TEBLİĞ

Türkiye Cumhuriyet Merkez Bankasından:

ÖDEME VE ELEKTRONİK PARA KURULUŞLARININ BİLGİ SİSTEMLERİ İLE ÖDEME HİZMETİ SAĞLAYICILARININ ÖDEME HİZMETLERİ ALANINDAKİ VERİ PAYLAŞIM SERVİSLERİNE İLİŞKİN TEBLİĞ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 – (1) Bu Tebliğin amacı, ödeme kuruluşları ve elektronik para kuruluşlarının faaliyetlerinin yürütülmesinde kullandıkları bilgi sistemlerinin yönetimi ve yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesi ile ödeme hizmeti sağlayıcılarının ödeme hizmetleri alanındaki veri paylaşım servislerine ilişkin usul ve esasları düzenlemektir.

Dayanak

MADDE 2 – (1) Bu Tebliğ, 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunun 12 nci, 14 üncü, 14/A, 18 inci ve 21 inci maddelerine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 3 – (1) Bu Tebliğde yer alan;

a) Açık rıza: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin birinci fıkrasının (a) bendinde tanımlanan açık rızayı,

b) Alıcı: Ödeme işlemine konu fonun ulaşması istenen gerçek veya tüzel kişiyi,

c) Anonim ön ödemeli araç: Herhangi bir şekilde ödeme hesabına bağlı olmayan ve kimlik tespiti veya doğrulaması yapılmamış, önceden ödeme ya da yükleme yapılması suretiyle kullanılabilir hale gelen, tekrar yükleme yapılma imkanı bulunan veya bulunmayan şekilde ihraç edilebilen ve yüklenen bakiye kadar kullanıma izin verilen ön ödemeli aracı,

ç) API: Farklı yazılımların birbirleri üzerinde tanımlanmış servisleri kullanabilmesi ve aralarında veri alışverişi yapabilmesi için belirli koşul ve kurallar çerçevesinde oluşturulmuş arayüzleri,

d) Aydınlatma: 6698 sayılı Kanunun 10 uncu maddesi kapsamında yapılacak bilgilendirmeyi,

e) Bağımsız denetim kuruluşu: Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından yetkilendirilmiş bağımsız denetim kuruluşlarından Bankacılık Düzenleme ve Denetleme Kurumu tarafından yayımlanan Bankalarda Bilgi Sistemleri Denetimi Yapmaya Yetkili Bağımsız Denetim Kuruluşları listesinde yer alan bağımsız denetim kuruluşunu,

f) Banka: Türkiye Cumhuriyet Merkez Bankası Anonim Şirketini,

g) Banka ödeme sistemi: Banka tarafından işletilen ödeme sistemlerini,

ğ) Bilgi sistemleri: Ödeme hizmetine ilişkin faaliyetlerin yürütülmesi amacıyla ödeme hizmeti sağlayıcısının bilgi ve verilerle ilgili olarak mevzuatla belirlenmiş sorumluluklarının yerine getirilmesini sağlayan donanım, yazılım, veri, süreç ve insan kaynağından oluşan yapının tamamını,

h) Bilgi varlığı: Kurumsal bilgiye erişimde ve bu bilginin işlenmesinde, iletilmesinde, saklanmasında, korunmasında ve imhasında kullanılan donanım, yazılım, belge, veri ve insan gibi her türlü kaynağı,

ı) Birincil merkez: Birincil sistemlerin tesis edildiği yapıyı,

i) Birincil sistemler: Kanun, Yönetmelik, bu Tebliğ ve Bankaca Kanun kapsamında çıkarılacak ilgili diğer düzenlemelerde yer alan hususlarla ilgili bütün bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanıldığı sistemler ile faaliyetlerin yürütülmesinde kullanılan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamını,

j) Biyometrik veri: Kimlik doğrulama işlemlerinin gerçekleştirilmesi esnasında kullanılan retina, iris, yüze ait karakteristik özellikler, ses ve parmak izi benzeri kişiye özgü ölçülebilir biyolojik veya davranışsal karakteristiği,

