

4) Kaynak belgelerdeki hataların ele alınması: Veri oluşturma sürecinde kullanılan hata ele alma prosedürleri, hataların ve düzensizliklerin tespit edilmesini, raporlanmasını ve düzeltilmesini temin eder.

5) Kaynak belgelerin muhafazası: Gerektiğinde veriye ulaşılabilmelerini sağlamak amacıyla, orijinal kaynak belgelerin yeterli bir süre boyunca saklanmasını veya yeniden oluşturulabilir biçimde tutulmasını temin etmek için prosedürler bulunmalıdır.

b) Girdi kontrolleri:

1) Girdi yetkilendirme prosedürleri: Yalnızca yetkilendirilmiş kaynaklardan veri girişi yapılabilmesini temin eden prosedürler bulunmalıdır.

2) Doğruluk, bütünlük ve yetkilendirme kontrolleri: Personel veya sistem tarafından üretilen, ya da arayüzlerden işlenmek üzere girilen hareket verileri doğruluk, bütünlük ve geçerlilik kontrolü için çeşitli testlere tabi tutulur. Ayrıca, girdi verilerinin kaynak noktasına en yakın yerde değiştirilmesini ve onaylanmasını temin eden prosedürler bulunmalıdır.

3) Veri girdilerindeki hataların ele alınması: Hatalı girilen verilerin düzeltilmesini ve tekrar işleme alınmasını temin eden prosedürler bulunmalıdır.

c) Veri işleme kontrolleri:

1) Veri işlemede bütünlük: Veri işleme prosedürleri, görevler ayrılığı prensibine uyulmasını ve yapılan işlerin doğrulanmasını temin eder. Bu prosedürler ayrıca, çalıştırmadan çalıştırmaya kontrol toplamları ve esas dosya

güncelleme kontrolleri gibi yeterli güncelleme kontrollerinin varlığını da temin eder.

2) Veri işlemede onaylama ve değiştirme: Veri işlemede onaylama, kullanıcı doğrulaması ve değiştirmenin kaynak noktasına en yakın yerde gerçekleştirilmesini temin eden prosedürler bulunmalıdır.

3) Veri işlemedeki hataların ele alınması: Veri işlemedeki hataların ele alınmasına ilişkin prosedürler, hatalı hareketlerin işlenmeden belirlenmesini sağlar ve diğer geçerli hareketleri kesintiye uğratmasını engeller.

ç) Çıktı kontrolleri:

1) Çıktıların ele alınması ve muhafazası: Bilgi sistemleri uygulamalarının çıktılarının ele alınması ve muhafazasında belirlenmiş prosedürler izlenmeli, gizlilik ve güvenlik gereksinimleri dikkate alınmalıdır.

2) Çıktıların dağıtımı: Bilgi sistemleri çıktılarının dağıtımı ile ilgili prosedürler tanımlanmış, duyurulmuş ve takip ediliyor olmalıdır.

3) Çıktı uyumluluğu ve mutabakatı: Çıktıların kontrol toplamlarıyla uyumluluğu rutin olarak kontrol edilmelidir. Denetim izleri, hareketlere ilişkin işlemlerin takip edilmesini ve sorunlu verilerle ilgili mutabakat sağlanmasını kolaylaştırır.

4) Çıktıların gözden geçirilmesi ve hataların ele alınması: Çıktı raporlarının doğruluğunun, çıktıları sağlayan kişiler ve uygun kullanıcılar tarafından gözden geçirilmesini temin eden prosedürler bulunmalıdır. Ayrıca, çıktılarda bulunan hataların tanımlanması ve ele alınması ile ilgili de prosedürler olmalıdır.

5) Çıktı raporlarının güvenliğinin sağlanması: Hem kullanıcılara dağıtımı yapılmış hem de dağıtım için bekleyen çıktı raporlarının güvenliğinin sağlanmasıyla ilgili prosedürler bulunmalıdır.

d) Sınır kontrolleri:

1) Aslına uygunluk ve bütünlük kontrolleri: Organizasyon dışında üretilen, telefon, sesli posta, kâğıt, faks veya e-posta ile alınmış verinin aslına uygunluğu ve bütünlüğü, veri üzerinde kritik bir işlem yapılmadan uygun bir şekilde kontrol edilmelidir.

