

## **BANKALARIN BİLGİ SİSTEMLERİ VE ELEKTRONİK BANKACILIK HİZMETLERİ HAKKINDA YÖNETMELİK**

### **BİRİNCİ KISIM Başlangıç Hükümleri**

#### **Amaç ve kapsam**

**MADDE 1 –** (1) Bu Yönetmeliğin amacı, bankaların faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrollerini düzenlemektir.

#### **Dayanak**

**MADDE 2 –** (1) Bu Yönetmelik, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 93 üncü maddesi uyarınca düzenlenmiştir.

#### **Tanımlar ve kısaltmalar**

**MADDE 3 –** (1) Bu Yönetmelikte yer alan;

a) Açık bankacılık servisleri: Müşterilerin ya da müşteriler adına hareket eden tarafların API, web servis, dosya transfer protokolü gibi yöntemlerle bankanın sunduğu finansal servislere uzaktan erişerek bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektronik dağıtım kanalını,

b) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

c) API: Bir yazılımın başka bir yazılımda tanımlanmış işlevleri kullanabilmesi için oluşturulmuş uygulama programlama arayüzünü,

ç) ATM: Otomatik para çekme işleminin yanı sıra diğer bankacılık işlemlerinin tamamının veya bir bölümünün gerçekleştirilmesine imkân veren elektronik işlem cihazlarını,

d) Banka: Kanunun 3 üncü maddesinde tanımlanan bankaları,

e) Bilgi sistemleri (BS): Bilginin toplanması, işlenmesi, saklanması, dağıtımı ve kullanımına yönelik insan kaynağı, operasyonel faaliyetler ve süreçler ile bunlarla etkileşim içinde bulunan bilgi teknolojilerini,

f) Bilgi sistemleri süreklilik planı: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan bilgi sistemleri süreklilik planını,

g) Bilgi sistemleri yönetimi: Bankaca gerçekleştirilen faaliyetlerin ve verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yürütülmesine; mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesine; 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; bilgi sistemlerinin kullanılmasından kaynaklanan risklerin kontrolünün ve izlenmesinin sağlanmasına; bu amaçla gerekli sistemsel ve yönetsel önlemlerin alınmasına ilişkin faaliyetleri,

ğ) Bilgi teknolojileri (BT): Herhangi bir biçimdeki verinin, girişinin yapılması, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim altyapısı ve ilgili diğer teknolojileri,

h) Bilgi varlığı: Bankacılık faaliyetlerinin yürütülmesinde kullanılan veriler ile bu verilerin taşındığı, saklandığı, iletildiği veya işlendiği sistem, yazılım, ağ cihazları, BT donanımları, iş süreçleri gibi Banka için değeri olan varlığı,

1) Birincil merkez: Birincil sistemlerin tesis edildiği yapıyı,

i) Birincil sistemler: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan birincil sistemleri,

j) Biyometrik kimlik doğrulama bileşeni: Kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla kullanılan bir kişiye özgü ölçülebilir biyolojik veya davranışsal karakteristiği,

k) Dış hizmet: 5/11/2011 tarihli ve 28106 sayılı Resmî Gazete’de yayımlanan Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik kapsamındaki destek hizmetleri de dâhil olmak üzere bankaların bilgi sistemlerine ilişkin dışarıdan temin ettikleri, bankacılık verilerinin gizliliği, bütünlüğü ve erişilebilirliği ile bankacılık hizmetlerinin sürekliliğini etkileme potansiyeli olan, bankacılık verilerine erişimi bulunan ya da bu verilerin paylaşıldığı hizmet alımlarını,

l) Elektronik bankacılık hizmetleri: İnternet bankacılığı, mobil bankacılık, telefon bankacılığı, açık bankacılık servisleri ile ATM ve kiosk cihazları gibi müşterilerin, uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri her türlü elektronik dağıtım kanalını,

m) Elektronik imza: 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanan elektronik imzayı,

n) Güvenlik duvarı: Farklı güvenlik seviyelerine sahip ağlar veya ağa bağlı cihazlar arasındaki trafik akış kontrolünü sağlayan donanım ya da yazılımları,

o) Hassas veri: Kimlik doğrulamada kullanılan veriler başta olmak üzere; müşteriye ait olan, çeşitli sebeplerle bankaca muhafaza edilen ve üçüncü kişilerce ele geçirilmesi halinde, bu kişilerin müşteri olan kişilerle ayırt edilebilme mekanizmalarının zarar göreceği ve dolandırıcılık ya da müşteriler adına sahte işlem yapılmasına imkân verebilecek nitelikteki verileri,

ö) İkincil merkez: İkincil sistemlerin kullanıma hazır olacak şekilde tesis edildiği ve birincil sistemlerde herhangi bir kesinti yaşanması durumunda personelin çalışmasına imkân tanyacak ve birincil merkez ile aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı,

p) İkincil sistemler: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan ikincil sistemleri,

r) İnternet bankacılığı: Bankaların kendi ticaret unvanı, işletme adı ya da herhangi başka bir ad altındaki bir web sayfası üzerinden sundukları hizmetlere müşterilerin, kullandıkları cihaz ya da platformdan bağımsız olarak, internet yoluyla ulaşabildiği ve kendilerine ait finansal veya kişisel verileri görüntüleyebildiği, değiştirebildiği ya da finansal sorumluluk yaratacak işlemler gerçekleştirebildiği elektronik dağıtım kanallarını,

s) İSEDES Yönetmeliği: 11/7/2014 tarihli ve 29057 sayılı Resmî Gazete’de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliği,

ş) İş etki analizi: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan iş etki analizini,

t) Kanun: 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununu,

u) Kesinti: Bir bankanın faaliyetlerindeki sürekliliğin, planlı geçişler haricinde sekteye uğramasını,

ü) Kimlik doğrulama: Bildirilen bir kimliğin gerçekten bildiren şahsa ait olduğuna dair güvence sağlayan mekanizmayı,

v) Kişisel veri: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununda tanımlanan kişisel veriyi,

y) Kontrol: Banka içerisinde BT süreçlerinde gerçekleştirilen ve iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvenciyi oluşturma amacı güden politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,

z) Kullanıcı: Banka personeli, dış hizmet sağlayıcı çalışanı veya banka müşterisi gibi bankanın bilgi sistemleri üzerinde işlem gerçekleştirmek üzere kendilerine hesap tanımlanmış olan her türlü kullanıcıyı,

aa) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

bb) Kurumsal SOME: 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete’de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinde ifade edilen Kurumsal SOME’yi,

cc) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

çç) Mobil bankacılık: Akıllı telefon veya tablet gibi mobil bir cihaz üzerinde yüklü, bankaya ait mobil uygulama üzerinden müşterilerin bankacılık işlemlerini gerçekleştirebildikleri özelleşmiş internet bankacılığı dağıtım kanalını,

dd) Oturum: Veri aktarımı, sunuşu veya gerçekleştirilecek finansal işlemler için taraflar arasında kurulan mantıksal bağı,

ee) Parola: Kimlik doğrulamada kullanılan, gizli harf, rakam ve/veya özel işaretlerden oluşan karakter dizisini,

ff) Risk limitleri: İSEDES Yönetmeliğinin 38 inci maddesinde açıklanan risk limitlerini,

gg) Sektörel SOME: Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 7 nci maddesinde ifade edilen Kurum bünyesinde teşkil edilmiş Sektörel SOME'yi,

ğğ) Sızma testi: Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen güvenlik testlerini,

hh) Siber olay: Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 3 üncü maddesinde tanımlanan siber olayı,

ıı) Siber olaya müdahale: Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 3 üncü maddesinde tanımlanan siber olaya müdahaleyi,

ii) SMS OTP: Elektronik haberleşme işletmecilerinin sunduğu kısa mesaj servisi aracılığıyla iletilen tek kullanımlık parolayı,

jj) Tek kullanımlık parola: Kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele oluşturulan harf ve/veya rakamlar dizisini,

kk) Uçtan uca güvenli iletişim: İletişime konu veriye sadece alıcısının erişebilmesi amacıyla, verinin gönderen tarafından sadece alıcının çözebileceği şekilde şifrelenerek iletilmesini,

ll) Üst düzey yönetim: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan üst düzey yönetimi,

mm) Üst yönetim: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan üst yönetimi,

nn) Varlık muhafızı: Varlık sahibinin tanımladığı güvenlik gereksinimlerine uygun olarak, bir bilgi varlığının saklanması, taşınması, işlenmesi veya iletilmesi esnasında korunmasından sorumlu olan kişiyi,

oo) Varlık sahibi: Bilgi varlıklarına yönelik güvenlik gereksinimlerini belirleyerek varlık muhafızlarına ileten ve bu gereksinimlere uygun güvenlik kontrollerinin varlık muhafızları tarafından uygulandığını gözeterek bilgi varlığının idamesi ve erişilebilirliğinden sorumlu olan kişiyi,

öö) Yama: Programlarda tespit edilen güvenlik açıkları veya programın içeriğindeki hatalı bir fonksiyonu düzeltme amaçlı hazırlanan program eklentisini,

ifade eder.

## İKİNCİ KISIM

### Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi

## BİRİNCİ BÖLÜM

### Bilgi Sistemleri Yönetimi

#### Yönetim gözetimi, roller ve sorumluluklar

**MADDE 4 –** (1) Banka yönetim kurulu, bilgi sistemlerinin yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele almakla, bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağını tahsis etmekle, bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesini sağlamakla ve gelişen yeni teknolojileri de göz önünde bulundurarak bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesi için etkin bir gözetim yürütmekle sorumludur. Bu amaçla, yönetim kurulu tarafından onaylanmış bir BS strateji planı, BS Strateji Komitesi ve BS Yönlendirme Komitesi oluşturulur. Banka yönetim kurulu bankanın ölçeği, bilgi sistemlerine bağımlılığı, personel sayısı ve bilgi sistemleri konusunda alınan dış hizmetler gibi kriterleri esas alarak strateji ve yönlendirme komitelerini birleştirebilir. Bu komitelerin görev tanımları ve çalışma esasları yönetim kurulu tarafından onaylanır.

(2) BS Strateji Komitesi, yönetim kurulu adına, BS strateji planı doğrultusunda BS yatırımlarının uygun bir şekilde kullanılıp kullanılmadığının ve bankanın iş hedefleri ile BS hedeflerinin birbiriyle uyumluluğunun gözetimini yürütmekle; bu hususlarda yönetim kuruluna doğrudan ve düzenli olarak raporlama yapmakla; BS strateji planını yılda en az bir defa olmak üzere gözden geçirerek gerekli olduğu durumlarda revize ederek yönetim kurulu onayına sunmakla ve BS Yönlendirme Komitesinin faaliyetlerini gözetmekle sorumludur.

(3) BS Strateji Komitesinde en az bir yönetim kurulu üyesinin bulunması ve bilgi sistemlerinden sorumlu üst düzey yönetici ile bankanın ilgili iş birimlerinden üst düzey yöneticilerin bu komiteye üye olması esastır. BS Strateji Komitesi, BS strateji planının düzgün bir şekilde uygulanıp uygulanmadığını gözden geçirmek ve önemli BS yatırım kararlarını değerlendirmek üzere yılda en az iki defa bir araya

gelir ve yılda en az bir defa yönetim kuruluna rapor sunar.

(4) BS stratejisinin yönetim kurulu onayı doğrultusunda uygulanmasında, BS Strateji Komitesine ve üst düzey yönetime yardımcı olmak amacıyla bir BS Yönlendirme Komitesi oluşturulur. BS Yönlendirme Komitesi, BS yatırımlarının ve projelerinin öncelik sırasını belirlemek, devam eden BS projelerinin durumunu takip etmek, projeler arasındaki kaynak çatışmalarını çözüme kavuşturmak, BS mimarisi ve BS projelerinin mevzuata uyumluluğunu sağlamak üzere gerekli yönlendirmeleri yapmak ve BS servislerine ilişkin hizmet seviyelerini izlemekten sorumludur. BS Yönlendirme Komitesinde BS, insan kaynakları, bankanın ilgili iş birimlerinden temsilcilerin ve banka organizasyonunda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin bulunması esastır. BS Yönlendirme Komitesi, yılda en az iki defa bir araya gelir ve yılda en az bir defa BS Strateji Komitesine rapor sunar.

(5) BS organizasyonu ve bilgi sistemlerinin kapsamlılık düzeyinin, bankanın büyüklüğü ve faaliyetlerinin karmaşıklığı ile orantılı olması ve BS organizasyon şemasının da bu doğrultuda oluşturulması esastır. BS organizasyon şeması kapsamındaki birimlerin görev ve sorumlulukları ile bu birimlerdeki personelin görev tanımları açık bir şekilde yazılı hale getirilir, yönetim kurulu ya da yönetim kurulunun bu yönde yetkisini devrettiği üst düzey yöneticilerce onaylanır, bu görev tanımlarının uygunluğu düzenli olarak gözden geçirilir.

(6) BS personelinin kendilerine atanan görev ve sorumluluklar hakkında farkındalığa sahip olması ve kendilerine ait görev ve sorumluluklarda değişiklik yapılması halinde bu değişikliklerden haberdar olmaları sağlanır.

#### **Bilgi sistemleri politika, prosedür ve süreç dokümanları**

**MADDE 5 –** (1) Banka, bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden BS politika, prosedür ve süreç dokümanlarını oluşturur.

(2) Dokümanların gizlilik derecesi ve banka çalışanlarının görev ve sorumluluklarının uygunluğu nispetinde dokümanlara erişim imkânı verilir. Dokümantasyonda asgari olarak doküman kodu ve dokümanın gizlilik derecesine yer verilir.

(3) BS politikaları yönetim kurulu tarafından, BS prosedürleri ve süreç dokümanları ise yönetim kurulu ya da yönetim kurulunun bu yönde yetkisini devrettiği yöneticilerce onaylanır.

(4) BS politika, prosedür ve süreç dokümanlarının gerekleri, bankanın organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözetim ve takip gerçekleştirilir. Politika ve prosedürlerin işletilmesinden sorumlu birimler ve görev tanımları ile süreç dokümanlarının işletilmesinden sorumlu süreç sahipleri ilgili politika, prosedür ve süreç dokümanları içinde belirtilir.

(5) BS politika, prosedür ve süreç dokümanları yılda en az bir defa gözden geçirilir ve gerekli güncellemeler yapılır. Dokümanlarda meydana gelen değişiklikleri takip edebilmek adına, dokümanın önceki versiyonu ile asgari olarak dokümanı onaylayan, revizyon tarihi ve gözden geçirme tarihi bilgileri kayıt altına alınır.

## **İKİNCİ BÖLÜM**

### **Bilgi Sistemleri Risklerinin Yönetilmesi**

#### **Bilgi varlıkları envanteri ve sınıflandırılması**

**MADDE 6 –** (1) Banka, bilgi varlıklarının güvenlik gereksinimlerine uygun kontroller tesis etmek için bu varlıkları sınıflandırarak detaylı bir varlık envanteri hazırlar. Hazırlanacak varlık envanterinde her bir bilgi varlığı için;

- a) Varlığın ne olduğunu açıkça belirtecek tanımına,
  - b) Banka için görece değerine,
  - c) Bulunduğu konuma,
  - ç) Varlığın güvenlik sınıfına ve bu sınıfın belirlenmesini sağlayan gizlilik, bütünlük, erişilebilirlik gibi değerlerine,
  - d) Varlığın sahibine,
  - e) Varlığın muhafızına,
- yer verilir.

(2) Bilgi varlıklarının değeri ele alınırken bu varlıkların ilişkili olduğu iş hedefleri ve iş süreçleri ile bunların bağlı olduğu diğer iş hedefleri ve iş süreçleri dikkate alınır.

(3) Bilgi varlıklarının bir parçası olan veriler için oluşturulacak veri envanterine birinci fıkrada belirtilen detaylara ilave olarak kişisel veri olup olmadığı bilgisi dâhil edilir.

(4) Varlık sahipleri ile birlikte çalışılmak suretiyle, her bir varlığın tanımlı ve onaylı bir güvenlik sınıfına ve erişim kısıtlamasına sahip olması sağlanır. Güvenlik sınıfları ve erişim kısıtlamaları iki yıldan uzun olmayacak periyotlarla düzenli olarak gözden geçirilir.

(5) Bilgi varlıklarının, nasıl sınıflandırılacağına yönelik olarak Bilgi Güvenliği Komitesi tarafından onaylı bir varlık sınıflandırma kılavuzu hazırlanır. Varlıkların güvenlik sınıfı belirlenirken gizlilik derecesi, bütünlük gereksinimi, erişilebilirlik gereksinimi, saklama süresi ve asgari yedekleme sıklığı gibi kriterler göz önünde bulundurulur.

(6) Verilerin güvenlik sınıfı asgari olarak bu verilerin gizlilik derecesi, bütünlük gereksinimi, erişilebilirlik gereksinimi ve hassas veri, kişisel veri ya da sır kapsamındaki veri olup olmadığı gibi kriterler göz önünde bulundurulur olarak belirlenir.

### **Bilgi sistemleri risk yönetim süreci**

**MADDE 7 -** (1) Banka, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri analiz etmek, azaltmak, takip etmek ve raporlamak üzere bir BS risk yönetim süreci tesis eder.