k) BKM: Bankalararası Kart Merkezi Anonim Şirketini,

l) BKM-API Geçidi: Kanunun 12 nci maddesinin birinci fıkrasının (f) ve (g) bentlerinde yer alan ödeme hizmetlerinin sunulması için Yönetmeliğin 59 uncu maddesinin beşinci fıkrası uyarınca BKM tarafından kurulacak yapıyı,

m) BSDHY: 13/1/2010 tarihli ve 27461 sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliği,

n) Değişiklik yönetimi: Önceden belirlenmiş prosedürlerin kullanımı yoluyla bilgi sistemleri ile ilgili tüm değişikliklerin etkin ve güvenli bir şekilde ve zamanında gerçekleştirilmesini sağlamayı ve bu değişikliklerden kaynaklanabilecek olayların sayısı ile bu olayların sunulan hizmetler üzerindeki etkisini asgari düzeye indirmeyi amaçlayan bilgi sistemleri hizmet yönetimi disiplinini,

o) Denetim izleri: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtlar ile bilgi varlıklarına kimin eriştiğini veya erişmeye çalıştığını ve kullanıcının hangi işlemleri gerçekleştirdiğini gösteren kayıtları,

ö) Dış hizmet sağlayıcı: Kuruluşun, Yönetmeliğin 21 inci maddesi çerçevesinde münhasıran kendisi tarafından yapılması gerekenler dışında kalan faaliyetlerini kuruluş adına gerçekleştiren ya da gerçekleştirilmesinde kuruluşa yardımcı nitelikte hizmet veren tüzel kişiyi,

p) Elektronik kanal: Müşterilerin ödeme hizmeti sağlayıcısının fiziksel şube ve temsilcilerine gitmeden uzaktan ödeme hizmeti alabildikleri mobil uygulama, internet şubesi, telefon hizmetleri, ATM, kiosk cihazı, API ve benzeri her türlü elektronik hizmet yöntemini,

r) Elektronik para: Elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, Kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değeri,

s) Elektronik para ihraç eden kuruluş: Elektronik para kuruluşlarını, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki bankaları ve Posta ve Telgraf Teşkilatı Anonim Şirketini,

ş) Elektronik para kullanıcısı: Gönderen, alıcı veya her ikisi sıfatıyla elektronik para ihraç eden kuruluşların sunduğu elektronik para ihracı ve fona çevirme hizmetlerinden faydalanan gerçek veya tüzel kişiyi,

t) Elektronik para kuruluşu: Kanun kapsamında elektronik para ihraç etme yetkisi verilen tüzel kişiyi,

u) Fon: Banknot, madeni para, kaydi para veya elektronik parayı,

ü) Gönderen: Kendi ödeme hesabından veya ödeme hesabı bulunmaksızın ödeme emri veren gerçek veya tüzel kişiyi,

v) Güçlü kimlik doğrulama: Kimlik doğrulamada kullanılan ve bir bileşenin ele geçirilmesinin diğer bileşenin güvenliğini tehlikeye atmayacağı en az iki bileşenden oluşan, bu iki bileşenin de müşterinin bildiği, sahip olduğu veya biyometrik bir karakteristiği olan bileşen sınıflarından farklı ikisine ait olacak şekilde seçildiği yöntemi,

y) Güvenli bileşen: İçinde barındırdığı gizli verilerin yetkisiz kişilerce erişilmesine, kopyalanmasına ve kendi dışına çıkarılmasına imkân vermeyen SIM kart, akıllı kart gibi bileşeni,

z) Hassas müşteri verisi: Ödeme emrinin verilmesinde veya müşterinin kimliğinin doğrulanmasında kullanılan ve üçüncü kişilerce ele geçirilmesi veya değiştirilmesi halinde dolandırıcılık ya da müşteri adına sahte işlem yapılmasına imkân verebilecek kişisel veriler ile müşteri güvenlik bilgilerini,

aa) Hesap bilgisi hizmeti: Kanunun 12 nci maddesinin birinci fıkrasının (g) bendinde tanımlanan hizmeti,

bb) Hesap bilgisi hizmeti sağlayıcısı - HBHS: Kanunun 12 nci maddesinin birinci fıkrasının (g) bendinde tanımlanan ödeme hizmetini sunan tüzel kişiyi,

cc) Hesap hizmeti sağlayıcısı (HHS): Nezdinde ödeme hesabı bulunan ödeme hizmeti sağlayıcısı,