2) Hassas bilginin iletim ve nakil esnasında korunması: Hassas bilginin, iletim ve nakil esnasında, yetkisiz erişim, değişiklik ve yanlış yönlendirmeye karşı uygun bir biçimde korunması gerekir.

Genel kontroller

MADDE 22 – (1) Bilgi sistemleri genel kontrolleri, banka bilgi sistemlerinin tamamına veya büyük bir bölümüne tatbik edilen, bilgi sistemlerinin kendilerinden beklenen fonksiyonları doğru bir şekilde yerine getirmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvence oluşturulması ile uygulama kontrollerinin işlevselliği için güvenilir bir ortamın oluşturulmasını hedefleyen politika ve prosedürlerden oluşur. Genel kontroller, bankanın bilgi sistemlerinin bir bütün olarak kendisinden beklenen fonksiyonları doğru, zamanında ve güvenilir bir şekilde gerçekleştirilmesine yönelik ortamın tesisinde temel unsurlardır.

(2) Banka, genel kontrollerin tesisi amacıyla uluslararası kabul görmüş bir standart, çerçeve veya metodolojiyi belirleyerek, buna göre kontrolleri tesis eder. Seçilecek standart, çerçeve veya metodoloji, bankanın faaliyet kapsamı ve faaliyetlerde yararlanılan bilgi teknolojileri ağırlığı ve karmaşıklığı göz önünde bulundurularak belirlenir. Bankanın bilgi sistemleri genel kontrollerini tesis etmek üzere kullanacağı standart, çerçeve veya metodolojinin COBIT'te ele alınan kontrol hedeflerini gerçekleştirebilmesi, eğer bu konuda eksiklikleri varsa buna ilişkin kontrollerin ayrıca ele alınarak tesis edilmesi gerekir.

(3) Banka, genel kontrol konusu her bir sürece ilişkin olarak aşağıda sayılan hususlara uygun bir ortam tesis eder:

a) Süreç sahibi: Her genel kontrol konusu süreç için sorumluluğu açıkça tanımlanmış bir süreç sahibi atanır.

b) Tekrarlanabilirlik: Genel kontrol konusu süreçler tekrarlanabilir biçimde tanımlanır.

c) Hedefler ve amaçlar: Etkin bir biçimde çalışmalarını sağlamak amacıyla her genel kontrol konusu süreç için açıkça tanımlanmış hedefler ve amaçlar oluşturulur.

ç) Roller ve sorumluluklar: Etkin bir biçimde çalışmalarını sağlamak amacıyla her genel kontrol konusu süreç için açık bir şekilde roller, faaliyetler ve sorumluluklar tanımlanır.

d) Süreç performansı: Belirlenen hedeflere göre her genel kontrol sürecinin performansı ölçülür.

e) Politikalar, planlar ve prosedürler: Her bir genel kontrol süreciyle ilgili politikalar, planlar ve prosedürler yazılı hale getirilir, belli aralıklarla gözden geçirilir, güncellenir, onaylanır ve tüm ilgili birimlere duyurulur.

Kontrollerin takibi

MADDE 23 – (1) İç Sistemler Yönetmeliğinde ifade edilen iç kontrol faaliyetlerinin bir parçası olarak, bilgi sistemleri kontrollerinin etkinliğinin, yeterliliğinin ve uygunluğunun yanı sıra kontrol ile hedeflenen risk ya da risklerin etkisini azaltmaya yönelik performansı devamlı bir şekilde takip edilir ve değerlendirilir. Değerlendirme neticesinde tespit edilen önemli kontrol eksikleri üst yönetim ya da ilgili komitelere raporlanır ve gerekli tedbirlerin alınması sağlanır.