(2) BS risk analizi kapsamında aşağıdaki faaliyetler yerine getirilir:

a) 6 ncı maddenin birinci fıkrası kapsamında oluşturulan varlık envanterindeki bilgi varlıklarına ilişkin tehdit ve güvenlik açıklarının tespit edilmesi suretiyle risklerin belirlenmesi,

b) Tespit edilen tehditlere ve güvenlik açıklarına göre bilgi varlıklarının riske maruz kalma olasılıklarının belirlenmesi,

c) Risklerin gerçekleşmesi durumunda ilişkili bilgi varlığının gizliliği, bütünlüğü, erişilebilirliği gibi kriterlerine olan etkilerin belirlenmesi suretiyle ilgili bilgi varlığına yönelik etki hesaplaması yapılması,

ç) Bilgi varlıklarını tehdit eden risklerin belirlenen olasılık ve etki değerlerine göre risk derecelendirmesinin yapılması,

d) Risk analizinde gerçekleştirilen çalışmaların bütünü temsil eden özet risk değerlendirme raporunun hazırlanarak üst yönetime sunulması.

(3) Risk analizi sonuçlarına göre tespit edilen her bir BS riskine ilişkin, bu risklerin ilişkili olduğu bilgi varlıklarının değerine ve bankanın risk limitlerine uygun olacak şekilde risklere ilişkin aksiyonlar belirlenir. Risk aksiyonlarının belirlenmesi aşamasında, riskin ilgili olduğu iş biriminin temsilcileriyle beraber risk analizi sonucunda, riskin azaltılması, riskten kaçınma, riskin kabulü ve riskin transferi gibi yöntemlerle nasıl ele alınacağına karar verilir.

(4) Her bir risk için belirlenen aksiyonlar risk aksiyon planına dönüştürülür. Alınacak aksiyonlar için yapılacak kaynak aktarımında ve aksiyonların tamamlanma tarihlerinin önceliklendirilmesinde, risk analizi aşamasında belirlenen risk dereceleri dikkate alınır. Aksiyon planının uygulanması sonucunda kalacak artık riskler için de alınacak aksiyonlar planlanır ve aksiyon planı güncellenir.

(5) Riskin kabul edilebilmesi için bilgi sistemlerinden sorumlu üst düzey yöneticinin onayının bulunması, riskin BS stratejisine ve mevzuata aykırılık teşkil etmemesi şarttır. Kabul edilecek riskin aynı zamanda bir iş süreci veya iş uygulamasıyla ilgili olması durumunda ilgili iş biriminin üst düzey yöneticisinin de riskin kabul edildiğine ilişkin onayının bulunması gerekir. Sonradan telafi edici yeni kontrol tekniklerinin ya da yeni güvenlik çözümlerinin ortaya çıkmış olması veya riskin eskiye nazaran artıp artmadığı yönünde koşulların değişmiş olması ihtimaline karşı, önceden kabul edilmiş olan riskler periyodik olarak gözden geçirilir.

(6) Risk analizleri sonucu hazırlanan güncel risk değerlendirme raporu ve güncel risk aksiyon planı birleştirilerek bankanın BS risk envanteri oluşturulur. Banka, yılda en az bir defa olmak üzere veya bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce risk analizlerini tekrarlar. Tekrarlanan risk analizi sonuçlarına göre risk aksiyon planı ve BS risk envanterinin güncellenmesi sağlanır. Banka bünyesinde gerçekleştirilen BS iç kontrol ve iç denetim çalışmalarının sonuçlarının veya tespit edilen bulguların risk envanterine girdi teşkil etmesi sağlanır.

(7) Bankanın kurumsal risk yönetimi sürecinin, BS risklerini de kapsamı esastır. BS risklerinin bankacılık faaliyetlerinden kaynaklanan diğer risklerin de bir çarpanı olabileceği dikkate alınarak banka

genelinde, bilgi sistemlerinden kaynaklanan riskleri de içerecek şekilde, bütünsel bir risk yönetim metodolojisi uygulanır. BS risk yönetim süreci çıktılarından elde edilen verilerin bankanın bütünsel risk yönetim çerçevesinin bir parçası haline gelmesi sağlanır. Bilgi sistemlerinden kaynaklanan riskler ele alınırken gelişen yeni teknolojilerin getireceği riskler ayrıca değerlendirilir. BS risk envanteri kapsamında riskler takip edilerek yönetim kuruluna ve üst düzey yönetime yılda en az bir defa raporlanır.

## **ÜÇÜNCÜ BÖLÜM** **Bilgi Güvenliği Yönetimi**

### **Bilgi güvenliği organizasyonu, roller ve sorumluluklar**

**MADDE 8 – (1)** 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 sisteminin ulusal veya uluslararası standartları ya da en iyi uygulamaları referans alması ve aşağıdaki faaliyetleri içermesi esastır.

- a) Bilgi varlıklarına yönelik olarak düzenli bir şekilde tehdit ve risk değerlendirme çalışmalarının yapılması,
- b) Bilgi varlıklarının sınıflandırılarak varlık sahipliklerinin belirlenmesi ve varlık sınıflarına uygun güvenlik önlemlerinin alınması,
- c) Bilgi güvenliği ihlaline ilişkin olayların izlenmesi ve raporlanması,
- ç) Banka genelinde verilen bankacılık hizmetlerinde, görevler ayrılığı prensibi ile tutarlı etkin bir kimlik doğrulama ve erişim yönetimi tesis edilmesinin sağlanması,
- d) Bilgi güvenliğinin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların test edilmesi ve test sonuçlarının takip edilerek raporlanması,
- e) Bilgi varlıklarına yönelik güncel güvenlik açıklarının takip edilmesi ve gerekli aksiyonların alınmasının sağlanması,
- f) Üst yönetim de dâhil olmak üzere banka çalışanları, dış hizmet sağlayıcılar ve müşteriler gibi bankanın bilgi güvenliğini ilgilendiren paydaşlara yönelik, bilgi güvenliği farkındalığını artıracak çalışmaların yapılması,
- g) İş sürekliliği yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer almasının sağlanması,
- ğ) Dış hizmet alımlarının yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer almasının sağlanması.

(2) Bilgi güvenliği yönetim sisteminin banka genelinde nasıl uygulanacağı bilgi güvenliği politikası, prosedürleri ve süreç dokümanları ile düzenlenir. Bankanın bilgi güvenliği politikası yönetim kurulu tarafından onaylanır ve banka genelinde çalışanlara ulaştırılması sağlanır. Bu kapsamda bilgi sistemlerine ilişkin kabul edilebilir kullanım standartları belirlenir.

(3) Bilgi güvenliği politikasının oluşturulması ve uygulanması faaliyetleri yönetim kurulu adına Bilgi Güvenliği Komitesi tarafından gerçekleştirilir. Bilgi Güvenliği Komitesine, belirlenen bir yönetim kurulu üyesi veya genel müdür başkanlık eder ve komitenin koordinasyonunu bilgi güvenliği sorumlusu yerine getirir. Bilgi Güvenliği Komitesi toplantılarına bilgi sistemlerinden sorumlu üst düzey yöneticinin, bankanın ilgili iş birimlerinden üst düzey yöneticilerin, insan kaynakları, risk yönetimi birimlerinden ve banka organizasyonunda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin de katılması esastır. Bilgi Güvenliği Komitesinin görev tanımları ve çalışma esasları, yönetim kurulu tarafından onaylı olacak şekilde yazılı hale getirilir, yılda en az iki defa toplanması ve yılda en az bir defa yönetim kuruluna rapor sunması sağlanır.

(4) Bilgi güvenliği politikası, prosedürleri ve süreç dokümanları yılda en az bir defa gözden geçirilir. Önemli güvenlik olayları, yeni güvenlik açıkları ya da teknik altyapıdaki önemli değişikliklerden sonra da bunların ayrıca gözden geçirilmesi sağlanır.

(5) Banka bünyesinde, bilgi sistemlerinden sorumlu üst düzey yönetici ve ona bağlı birimlerden meydana gelen BS fonksiyonundan ayrı ve bağımsız olacak şekilde bir BS güvenlik fonksiyonu oluşturulur. BS güvenlik fonksiyonunun doğrudan yönetim kuruluna veya genel müdüre bağlı olması

esastır. Bankanın BS güvenlik fonksiyonu, bilgi güvenliği sorumlusu tarafından yönetilir.

(6) Bilgi güvenliği sorumlusu aşağıdaki görevleri yerine getirir:

a) Bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulması, bunların güncellenmesi ve onaya sunulması,

b) Bilgi güvenliği bakış açısıyla, bilgi varlıklarının sınıflandırılması ve bilgi varlıklarına yönelik gizlilik, bütünlük, erişilebilirlik kriterleri bakımından BS risk yönetimi çalışmalarına aktif katkı sunulması ve yardımcı olunması,

c) İlgili birimlerle uyum içinde, iş gereksinimleri ve iş hedefleriyle uyumlu banka genelinde bilgi güvenliğinin tesis edilmesi,

ç) Bilgi güvenliği ile ilgili mevzuat hükümlerine, standartlara, politika, prosedür ve süreç dokümanlarına uyumun takip edilmesi,

d) Bilgi güvenliği faaliyetlerinin ve testlerinin yürütülmesinin sağlanması ve bunların takip edilmesi,

e) Önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunulması,

f) Bankanın bilgi güvenliğini ilgilendiren paydaşlara yönelik bilgi güvenliği farkındalık programının yürütülmesi.

### **Veri gizliliği**

**MADDE 9** – (1) Banka, bankacılık faaliyetlerinin yürütülmesinde kullanılan verilerin taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu ortamlarda gizliliğini sağlayacak önlemleri alır. Verilerin tutulduğu ortamın kâğıt veya elektronik ortam olmasından bağımsız olarak alınacak önlemlerin, gizliliği sağlanmaya çalışılan verilerin gizlilik derecesine uygun olması ve gerekli yerlerde ek kontrollerin tesis edilmesi esastır. Veri barındıran medya ya da cihazların kullanımdan kaldırılması durumunda, içerdikleri verilerin gizlilik derecesine uygun olarak güvenli bir şekilde imha edilmesi sağlanır.

(2) Veri gizliliğini sağlamada kullanılacak şifreleme teknikleri için güncel durum itibarıyla güvenilirliğini yitirmemiş ve günün teknolojisine uygun algoritmalar kullanılır. Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanılacağı zaman zarfında kırılmayacak şekilde uzun seçilir ve ilgili veri ya da operasyonun kritiklik seviyesine göre bu anahtarların geçerlilik süresi belirlenir. Geçerlilik süresi dolan ya da güvenilirliğini yitirdiği tespit edilen şifreleme anahtarlarının kullanımı derhal engellenir. Şifreleme anahtarlarının yaşam döngüsü boyunca güvenliğinin sağlanması, güvenli bir şekilde oluşturulması, müşteri ve personel kullanımına sunulması ve saklanması esastır.

(3) Hassas verilerin farklı güvenlik seviyesine sahip ortamlar arasında iletiminde uçtan uca güvenli iletişimin kullanılması ve bu verilerin şifrelenmiş bir şekilde saklanması esastır. Bankanın personeline tahsis ettiği hassas veya sır kapsamındaki veri içeren masaüstü, dizüstü ve mobil cihazların içeriğinin şifrelenmesi sağlanır ve ağa bağlı sunucu cihazlar üzerinde açık metin halinde hassas verilerin bulunup bulunmadığını belirlemek için sunucu makineleri taranır.

### **Verilerin paylaşılması**

**MADDE 10** – (1) Banka, müşterinin kendisinden gelen ve yazılı şekilde ya da kalıcı veri saklayıcısı yoluyla kanıtlanabilir nitelikte olan bir müşteri talebi olmaksızın, faaliyetlerinin ifası sırasında ve her türlü dış hizmet alımlarında bilgi sistemleri aracılığıyla edindiği, sakladığı veya işlediği müşteri sırrı niteliğindeki bilgileri, Kanunda yer alan istisnai haller haricinde yurtiçindeki ve yurtdışındaki üçüncü kişilerle paylaşamaz ve bunlara aktaramaz.

(2) Müşterinin, bilgilerini paylaşmaya dair açık rıza göstermesi verilecek hizmet için bir ön şart haline getirilemez.

### **Kimlik ve erişim yönetimi**

**MADDE 11** – (1) Banka, bilgi varlıklarına olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş ve kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrolleri uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesini sağlamakla yükümlüdür. Banka, süreçler ve sistemler üzerinde kullanıcılarına sağlayacağı yetkilerin, kullanıcılara görev ve sorumluluklarına uygun roller ve/veya profiller aracılığı ile temin edilmesini

sağlar ve kullanıcıların görev tanımlarına uygun uygulama ve sistemler üzerindeki rolleri dokümente eder.

(2) Bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek süreci kapsayacak şekilde tesis edilir ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alınır.

(3) Banka, bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgilerinin güvenliğine yönelik; kimlik doğrulama bilgilerinin veritabanlarında şifreli olarak veya matematiksel olarak geriye dönüştürülmesi mümkün olmayan yöntemlerle muhafaza edilmesi, kimlik doğrulama amacıyla aktarılırken şifrelenmesi, yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunması, bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtlarının tutulması ve bu iz kayıtlarının güvenliğinin sağlanması gibi önlemler alır.

(4) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasının aşağıdaki fonksiyonları yerine getirmesi sağlanır:

a) Başarısız kimlik doğrulama teşebbüslerinin belirli bir sayıyı aşması halinde ilgili kullanıcının erişimini engellemesi,

b) Başarısız kimlik doğrulama teşebbüsleri sonrasında, bu teşebbüsü gerçekleştiren kişiye, hatalı girilen kullanıcı adı bilgisi veya parola ile ilgili, böyle bir kullanıcı adının sistemde olmadığı veya parolanın hatalı girildiği bilgisini vermemesi,

c) Hiçbir işlem yapılmayan hareketsiz oturumlar için oturumu belirli bir süre sonra sonlandırması veya kilitlemesi,

ç) Birden fazla kullanıcının aynı kullanıcı hesabını kullanabilmesi ya da bir kullanıcının aynı anda farklı oturumlar açabilmesi konusunda bilgi güvenliği sorumlusunun onay verdiği durumlar hariç olmak üzere, aynı kullanıcı için aynı anda birden fazla oturum açılmaya çalışılması durumunda buna izin vermemesi ve kullanıcıya uyarı vermesi.

(5) Kullanıcılara uygulanacak erişim kontrolleri ve atanacak yetkilerin belirlenmesinde görevler ayrılığı prensibi esas alınır. Süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir. Banka, görevler ayrılığı prensibinin uygulanmasına yönelik bankacılık ve BS süreçlerinde uygulanacak erişim kontrollerini ve atanacak yetkileri net olarak belirler ve dokümente eder. Erişim yetkilerinin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması sağlanır. Görevlerin tam manasıyla ve uygun şekilde ayrıştırılmasının mümkün olmadığı durumlarda, bu durumdan kaynaklanabilecek hata ve suistimalleri önlemeye yönelik risk azaltıcı veya telafi edici ilave kontroller tesis edilir.

(6) Kullanıcılar, geçerli bir iş ihtiyacının mevcut olduğu ve erişimin gerekli olduğu süre zarfında, bilgi varlıklarına erişebilmeleri için yetkilendirilir. Bilgi varlıklarına erişim yetkisi olan kullanıcılar, ilgili bilgi varlığı sahibi tarafından yılda en az bir defa gözden geçirilir. Kullanıcıların görev ve sorumlulukları göz önünde bulundurularak sadece bu görevleri yerine getirmelerine yetecek ve sadece bilmeleri gereken verilere erişmelerini sağlayacak kadar yetkiye sahip olmaları sağlanır.

(7) Ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile ilgili asgari olarak aşağıdaki tedbirlerin alınması sağlanır:

a) Kimlik doğrulamayla birlikte ek güvenlik kontrollerinin uygulanması,

b) Ayrıcalıklı yetkilerin yalnızca gerekli olan kullanıcılara atanması ve sadece gerekli olan durumlarda bu tür hesapların kullanılması,

c) Bu tür hesaplar ile gerçekleştirilen işlemleri takip edecek şekilde iz kayıtlarının tutulması ve bunların düzenli olarak gözden geçirilmesi,

ç) Hesap oluşturulması veya silinmesi gibi işlemler için iz kaydı tutulması ve uyarı üretilmesi,

d) Yapılan başarısız giriş denemeleri için iz kaydı tutulması ve uyarı üretilmesi,

e) Hesapların ortaklaşa kullanılmasının engellenmesi veya bu hesapları kullanan gerçek kişilere sorumluluk atayacak tekniklerin kullanılması,

f) Parolaların güvenli ortamlarda saklanması ve bu parolaların belirli periyotlarda değiştirilmesini sağlayacak konfigürasyonların yapılması,

g) Parolaların tahmin edilmesi zor ve günün teknolojisine uygun uzunluk ve zorlukta olacak şekilde sıklıkla değiştirilmesi,

ğ) Sistemsel sebeplerle uygulama hesaplarına yönelik iz kayıtlarının oluşturulamaması veya takip edilememesi durumunda bu hesapların son kullanıcı tarafından kullanımının engellenmesi.

(8) Acil durumlara özgü yetkilendirmeler geçici olarak yapılır ve bu yetkilendirme süresince gerçekleştirilecek işlemlerin takibine imkân verecek iz kayıtlarının tutulması sağlanır.