çç) Hizmet seviyesi: Hizmetlerin maliyeti ile söz konusu hizmetleri alanların gereksinim ve beklentilerinin göz önünde bulundurulması suretiyle, hizmeti sunan tarafından hizmetin içeriği ile kalitesine ilişkin yazılı olarak önceden belirlenen ve ilgili taraflarla paylaşılan seviyeyi,

dd) İkincil merkez: Birincil merkezin kullanılamadığı durumlarda, birincil ve ikincil sistemlere kullanıma hazır olacak şekilde erişilebildiği, personelin çalışmasına imkân tanıyacak ve birincil merkezin tesis edildiği yapı ile aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı,

ee) İkincil sistemler: Birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve Kanun, Yönetmelik, bu Tebliğ ve Bankaca Kanun kapsamında çıkarılacak ilgili diğer düzenlemelerde yer alan hususlarla ilgili bütün bilgilere erişilmesini sağlayan birincil sistem yedeklerini,

ff) İnsansız hizmet noktası: Müşterilerin, ödeme işlemi ya da elektronik para ile ilgili işlemleri kendi kendine yapabildiği, sahipliği bir veya birden fazla kuruluşa ait olan ve fiziki bir lokasyonu bulunan ATM, kiosk gibi cihazları,

gg) İnternet şubesi: Müşterilerin, ödeme hizmeti sağlayıcılarının Kanun kapsamında sundukları hizmetlere, 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 ve hizmetlerin internet sitesi üzerinden sunulduğu elektronik kanalları,

ğğ) İşlem bilgisi: Gerçekleştirilen işleme ilişkin işlem zamanını, işlemin niteliğini ve ödeme işlemi için ödeme emrinin masraf, komisyon ve ücretler de dahil hesabın borçlandırılacağı toplam tutarını ve ödemenin göndereni ile alıcısını veya toplu ödeme emrinin masraf, komisyon ve ücretler de dahil hesabın borçlandırılacağı toplam tutarını ve göndereni ile alıcılarını içeren bilgiyi,

hh) İşlem doğrulama kodu: Kimlik doğrulama yöntemlerinden biriyle kendisini sisteme tanıtan bir müşterinin gerçekleştirmek istediği işleme özgü olmak ve belirli bir geçerlilik süresi içinde işlem onayında kullanılmak üzere oluşturulan, finansal sonuç doğuran işlemlerde kişiye onay anında ilgili işlem bilgisi ile birlikte gösterilen ve alıcı veya tutarın değişmesiyle geçersiz hale gelen bilgiyi,

ıı) İşyeri: Ödeme hizmeti sağlayıcısı ile yaptığı sözleşme çerçevesinde ödeme hizmeti kapsamına giren bir ödeme yöntemi ile mal ve hizmet satmayı kabul eden gerçek veya tüzel kişiyi,

ii) Kanun: 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunu,

jj) Karşılıklı doğrulama: İletişimde bulunan bilgi sistemlerinin birbirlerinin kimliklerinden emin olmalarını sağlamak amacıyla kullanılan, iki tarafın da kendi kimliğini diğer tarafa doğruladığı kimlik doğrulama yöntemini,

kk) Kesinti: Planlı olanlar dışında, ödeme hizmeti sağlayıcısının Kanun kapsamındaki faaliyetlerine ilişkin operasyonel iş ve süreçlerinin sekteye uğramasını,

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

mm) Kimlik tanımlayıcı: Ödeme hizmeti sağlayıcısı tarafından kimliğinin belirlenmesi ve diğer kullanıcılardan ayırt edilmesi amacıyla müşteriye özgülenen sayı, harf veya sembollerden oluşan kombinasyonu,

nn) Kişisel veri: 6698 sayılı Kanunun 3 üncü maddesinin birinci fıkrasının (d) bendinde tanımlanan bilgiyi,

oo) Kullanıcı: Personel veya müşteri gibi ödeme hizmeti sağlayıcısının bilgi sistemleri üzerinde işlem gerçekleştirmek üzere kendilerine hesap tanımlanmış olan her türlü kullanıcıyı,