ÜÇÜNCÜ KISIM **Özellik Arz Eden İşlemler**

BİRİNCİ BÖLÜM **İnternet Bankacılığı**

İnternet bankacılığında uygulanacak hükümler

MADDE 24 – (1) Bu bölümde yer alan hükümler müşteriye ait finansal veya kişisel bilgilerin görülmesine, değiştirilmesine veya finansal sorumluluk yaratacak işlemlerin gerçekleştirilmesine imkân tanyacak internet bankacılığı hizmetleri için geçerlidir. İnternet bankacılığına ilişkin her türlü altyapı bankanın bilgi sistemlerinin bir parçası olarak değerlendirilir. Bu bakımdan Tebliğin diğer bölümlerinde yer alan hükümler internet bankacılığı kapsamında yapılan çalışmalar için de geçerlidir. Bu bölüm altında yer alan maddelerin içerdiği hükümler, Tebliğin İkinci Kısım Birinci Bölümü altında yer alan aynı başlıklı maddelerin içerdiği hükümlere ilave olacak şekilde değerlendirilir.

Yönetim gözetimi

MADDE 25 – (1) İnternet bankacılığı faaliyetleri kapsamında sunulan bankacılık hizmetlerinin, internetin doğasından kaynaklanan güvenliği sağlayamama, kimliği doğru belirleyememe, inkâr edebilme ve sorumluluk atayamama gibi konularda bir takım ek risklere maruz kalacağı da göz önünde bulundurulur ve ilgili hizmetlere ilişkin süreçler üzerinde bu Tebliğin 26 ila 31 inci maddeleri arasında yer alan hükümler doğrultusunda ilave kontroller tesis edilir.

Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi

MADDE 26 – (1) Güvenlik kontrollerinin yeterliliğini test etmek üzere bağımsız ekiplere, en az yılda bir kez olmak üzere, internet bankacılığı faaliyetleri kapsamındaki sistemler için sızma testleri yaptırılır.

(2) Banka, internet bankacılığı faaliyetleri kapsamında gerçekleşen sıra dışı ve şüpheli işlemleri tespit etmek için takip mekanizmaları kurar.

Kimlik doğrulama

MADDE 27 – (1) Banka, sunmakta olduğu internet bankacılığı hizmetleri için, bu hizmetlerin arz ettiği risk seviyelerine uygun ve güvenilir bir kimlik doğrulama mekanizması tesis eder. Müşterilerin, kurulan kimlik doğrulama mekanizmasından geçmeden hizmetlerden yararlanmasına müsaade etmeyecek bir yapı banka tarafından kurulur.

(2) Hizmetler için risk seviyelerinin tespiti yapılırken asgari olarak;

- a) Müşteri tipi,
 - b) Müşteriye sunulan işlemsel olanaklar,
 - c) Banka ile müşteri arasında paylaşılan bilgilerin hassasiyeti,
 - ç) Kullanılan iletişim alt yapısı ve
 - d) İşlem hacmi
- hususları dikkate alınır.

(3) İnternet bankacılığı için kimlik doğrulama işlemi, gerçekleştirilecek işleme taraf banka, müşteri ve varsa destek hizmeti kuruluşu gibi diğer müdahil tüm taraflar için yapılır.

(4) Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Müşterinin "bildiği" unsur olarak parola/değişken parola bilgisi gibi bileşenler, "sahip olduğu" unsur olarak tek kullanımlık parola üretim cihazı, kısa mesaj servisi ile sağlanan tek kullanımlık parola gibi bileşenler kullanılabilir. Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kimlik doğrulama gerçekleştirilememeli, hizmetlere erişim sağlanamamalıdır.

(5) Kimlik doğrulamada elektronik imza kullanılması durumunda, yalnızca 15/01/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 4 üncü maddesinde düzenlenen güvenli elektronik imza kullanıldığı takdirde bu maddenin dördüncü fıkrasındaki hükümler yerine getirilmiş sayılır. Elektronik imza vasıtasıyla kimlik doğrulama gerçekleştirmede yabancı elektronik sertifikaların kullanılması halinde, bu fıkrada anılan Kanunun "Yabancı elektronik sertifikalar" başlıklı 14 üncü maddesinde ve ilgili alt düzenlemelerde yer alan hükümler geçerlidir.