(9) Personelin işten ayrılması ve görev değişikliği gibi insan kaynaklarında yaşanan değişiklikler sonrasında, gecikmeksizin ilgili kullanıcı hesaplarının silinmesi, askıya alınması, kullanıcıya atanmış yetkilerin geri alınması ya da değiştirilmesi gibi işlemler yerine getirilir. İnsan kaynakları değişikliklerine dayanan yetkilendirme işlemleri otomatik olarak gerçekleştirilmiyorsa, manuel değişiklik gerçekleştirme sürecinde görevler ayrılığı prensibi uygulanır ve değişikliği gerçekleştirmeye yetkili personelin faaliyetlerine ilişkin iz kayıtları ile insan kaynaklarındaki değişikliklerin uyumlu olup olmadığı düzenli olarak gözden geçirilir.

(10) Bilgi sistemleri üzerindeki kullanıcılar için benzersiz kullanıcı tanımlama kodları belirlenir ve zorunlu olmadığı müddetçe ortak veya ön tanımlı kullanıcı hesapları kullanılmaz. Ortak veya ön tanımlı kullanıcı hesaplarının kullanımının zorunlu olduğu durumlarda ise bu kullanıcı hesapları ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edilir.

(11) Kullanıcı parolalarının yönetiminde asgari olarak aşağıdaki tedbirlerin alınması sağlanır:

a) Sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesinin sağlanması,

b) Kullanıcıların, parolalarını belirlerken tahmin edilmesi zor, günün teknolojisine uygun uzunlukta ve zorlukta parola seçimine zorlanması,

c) Kullanıcıların, düzenli aralıklarla ve sistem güvenliği ile ilgili bir kuşku oluşması halinde parolalarını değiştirmeye zorlanması,

ç) Kullanıcıların eski parolalarının hatırlanması suretiyle geriye dönük olarak belirli sayıda eski parolanın kullanılmasının engellenmesi.

(12) Banka, kullanıcı hesaplarına yönelik olarak kilitli hesaplar, devre dışı bırakılmış hesaplar, parola geçerlilik süresini aşan hesaplar ve parola son kullanma süresi hiçbir zaman dolmayacak şekilde ayarlanmış hesaplar için otomatik olarak rapor üreten yöntemler kullanır ve bu raporları gerekli önlemleri alması için ilgili sistem yöneticisine iletir.

(13) Zorunlu bir iş gereksinimi olmadıkça ve bilgi güvenliği sorumlusu tarafından onaylanmadıkça banka personelinin ya da dış hizmet sağlayıcıların yerel yönetici haklarına sahip olması engellenir.

(14) Banka, her kullanıcının normal günlük kullanım ve erişim süresini belirleyerek tipik hesap kullanım profilleri oluşturur. Bu kullanım profilleri, olağandışı saatlerde giriş yapmış, normal giriş sürelerini aşmış ya da genel olarak çalıştığı bilgisayar dışındaki bir bilgisayardan işlem gerçekleştirmiş olan kullanıcıların raporlanarak olağandışı durumların tespit edilmesinde veya uzun süredir hiç bir aktivite göstermeyen pasif hesapların tespit edilip bu tür hesaplar için gerekli bir iş ihtiyacı kalmamış ise bunların kullanımının engellenmesinde kullanılır.

### **Bütünlük kontrolleri**

**MADDE 12** - (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. Dış hizmet sağlayıcılar 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 olmamasını gerektirir.

### **İz kayıtlarının oluşturulması ve takibi**

**MADDE 13** - (1) Banka, bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığıyla orantılı olacak şekilde bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması tesis eder. İz kayıtları, işlemin doğasına uygun detay ve içerikte, asgari olarak aşağıdaki bilgileri barındırır:

a) Kaydı oluşturan sistem,

b) Kaydın oluşturulduğu tarih, saat ve zaman dilimi bilgisi,  
c) Kaydı oluşturan işlem ya da olayla birlikte, gerçekleştirilen değişikliğin ne olduğunu gösteren bilgi,

ç) Kaydın ilişkili olduğu tekil kullanıcıyı veya sistemi gösteren bilgi.

(2) Tesis edilecek iz kayıt mekanizmasının, yaşanan bilgi güvenliği olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte olması sağlanır.

(3) Bilgi sistemleri dâhilinde gerçekleşen ve bankacılık faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemler ile hassas ya da sır kapsamındaki verilere erişilmesine veya bunların sorgulanmasına, görüntülenmesine, kopyalanmasına, değiştirilmesine yönelik işlemler ve kritik bilgi varlıklarına yönelik erişim yetkilerinin verilmesine, değiştirilmesine ve geri alınmasına yönelik aktiviteler ile bu varlıklara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları asgari beş yıl boyunca banka nezdinde saklanır.

(4) Bankanın, web servisleri, API ya da benzeri metotlarla diğer kurum veya kuruluşlar nezdinde tutulan verilere ilişkin yaptığı sorgulamalar ve bu sorgulamaları hangi amaçla yaptığına ilişkin iz kayıtları beş yıl boyunca banka nezdinde saklanır ve bu tür sorgulamalara ilişkin iz kayıtları en geç aylık periyotlarla raporlanarak yetkisiz ya da amaç dışı sorgulama yapıp yapılmadığına dair inceleme yapılır ve bu incelemeden elde edilen sonuçların gerekleri yerine getirilir.

(5) İz kayıtları güvenilir ortamlarda yedeklenir ve ihtiyaç duyulması halinde makul bir sürede bu yedeklerden geri dönüş sağlanarak inceleme yapılmasına imkân verecek şekilde banka nezdinde saklanır.

(6) İz kayıtlarının bütünlüğünün bozulmasının önlenmesine ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin teknikler kullanılır. İz kayıtlarına, bilmesi gerektiği kadar prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabilmesi ve kayıt sisteminin her türlü yetkisiz değişiklik ve müdahalelere karşı korunması sağlanır. Kullanıcıların kendi faaliyetlerine ilişkin iz kayıtlarına müdahalesi engellenir ve iz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(7) Banka, iz kayıt sisteminin önceden belirlenmiş ve belirli periyotlarla güncellenen senaryolar çerçevesinde düzenli olarak gözden geçirilmesine, takip edilmesine ve olağan dışı durumlar ile riskli işlemlerin raporlanmasına ilişkin süreçleri tesis eder. Olağan dışı durumlar ile riskli işlemlere yönelik rapor üretilmesi ve rapor sonuçlarının banka denetim birimlerince takip edilmesi sağlanır.

(8) Banka, dış hizmet sağlayıcıları tarafından tutulan iz kayıtlarının kendi standartlarına uygunluğunu ve bu iz kayıtlarının kendisi tarafından erişilebilir olmasını temin eder.

### **Ağ güvenliği**

**MADDE 14 -** (1) Banka, gerek kendi kurumsal ağı gerek dış ağlardan gelebilecek tehditler için gerekli ağ güvenlik kontrol sistemlerini tesis eder. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır.

(2) Banka, dış ağı ve iç ağı arasındaki trafiği kontrol altında tutmak için gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıları tespit edebilecek ve önleyebilecek günün teknolojisine uygun sistemler kullanır.

(3) İç ağdan gelebilecek tehditlerin etkisini azaltmak ve banka iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere banka iç ağındaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşmasını sağlayacak şekilde banka iç ağı alt bölümlere ayrılır. Farklı ağ segmentleri arasındaki veri trafiğinin güvenliği sağlanır. İç ağı sadece yetkilendirilmiş cihazların bağlanabilmesi sağlanır.

(4) Hassas veya sır kapsamındaki verilere sahip sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanır. Özel iç ağdaki sistemlerle yalnızca vekil uygulamalar veya güvenlik duvarı cihazları üzerinden iletişim kurulur.

(5) Ağ üzerinde kimlik ve erişim yönetimine yönelik kurulan etki alanı yönetimi sunucuları gibi yapıların bankaya özgü oluşturulmuş olması ve banka dışındaki başka bir etki alanı ya da benzerinin parçası olmaması esastır.

(6) Kritik ağ segmentlerine yapılan bağlantılar düzenli olarak tespit edilerek bu bağlantıların her biri için gereksinim değerlendirmesi yapılır ve gereksiz bağlantıların sonlandırılması sağlanır.

(7) Bilgi güvenliği sorumlusu tarafından onaylanmadıkça banka personeli ya da dış hizmet sağlayıcıları tarafından banka içi uygulama ve sistemlere, banka dışından uzaktan erişim gerçekleştirilmez. Uzaktan erişimin gerçekleştiği hallerde ise çok bileşenli kimlik doğrulamaya dayanan güvenli bağlantı yöntemleri uygulanır, erişimlere ilişkin iz kayıtları tutulur, bağlantının süresi ve bağlantının yapılabileceği cihazlar kısıtlanır ve kullanıcı belli aralıklarla kimliğini tekrar doğrulamaya zorlanır.

(8) İnternet üzerinden veya banka dış ağından görünür olan sunucu ve sistemler, görünür olmalarını gerektirecek geçerli bir iş ihtiyacı olup olmadığının tespit edilmesi amacıyla düzenli olarak kontrol edilir ve eğer gerekli değilse bu sunucu ve sistemlerin banka iç ağına taşınması ve iç ağ IP adreslerine sahip olması sağlanır.

(9) Banka, iç ağından dış ağa akan trafik içeriğini kontrol eder. Yapılacak içerik kontrolünün, zararlı IP adreslerine olan trafik akışını ve hassas veriler ile sır kapsamındaki verilerin sızdırılmasını engelleyecek nitelikte olması ve oturum bilgilerini kayıt altına alarak olağan dışı uzun süreli oturumları tespit edecek ve bunlar için uyarı üretebilecek yetenekte olması sağlanır.

(10) Bankadan gönderilen e-postalar için e-posta sunucularında gönderici kimliğini doğrulayıcı teknikler kullanılır.

### **Güvenlik konfigürasyonu yönetimi**

**MADDE 15** – (1) Banka; masaüstü, dizüstü, mobil cihazlar ve sunucuları üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi ağ cihazları için sıkılaştırılmış ve test edilmiş güvenli standart konfigürasyon bilgilerini oluşturur. Bu standart konfigürasyon bilgileri, standart konfigürasyondan sapmalar veya standart konfigürasyondaki güncellemeler değişiklik yönetiminin bir parçası olarak kayıt altına alınır ve onay mekanizmasına tabi tutulur. Güvenli standart konfigürasyon dışında kalacak her türlü değişiklik isteği için bu değişikliği gerektiren iş gereksinimi ve bu iş gereksinimine ihtiyaç duyan iş sorumlusunun kim olduğu ve gereksinim süresi gibi bilgiler de kayıt altına alınır.

(2) Birinci fıkradaki kontrollere ek olarak, banka kullanmakta olduğu veya ihtiyaç duyabileceği uygulamalar için bir beyaz liste uygular. Böylelikle yalnızca ihtiyaç duyulan uygulamaların sistemlerde yüklü olması ve bu beyaz liste dışındaki herhangi bir uygulamanın sistemlere yüklenmesinin veya çalıştırılmasının engellenmesi sağlanır. Banka aynı zamanda, sistemleri üzerinde beyaz listede yer almayan herhangi bir uygulamanın yüklü olup olmadığına yönelik düzenli olarak tarama gerçekleştirir. Beyaz listedeki uygulamaların çalıştırılabilir dosyalarının veya bunların kullandığı kütüphane dosyalarının zararlı yazılımlar yoluyla değiştirilip değiştirilmediği, dosya bütünlük kontrol araçları kullanılarak kontrol edilir.

(3) Banka; masaüstü, dizüstü, mobil cihazlar ve sunucular üzerindeki işletim sistemleri için bu işletim sistemlerinin tipi, versiyon numarası, yama seviyesi ve üzerinde yüklü olan veritabanları ve uygulamaların listesini gösterecek şekilde bir yazılım envanteri tutar. Kullanılacak yazılım envanterinin aynı zamanda donanım envanteri ile de entegre olması ve tek bir noktadan hangi donanım üzerinde hangi yazılımların olduğu bilgisinin takip edilebilir olması sağlanır.

(4) Bankanın masaüstü ve dizüstü makineleri ile sunucuları, bu makinelere taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılır ve zararlı yazılım engelleme araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanır. Bunun yanında bu tür harici cihazların makinelere bağlanacağı bağlantı arayüzlerinin ön tanımlı olarak kullanıma kapatılarak bu tür cihazların kullanımının yalnızca iş gereksinimi olan kullanıcılarla sınırlı tutulması ve harici cihazları kullanma denemesi yapılan durumların da takip edilmesi sağlanır.

(5) Ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alınarak önemli sunucu ve sistemler için düzenli olarak port taraması gerçekleştirilir ve güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portların kapatılması sağlanır.

### **Güvenlik açıkları ve yama yönetimi**

**MADDE 16** – (1) Bankacılık faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak için sistem, yazılım ve cihazlardaki güvenlik

açıklarını hızlı ve etkin bir şekilde ele alacak bir güvenlik açıkları ve yama yönetimi süreci tesis edilir. Güvenlik açıkları ve yama yönetimi süreci kapsamında gerçekleştirilen faaliyetler değişiklik yönetiminin bir parçası olarak kayıt altına alınır ve onay mekanizmasına tabi tutulur. Bu süreç kapsamında aşağıdaki faaliyetler yerine getirilir:

a) Uygulanacak yamaların güvenilir bir kaynaktan gelmesini sağlayacak ve bunu doğrulayacak teknikler kullanılması,

b) Banka tarafından kullanılan sistem, yazılım ve cihazlarda yer alan güvenlik açıklarının ve bu açıklara yönelik yamaların tespit edilmesi,

c) Tespit edilen yamaları uygulamanın ya da uygulamamanın etkisinin değerlendirilmesi,

ç) Uygulanacak yamaların uygulama öncesi test edilmesi,

d) Yamaların nasıl uygulanacağına ilişkin metotların tanımlanması,

e) Uygulanan ya da uygulanmamasına karar verilen yamalarla ilgili olarak bilgi güvenliği sorumlusuna düzenli rapor verilmesi,

f) Yamaların yanlış uygulanması ya da uygulanması sırasında sorun çıkması halinde sorunun ne şekilde çözüme kavuşturulacağına dair metotların tanımlanması,

g) Uygulanamayan yamaların gidermeye çalışıldığı güvenlik açıklarına ilişkin riskleri azaltmaya yönelik telafi edici kontrollerin tesis edilmesi.

(2) Sağlayıcı veya üretici desteği biten sistem, yazılım ve cihazlar artık güncellenemediğinde, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmaması ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamaması halinde sistem, yazılım ve cihazlar kullanımdan kaldırılır.

(3) Banka, ağa bağlı olan sistem ve cihazlarına yönelik olarak otomatik güvenlik açığı tarama araçları kullanır. Tespit edilen her bir güvenlik açığıyla ilgili olarak bilgi güvenliği sorumlusuna ve açığın tespit edildiği sistemden sorumlu sistem yöneticisine en kritik güvenlik açıklarını öncelikli olarak listeleyecek şekilde raporlama yapılır.

(4) Banka, masaüstü ve dizüstü makineleri ile sunucularını, sürekli bir şekilde izleyerek üzerindeki zararlı yazılımları tespit etmekle yükümlüdür.

(5) Banka, e-posta sunucusuna gelen ve giden e-postaları tarayarak zararlı yazılım barındıran ya da bankanın iş ihtiyaçları doğrultusunda gereksiz olan eklentiler içeren e-postaları engelleyecek çözümler kullanır.

### **Fiziksel güvenlik kontrolleri**

**MADDE 17** – (1) Kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip veri merkezleri, sistem odaları, ağ ekipman odaları gibi güvenli alanlarda barındırılır. Bu alanlara erişim, sadece erişim yetkisine sahip olması gereken personelle sınırlandırılır, erişim yetkileri düzenli olarak gözden geçirilir ve güncellenir.

(2) Banka, veri merkezlerinin yerlerini seçerken doğal riskleri ve çevresel tehditleri göz önünde bulundurur. Binaların, barındırdıkları bilgi işlem tesislerinin varlığını açık edecek işaretler ve bilgiler bulundurmaması sağlanır.

(3) Banka, veri merkezlerinin çalışmasını olumsuz etkileyebilecek elektrik kesintisi, yangın, duman, sıcaklık, su, toz ve nem gibi çevresel koşulları izleyecek sistem ve sensörler kullanır, bunların bakımlarını düzenli olarak yapar.

(4) Birinci fıkra kapsamında yetkilendirilen personel dışında kalan herhangi bir banka personeli, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimleri onay mekanizmasına tabi tutulur, veri merkezindeki çalışmaları boyunca faaliyetleri yakından izlenir ve mutlaka kendilerine refakat edilir. Veri merkezlerine ve sistem odalarına yapılan erişim talepleri ve onayları ile bu erişimler kapsamında gerçekleştirilen işlemler ve giriş çıkışlar için iz kaydı tutulur. Bu alanlar için kör nokta barındırmayacak ve en az bir yıl süreyle kayıt saklayacak şekilde kamera kayıt sistemleri kullanılır. Kamera kayıt sistemleri tarafından kaydedilen görüntülerin farklı bir konumda yedeklenmesi sağlanır.

### **Siber olay yönetimi, sızma testi ve siber istihbarat paylaşımı**

**MADDE 18** – (1) Banka, siber olaylardan sonra bankacılık faaliyetlerini en az etkileyecek şekilde ve mümkün olan en kısa sürede BS hizmetlerini normal işleyişine döndürmek üzere gerçekleşen siber olayların ele alınmasına ve takibine yönelik siber olay yönetimi ve siber olaylara müdahale süreci oluşturur. Yeterli teknik ve operasyonel becerilere sahip bir Kurumsal SOME kurulması, bu Kurumsal SOME'ye ilişkin güncel iletişim bilgilerinin Kuruma iletilmesi ve siber olayların Kuruma ve ilgili yönetim birimlerine raporlanması sağlanır.