öö) Kuruluş: Ödeme kuruluşları ve elektronik para kuruluşlarını,

pp) Mobil uygulama: Akıllı telefon veya tablet gibi mobil bir cihazda bulunan ödeme hizmeti sağlayıcısına ait uygulama üzerinden müşterilerin Kanun kapsamına giren işlemlerini gerçekleştirebildikleri özelleşmiş elektronik kanalı,

rr) Mobil uygulama etkinleştirme: Mobil uygulama için müşterinin mobil cihazının müşteri ile eşleştirilmesini,

ss) Müşteri: Ödeme hizmeti kullanıcısı ile elektronik para kullanıcısını,

şş) Müşteri bilgisi: Müşterilere ait, işlem bilgisi, bakiye bilgisi, kişisel veri, kimlik tanımlayıcısı, unvan dahil olmak üzere müşterinin kişisel ve finansal durumuna ilişkin doğrudan veya dolaylı yoldan edinilen her türlü bilgiyi,

tt) Müşteri güvenlik bilgileri: Kimlik doğrulama işleminin yapılması amacıyla ödeme hizmeti sağlayıcısı tarafından müşterisine verilen veya müşteri tarafından belirlenerek ödeme hizmeti sağlayıcısı ile mutabık kalınan özelleştirilmiş bilgiyi,

uu) Olay: Bilgi sistemlerinin işleyişinde bir kesintiye ya da siber olay dâhil hizmet kalitesinde düşüşe neden olan her türlü gelişmeyi,

üü) Oturum: Kullanıcıların elektronik kanallar üzerinden kimlik doğrulama mekanizması ile bilgi sistemlerine dâhil olmalarından işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde tesis edilen, veri aktarımı, sunuşu veya gerçekleştirilecek finansal işlemler için taraflar arasında kurulan mantıksal bağı,

vv) Ödeme aracı: Ödeme hizmeti sağlayıcısı ile müşteri arasında belirlenen ve müşteri tarafından ödeme emrini vermek için kullanılan kart, cep telefonu, şifre ve benzeri kişiye özel aracı,

yy) Ödeme emri: Müşteri tarafından ödeme işleminin gerçekleşmesi amacıyla ödeme hizmeti sağlayıcısına verilen talimatı,

zz) Ödeme emri başlatma hizmeti: Kanunun 12 nci maddesinin birinci fıkrasının (f) bendinde tanımlanan hizmeti,

aaa) Ödeme emri başlatma hizmeti sağlayıcısı - ÖBHS: Kanunun 12 nci maddesinin birinci fıkrasının (f) bendinde belirtilen ödeme hizmetini sunan tüzel kişiyi,

bbb) Ödeme hesabı: Müşteri adına açılan ve ödeme işleminin yürütülmesinde kullanılan hesabı,

ccc) Ödeme hizmeti: Kanunun 12 nci maddesi çerçevesinde ödeme hizmeti olarak kabul edilen hizmetleri,

ççç) Ödeme hizmeti kullanıcısı: Gönderen, alıcı veya her ikisi sıfatıyla belirli bir ödeme hizmetinden faydalanan gerçek veya tüzel kişiyi,

ddd) Ödeme hizmeti sağlayıcısı: 5411 sayılı Kanun kapsamındaki bankalar, elektronik para kuruluşları, ödeme kuruluşları ve Posta ve Telgraf Teşkilatı Anonim Şirketini,

eee) Ödeme işlemi: Gönderen veya alıcının talimatı üzerine gerçekleştirilen fon yatırma, aktarma veya çekme faaliyetini,

fff) Ödeme kuruluşu: Ödeme hizmeti sağlamak ve gerçekleştirmek için Kanun kapsamında yetkilendirilmiş tüzel kişiyi,

ggg) Ön ödemeli araç: Müşterinin ödemelerde kullanılabilecek fonu ödeme aracını ihraç eden ödeme hizmeti sağlayıcısına harcama yapmadan önce ödediği ve ödenene eşdeğer tutarda fonun elektronik para olarak ödeme hizmetlerinde kullanılmasına imkân veren fizikî veya fizikî varlığı bulunmayan ödeme aracını,