(6) Müşterilere uygulanan kimlik doğrulamada kullanılacak parolaların ve değişken parolaların yönetilmesi için politika belirlenmeli, bu politika asgari olarak aşağıdaki hususları içermelidir;

a) Parolaların ve değişken parolaların tahmin edilmesi ve kırılması zor bir karmaşıklıkta ve uzunlukta olması, müşterilerin parolalarını ve değişken parolalarını belirlerken bu karmaşıklığı sağlayacak biçimde sistemsal olarak zorlanması,

b) Değişken parolaların, belirli bir süre için kullanılması, bu süre sonunda kullanım dışı kalması, müşterinin yeni bir değişken parola belirlemeye zorlanması; yeni değişken parolanın, son kullanılan belirli sayıdaki değişken paroladan farklı olmadığı sürece sistemin yeni değişken parolayı kabul etmemesi,

c) Parolaların ve değişken parolaların sıfırlanması işlemlerinin yeterli güvenlik kontrollerini içermesi,

ç) Müşterilerin, uygun parola ve değişken parola belirleme ve bunların gizliliğinin sağlanmasının önemi konusunda bilgilendirilmesi.

(7) Kimlik doğrulamada kullanılacak şifreleme teknikleri, güncel durum itibarıyla literatürde kabul görmüş ve güvenilirliğini yitirmemiş algoritmaları baz almalıdır. Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanılabilmesi zaman zarfında kırılmayacak şekilde uzun seçilmelidir. Geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılabilirliği engellenmelidir.

(8) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyecek yöntemler barındıracak şekilde müşteri

kullanımına sunulur. Şifreleme anahtarları kimlik doğrulama için kullanılmak istendiklerinde parola, PIN (Kişisel Tanımlama Numarası) veya biyometrik bir bileşen bilgisi ile erişilebilir olmalıdır.

(9) İnternet bankacılığı faaliyetleri kapsamındaki işlemlerin gerçekleştirilmesi için müşteriye işlem doğrulama kodu sorulması durumunda, kullanılacak doğrulama kodları tahmin edilmesi zor olacak şekilde yeterli uzunlukta alfabetik ve/veya rakamsal karakterden oluşmalı, rastgele yaratılmalı ve müşteriye internet kanalı haricinde bir iletim ortamı üzerinden ulaştırılmalıdır. İşlem doğrulama kodları, geçerli bir kodun tahmin edilmesine imkân vermeyecek şekilde değişken ve eşsiz olarak üretilmelidir.

(10) Tek kullanımlık parola sunan cihazlardaki bu bilgi belirli bir süre sonra siliniyor olmalı ve/veya bir temizleme olanağı ile cihazdan silinebilmeli, bu cihazların ürettiği parolalar, bilinen parola tahmin yöntemleriyle belirlenmesi imkânsız, değişken ve eşsiz olmalıdır.

(11) Müşterilere uygulanacak kimlik doğrulama mekanizmasında kullanılacak parola, değişken parola, tek kullanımlık parola cihazı, şifreleme gizli anahtarı, akıllı kart ve işlem doğrulama kodu gibi bileşenlerin üretim aşamalarından başlayarak müşteriye ulaştırılmasına kadar geçen sürecin tamamı boyunca güvenliği sağlanır ve müşteri kullanımına sunulduğu anda güvenilirliğinin bozulmadığından bankaca emin olunur.

(12) Banka tarafından internet bankacılığı faaliyetleri kapsamındaki işlemlerde kullanılmak üzere müşterilerine sunulan her türlü yazılımın kaynağının, ilgili banka olduğunun doğrulanabiliyor olması sağlanır ve bu yazılımların kullanıcı güvenliğini tehlikeye sokacak herhangi bir kod içermediğinin belirlenmesini sağlayacak kontroller banka tarafından yapılır.