(2) Kurumsal SOME siber olay öncesinde, bilgi işlem varlıkları üzerinde rutin sızma testi çalışması yapmak veya yaptırmakla, kayıt yönetimi sistemi arayüzünden rutin olarak iz kayıtlarını takip etmekle, iz kayıtları arasında anlamlı sonuçlar doğurabilecek korelasyonları kontrol etmekle; siber olay esnasında ise, BS fonksiyonunun yapacağı müdahaleyi yönetmekle ve BS fonksiyonunda görevli ilgili personeli koordine etmekle sorumludur.

(3) Siber olayların önem derecelerine uygun olacak şekilde ele alınmasını sağlamak üzere, siber olayların önemlilik sınıflandırmasına yönelik kriterler yazılı hale getirilir ve gerçekleşen her bir siber olayın bu kriterlere göre belirlenen önem düzeyiyle orantılı olan bir zaman zarfında ele alınması ve çözüme kavuşturulmasına yönelik prosedürler ile müdahale planları oluşturulur. Oluşturulan müdahale planlarında öngörülen senaryolar için, faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci tesis edilir. Müdahale planlarının işlerliği yılda en az bir kez test edilir ve test sonuçları üst yönetime raporlanır.

(4) Müdahale planları kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulma, yetkili birimlere ulaşma, olayın potansiyel boyutunu, etkisini, hasarı ve etkilenen müşterileri tespit etme ve olayı çözüme kavuşturma süreçleri ele alınır.

(5) Banka, yaşanan bir siber olayın büyüerek bir krize dönüşmesi, verilerin sızması ya da ifşası ile sonuçlanması, Bilgi Sistemleri Süreklilik Planının ya da ikincil merkezin devreye alınması gibi hallerde derhal Sektörel SOME'yi bilgilendirir. Hassas verilerin ya da kişisel verilerin sızmasına ya da ifşasına yol açan bir siber olayın yaşanması halinde banka tarafından yapılacak değerlendirme sonrasında müşterilerin bilgilendirilmesi sağlanır.

(6) Banka, BS hizmetlerinde ciddi kesintilere veya bozulmalara yol açan önemli siber olaylar için bir kök neden ve etki analizi yapmak ve benzer olayların tekrarını önlemek için iyileştirici önlemleri almakla ve yapılan çalışmaları Sektörel SOME'ye bildirmekle yükümlüdür.

(7) Banka, bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırır.

(8) Banka, Kurumun belirleyeceği usul ve esaslar çerçevesinde, tespit ettiği ya da haber aldığı yeni siber tehditler, zararlı yazılımlar, siber olaylar ya da bankacılık sektöründe ortaya çıkan yeni dolandırıcılık yöntemleri hakkında bilgilendirmeleri yapmakla ve dolandırıcılıkla mücadelede erken müdahaleyi sağlamak amacıyla 7/24 irtibat kurulabilecek bir irtibat görevlisi atamakla yükümlüdür.

### **Bilgi güvenliği farkındalığını artırma**

**MADDE 19** – (1) Banka genelinde bilgi güvenliği farkındalık seviyesini artırmak için kapsamlı bir bilgi güvenliği farkındalığı eğitim programı oluşturulur. Eğitim programı, bilgi güvenliği politikaları ve standartları ile birlikte, bilgi güvenliği ve verilerin korunması konusundaki bireysel sorumlulukların neler olabileceği ve bilgi varlıklarını korumak için alınması gereken önlemler hakkında bilgi içerir. Bu eğitimler yoluyla bankanın BT kaynaklarına ve sistemlerine erişimi olan herkesin bu kaynakların kullanımı ile ilgili mevzuat ve yönergeler hakkında bilgi sahibi olması sağlanır.

(2) Bilgi güvenliği farkındalığı eğitim programı Bilgi Güvenliği Komitesi tarafından onaylanır ve programın içeriği yılda en az bir defa yeni teknolojiler ve ortaya çıkan yeni riskler dikkate alınarak gözden geçirilir ve güncellenir. Bankanın BT kaynaklarına ve sistemlerine erişimi olan yeni ve mevcut personelin ve ilgili olduğu alanlar doğrultusunda BT kaynaklarına ve sistemlerine erişimi olan dış hizmet sağlayıcıların bu eğitimlerden geçmesi veya eğitimi aldıklarını belgelendirmeleri ve eğitim programı güncellendikçe ilgili kişilerin güncellenen kısımlarla ilgili tekrar eğitim alması sağlanır.

(3) Banka, bilgi güvenliği farkındalığını artırmak üzere eğitim programının haricinde kurum içi bültenler hazırlar, varsa banka iç portalında bilgi güvenliği ile ilgili bir bölüm oluşturur, çalışanlarına periyodik olarak bilgi güvenliğiyle ilgili hatırlatma mesajları gönderir, çalışanlara yönelik düzenli olarak bilgi güvenliği farkındalığını ölçecek anketler yapar.

(4) Banka bu madde kapsamındaki farkındalık artırıcı çalışmaların etkinliğini doğrulamak ve

geliştirilmesi gereken eksiklikleri tespit etmek amacıyla gerekli çalışmaları yapar. Güncel saldırı yöntemlerini dikkate alarak gerekli sosyal mühendislik senaryoları üzerinden çalışanlara yönelik periyodik testler gerçekleştirir ve bu testlerden geçemeyen çalışanlara yönelik ilave hedefli eğitimler verilmesini sağlar.

## **DÖRDÜNCÜ BÖLÜM**

### **Sistem Geliştirme ve Değişiklik Yönetimi**

#### **Bilgi mimarisinin tanımlanması**

**MADDE 20** – (1) Banka, bilgi sistemleri yoluyla işlenecek ve saklanacak verilerin bütünlüğünü ve tutarlılığını sağlayacak, veri tekrarını en aza indirecek bir kurumsal bilgi mimarisi modelini esas alır.

(2) Banka, bilgi mimarisi modelinin bir parçası olarak veri söz dizimi kurallarını belirler ve bu söz dizimi kuralları doğrultusunda verilerin uyması gereken standart yapıları tarif eden veri sözlüğünü oluşturarak yazılım geliştirme ve veritabanları yönetimi süreçlerinde bu veri sözlüğünün kullanılmasını sağlar. 6 ncı madde kapsamında oluşturulan veri envanteri ile bilgi mimarisi modelinin entegre olması sağlanır.

(3) Bilgi mimarisi modeli, veri söz dizimi kuralları ve veri sözlüğünün merkezi olarak takibi ve yönetilmesi için ilgili sorumluluklar atanır, uygulamalarda veya veritabanlarında meydana gelecek mimariyi etkileyen değişiklikler için sorumluların onayı alınır ve değişikliklerin bilgi mimarisi modeline yansıtılarak güncellenmesi sağlanır.

#### **Proje yönetimi**

**MADDE 21** – (1) Banka, yürüteceği BS projelerinin doğru önceliklendirilmesini ve koordinasyonunu sağlamak ve bu projeler yoluyla edinilecek ya da geliştirilecek bilgi sistemlerinin, zamanında ve gerekli işlevsellik düzeyine sahip olacak şekilde teslim edilmesini sağlamak üzere bir proje yönetim süreci uygular. Proje yönetim süreci, projelerin büyüklüklerine, karmaşıklıklarına ve riskliliklerine göre uygun bir yönetim yapısı tesis edilmesini sağlar.

(2) Hangi kapsamdaki işlerin proje olarak sınıflandırılacağına ve bunların önceliklendirilmesine ilişkin somut kriterler tanımlanır ve bu kriterler çerçevesinde proje talepleri ele alınarak projelerin işletilmesi ve gözetimi gerçekleştirilir.

(3) Süreç, asgari olarak proje gereksinimlerinin belirlenmesi, rol ve sorumlulukların belirlenmesi, zaman ve kaynak planlamasının yapılması, proje kapsamında gerçekleştirilecek faaliyet detaylarının tanımlanması, proje aşamalarının ve çıktılarının tanımlanması, anahtar bağımlılıkların belirlenmesi, kalite temin, risk değerlendirmesi ve onay adımlarını içerir.

(4) Proje gereksinimlerinin belirlenmesi adımı, gereksinimlere detaylı olarak yer verilen bir analiz dokümanı hazırlanır. Bu analiz dokümanında, proje yaşam döngüsü boyunca yasal gereksinimler, kimlik doğrulama, yetkilendirme, erişim kontrolleri, onay mekanizmaları, şifreleme, iz kaydı gibi güvenlik ve gizlilik gereksinimleri, beklenen kullanım yoğunluğu ve kullanıcı sayısı gibi performans gereksinimleri ile hizmet seviyeleri ve yedekleme düzeni gibi erişilebilirlik gereksinimlerinin neler olabileceği belirlenir.

(5) Banka, BS projeleri için proje planı hazırlar ve proje planlarında, projenin her aşamasında gerçekleştirilecek çıktılar ve ulaşılması gereken kilometre taşları açıkça belirtilir. Proje planlarında belirtilen kilometre taşlarına ulaşılmasını ve teslimin zamanında gerçekleştirilmesini sağlamak ve proje risklerini yönetmek üzere, banka proje ilerleyişini takip eder ve gerektiğinde BS Yönlendirme Komitesine, projelerin gidişatı ve karşılaşılan sorunlara ilişkin bilgilendirme yapılmasını sağlar.

#### **Sistem geliştirme, taşıma ve kurulum**

**MADDE 22** – (1) Banka, yazılım geliştirme sürecinde görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlar. Sistem ve uygulamaların geliştirilme süreci, kaynak kodlarının tek bir kişi tarafından hazırlanıp derlenerek geliştirme, test ve üretim ortamları arasında taşınmasına imkân vermeyecek şekilde görevler ayrılığı prensibine uygun olarak işletilir.

(2) Yalnızca geçerli bir iş ihtiyacı ve zorunluluk halinde ve sadece onay mekanizmasından geçmek suretiyle, yazılım geliştirmeden sorumlu personelin üretim ortamına erişimine izin verilebilir. Böyle durumlarda dahi personelin üretim ortamında gerçekleştirdiği işlemler takip edilir ve kayıt altına alınır.

Banka üretim ortamına erişimde kullanılan yöntemleri kayıt altına alarak yazılı hale getirir ve üst düzey yöneticilerce onaylanmasını sağlar.

(3) Bankanın yazılım geliştirme sürecinde bulunan aşamalar ve bu aşamalara ilişkin geçiş koşulları, dokümantasyon gereksinimleri, kodlama standartları ve iş birimleri ile diğer paydaşların hangi aşamalarda sürece dâhil olacağı ve onaylarının alınacağı yazılı olarak belirlenir. Yazılım geliştirme süreci kapsamında, dış hizmet alımları da dâhil olmak üzere bankanın yazılım geliştirme yaşam döngüsüne, mevzuat gereksinimleri ile banka içi politikalara uyumu sağlanır.

(4) Yazılım kalitesini artırmak ve güvenlik açıklarını en aza indirmek amacıyla bilgi güvenliği, yazılım geliştirme yaşam döngüsünde dikkatle ele alınır. Yazılım geliştirme veya tedarik sürecinin başından itibaren, iş gereksinimlerinin ve yazılımdan beklenen fonksiyonel gereksinimlerin neler olduğunun belirlenmesinin yanında, yetkilendirme ve erişim, kimlik doğrulama, veri bütünlüğü, iz kayıtları, istisnai durum yönetimi gibi güvenlikle ilgili gereksinimlerin neler olduğu da belirlenir ve bankanın güvenlik standartlarına, politikalarına ve mevzuat gerekliliklerine ilişkin uyum durumu kontrol edilir.

(5) Banka içinde geliştirilen veya dışarıdan tedarik edilen internete açık uygulamalar, kurulumları yapılmadan önce ve bu uygulamalarda yapılan güncellemeler sonrası düzenli olarak yinelenen bir temelde, güvenlik açıkları bakımından taranır.

(6) Alınan hizmetin kritikliği, riskliliği ve tedarikçinin iş dışı kalması olasılığı dikkate alınarak yazılımı dış bir firma tarafından geliştirilen ve kaynak kodu tedarik edilemeyen uygulamalar için üçüncü tarafların da katılımıyla bir yazılım saklama sözleşmesi yapılır. Ürün güncellemelerinin ve program düzeltmelerinin de saklama sözleşmesi kapsamında yer alması sağlanır.

(7) Banka, yazılım geliştirme personelinin, kullandıkları yazılım geliştirme ortamları özelinde güvenli kod geliştirme eğitimlerini almasını sağlar.

(8) Bankanın yazılım geliştirme sürecinde yapılan yeni veri tanımları ya da veri tanımlarında yapılan değişikliklerin bilgi mimarisi ile veri sözlüğü açısından tutarlılığı değerlendirilerek gerekli güncellemelerin yapılması sağlanır.

(9) Yazılım kodlarının geliştirme, test ve üretim ortamları arasında taşınması esnasında bunların içine yetkilendirilmemiş ya da zararlı kod parçalarının eklenmesini engellemek üzere versiyonlama ve sürüm kontrollerine dayanan bütünlük kontrolleri gerçekleştirilir. Üretim ortamına aktarım sırasında ilgili kullanıcı ya da uygulama sahiplerinin onayları alınır.

(10) Test ortamının işletim sistemi, veritabanı yönetim sistemi, entegre olunan uygulamalar ve sistemler itibarıyla üretim ortamını temsil etmesi ve test verilerinin sayı ve nitelikçe üretim ortamında gerçekleşen operasyonu temsil etmesi ve müşterilere ait üretim ortamı verilerinden arındırılması sağlanır.

### **Uygulama kontrolleri**

**MADDE 23** - (1) Bankada geliştirilen ya da dışarıdan tedarik edilen uygulamalar, ilgili oldukları bankacılık faaliyetlerini ve iş süreçlerini banka içi politikalara ve mevzuat gereksinimlerine uygun olarak yürütmek ve bu uygulamalara girilen, bu uygulamalar tarafından değiştirilen, işlenen veya üretilen verilerin doğruluğunu, tamlığını, güvenilirliğini sağlamak üzere sistemsel veya manuel kontroller barındırır. Bu kontroller, uygulamaya girdi teşkil edecek verilerin tanımlanması; türü, tipi, formatı ve büyüklüğünün kontrol edilmesi; kaynağının doğrulanması; uygulamanın işlediği verilerin bütünlük ve güvenilirliğinin sağlanması; verilere erişimin görevler ayrılığı prensibine uygun olarak yetkilendirilmesi; gerekli olduğu durumlarda girişçi-onaycı yapısının tesis edilmesi; uygulamanın çıktısı olan verilerin gizliliğinin, bütünlüğünün, mutabakatının ve sadece gerekli taraflara dağıtımının sağlanması gibi fonksiyonları yerine getirir. Banka, uygulama kontrollerinin mümkün mertebe sistemsel kontroller olmasına ve manuel yordamlarla yürütülmemesine dikkat eder, uygulamaların kurulumundan önce banka içi politikalara ve mevzuat gereksinimlerine uyduklarından emin olmak için barındırdıkları kontrolleri test eder ve test sonuçlarını kayıt altına alır.

### **Değişiklik yönetimi**

**MADDE 24** - (1) Banka, meydana gelen değişiklikler sebebiyle gerçekleşebilecek hata ve sorunların sayısını ve etkisini en aza indiren, değişikliklerin etkili, hızlı ve kontrollü bir şekilde gerçekleştirilmesini ve değişiklikler sırasında yapılan işlemlerin değişiklik sonrasında da denetlenebilir olmasını sağlayacak etkin bir değişiklik yönetimi süreci tesis eder. Ağ altyapısı, donanım, işletim

sistemleri, yazılım gibi bilgi sistemleri öğeleri ile sistem, servis, uygulama konfigürasyonu ve parametrelerinde yapılacak her türlü değişikliğin değişiklik yönetimi süreci çerçevesinde başlatılması, değişiklik talebinin geçerli bir iş ihtiyacına dayalı olması ve görevler ayrılığı prensibine uygun olarak yetkilendirilmesi, test edilmesi, gerçekleştirilmesi, kaydedilmesi ve dokümantasyonu sağlanır. Değişikliklerin, kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş yetkili kullanıcılar tarafından yapılması, bunlar için yeterli iz kaydı tutulması ve tutulan iz kayıtlarının düzenli olarak gözden geçirilmesi esastır.

(2) Banka, bilgi sistemi yazılım bileşenlerinin ana versiyonunun kaydını tutar ve bilgi sistemi bileşenlerinde meydana gelen değişiklikleri, meydana geldiği sırayla ve değişimin gerçekleştiği tarihle birlikte kaydeder.

(3) Değişiklik yönetimi süreci, asgari olarak talep yönetimi, risk değerlendirmesi, yetkili merci onayı, yapılan değişikliğin uygulanması, test edilmesi ve doğrulanması adımlarını içerir. Bu kapsamda;

a) Değişiklik taleplerinin kayıt altına alınması, sadece yetkili kişilerden gelen değişiklik taleplerinin kabul edilmesi, bunlara ilişkin bir risk ve etki analizi yapılması, gelen taleplerin sınıflandırılması ve önceliklendirilmesi sağlanır.

b) Değişikliklerin bir güvenlik zafiyetine neden olmadığından emin olmak için, kaynak kod incelemesi de dâhil olmak üzere mümkün olduğunca yüksek güvence veren inceleme faaliyetleri gerçekleştirilir.

c) Değişiklikler uygun test planları doğrultusunda test edilir ve değiştirilen modüllerin üretim ortamına aktarılmasından önce kullanıcıların ve ilgili birimlerin onayları alınır.