(13) Banka tarafından oluşturulacak kimlik doğrulama mekanizmasının;

a) Başarısız kimlik doğrulama teşebbüsleri hakkında, ilgili müşterinin sisteme ilk girdiği anda bilgi vermesi, başarısız teşebbüslerin belirli bir sayıyı aşması halinde ise ilgili müşterinin internet bankacılığına erişimini bloke etmesi,

b) Başarısız kimlik doğrulama teşebbüsleri sonrasında, bu teşebbüsü gerçekleştiren kişiye, yanlış girilen kullanıcı bilgisi veya parolası/değişken parolası ile ilgili, örneğin böyle bir kullanıcının sistemde olmadığı veya parolanın/değişken parolanın yanlış girildiği gibi, gereksiz bilgi vermemesi gerekir.

(14) Banka, tesis edeceği sistemler ve geliştireceği uygulamalarda müşterilerine ve personeline ait kimlik doğrulama bilgilerini ele geçirmeye yönelik bilinen saldırılara karşı gerekli sistemsel ve yazılımsal önlemleri alır.

(15) Olası tehditleri önceden belirleyebilmek ve gerekli önlemleri alabilmek adına, internet bankacılığı hesaplarına erişim için başarılı ve başarısız erişim teşebbüsleri düzenli olarak banka tarafından takip edilir, oransal bir anormallik görüldüğünde incelemeye alınır.

İnkâr edilemezlik ve sorumluluk atama

MADDE 28 – (1) Banka, sunmakta olduğu internet bankacılığı faaliyetleri kapsamında gerçekleştirilen işlemler için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikleri kullanır ve kontrolleri tesis eder. Kullanılacak teknikler ve tesis edilecek kontroller, gerek banka için gerekse müşteri için, finansal sonuç doğuran her türlü işlemde, hem işlemi başlatan hem de işlemi sonuçlandıran tarafın gerçekleştirdiği işlemleri inkâr edememesini sağlamalıdır. Kullanılan tekniğin veya tesis edilen kontrollerin oluşturduğu denetim izleri delil teşkil edecek ve sorumluluk atayacak nitelikte olmalıdır.

(2) Kullanılacak teknikler kimlik doğrulama mekanizmasına dayalı ve onunla bütünleşik olabileceği gibi, tamamen inkâr edilemezliği ve sorumluluk atamayı sağlamaya yönelik de olabilir.

(3) Banka tarafından sunulan internet bankacılığı servisi, müşterilerin yanlış işlem yapma ihtimalini azaltacak gerekli kontrolleri içerecek şekilde düzenlenmeli ve başlattıkları işlemlere ilişkin riskleri tamamen anlamalarını temin etmelidir.

Denetim izlerinin oluşturulması

MADDE 29 – (1) Banka, tüm internet bankacılığı faaliyetleri için yeterli ve etkin bir denetim izi tutma mekanizması tesis eder. Banka asgari olarak;

a) Hesap açılışı, kapanışı ve hesapta değişiklik faaliyetlerine,

b) Finansal sonuç doğuran işlemlere,

c) Müşteri için verilen limit aşım onaylarına,

ç) İnternet bankacılığı sistemine erişimi düzenleyen hak, ayrıcalık ve kısıtlamalarda yapılan her türlü değişikliğe

ilişkin denetim izlerini tutar. Denetim izlerinin, gerçekleşen işlemlerin başlangıcından sonuna kadar akışını ve kaynağını gösterecek detayda bilgi içermesi gerekir.

(2) Banka, internet bankacılığı faaliyetlerine ilişkin işlem ve kayıt tutma süreçlerinin ve alt yapısının, delil üretecek ve bu delillerin bozulmasını önleyecek, yanıltıcı delilleri ayırt edebilecek ve taraflara sorumluluk yüklemeye kullanılabilecek bilgileri sunacak şekilde yapılanmasını temin eder.

(3) Bu maddede bilgi ve belge tutulmasına ilişkin yer alan hükümler, diğer mevzuatın bilgi ve belge saklama ile ilgili hükümleri aynen saklı kalmak koşuluyla uygulanır.