ç) Değişiklikler ile bağlantılı riskleri en aza indirmek için değişiklik yönetim süreci risk değerlendirmesine bağlı olarak değişiklikten önce, değişiklikten etkilenecek sistem veya uygulamaların yedekleri alınır, üretim ortamına aktarım sırasında veya sonrasında bir sorunla karşılaşıldığında sistem ya da uygulamaların eski bir versiyonuna dönebilmek için bir geri alma planı oluşturulur.

d) Değişiklikler gerçekleştirildikten sonra, operasyonel prosedürler, konfigürasyon bilgileri, uygulama dokümantasyonu, yardım ekranı ve eğitim materyalleri gibi ilgili sistem ve kullanıcı dokümanları ve prosedürlerinde de değişiklikleri yansıtacak gerekli güncellemeler yapılır.

(4) Acil durum değişiklikleri kapsamında değişiklik yönetim süreci içerisinde tanımlanan istisnalar dolayısıyla sürecin normal işleyişinde yer aldığı halde alınamayan onaylar ya da oluşturulamayan belge ve kayıtların, değişiklik sonrasında mümkün olan en kısa sürede tamamlanması sağlanır.

## BEŞİNCİ BÖLÜM

### Bilgi Sistemleri Sürekliliği ve Erişilebilirlik Yönetimi

#### Birincil ve ikincil sistemler

**MADDE 25** – (1) Bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.

(2) Birincil sistemlerin kaçınıcı yedeği olduğuna bakılmaksızın birincil sistemlerin her türlü yedeği ikincil sistemler olarak kabul edilir ve birinci fıkraya hükmüne tabidir.

(3) Bankacılık faaliyetlerinin yürütülmesi veya Kanun ve mevzuatta tanımlanan sorumlulukların yerine getirilmesi amacını taşımayan banka içi mesajlaşma sistemleri, piyasa izleme platformları gibi sistemler birincil sistemler kapsamında değildir. Bankanın kullanmakta olduğu herhangi bir sistem ya da uygulamanın birincil sistemler kapsamına girmemesi için sistem veya uygulama üzerinden herhangi bir iş sürecinin yürütülmemesi, hassas veri ya da sır kapsamına girebilecek verilerin işlenmemesi, iletilmemesi ve saklanmaması gereklidir.

(4) İşlemlerin doğası gereği yurt dışı ile etkileşimin gerekli olduğu ödeme veya mesajlaşma sistemleri gibi bankacılık işlemleri hariç olmak üzere, bankanın yurt dışında kurulu bir sistemden herhangi bir onay sürecine tabi olmaksızın bankacılık işlemlerini gerçekleştirebilmesi ve yurt dışı iletişim ağlarıyla bağlantılarının kesildiği durumlarda dahi yurt içinde kurulu bulunan birincil ve ikincil sistemleri aracılığıyla ülke içerisinde bankacılık faaliyetlerini sunmaya devam edebilmesi esastır.

(5) Birincil veya ikincil sistemler kapsamında olan bir faaliyet için dış hizmet ya da bulut bilişim hizmeti alınması halinde, dış hizmet sağlayıcının sunduğu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de birincil ve ikincil sistemler kapsamında ele alınır ve yurt içinde bulundurulur.

### **BT operasyon yönetimi**

**MADDE 26** – (1) Banka, BS servislerinin tanımlanmış hizmet seviyelerine uygun olarak sunulmasını sağlamak üzere BT altyapısının günlük yönetim ve bakımını yerine getiren bir BT operasyon yönetimi fonksiyonu işletir. BS strateji planındaki hedefler ve iş gereksinimleriyle uyumlu olacak şekilde iş birimlerinin de katılımı ve onayıyla bu servislere ilişkin hizmet seviyeleri tanımlanır.

(2) Banka, BT operasyonel olaylarına derhal müdahale etmek, teknoloji ile ilgili sorunlarda kullanıcılara destek sağlamak, araştırılması ve çözümü için sorunları ilgili BT birimlerine aktarmak, rapor edilen sorunların düzeltilmesine kadar olayların kaydını tutmak, analiz etmek ve takip etmek üzere bir yardım masası fonksiyonu ve problem yönetim sistemi tesis eder.

(3) Banka, bilgi sistemlerinin performansının sürekli olarak izlenmesini ve beklenmedik durumların zamanında raporlanmasını sağlamak için bir performans izleme süreci uygular. Performans izleme süreci, sistem performansını etkilemeden önce sorunların tanımlanmasını ve düzeltilmesini sağlayacak bir erken uyarı fonksiyonu içerir, planlanan iş hedefleri doğrultusunda kapasite planı için ihtiyaç duyulan bilgileri sağlar ve iş yükü tahminlerinin hazırlanmasına yardımcı olur.

(4) Banka, BS strateji planında belirtilen mevcut ve gelecekteki iş gereksinimlerini, tanımlanan hizmet seviyelerine ve iş yükü tahminlerine uygun olarak karşılayabilecek BT kapasitesinin mevcut olmasını sağlamak üzere kapasite yönetimi ve planlaması yapar. Banka, kapasite planının sürekli bir şekilde bakımını ve güncellenmesini sağlar ve BS servislerinin performansını, mutabık kalınan hizmet seviyelerindeki performans hedeflerini karşılayacak veya aşacak şekilde yönetir, kapasite ile ilgili olayların ve problemlerin teşhisi ve çözümünü sağlar.

(5) Banka, ay sonu, resmi tatil sonrası, maaş ödemesi yapılan günler gibi müşterilerin yoğun olarak işlem yaptığı günlerde tekrar eden sistem performansı azalması, kapasitenin yetmemesi, teknik arızalarla karşılaşılması gibi sorunların belirli bir desen takip ettiğini tespit edecek yöntemler kullanmakla ve bu sorunların kök nedenlerini tespit ederek çözüme kavuşturulmasını sağlamakla yükümlüdür.

### **Erişilebilirlik yönetimi ve yedekleme**

**MADDE 27** – (1) Banka, herhangi bir donanım veya yazılım bileşeninin beklediği gibi çalışmadığı durumlarda, sistemin veya bankacılık faaliyetlerinin önemli bir bölümünün çalışamaz hale gelmesini önlemek adına kritik donanım ve sistemler için yedekli çalışma ya da hazırda bekleme düzenleri kurmakla yükümlüdür. Hangi donanım ve sistemlerin kritik olduğu belirlenirken, 28 inci maddede belirtilen BS servisleri ve bunların bağlı olduğu hizmet seviyeleri ile 6 ncı maddede belirtilen bilgi varlıklarının erişilebilirlik gereksinimleri dikkate alınır.

(2) Banka, verilerin erişilebilirliğini sağlamak adına 6 ncı maddede belirtilen her bir verinin erişilebilirlik gereksinimlerine uygun yedekleme düzenini tesis etmekle yükümlüdür. Sistemin alınan yedeğinden geri yüklenebilmesi için, işletim sistemi, uygulama yazılımı ve veriler gibi sistemin çalışmasını sağlayan bileşenler yedekleme prosedürüne dâhil edilir. Yedeklemenin düzgün bir şekilde çalıştığından emin olmak için, geri yükleme işlemleri gerçekleştirilerek yedekleme ortamındaki veriler düzenli olarak test edilir. Yedeklerin taşınırken, uygun şifreleme teknikleri ve fiziksel güvenlik kontrolleri yoluyla korunması sağlanır.

(3) Banka, ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif iletişim kanalları oluşturmakla yükümlüdür.

(4) Banka, hangi sistem, sunucu ve veri yedeklerinin, hangi sıklıkta ve hangi yöntemlerle alındığını ve bu yedeklerin hangi ortam ve konumlarda tutulduğunu, güncel durumu yansıtacak şekilde kayıt altına almakla yükümlüdür.

(5) Banka, soruşturma veya kovuşturma yürüten adli merciler ile Kurumdan gelen veri taleplerini alır almaz bu verilerin bir kopyasını alarak yedeklemekle ya da talep yerine getirilene kadar aslını saklamakla yükümlüdür. Banka verileri, talepte bulunan mercilerin kolaylıkla inceleyebileceği bilinen formatlara dönüştürerek tevdi etmekle veya talepte bulunan mercilere bu verilerle birlikte verilerin incelenmesini mümkün kılan uygulama ve araçları temin etmekle yükümlüdür. Banka, bu fıkra kapsamında kendisine iletilen veri taleplerini geç işleme almasından dolayı mevzuattaki veri saklama sürelerinin geçmiş olduğunu ve bu sebepten verilerin erişilemez olduğunu ileri süremez. Banka bu fıkra kapsamında kendisinden talep edilen verilere ilişkin almış olduğu kopyaları veya ilave yedekleri en az iki yıl süreyle saklar.

### **Bilgi sistemleri sürekliliğinin sağlanması**

**MADDE 28** – (1) Bankacılık faaliyetlerini yürütmede kullanılan BS servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetiminin ve planının bir parçası olan BS süreklilik yönetimi süreci ve Yönetim Kurulu onaylı bir BS süreklilik planı hazırlanır, BS süreklilik yönetimi süreci sorumlusu atanır ve BS Süreklilik Komitesi tesis edilir. BS Süreklilik Komitesi, bankanın insan kaynakları, ilgili iş birimleri, BS güvenlik fonksiyonu, ilgili BS birimlerinin temsilcileri ve organizasyonda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonların temsilcilerinden oluşur ve BS süreklilik yönetimi süreci sorumlusu bu komiteye başkanlık eder. BS Süreklilik Komitesi meydana gelen olaylarla ilgili bütün faktörleri göz önünde bulundurarak kriz durumu olduğunu ilan etmekle, BS planın devreye alınmasına karar vermekle ve diğer kurtarma, süreklilik ve müdahale ekipleriyle koordinasyonu sağlamakla yükümlüdür.

(2) BS süreklilik yönetimi sürecinin ulusal veya uluslararası standartları ya da en iyi uygulamaları referans alması esastır. Bu süreç kapsamında banka BS süreklilik planıyla ilgili olarak aşağıdaki faaliyetleri yerine getirir:

a) İş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi sistemleri süreklilik yönetim süreci tesis etmek,

b) İş birimlerinin de katılımıyla gerçekleştirilen iş etki analizi ve önceliklendirilen iş hedefleri çerçevesinde planı geliştirmek ve kurtarma için gerekli olan işlemleri belirlemek,

c) Planın uygulanabilir olmasını ve bakımını sağlamak,

ç) Planın müdahale planları, kapasite planı gibi diğer planlarla ve mevzuat gereksinimleriyle uyumlu olmasını sağlamak,

d) Yılda en az bir defa, denetimler ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da BS sürekliliğini etkileyen değişikliklerden sonra planın gözden geçirilerek güncellenmesini sağlamak,

e) Yaşanan acil durum ve felaketlerden kaynaklanan yasal konuları ele almak ve halkla ilişkiler ve basın ile olan iletişimi yürütmek,

f) İlgili ekiplere ve çalışanlara plan kapsamında eğitim verilmesini ve farkındalığın artırılmasını sağlamak.

(3) Planın hazırlanması sürecinde, bilgi varlıklarının ve tutulan verilerin önem düzeyi değerlendirilerek iş etki analizi çerçevesinde her bir BS servisi için kabul edilebilir kesinti süreleri ile kabul edilebilir veri kayıpları belirlenir ve belirlenen bu limitler doğrultusunda servislerin tekrar erişime açılabilmesine imkân tanıyacak kurtarma prosedürleri geliştirilir. Banka, felaket durumunun sona ermesi sonrasında ikincil merkezden birincil merkeze geri dönüşün sağlanmasına yönelik prosedürleri hazırlar.

(4) Plan kapsamında ikincil merkez tesis edilir. Veri ve sistem yedeklerinin ikincil merkezde kullanıma hazır bulundurulması sağlanır. İkincil merkezin coğrafi olarak, deprem, yangın, patlama, sel, su baskını, heyelan, elektrik ve iletişim hattı kesintisi gibi sebeplerden kaynaklanacak zararlar açısından birincil merkez ile aynı risklere maruz olmaması esastır.

(5) Planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan personel, her yıl sorumlulukları ile orantılı bir detay ve içerikte BS sürekliliği eğitimine tabi tutulur ve plan kapsamındaki görev ve sorumlulukları hakkında bilgilendirilir.

(6) Birincil sistemlerin tamamen devre dışı kaldığı felaket senaryolarında dahi bankanın en geç yirmi dört saat içerisinde faaliyetlerini yeniden sürdürebiliyor olması esastır. Planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa gerçek bir felaket senaryosunu sağlamaya ve ikincil merkez üzerinden faaliyetleri sürdürmeye yönelik testler yapılır. Testlere varsa dış hizmet sağlayıcılar da dâhil edilir, test sonuçları üst yönetime raporlanır ve bu sonuçlara göre plan güncellenir. Bu fıkranın uygulanmasına ilişkin ilave usul ve esasları belirlemeye Kurum yetkilidir.

(7) Planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan personelin ve dış hizmet sağlayıcıların iletişim bilgilerinin geçerliliği ve bu kişilerin göreve hazır olarak ulaşılabilir olduğu, iletişim zinciri testleri ile yılda en az iki defa test edilir. İletişim bilgileri ile planın ve ilgili kurtarma veya geri dönüş prosedürlerinin güncel kopyalarının, yalnızca bilmesi gereken kişilerin erişebileceği şekilde sürekli olarak erişime açık tutulması ve gereken konularda kopyalarının bulundurulması sağlanır.

(8) Banka, birincil merkezdeki sistem, sunucu, ağ cihazı ve diğer BT bileşenlerinde yapılan

güncellemelerin, yama yüklemelerinin ve konfigürasyon değişikliklerinin ikincil merkezdeki yedeklerinde de aynı şekilde uygulanmasını sağlar, ikincil merkeze kopyalanan veri ve sistem yedeklerinin birincil merkez ile aynı olduğunu garanti edecek bütünlük kontrollerini gerçekleştirir.

(9) Banka, ikincil merkez kapsamına aldığı BS servisleri, sunucu, sistem, uygulama ve verilerin listesi ile ikincil merkez kapsamına almadığı BS servisleri, sunucu, sistem, uygulama ve verilerin listesini güncel durumu yansıtacak şekilde belgelendirir.

(10) Birincil veya ikincil merkez için dış hizmet alınması ya da başka kuruluşlarla paylaşılan bir veri merkezinde barındırılması halinde, veri merkezlerinin bulunduğu konumda veya bölgesel olarak yaşanacak gerçek bir felaket anında birincil ve ikincil merkezdeki çalışma ortamının ve dış hizmet sağlayıcıların bankaya ayıracağı kaynağın, bankanın iş sürekliliğini sağlamayı garanti edecek nitelikte olması esastır.

## **ALTINCI BÖLÜM**

### **Dış Hizmet Alımı**

#### **Dış hizmet alımı sürecinin yönetimi**

**MADDE 29** – (1) Banka üst yönetimi, dış hizmet olarak alınacak hizmetlerin banka açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve dış hizmet sağlayıcı ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayan yeterli bir gözetim mekanizması tesis eder. Dış hizmet alımı kapsamında;

- a) Alınacak dış hizmetin doğuracağı risklerin tüm yönleriyle değerlendirilmesi,
  - b) Dış hizmet sağlayıcının seçiminde gerekli özenin gösterilmesi,
  - c) Hizmet alınan dış hizmet sağlayıcılar ile bunların hizmet alanları, iletişim bilgileri ve hizmetlerin sonlanma tarihlerinin yazılı hale getirilmesi,
  - ç) Dış hizmet alımına konu edilen hizmetlerin erişilebilirliğinin, performansının, kalitesinin, taahhüt edilen hizmet seviyelerine uyulup uyulmadığının, bu hizmetler kapsamında gerçekleşen güvenlik ihlali olaylarının, dış hizmet sağlayıcının gizlilik, bütünlük ve erişilebilirlik ile ilgili güvenlik kontrollerinin, operasyonel ve finansal durumunun yükümlülüklerini yerine getirmeye uygun olup olmadığının ve sözleşme şartlarına uygunluğunun düzenli aralıklarla takip edilmesi,
  - d) Dış hizmet alımı kapsamındaki sistem ve süreçlerin bankanın kendi risk yönetimi, güvenlik ve müşteri mahremiyeti politikalarına uygun olması,
  - e) Dış hizmet alımı kapsamında banka verilerinin dış hizmet sağlayıcıya aktarılmasının gerekli olduğu durumlarda, dış hizmet sağlayıcının güvenlik konusundaki prensip ve uygulamalarının en az bankanın uyguladığı düzeyde olması için gerekli tedbirlerin alınması,
  - f) Dış hizmet alımı kapsamındaki faaliyetlerin banka bünyesinde gerçekleştirilmesi durumunda hangi denetimlere tabi tutulması öngörülüyorsa, herhangi bir kapsam daraltılmasına gidilmeden dış hizmet sağlayıcının da aynı denetimlere tabi tutulması,
  - g) Dış hizmet alımına ilişkin hususların banka iş süreklilik planı göz önünde bulundurulacak düzenlenmesi ve gerekli önlemlerin alınması,
  - ğ) Dış hizmet alımının, planlananın dışında sonlanması veya kesintiye uğraması durumlarına ilişkin risklerin yönetilmesine uygun bir çıkış stratejisinin belirlenmesi,
  - h) Alınan dış hizmetin alt yüklenicilere devrinin bankanın izin vermesi halinde mümkün olması sağlanır.
- (2) Dış hizmet alımına ilişkin koşul, kapsam ve her türlü diğer tanımlama yazılı sözleşmeye bağlanır. Sözleşme, asgari olarak aşağıdaki hususları içerir;
- a) Hizmet seviyelerine ilişkin tanımlamalar,
  - b) Hizmetin sonlanma koşulları,
  - c) Bankanın iş sürekliliğinin sektöre uğramasını engellemek üzere dış hizmet sağlayıcının alması gereken önlemlere ilişkin hükümler,
  - ç) Bankanın güvenlik politikası dâhilinde hassasiyet arz eden konulara ilişkin gereklilikler ve gerek hizmet sırasında gerek hizmetin sonlanması halinde dış hizmet sağlayıcının banka ve müşterileri hakkında öğrendiği bilgiler hususunda gizliliğe riayet etmesini sağlayacak hükümler,
  - d) Dış hizmet sağlayıcı bünyesinde gerçekleşen güvenlik ihlali veya veri sızıntısı gibi olayların derhal bankaya bildirilmesini sağlayacak hükümler,
  - e) Sözleşmeye konu ürün ve hizmetlerin sahipliği ve fikri mülkiyet haklarına ilişkin hükümler,

f) Sözleşmede dış hizmet sağlayıcı için yükümlülük teşkil eden hükümlerin, alt yüklenici kuruluşlar ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler,

g) Dış hizmet alımının, planlananın dışında sonlanmasından veya kesintiye uğramasından kaynaklanacak risklerin yönetilmesine ilişkin hükümler,

ğ) Alınan hizmetin sonlanması halinde, banka ve müşteri verilerinin uygun bir şekilde bankaya teslim edilmesini ve imha edilmesini sağlayacak hükümler,

h) Bankanın tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde dış hizmet sağlayıcılar için de uygulanmasını sağlayacak hükümler,

ı) Dış hizmet sağlayıcıların, gerçekleştirdikleri faaliyetlere ilişkin olarak Kurumca talep edilen her tür bilgi ve belgeyi zamanında ve doğru olarak vermekle ve bunlara ilişkin her türlü elektronik, manyetik ve benzeri ortamlardaki kayıtları ve bu kayıtlara erişim ve kayıtları okunabilir hale getirmek için gerekli sistem ve şifreleri incelemeye hazır bulundurmakla ve işletmekle yükümlü olduğuna ilişkin hükümler,

i) Banka ile bağımsız denetçisinin, dış hizmet alınan konuyla ilgili olarak dış hizmet sağlayıcıdan her türlü bilgi ve belgeyi talep etme yetkisinin bulunduğuna ilişkin hükümler.

(3) Banka, ikinci fıkrada belirtilen sözleşmede bulunması gereken yükümlülükleri uygulatma imkânının bulunmadığı standart sözleşmeler çerçevesinde yürütülen dış hizmet modelleri ile kritik servis ve hizmetleri edinemez ve kritik iş akışlarını bu tür dış hizmet modelleri yoluyla yürütemez.

(4) Banka, sunmakta olduğu bankacılık hizmetlerine yönelik reklam hizmeti almak istediği arama motoru, sosyal medya platformu gibi sağlayıcıların banka adına verilen sahte reklamları engellemeye yönelik tedbirleri alıp almadığını kontrol eder ve uygun tedbirleri almayan sağlayıcılardan reklam hizmeti alamaz. Banka, reklam hizmeti aldığı arama motoru, sosyal medya platformları gibi sağlayıcılarla yapacağı sözleşmelerde, sahte reklam yayımlanması durumunda, müşteriyi korumak adına, olaya özel gerekli bilgiyi alabileceğine dair hükümleri ekletmek zorundadır. Bankanın bu kapsamda reklam hizmeti almak üzere anlaştığı aracı firmalar ile yapılan sözleşmeler için de bu fıkra hükümleri geçerlidir.

(5) Banka, güvenlik politikasının tanımladığı ilkeler doğrultusunda, dış hizmet alımından kaynaklanan riskleri kontrol altında tutmak üzere gerekli organizasyonel değişiklikleri yapar, idari prosedürleri tanımlar ve dış hizmet sağlayıcıyla ilişkileri yürütecek, yeterli bilgi ve tecrübeye sahip bir sorumlu atar.

(6) Dış hizmet sağlayıcıya verilen erişim hakkı tipleri özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılır, risk değerlendirmesi sonucuna göre ilave kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim tipi, erişilen verinin değeri, dış hizmet sağlayıcı tarafından yürütülmekte olan kontroller ve bu erişimin banka bilgilerinin güvenliği üzerindeki etkileri dikkate alınır.

(7) Banka, dış hizmet alımlarında kendisine ve kullanıcılarına ait gizli bilgilerin güvenliğinin sağlanması için gerekli tedbirleri almakla yükümlüdür. Dış hizmet sağlayıcılara verilecek sisteme erişim, veriye erişim veya veriyi görme yetkisi, işin gerektirdiği bilgiyi kapsayacak şekilde sınırlandırılır. Dış hizmet sağlayıcı tarafından kuruluşa ve kullanıcılarına ait gizli bilgilerin korunmasına yönelik tedbirlerin alınmasını sağlamak bankanın sorumluluğundadır.

(8) Bu Yönetmelik kapsamında belirtilen BS iç kontrol ve iç denetim faaliyetleri dış hizmet alımına konu edilemez ve bankanın kendi personeli tarafından yerine getirilir.

(9) Bankanın bilgi sistemlerinin bir bütün olarak veya kısmen dış hizmet alımına konu edilebilmesi;

a) Bankacılık mevzuatının gerektirdiği bankacılık faaliyet ve yükümlülükleri bakımından bankanın bilgi sistemleri üzerinde yönetim, içerik tasarımı, erişim, kontrol, denetim, güncelleme, bilgi/rapor alma gibi konularla alakalı hususlarda herhangi bir sınırlama olmaksızın karar alma gücünün ve hâkim rolün bankada bulunması,

b) Dış hizmet alımına konu edilen bilgi sistemleri ile ilgili yönetsel tüm detaylara bankanın vâkıf olması,

c) Bankanın veritabanlarına ve verilerine erişim yetkilerinin, kritik bilgi olsun veya olmasın mutlaka bankanın kendi vereceği izinler doğrultusunda gerçekleştirilmesini sağlayacak bir yetkilendirme mekanizması tesis edilmesi ve bankanın kullanmakta olduğu uygulamaların tamamının yetkilendirmesini ve iz kayıtlarının gözden geçirilmesi gibi iç kontrol faaliyetlerini bizzat bankanın kendisinin yapması,

ç) Yazılıma ilişkin fikri mülkiyet hakları saklı olmak üzere, alınan dış hizmet kapsamında oluşan hesap, kayıt ve işlemlere ait her türlü bilgi ve belgenin mülkiyetinin bankaya ait olması şartıyla mümkündür.

(10) Kritik bilgi sistemleri ve güvenlik kapsamında alınacak ürün ve hizmetlerin Türkiye'de üretilmesi veya üreticilerinin ar-ge merkezlerinin Türkiye'de bulunması için azami özen gösterilir ve dış hizmet alımında önemli bir kriter olarak değerlendirilir. Bu tür sağlayıcıların ve üreticilerin Türkiye'de müdahale ekiplerinin bulunması şarttır. Kurum, bankaların kullanacağı güvenlik ürünleri ve diğer BT unsurları hakkında ilave şartlar belirlemeye yetkilidir.

(11) Banka, bir dış hizmet olarak bulut bilişim hizmetlerini kullanabilir. Birincil veya ikincil sistemler için bulut hizmeti tek bir bankaya tahsis edilmiş donanım ve yazılım kaynakları üzerinden özel bulut hizmet modeliyle alınabilir. Bunun yanında, sadece Kurum denetimine tabi kuruluşlara tahsis edilmiş donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal olarak her bankaya özgü ayrı kaynağın atandığı topluluk bulutu hizmet modeliyle dış hizmet alınması Kurul iznine tabidir. Kurul, gerekli gördüğü hallerde topluluk bulutu hizmeti kapsamına dâhil olabilecek kuruluşları değiştirmeye yetkilidir.

## **YEDİNCİ BÖLÜM**

### **Bilgi Sistemleri İç Kontrol ve İç Denetim Faaliyetleri**

#### **Bilgi sistemleri iç kontrol faaliyetleri**

**MADDE 30** – (1) Banka ve bankanın dış hizmet sağlayıcıları nezdindeki BS yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen BS kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğunu kontrol etmek üzere BS iç kontrol fonksiyonu oluşturulur, BS iç kontrol sorumlusu atanır ve BS iç kontrol faaliyetleri bu kişinin sorumluluğunda yürütülür. BS iç kontrol fonksiyonu ilave olarak aşağıdaki faaliyetleri de yerine getirir:

- a) Kontroller sonucunda belirlenen eksikliklerin giderilmesi ve aksiyon alınması amacıyla ilgili birimlere ve üst yönetime bildirimde bulunulması,
- b) Kontroller sonucunda gerekli olduğu anlaşılan süreçsel veya sistemsel iyileştirme önerilerinin ilgili birimlere ve üst yönetime bildirilmesi,
- c) Talep halinde bankanın ürünlerinde ve süreçlerinde planlanan değişiklikler, yenilikler veya banka içi politika, prosedür ve süreç dokümanları hakkında görüş oluşturulması,
- ç) Görev alanına giren kritik süreçlerle ilgili proje ve çalışma gruplarına, kurul ve komitelere katılım sağlanması ve ilgili toplantılarda riski en aza indirmeye yönelik öneriler getirilmesi,
- d) BT yönetimi ve dış hizmet alımından kaynaklı risklerin takibinin sağlanmasına yönelik üst yönetim, denetim komitesi ve iç kontrol birimi yöneticisine periyodik olarak raporlama yapılması,
- e) Bir sonraki yıl yapılacak planlı incelemeleri gösterecek şekilde her yıl BS iç kontrol inceleme planları oluşturulması ve bunların banka denetim komitesinin onayından geçirilmesi.

(2) BS iç kontrol sorumlusunun BS iç kontrol, BS denetimi, BS yönetimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde ya da birkaçında toplamda en az beş yıllık mesleki tecrübesinin bulunması şarttır. BS iç kontrol fonksiyonunda görev alacak personelin de, ilgili alanlarda öğrenim durumları itibarıyla veya aldıkları sertifikalarla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur.

(3) BS iç kontrol faaliyetleri kapsamında yapılan periyodik kontroller kayıt altına alınır ve yapılan kontrollere ilişkin çalışma kanıtları en az üç yıl banka nezdinde saklanır.

#### **Bilgi sistemleri iç denetim faaliyetleri**

**MADDE 31** – (1) Banka ve bankanın dış hizmet sağlayıcıları nezdindeki BS yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen BS kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğu ve bilgi sistemlerine ilişkin iç kontrol ve risk yönetimi faaliyetlerinin etkinliği ve yeterliliği hususunda yönetim kuruluna güvence sağlamak üzere BS iç denetim fonksiyonu oluşturulur, BS iç denetim sorumlusu atanır ve BS iç denetim faaliyetleri bu kişinin sorumluluğunda yürütülür.

(2) BS iç denetim sorumlusunun BS iç kontrol, BS denetimi, BS yönetimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde ya da birkaçında toplamda en az beş yıllık mesleki tecrübesinin bulunması şarttır. BS iç denetim fonksiyonunda görev alacak personelin de, ilgili alanlarda

öğrenim durumları itibarıyla veya aldıkları sertifikalarla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur.

(3) BS iç denetimlerinin kapsamının kritik BS servisleri, süreçleri ve kritik varlıkları içerecek ve bunlara ilişkin güvence verecek derinlikte ve detayda olması esastır. Yıllık olarak denetlenebilir BS alanlarından oluşan bir BS denetim planı oluşturularak banka denetim komitesinin onayından geçirilir.

(4) Bankanın BS iç denetimlerinin sıklığı ve denetim döngülerinin; BS servislerinin, süreçlerinin ve varlıklarının kritikliği ve riski ile orantılı olması sağlanır. Bu Yönetmelikte yer alan hükümlerin tamamının banka tarafından yerine getirildiği konusunda güvence vermek üzere yapılacak BS iç denetimleri için denetim döngüsü iki yılı aşmayacak şekilde belirlenir.

(5) BS iç denetim fonksiyonu tarafından gerçekleştirilecek BS denetimleri için denetim rehberleri ve kontrol listeleri hazırlanarak yazılı hale getirilir ve günün teknolojisine uygun olacak şekilde düzenli olarak gözden geçirilerek güncellenir. Yapılan denetimlere ilişkin çalışma kanıtları en az üç yıl banka nezdinde saklanır.

### **Bulguların takibi ve güvence sağlanması**

**MADDE 32** – (1) Banka denetim komitesi, BS iç kontrol, BS iç denetim ve diğer BS denetim çalışmaları sonucu tespit edilen bulguların ele alınması konusunda yeterli zaman ayırır, bu çalışmalar sonucu tespit edilen kritik konuları bizzat gözden geçirir ve gerekli önlemlerin alınması konusunda üst yönetime rehberlik eder. Banka denetim komitesi üyelerinin kompozisyonu, BS iç kontrol ve BS iç denetim raporlarını ve bulgularını uygun bir şekilde değerlendirebilecek mesleki tecrübeye veya bilgi birikimine sahip olacak şekilde oluşturulur.

(2) Banka, BS iç kontrol, BS iç denetim ve diğer BS denetim çalışmaları sonucu tespit edilen bulguların aksiyon planına bağlanarak takip edilmesini sağlar. Bulguların kapatılmasına yönelik olarak aksiyon planında hedef tamamlanma tarihi atanamayan, aşılın, aşma süresi bir seneden fazla uzatılan veya iptal edilen bulgular denetim komitesine düzenli olarak raporlanır ve bu bulgular denetim komitesinde kritik konular olarak ele alınır.

(3) BS iç kontrol ve iç denetim fonksiyonu, tespit ettiği bulguların giderilmesine yönelik olarak denetlenen ilgili birim tarafından alınabilecek önlemler ve aksiyonlara yönelik önerilerde bulunur ya da denetlenen ilgili birimin bu yönde almayı planladığı aksiyonlar konusunda mutabık kalır. Öneri ve aksiyonların uygulamasının tamamlanması neticesinde kapatılabilir duruma gelen bulgulara ilişkin nihai karar, bulgunun sahibi olan BS iç kontrol ya da BS iç denetim fonksiyonu tarafından incelenmesi neticesinde verilir.

(4) BS iç kontrol ve iç denetim fonksiyonları tarafından gerçekleştirilen çalışmalar sonucunda, bankanın BS kontrollerinin incelenmesi ve bağımsız denetim kuruluşları tarafından gerçekleştirilen çalışmalardan bağımsız olarak bu kontroller hakkında bütün önemli kontrol eksikliklerini ortaya koymak üzere bir değerlendirme yapılması ve bu kapsamda:

a) Bankanın BS kontrollerinde, İSEDES Yönetmeliğinin “İç Kontrol Sistemi” başlıklı İkinci Kısmı ile bu Yönetmelikte belirtilen usul ve esaslar açısından etkinlik, yeterlilik veya uyumluluğa engel teşkil edecek herhangi bir önemli kontrol eksikliğinin bulunmadığı,

b) Finansal tablolarda önemli yanlış beyana sebep olan veya başta finansal veriler olmak üzere banka açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliğini önemli ölçüde etkileyen bir durumun ya da yöneticiler ile iç kontrol sisteminde kritik görevleri bulunan diğer görevlilerin dâhil olduğu bir suistimalin ya da yolsuzluğun bulunmadığı,

c) Tespit edilen bulgular arasında (a) ve (b) bentleri kapsamına giren hususlar varsa, bunların hepsinin banka denetim komitesine ve yönetim kuruluna raporlandığı,

hususlarında güvence sağlanması esastır.

### **Personelin eğitilmesi ve kaynak tahsisi**

**MADDE 33** – (1) BS iç kontrol ve BS iç denetim faaliyetlerinin etkin bir biçimde yerine getirilmesini sağlamak üzere, yeterli nitelik ve sayıda personel istihdam edilmesi ve banka tarafından yeterli kaynağın tahsis edilmesi esastır. BS iç kontrol ve iç denetim fonksiyonlarında görev alacak personelin, yılda en az yirmi saat, üç yılda en az yüz yirmi saat olmak üzere BS iç kontrol, BS denetimi, BS yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarında eğitim almaları, konferans ve seminerlere katılımları sağlanır.

(2) BS iç kontrol ve BS iç denetim faaliyetlerinin karşılıklı iş birliği ve bilgilendirmeye dayalı olarak koordineli bir şekilde yürütülmesi, önemlilik arz eden sistem, süreç ve alanların zamanında ve öncelikli olarak değerlendirilmesini sağlayacak şekilde iç kontrol ve iç denetim faaliyetlerinin planlanması ve bu faaliyetler için gerekli kaynakların sağlanması esastır.