Müşterilerin bilgilendirilmesi

MADDE 30 – (1) Banka, internet bankacılığı hizmetine ilişkin mevcut politika ve prosedürler ile dikkat edilmesi gereken hususlar konusunda müşterilerini bilgilendirir, gerekli uyarılarda bulunur.

(2) Banka, müşteri talebi olmadan internet bankacılığı hizmetini ilgili müşteri için kullanıma açamaz. Müşteri, internet bankacılığı hizmetine erişimi kapatmışsa veya kapatırmışsa, müşterinin yeni bir talebi olmadan internet bankacılığı hizmeti kullanıma açılmaz.

(3) Banka, internet bankacılığı hizmetinin verildiği internet sitesinde, erişilen sitenin bankaya ait olduğunu gösterecek teknikleri kullanır.

(4) Banka, internet bankacılığı hizmetini sunduğu internet sitesi üzerinden, kimliği ve kanuni statüsü ile ilgili bilgiler sunar. Bu kapsamda asgari olarak aşağıdaki bilgileri verir:

a) Bankanın ticari unvanı, genel müdürlük adresi,

b) Bankanın denetiminden sorumlu olan Bankacılık Düzenleme ve Denetleme Kurumuna ilişkin iletişim bilgileri,

c) Mevduatların sigortalanma koşul ve kapsamına ilişkin bilgiler.

(5) Banka;

a) İnternet bankacılığı servislerinin kullanımının taşıdığı riskler ve sağladığı faydalar ile internet bankacılığı servislerinden yararlanacak müşterilerin sorumluluk ve hakları hususunda müşterilerine açık ve anlaşılır bilgiler sunmakla,

b) Müşterilerin kişisel bilgilerinin gizliliğini sağlamaya ilişkin politika ve prosedürleri, banka güvenliğini zafiyete uğratmama hususunu gözeterek, müşteri dikkatine sunmakla,

c) İnternet bankacılığı servisi kapsamında hangi hizmetlerin verildiği ve bu hizmetlere erişim şartları ile güvenlik gereklilikleri konularında müşterilerini bilgilendirmekle,

ç) Müşterilerinde farkındalık yaratmayı amaçlayan yönlendirici güvenlik kılavuzları yayınlamakla ve banka güvenliğini zafiyete uğratmama hususunu gözeterek bu konudaki politika ve prosedürlerini müşterilerin dikkatine sunmakla,

d) İnternet bankacılığı sisteminde veya internet bankacılığı hizmetinin sunulduğu internet sitesinde yapılan erişilebilirliği etkileyebilecek değişiklikler hakkında müşterilerin bilgilendirilmesini sağlamakla yükümlüdür.

(6) Banka ayrıca aşağıdaki hususlarda müşterilerini bilgilendirir;

a) İnternet bankacılığı hizmeti kapsamında sunulan servislerin nasıl kullanılacağı,

b) İnternet bankacılığı kanalı üzerinden bankacılık işlemlerinin güvenli bir şekilde gerçekleştirilebilmesi için müşteriler tarafından nelerin yapılması gerektiği, parola veya değişken parola seçiminde nelere dikkat edilmesi gerektiği, bunların güvenliğini sağlamaya ilişkin müşteri sorumlulukları,

c) Herhangi bir problemle karşılaşılması durumunda nelerin yapılması gerektiği,

ç) Sunulan ve alınan her bir hizmete ilişkin koşullar; tarafların açık ve tereddüde yer bırakmayacak şekilde sorumluluklarının ve görevlerinin tanımı.

(7) Bu madde kapsamında tanımlanmış olan müşteri bilgilendirmesine yönelik her türlü açıklama, bankanın internet bankacılığı hizmetini sunduğu internet sitesi üzerinden müşteri erişimine daima açık tutulur. Tüm açıklamalar mümkün olduğunca kısa ve anlaşılır olmalıdır. Açıklamalar internet bankacılığı hizmetinin verildiği sitede dikkat çekici bir yere yerleştirilir, müşterilerin en az bir kere okumasını garanti edecek şekilde yönlendirmeler ve sistemsel kısıtlamalar uygulanır.