## **ÜÇÜNCÜ KISIM Elektronik Bankacılık Hizmetleri**

### **BİRİNCİ BÖLÜM Ortak Hükümler**

#### **Kimlik doğrulama ve işlem güvenliği**

**MADDE 34** – (1) Bu Yönetmelikte aksi belirtilmedikçe, müşteri bilgilerinin görüntülenmesi gibi finansal sonuç doğurmayan işlemler de dâhil olmak üzere elektronik bankacılık hizmetleri için bankaların müşterilerine birbirinden bağımsız en az iki bileşenden oluşan bir kimlik doğrulama mekanizması uygulaması ve bu bileşenlerin kimlik doğrulama sürecinde kullanılmaları esnasında barındırdıkları kimlik doğrulama verilerinin gizliliğini sağlayacak önlemleri alması esastır. Bu iki bileşen; müşterinin “bildiği”, “sahip olduğu” veya “biyometrik bir karakteristiği olan” unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Bileşenlerin bağımsız olması, bir bileşenin ele geçirilmesinin diğer bileşenin güvenliğini tehlikeye atmamasını ifade eder. Müşterinin sahip olduğu bileşenin müşteriye özgü olması ve taklit edilememesi esastır.

(2) Kimlik doğrulamada T.C. Kimlik Kartının kart PIN'i veya biyometrik veri ile birlikte kullanılması veya elektronik imzanın kullanılması hallerinde birinci fıkranın gerekleri yerine getirilmiş sayılır.

(3) Kurum, elektronik bankacılık dağıtım kanalları üzerinden gerçekleştirilebilen işlemler bazında, birinci fıkranın uygulanmasına ilişkin istisna veya ilave güvenlik önlemleri tanımlamaya veya ilave usul ve esaslar belirlemeye yetkilidir. Birinci fıkraya uygun olmayacak şekilde iki bileşenli kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü bankaya aittir.

(4) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasında kullanılacak bileşenlerin üretim aşamalarından başlayarak kullanıcıya ulaştırılmasına kadar geçen sürecin tamamı boyunca güvenliği sağlanır.

(5) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyen yöntemler barındıracak şekilde müşteri kullanımına sunulur.

(6) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasının, başarısız kimlik doğrulama teşebbüsleri hakkında ilgili kullanıcıya sisteme ilk girdiği anda bilgi vermesi sağlanır. Başarısız teşebbüslerin belirli bir sayıyı aşması halinde müşterinin erişimi için ilave güvenlik önlemleri alınır, başarısız kimlik doğrulama teşebbüslerinin devam etmesi halinde ise ilgili kullanıcının erişimi engellenir.

(7) Banka, mobil bankacılık uygulamasını yükleyerek aktifleştirmiş olan müşterilerine, oturum açma ya da oturumun devamında herhangi bir işlemin doğrulanması için hiçbir şekilde SMS ile OTP ya da doğrulama kodu gönderemez ve bunu bir kimlik doğrulama unsuru olarak kullanamaz. Mobil bankacılık uygulamasının ilk kurulumu, aktifleştirilmesi, yeniden aktifleştirilmesi aşamalarında ya da uygulamanın kullanılamaz olması durumunda SMS ile OTP ya da doğrulama kodu gönderilmesi bu fıkra hükmüne aykırılık teşkil etmez.

(8) Banka, SIM kart değişikliği gerçekleştirmiş veya numara taşıma yoluyla elektronik haberleşme işletmecisini değiştirmiş müşterilerini Türkiye’de yerleşik mobil haberleşme işletmeleriyle

gerekli entegrasyonu sağlayarak SMS OTP göndermeden önce belirler ve ilgili müşterilere, değişiklikler teyit edilmediği müddetçe, değişikliğin yapıldığı tarihten itibaren 90 gün boyunca elektronik bankacılık hizmetleri sunulurken SIM karta dayalı unsur kimlik doğrulama unsuru olarak kullanılamaz. Değişiklikler teyit edilirken iki bileşenli kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü bankaya aittir.

(9) Müşterilere kimlik ya da işlem doğrulama amacıyla kullanılacak tek kullanımlık parolaların, tahmin edilmesi zor olacak şekilde yeterli uzunlukta, rastgele, değişken ve eşsiz olarak üretilmesi ve belirli bir süre için geçerli olması sağlanır.

(10) Müşterinin kimliğini tespit etmeye yarayan ve resmi kimlik belgesi yerine geçen belgeler üzerinde yer alan bilgiler ile anne kızlık soyadı, elektronik bankacılık hizmetlerinin sunulması esnasında hiçbir aşamada kimlik doğrulama amacıyla kullanılamaz. Bankanın kimlik doğrulamada müşterinin bildiği unsur olarak bir güvenlik sorusu kullanmak istemesi durumunda, bu güvenlik sorusunun resmi kimlik belgesi yerine geçen belgeler üzerinde yer alan bilgilerden birine ilişkin olmaması ve cevabının müşterinin kendisi tarafından belirleniyor olması gerekir.

(11) Bir kimlik doğrulama bileşeninin bir müşteri ile ilk defa ilişkilendirilmesi uzaktan gerçekleştirilecekse, ilişkilendirme güvenli yöntemlerle ve birinci fıkraya uygun olarak en az iki bileşenli kimlik doğrulama gerçekleştirilerek yapılır. 23/2/2006 tarih ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu kapsamındaki kartlar ve 20/6/2013 tarih ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamındaki ödeme aracına ait PIN, ilgili elektronik bankacılık dağıtım kanalının aktifleştirilmesinden ve ilk parolanın alınmasından sonra kartın sahip olunan unsur olarak kullanıldığı işlemler hariç olmak üzere birinci fıkrada belirtilen "müşterinin bildiği" kimlik doğrulama unsuru olarak kullanılamaz. Elektronik bankacılık dağıtım kanalının aktifleştirilmesinden ve ilk parolanın alınmasından sonra parolanın unutulmasından veya yanlış girilmesinden dolayı sıfırlanması gereken hallerde, yeni parolanın uzaktan belirlenmesi için birinci fıkraya uygun olarak en az iki bileşenli kimlik doğrulama gerçekleştirilmesi şartıyla yukarıda belirtilen PIN bilgisi müşterinin bildiği unsur olarak kullanılabilir.

(12) Banka elektronik bankacılık dağıtım kanallarından gerçekleştirilebilecek işlemler için müşterilerine, varsayılan ve müşteri tarafından güncellenebilecek erişim kısıtlamaları, günlük işlem limitleri, güvenli alıcılar listesi gibi ilave güvenlik önlemleri sunar. Güvenlik önlemlerinin tanımlanması, güncellenmesi veya değiştirilmesinin birinci fıkraya uygun olan bir kimlik doğrulama sonrasında gerçekleştirilmesi esastır. Banka kendi risk değerlendirmesi çerçevesinde güvenlik önlemlerinde yapılacak değişiklikler için birinci fıkraya ilave güvenlik önlemleri belirleyebilir.

(13) Elektronik bankacılık dağıtım kanallarından sunulmakta olan herhangi bir işlemin tersinin gerçekleştirilmesi mümkün ve orijinal işleme göre eşit ya da daha az riskliyse, banka orijinal işlemin tersi olan bu işlemlerin de aynı elektronik dağıtım kanalından gerçekleştirilmesini sağlar.

(14) Bankanın elektronik bankacılık hizmetlerinde kullanmak üzere müşterilerine sunduğu her türlü yazılım ya da mobil uygulamanın kaynağının, ilgili banka olduğunun doğrulanabiliyor olması sağlanır. Banka bu yazılım ya da mobil uygulamaların, müşteri güvenliğini tehlikeye sokacak herhangi bir kod içermemesini sağlamakla, güvenlik açıklarını giderecek gerekli yamaları ve güncellemeleri müşteri kullanımına sunmakla yükümlüdür.

(15) Banka, akıllı telefonlar gibi birden fazla kimlik doğrulama bileşeninin bankaya iletilmesinde kullanılan mobil cihazlar üzerindeki bankacılık uygulamalarının kullandığı hassas verilerin, aynı mobil cihaz üzerindeki diğer uygulamalar ve çalışmakta olan işlemler tarafından erişilemez olmasını sağlayacak önlemler alır. Banka, söz konusu mobil cihazların kaybolması ya da çalınması halinde bunlar üzerindeki hassas verilerin yetkisiz kişilerce erişilemez olmasını sağlamak ve mobil cihazların ele geçirilmesi, güvenilirliğinin bozulması, işletim sistemi yazılımının kırılması veya değiştirilmesi gibi hallerden kaynaklanacak risklerin azaltılması amacıyla günün teknolojisine uygun kontroller tesis etmekle yükümlüdür.

### **İnkâr edilemezlik ve sorumluluk atama**

**MADDE 35** – (1) Banka, sunmakta olduğu elektronik bankacılık hizmetleri kapsamında gerçekleştirilen işlemlerde hem banka hem de müşteri için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanır. Kullanılan tekniğin oluşturduğu iz kayıtlarının güvenilir delillerin elde edilmesini sağlayacak ve sorumluluk atayacak nitelikte olması sağlanır.

### **İşlemlerin takibi**

**MADDE 36** – (1) Banka, elektronik bankacılık hizmetleri kapsamında gerçekleşen olağan dışı, sahtekârlık amaçlı veya dolandırıcılık riski bulunan işlemleri tespit etmeye ve bunları önlemeye yönelik işlem takip mekanizmaları kurar. İşlem takip mekanizması kapsamında uygun olan durumlarda asgari olarak aşağıdaki risk unsurları takip edilir:

- a) Finansal sonuç doğuran işlemlere yönelik bilinen dolandırıcılık yöntemleri,
- b) Gerçekleştirilen her bir bankacılık işleminin tutarı ve bu tutarlara göre müşterinin konum bilgisi de kullanılarak normal dışı bir ödeme, fon transferi ya da davranış deseni gösterip göstermediği,
- c) Kaybolmuş, çalınmış ya da yetkisiz kişilerce ele geçirilmiş kimlik doğrulama unsurlarının listesi,
- ç) Her bir kimlik doğrulama oturumuna yönelik olarak zararlı yazılımların bulaşmış olabileceğini gösteren belirtiler.

(2) Banka, riskli işlemleri filtreleyerek değerlendirir ve bu filtrelere takılan müşterileri daha yakından takip eder. Riskli işlemlerin gerçekleştirildiğinin tespit edilmesi halinde banka, telefon ya da kısa mesaj gibi uygun yöntemlerle müşterilerin en kısa sürede uyarılmasını sağlar.

### **Müşterilerin bilgilendirilmesi**

**MADDE 37** – (1) Banka tarafından sunulan elektronik bankacılık hizmetlerinden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir. Bankanın elektronik bankacılık hizmetlerine ilişkin risklerin etkisini azaltmaya yönelik benimsediği güvenlik prensipleri ve bu risklerden korunmak için kullanılması gereken yöntemler müşterinin dikkatine sunulur. Bu Yönetmelik kapsamında belirtilen müşterilerin bilgilendirilmesine yönelik her türlü bilgi ve açıklama, bankanın gerek kendi internet sitesinde gerek internet bankacılığı hizmetini verdiği internet sitesinde, müşteri erişimine daima açık tutulur ve erişilen bu sitelerin bankaya ait olduğunu gösterecek teknikler kullanılır. Bilgi ve açıklamaların açık ve anlaşılır olması sağlanır, verildiği internet sitesinde dikkat çekici bir yere yerleştirilir ve ilgili elektronik bankacılık hizmetinden yararlanmaya başlamadan önce müşterilerin en az bir kere okumasını garanti edecek şekilde yönlendirmeler ve sistemsal kısıtlamalar uygulanır. Hizmetlerden yararlanmaya başladıktan sonra müşterilerin dikkatine sunulması gereken önemli güvenlik uyarıları ve duyurular için de müşterilerin bu uyarı ve duyuruları okumasını sağlayacak teknikler kullanılır.

(2) Birinci fıkra kapsamında, banka kendi internet sitesinde veya internet bankacılığı hizmetini verdiği internet sitesinde;

- a) Bankanın kimliği, ticaret unvanı, genel müdürlük adresi, kanuni statüsü, bankanın denetiminden sorumlu olan Bankacılık Düzenleme ve Denetleme Kurumuna ilişkin iletişim bilgilerine,
- b) Elektronik bankacılık hizmetlerinin kullanımının taşıdığı riskler, bu risklerden korunmak için müşterilerin kullanması gereken yöntemler, müşteri farkındalığını artıracak yönlendirici güvenlik kılavuzları ile bu hizmetlerden yararlanacak müşterilerin sorumluluk ve haklarına,
- c) Bankanın sunduğu elektronik bankacılık hizmetlerine, bu hizmetlerin ve bu hizmetler dâhilinde gerçekleştirilebilecek bankacılık işlemlerinin erişime açık olduğu gün ve saatlere ve hizmetlere ilişkin diğer koşullara,
- ç) Elektronik bankacılık hizmetlerinde iki saatten daha uzun süreli bir kesinti öngörülen planlı bakım ve değişikliklerde müşterilerin önceden bilgilendirilmesini sağlayacak duyurulara,
- d) Verilen hizmetlerle ilgili olarak müşterilerin herhangi bir sorunla ya da dolandırıcılık vakasıyla karşılaşması durumunda neler yapması gerektiğine ilişkin yönlendirici bilgilere, yer verilir.

(3) Elektronik bankacılık hizmetlerinden dolayı müşterilerin yaşayabileceği sorunları ve şikâyetlerini iletebileceği ve takip edebileceği mekanizmalar oluşturulur. Oluşturulacak şikâyet birimleri veya çağrı merkezlerinde müşteriyi karşılayacak menülerde ilgili elektronik bankacılık hizmetine ilişkin yaşanan dolandırıcılık vakalarının iletilmesi işleminin ana menüde ve ilk sıralarda müşterinin dikkatine sunulması ve bankaya ulaştırılan bildirimlerin en kısa sürede giderilmesine yönelik gerekli çalışmaların yapılması sağlanır.

(4) Banka tarafından sunulan elektronik bankacılık hizmetlerinde, müşterilerin yanlış işlem yapma ihtimalini en aza indirecek kontrollerin bulunması, müşterilerin başlattıkları işlemlere ilişkin ödemekle yükümlü oldukları her türlü tutar, komisyon ve ücret bilgilerinin işlem anında açıkça müşteri

bilgisine sunulması ve müşterinin bunları onaylaması halinde işlemlerin gerçekleştirilmesi temin edilir.

(5) Banka, müşteri talebi olmadan internet bankacılığı ve mobil bankacılık hizmetini ilgili müşterinin kullanımına açamaz. Müşteri, herhangi bir elektronik bankacılık hizmetine erişimini kapatmışsa veya kapattırmışsa, müşterinin yeni bir talebi olmadan ilgili hizmet kullanıma açılmaz.

(6) Banka, yapacağı pazarlama faaliyetleri, reklâmlar veya yayınlarda, müşterilerine sunmakta olduğu herhangi bir elektronik bankacılık hizmetinin mutlak manada güvenli olduğu veya bu hizmetlerde hiçbir güvenlik riskinin bulunmadığı izlenimini ve bilgisini verecek ifadeler kullanmaktan kaçınır.

(7) Bankanın sunduğu elektronik bankacılık hizmetleri için bu Yönetmelik kapsamında yapılması gereken bilgilendirmelerin, hizmetin verildiği platformdan ya da müşterinin hizmeti alırken kullandığı cihazdan kaynaklanan nedenlerle bilgilendirme olanakları açısından yetersiz kalması durumunda, müşterinin bilgilendirmelere farklı kanallar üzerinden ulaşması için gerekli yönlendirmeler yapılır.

(8) Bankanın elektronik ortamda müşterilerine ileteceği hassas veri veya sır niteliğinde veri içeren her türlü ekstre, dekont, hesap özeti gibi bilgilerin elektronik bankacılık hizmeti sunulan kanallar üzerinden gönderilmesi esastır. Banka, bu gibi bilgilerin sunulmasında elektronik dağıtım kanallarının kullanılması için müşterilerine gerekli yönlendirmeleri yapmakla yükümlüdür.

## **İKİNCİ BÖLÜM** **İnternet Bankacılığı**

### **İnternet bankacılığında kimlik doğrulama ve işlem güvenliği**

**MADDE 38 –** (1) İnternet bankacılığı dağıtım kanalında 34 üncü maddenin birinci fıkrasına göre gerçekleştirilecek kimlik doğrulama işleminin çevrimdışı olarak lokalde değil banka nezdinde çevrimiçi gerçekleşmesi ve müşterinin bildiği unsurun, mobil bankacılık uygulaması ya da internet tarayıcısı tarafından hatırlanarak veya bu unsurun başka lokal kimlik doğrulama yöntemlerine bağlanarak otomatik olarak gönderilmemesi gerekir. Müşterinin bildiği unsurun müşteri tarafından girilmesi zorunlu tutulur ve 34 üncü maddenin ikinci fıkrası hükmü saklı kalmak kaydıyla bu unsur lokalde değil banka nezdinde çevrimiçi doğrulanır.

(2) İnternet bankacılığı dağıtım kanalında kimlik doğrulama işlemi gerçekleştirilirken, müşteri tarafından ilk kimlik doğrulama bileşeni girildikten veya bankaya gönderildikten sonra ve internet bankacılığı oturumu açılmadan önce, müşteri tarafından 34 üncü maddenin birinci fıkrasına göre iki bileşenli bir kimlik doğrulama ile önceden belirlenmiş olan bir karşılama mesajının veya resminin, müşteriye gösterilmesi sağlanır.

(3) İnternet bankacılığı dağıtım kanalında 34 üncü maddenin birinci fıkrasına göre gerçekleştirilecek kimlik doğrulama işlemi için müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanacak şekilde tek kullanımlık bir doğrulama kodu üretilir. Doğrulama kodu aracılığıyla 34 üncü maddenin birinci fıkrasında belirtilen kimlik doğrulama unsurlarından hiçbiri hakkında bilgi edinilememesi, bilinen bir doğrulama kodu ile geçerli başka doğrulama kodlarının türetilmemesi, doğrulama kodlarının taklit edilememesi sağlanır. Finansal sonuç doğuran işlemler için doğrulama kodlarının, işlemi gerçekleştirirken müşterinin onayladığı tutar ve alıcı bilgisine göre spesifik olması, tutar veya fonun aktarılacağı alıcı bilgisindeki herhangi bir değişiklik halinde bu bilgilere göre oluşturulmuş ilgili doğrulama kodunun da geçersiz hale gelmesi temin edilir. Kurumsal internet bankacılığı müşterileri için yığın halinde birden fazla alıcı için toplu işlem gerçekleştirilmesine izin verilen fon transferi gibi işlemlerde, üretilecek doğrulama kodunun ilgili yığın işlem toplam tutarı ve alıcılar için spesifik olması gerekir. Müşteriye atanmış bir şifreleme gizli anahtarı ile doğrulama kodunun imzalanmasının mümkün olmadığı hallerde, 34 üncü maddenin yedinci fıkrası saklı kalmak kaydıyla, SMS yoluyla müşteriye doğrulama kodu iletilebilir.

(4) İnternet bankacılığında müşterinin gerçekleştirdiği finansal sonuç doğuran işlemler için doğrulama kodunun oluşturulması, iletilmesi ve kullanılması da dâhil olmak üzere doğrulama sürecinin her aşamasında, tutar ve alıcı bilgisi gibi müşteriye gösterilen ve onayına sunulan bilgilerin gizliliğini, güvenilirliğini ve bütünlüğünü sağlamaya yönelik ve internet bankacılığı oturumu esnasındaki veri iletişiminin yetkisiz kişilere yönlendirilmesi riskine karşı gerekli önlemlerin alınması sağlanır.

(5) Doğrulama kodunun üretilmesinde hata meydana gelmesi ya da üretilmemesi halinde, kimlik doğrulama teşebbüsünde bulunan kişi tarafından hatanın hangi kimlik doğrulama unsurundan kaynaklandığının anlaşılmasını sağlayacak önlemler alınır.

## ÜÇÜNCÜ BÖLÜM Mobil Bankacılık

### **Mobil bankacılıkta kimlik doğrulama ve işlem güvenliği**

**MADDE 39** – (1) Mobil bankacılık uygulamasına tanımlanan uygulama PIN'inin müşteriye özgü bir şifreleme anahtarına erişmek üzere kullanılması ve bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin banka nezdinde çevrimiçi olarak doğrulanması halinde, 34 üncü maddenin birinci fıkrasında belirtilen iki bileşenli kimlik doğrulama yerine getirilmiş kabul edilir. Benzer şekilde, müşteriye ait bir biyometrik kimlik doğrulama bileşeninin mobil bankacılık uygulamasında kullanılarak müşteriye özgü bir şifreleme anahtarına erişilmesi suretiyle bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin banka nezdinde çevrimiçi olarak doğrulanması halinde, 34 üncü maddenin birinci fıkrasında belirtilen iki bileşenli kimlik doğrulama yerine getirilmiş kabul edilir.

(2) Mobil bankacılık uygulaması kontrolünde olmayıp cihaz üreticisi kontrolünde olan parola, PIN ya da biyometrik veriler, 34 üncü maddenin birinci fıkrasında belirtilen müşterinin bildiği ya da biyometrik karakteristiği olan unsurlar olarak kullanılamaz.

(3) Mobil bankacılık uygulamasının yüklü olduğu cihazın ve/veya mobil bankacılık uygulamasının müşteriye bağlanmış olan, müşterinin sahip olduğu bir kimlik doğrulama unsuru olarak kullanılması şartıyla, müşterinin yalnızca mobil bankacılık uygulaması aracılığıyla müşteri ve hesap bilgilerini görüntülemek istemesi ya da daha önce tanımlanmış güvenli alıcılar listesine para transfer etmek veya ödeme yapmak istemesi halinde ilave bir kimlik doğrulama unsuruna gerek kalmadan tek bileşen ile yapılacak kimlik doğrulama 34 üncü maddenin birinci fıkrasına aykırılık olarak kabul edilmez. Müşterinin bu fıkra da belirtilen müşteri ve hesap bilgilerini görüntülemek üzere ilk defa oturum açması halinde ya da 34 üncü maddenin birinci fıkrasına göre iki bileşenle kimlik doğrulama gerçekleştirerek açtığı son oturumun üzerinden 90 günden daha fazla bir süre geçmiş olması halinde, iki bileşenli kimlik doğrulamaya tabi tutulması esastır.

## DÖRDÜNCÜ BÖLÜM Telefon Bankacılığı

### **Telefon bankacılığında kimlik doğrulama, işlem güvenliği ve hizmet kalitesi**

**MADDE 40** – (1) Müşteri 34 üncü maddenin birinci fıkrasına uygun olarak bir kimlik doğrulama gerçekleştirmediği müddetçe, telefon bankacılığında hizmet vermek üzere müşteriye karşılayan görevlinin müşteriye ilişkin bilgileri görememesi veya müşteriye ilişkin işlem menüsünün aktif olmaması sağlanır. Müşterinin kendi hesapları arasındaki finansal işlemler ile finansal olmayan işlemlerin gerçekleştirilmesi için uygulanacak kimlik doğrulamada PIN bilgisi müşterinin bildiği unsur olarak kullanılabilir. Kayıp, çalıntı ve dolandırıcılık gibi riskli işlem bildirim durumunda, görevliye bağlanan müşterilerin kimlik doğrulaması yapılmaksızın görevlinin bilmesi gerektiği kadar müşteri bilgisine erişebilmesi sağlanır ve gerekli güvenlik önlemleri alınır. Telefon bağlantısı olmaksızın ya da bağlantının sonlanması halinde kayıp, çalıntı ve dolandırıcılık gibi riskli işlem bildirim haricinde müşteriye ilişkin herhangi bir işlem gerçekleştirilemez.

(2) Müşterinin telefon bankacılığı kanalıyla, elektronik bankacılık dağıtım kanallarının herhangi birinde kullandığı kimlik doğrulama veya telefon bilgilerinde değişiklik gerçekleştirmek istemesi halinde bu değişikliğin görevli dahil ve erişimi olmadan otomatik sistemler üzerinden gerçekleştirilmesi sağlanır.

(3) Telefon bankacılığı hizmetlerinin verilmesi sırasında kimlik doğrulama gerçekleştirilirken, müşterinin bildiği kimlik doğrulama unsurları ile tek kullanımlık parola veya işlem doğrulama kodu gibi bileşenlerin, görevli dahil ve erişimi olmadan otomatik sistemler üzerinden girişinin yapılması sağlanır.

(4) Müşterinin bankada kayıtlı olan telefon numarasından aranması gerektiği durumlarda, arama gerçekleştirilmeden önce telefonun başka bir numaraya yönlendirilmemiş olduğuna ilişkin kontroller işletilir.

(5) Telefon bankacılığı hizmetlerinin verilmesi sırasında müşterinin gerçekleştirdiği işlemlere ilişkin alınan ses kayıtları için bu Yönetmelikte iz kayıtları hususunda belirtilen hükümler uygulanır. Alınan ses kayıtlarının güvenilir delillerin elde edilmesini sağlayacak ve sorumluluk atayacak nitelikte ve kalitede olması esastır.

(6) Banka, telefon bankacılığı hizmetlerinin müşterilere sunulmasında görev alan müşteri temsilcileri ve çağrı merkezi görevlileri gibi çalışanlara sosyal mühendislik saldırıları ve bilinen diğer dolandırıcılık yöntemleri konusunda periyodik eğitimler aldırarak ve bu çalışanların güvenlik farkındalıklarını artırıcı çalışmalar yapmakla yükümlüdür.

(7) Banka telefon bankacılığı hizmet kalitesini sağlamak adına asgari olarak aşağıdaki kriterleri yerine getirir:

a) Sesli yanıt sisteminin ana ve alt menülerinin, reklamlar, duyurular ve bilgilendirmeler dâhil, anons sürelerinin altmışar saniyeyi geçmemesi sağlanır.

b) Ses ile yönlendirme sisteminde müşterinin işlemini söylemeye başlaması için anonsu müteakip iki defa on saniye süre verilmesi, akabinde işlemini yapamayan müşterinin ana menüye aktarılması sağlanır.

c) Ana menüde veya alt menülerde çağrı merkezi görevlisi veya müşteri temsilcisine bağlanma seçeneği sunulur.

ç) Çağrı karşılama hedefinin tutturulması için çağrı merkezi görevlisi veya müşteri temsilcisinin müşteri ile görüşme süresinin sınırlandırılması gibi bir uygulamaya yer verilmemesi sağlanır.

## **BEŞİNCİ BÖLÜM** **Açık Bankacılık Servisleri**

### **Açık bankacılık servislerinde kimlik doğrulama ve işlem güvenliği**

**MADDE 41** – (1) Açık bankacılık servislerinin kullanılması sırasında, müşteri veya müşteri adına hareket eden taraf ile banka arasındaki iletişimin uçtan uca güvenli iletişim şeklinde olması, banka tarafından telafi edici ilave kontroller uygulanması ve müşterinin bağlantı kurabileceği kaynaklara ilişkin ilave kısıtlamalar getirilmesi şartıyla tek bileşen ile yapılacak kimlik doğrulama 34 üncü maddenin birinci fıkrasına aykırılık olarak kabul edilmez.

(2) Açık bankacılık servisleri aracılığıyla sunulabilecek hizmetler ve bu hizmetlere ilişkin usul ve esasları belirlemeye Kurul yetkilidir.

## **ALTINCI BÖLÜM** **ATM Bankacılığı**

### **ATM'lerde kimlik doğrulama ve işlem güvenliği**

**MADDE 42** – (1) Banka, ATM cihazları üzerinde kart kopyalama veya dolandırıcılığını önlemek için bilinen suç aygıtlarına ve tekniklerine karşı gerekli önlemleri almakla yükümlüdür. Banka asgari olarak aşağıdaki önlemleri alır:

a) Sahte önyüz, sahte klavye, kart sıkıştırma aparatları, kart kopyalama aparatları, nakit sıkıştırma aparatları, mobil kamera gibi kart okuyucu içerisine, para giriş ve çıkış noktalarına veya ATM'nin diğer birimlerine monte edilebilecek yabancı cihazların ATM'ye takılmasını ve mevcut ATM ekipmanlarının ATM'den çıkarılmasını zorlaştırıcı teknikler ile önleyici veya tespit edici kontroller kullanılır.

b) Yapılacak risk analizleri sonucunda belirlenen periyotlarda ATM cihazları yabancı cisimlerin mevcudiyetine karşı fiziksel olarak kontrol edilir. Kart kopyalama ve kart dolandırıcılığına yönelik cihazların monte edilme ihtimalinin yüksek olduğu tespit edilen ATM'ler için ilgili kontrol periyotları sıklaştırılır.

(2) ATM üzerine herhangi bir kart kopyalama ve dolandırıcılık amaçlı cismin monte edildiğinin veya ATM cihazının kurcalandığının tespit edilmesi, kart kopyalama ve dolandırıcılığı önlemeye yönelik çözümlerin alarm üretmesi veya bu çözümlerin çalışmadığının algılanması durumlarında; ATM'nin güvenlik amacıyla merkezden devre dışı bırakılabilmesi ve fiziksel olarak kontrol edilmeden ya da kamera görüntüleri incelenerek herhangi bir problemin bulunmadığı hususunda güvence sağlanmadan tekrar hizmete açılmaması temin edilir.

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

(4) ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler alınır, uygulamaların ve uygulamalara ilişkin kritik servis ve verilerin bütünlüğü periyodik olarak doğrulanır. ATM'ler üzerine güvenlik açıklarını gidermek

amacıyla otomatik olarak veya düzenli periyotlar ile gerekli güncellemeler ve yamalar yüklenir. ATM'ler üzerinde çalışan işletim sisteminin gerekli olan en az yetki ve ayrıcalıklara sahip olarak çalışacak şekilde ayarlanmış, gerekli güncellemeleri ve yamaları yüklenerek sıkılaştırılmış, stabil ve günün teknolojisine göre güvenli bir işletim sistemi olması sağlanır. Banka, ATM'lerde, kaynağını ve bütünlüğünü onaylayamadığı uygulama ve kodların çalışmasını engelleyecek önlemleri alır.

(5) ATM'lere yetkisiz kişilerin herhangi bir şekilde başka bir elektronik cihaz bağlamasına imkân verecek bütün giriş noktaları erişime kapatılır ve ATM cihazı ile banka arasındaki ağ bağlantısına yetkisiz olarak diğer cihazların bağlanmasını engelleyecek ilave güvenlik tedbirleri uygulanır.

(6) ATM cihazları üzerinden gerçekleştirilen işlemler için kullanılan iletişim ağının veri güvenliğini, gizliliğini ve bütünlüğünü sağlayacak özellikte olması sağlanır. ATM üzerinde saklanan, iletilen, işlenen her türlü verinin gizliliği ve bütünlüğü uygun yöntemlerle korunur. PIN bilgisi, parmak izi bilgisi, kart bilgisi gibi kimlik doğrulamaya ilişkin kritik bilgilerin sayısallaştırılarak sisteme girildiği aşamadan itibaren gizliliği ve bütünlüğü sağlanır.

(7) Banka, ATM cihazlarının güvenli kullanımı hususunda müşterilerinde farkındalık oluşturan çalışmalarda bulunur.

(8) Banka şubesinde gerçekleştirildiği takdirde yasal kimlik ibrazı zorunlu tutulan işlemlerin ATM'ler üzerinden yapılmak istenmesi durumunda 34 üncü maddenin birinci fıkrasına uygun olarak kimlik doğrulama uygulanır.

(9) Banka, ATM cihazlarının bulunduğu yerlere müşterinin klavye hareketlerini göremeyecek uygun bir açıyla güvenlik kamerası yerleştirir. Güvenlik kamerası kayıtları en az altı ay süreyle saklanır. Kamera kayıtlarındaki görüntünün delil niteliği teşkil etmesi ve görüntü kalitesinin ATM'deki müşterinin ve yakın çevresindekilerin eşkâllerinin belirlenmesini sağlayabilecek nitelikte olması esastır. Kameraların saatlerinin güncel, doğru olması ve ATM'de gerçekleştirilen işlem referans numarası, dekont numarası gibi parametrelerin zaman bilgisi ile uyumlu olması sağlanır. Kameranın herhangi bir sebeple görüntü kalitesinin düşmesi, görüntü alımının durması, lensinin dış bir etkenle kapatılması veya devre dışı kalması durumunu tespit edip gerekli aksiyonların alınmasını sağlayacak bir yapı kurulur.

(10) Görüntüleme alanı bakımından ATM'yi de kapsayan ve dokuzuncu fıkrada yer alan koşulları karşılayan bir güvenlik kamerası altyapısının varlığı durumunda ATM'ye özel ayrıca bir güvenlik kamerası kurulmasına gerek yoktur. 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**

#### **Uzaktan kimlik tespiti ve üçüncü tarafa güven**

**MADDE 43** – (1) Banka, 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ve alt düzenlemelerinde yer alan yükümlülükler saklı kalmak kaydıyla, müşterinin veya müşteri adına hareket eden kişinin kimliğini tespit etmek amacıyla, uzaktan kimlik tespiti yöntemleri kullanılabilir ya da hâlihazırda müşteri veya müşteri adına hareket eden kişi için daha önce kimlik tespitinde bulunmuş başka bir bankadan açık bankacılık servisleri aracılığıyla hizmet alabilir. Bu fıkranın uygulanmasına ilişkin usul ve esasları belirlemeye Kurul yetkilidir.

#### **Mesleki tecrübeye ilişkin alanlar ve süreler**

**MADDE 44** – (1) 2/1/2014 tarihli ve 2014/5885 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Bankacılık Düzenleme ve Denetleme Kurumu Teşkilat Yönetmeliğine göre Kurum tarafından ilgili kuruluşlarda BS yerinde denetimlerini yapmakla görevli daire başkanlığı bünyesinde görev alan Kurum meslek personeli, bu Yönetmelikte geçen mesleki tecrübeye ilişkin alanlarda çalışmış kabul edilir ve meslek personelinin ilgili daire başkanlığı bünyesinde çalıştığı süreler, bu Yönetmelikte geçen mesleki tecrübeye ilişkin alanlarda çalışılmış süreler olarak kabul edilir.

**İstisna hükmü**

**MADDE 45** – (1) Bu Yönetmelik kapsamında kurulacak komiteler, birimler ve sorumlular konusunda, bankaların ölçeđi, bilgi sistemlerine bađımlılıđı, personel sayısı, alınan dıř hizmetler gibi kriterler esas alınarak istisna tanımlamaya Kurum yetkilidir.

**İKİNCİ BÖLÜM**  
**Son Hükümler****Yürürlük**

**MADDE 46** – (1) Bu Yönetmelik 1/7/2020 tarihinde yürürlüđe girer.

**Yürütme**

**MADDE 47** – (1) Bu Yönetmelik hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.