(8) Banka, yaptığı pazarlama faaliyetleri, reklâmlar veya yayınlar vasıtasıyla müşterilerine internet bankacılığı sistemlerinin mutlak surette güvenli olduğu veya internet bankacılığı servislerinde hiçbir güvenlik riskinin bulunmadığı izlenimini ve bilgisini verecek ifadelerden kaçınır. Müşteriler internet bankacılığı risklerine ve tehditlerine karşı uyarılır ve bu hususlarda müşteri farkındalığı oluşturulması için azami özen gösterilir.

(9) Mobil iletişim cihazları üzerinden gerçekleştirilen internet bankacılığı işlemleri için de bu madde altında bahsedilen bilgilendirme zorunlulukları geçerlidir. Bu cihazların ilgili bilgilendirmeyi sağlama konusunda yetersiz kalması durumunda müşterinin söz konusu bilgilere farklı kanallar üzerinden ulaşması için gerekli yönlendirme yapılır.

Servis sürekliliği ve kurtarma planı

MADDE 31 – (1) Banka, internet bankacılığı servisi için beyan ettiği veya müşterilerine taahhüt ettiği düzeyde servis sürekliliğini sağlar. Servis kesintisinin doğurabileceği hukuki sorumlulukları en aza indirmek üzere banka gerekli önlemleri alır.

(2) Banka mücbir sebepler dışında müşterilerine önceden duymaksızın servis kesintilerine gidemez, internet bankacılığı servislerinde oluşacak kesintileri müşterilerine mümkün olduğunca önceden duyurur ve bu kesintilere ilişkin gerekçeleri de içerecek şekilde müşterilerini bilgilendirir.

(3) Servis süreklilik ve kurtarma planları geliştirilirken servis dışı bırakma atakları da göz önünde bulundurulur, bunlara karşı gerekli önlemler alınır.

İKİNCİ BÖLÜM

ATM

ATM güvenliği

MADDE 32 – (1) Banka, ATM cihazlarına ilişkin hırsızlık, sahtekârlık, fiziksel saldırı gibi tehditlere ilişkin

riskleri minimize edici önlemleri tesis eder ve ATM cihazlarının güvenli kullanımı hususunda müşterilerinde farkındalık yaratır.

(2) ATM cihazları üzerinde ön tanımlı olarak gelen her türlü parola/değişken parola, ATM cihazının bu ön tanımlı parolaları/değişken parolaları bilen kötü niyetli kişiler tarafından yönetilmesini engellemek amacıyla, kolaylıkla tahmin edilemeyecek şekilde değiştirilir.

(3) ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler alınmalı, cihaza yetkisiz kişilerin herhangi bir şekilde başka bir elektronik cihaz bağlamasını sağlayacak bütün giriş noktaları erişime kapatılmalıdır. ATM'ler üzerine, güvenlik açıklıklarını gidermek amacıyla otomatik olarak veya düzenli periyotlar ile gerekli güncellemeler ve yamalar yüklenir. ATM cihazı ile banka arasındaki ağ bağlantısına yetkisiz olarak diğer cihazların bağlanmasını engelleyecek ek güvenlik tedbirleri uygulanır.

(4) ATM cihazları üzerinden gerçekleştirilen işlemler için kullanılan iletişim ağı veri güvenliği, gizliliği ve bütünlüğünü sağlayacak özellikte olmalıdır. Müşterilerin girdiği PIN bilgileri ve gerçekleştirilecek işlemlere ilişkin bilgiler cihaz içinde ve cihaz dışındaki ATM ağı boyunca şifrelenmiş bir şekilde iletilmelidir.

(5) Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Müşterinin "bildiği" unsur olarak PIN bilgisi gibi bileşenler, "sahip olduğu" unsur olarak ATM kartı gibi bileşenler kullanılabilir. Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kimlik doğrulama gerçekleştirilememeli, hizmetlere erişim sağlanamamalıdır.

(6) ATM cihazlarının servis sürekliliğinin sağlanması ve sahtekârlık, fiziksel saldırı gibi maruz kalabilecekleri risklerin erken tespiti adına, Banka tarafından ATM cihazları için uzaktan yönetim ve takip sistemleri kurulur.

(7) ATM operatörleri ve teknisyenleri, ATM cihazlarına ilişkin güncel bütün sahtekârlık yöntemleri konusunda eğitilir ve bu gibi personelin ATM cihazlarını düzenli olarak kontrol etmeleri sağlanır. ATM cihazları özellikle, üzerlerine yabancı aparatlar veya başka elektronik cihazlar (kart kopyalama cihazları, sahte klavye, kamera gibi) yerleştirilmiş olma ihtimallerine karşı, operatörler tarafından düzenli periyotlarla dikkatle incelenmelidir.

(8) ATM'e ilişkin mutabakatlar, yeterli sıklıkta ve görevler ayrılığı prensibine uygun olarak en az iki kişi tarafından gerçekleştirilir.

(9) Banka, müşterilerinin ATM hizmetlerinden güvenli bir şekilde faydalanmasını sağlamak amacıyla, ATM güvenliği ve güncel sahtekârlık yöntemlerinden korunma hususunda müşterilerini bilgilendirir ve bu konu hakkında müşterilerinde farkındalık oluşmasını sağlar.

(10) Banka, ATM cihazlarının bulunduğu yerlere güvenlik kamerası koyar, ancak bu güvenlik kamerası, müşterinin klavye hareketlerini göremeyecek biçimde konumlandırılır. Güvenlik kamerası kayıtları en az iki ay süreyle saklanır ve kamera teçhizatları çalıştıklarına dair düzenli olarak kontrol edilir. Görüntüleme alanı bakımından ATM'i de kapsayan ve bu fıkradaki koşulları karşılayan bir güvenlik kamerası altyapısının varlığı durumunda ATM'e özel ayrıca bir güvenlik kamerası kurulmasına gerek yoktur. Ayrıca kamu güvenlik ve istihbarat kurumlarının faaliyet bölgesinde bulunan ATM'ler için güvenlik kamerası kurulma şartı, ilgili kamu güvenlik ve istihbarat kurumlarından izin alınabilmesi koşuluyla yerine getirilir.

DÖRDÜNCÜ KISIM

Çeşitli ve Son Hükümler

BİRİNCİ BÖLÜM

Çeşitli Hükümler

Kablosuz haberleşme teknolojileri

MADDE 33 – (1) Banka, bilgi sistemleri alt yapısında, gerek temel bankacılık faaliyetlerinin ifasında gerekse alternatif dağıtım kanallarının tesisinde kullanılan kablosuz haberleşme teknolojilerine ilişkin riskleri yönetmek üzere gerekli önlemleri alır. Kablosuz haberleşme teknolojilerinin bankacılık faaliyetlerinde kullanılmasına ilişkin risklerin yönetilmesi bilgi sistemleri yönetiminin bir bileşeni olarak ele alınır. Kablosuz teknolojilerin zayıf yanları da dikkate alınarak gerekli kontroller tesis edilir.

Tebliğde hüküm bulunmayan haller

MADDE 34 – (1) Bu Tebliğde hüküm bulunmayan hallerde; İç Sistemler Yönetmeliğinde yer alan usul ve esaslar, uluslararası kabul görmüş bilgi teknolojileri kontrol hedefleri sunan COBIT dokümanlarında yer alan usul ve esaslar uygulanır.

İKİNCİ BÖLÜM

Son Hükümler

Geçiş süreci

GEÇİCİ MADDE 1 – (1) Banka, bu Tebliğ hükümleri ile ilgili mevcut faaliyet ve sistemlerini, yürürlük tarihinden itibaren azami iki yıl içerisinde Tebliğ hükümlerine uygun hale getirir.

Yürürlük

MADDE 35 – (1) Bu Tebliğ 1/1/2008 tarihinde yürürlüğe girer.

Yürütme

MADDE 36 – (1) Bu Tebliğ hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.