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

hhh) Personel: Kuruluş personeli, temsilci personeli ve dış hizmet sağlayıcı çalışanı gibi kuruluşun bilgi sistemleri üzerinde işlem gerçekleştirmek üzere kendilerine yetki verilmiş olan her türlü kullanıcıyı,

ııı) Proje yönetimi: Önceden belirlenmiş metodolojilerin kullanımı yoluyla bilgi sistemleri projelerinin, öngörülen zaman planına, bütçeye ve kalite düzeyine uygun olarak tamamlanmasını temin edecek şekilde planlanmasını, organizasyonunu ve yürütülmesini sağlayan süreci,

iii) Rekabete duyarlı veri: Ücret, komisyon, faiz gibi fiyat ile ilişkilendirilebilir her türlü niceliksel veriyi,

jjj) Risk bazlı kimlik doğrulama: Çeşitli risk faktörlerinin dinamik bir şekilde değerlendirilmesi suretiyle kimlik doğrulama sürecinin düşük risk profili için kolaylaştırılması, yüksek risk profili için daha kapsamlı ve kısıtlayıcı hale getirilmesi yaklaşımını,

kkk) Sızma testi: Bilgi sistemlerinin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amaçlı gerçekleştirilen testi,

lll) Siber olay: 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 3 üncü maddesinde tanımlanan siber olayı,

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

nnn) SMS OTP: Elektronik haberleşme işletmecilerinin sunduğu SMS servisi aracılığıyla iletilen tek kullanımlık parolayı,

ooo) Sorun: Bir veya daha fazla olayın kök nedenini,

öööö) Sürekli iş ilişkisi: 10/12/2007 tarihli ve 2007/13012 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelikte tanımlanan sürekli iş ilişkisini,

ppp) Tek kullanımlık parola: Kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele oluşturulan harf, rakam ve/veya özel işaret dizisini,

rrr) Temsilci: Kuruluş adına ve hesabına hareket eden gerçek veya tüzel kişiyi,

sss) Terminal: Ödeme aracı üzerindeki bilgiler ile hassas müşteri verilerini esas alarak her türlü mal ve hizmet alımı veya nakit ödeme belgesi düzenlenmesi işlemleri ile ödeme işlemlerinin ve elektronik para ile ilgili işlemlerin gerçekleştirilmesinde kullanılan, ödeme hizmeti sağlayıcı tarafından temin edilen elektronik cihaz ya da yazılımı,

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

ttt) Uzaktan iletişim aracı: Mektup, katalog, telefon, faks, radyo, televizyon, elektronik posta mesajı, internet, SMS hizmetleri gibi fiziksel olarak karşı karşıya gelinmeksizin sözleşme kurulmasına imkan veren her türlü araç veya ortamı,

uuu) Üst yönetim: Kuruluşun yönetim kurulu üyeleri, genel müdür ve genel müdür yardımcıları, iç kontrol ve risk yönetimi birimlerinin yöneticileri ile başka unvanlarla istihdam edilseler dahi, danışmanlık birimleri dışındaki birimlerin, yetki ve görevleri itibarıyla genel müdür yardımcısına denk veya daha üst konumlarda görev yapan yöneticilerini,

üüü) Veri paylaşım servisleri: Müşteriler adına hareket eden tarafların API'ler vasıtasıyla HHS'nin sunduğu ödeme hizmetlerine uzaktan erişerek Kanun kapsamına giren işlemleri gerçekleştirebildikleri veya bu tür işlemlerin gerçekleştirilmesi için HHS'ye talimat verdikleri elektronik kanalı,

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

yyy) Yönetmelik: 1/12/2021 tarihli ve 31676 sayılı Resmî Gazete'de yayımlanan Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmeliği,

ifade eder.

İKİNCİ BÖLÜM
Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler

Bilgi sistemleri yönetimine ilişkin genel hükümler

MADDE 4 – (1) Kuruluş, bilgi sistemlerine ilişkin faaliyetlerini yürütürken işleyişinden sorumlu olduğu hizmetin kesintisiz, güvenli, etkin ve verimli bir şekilde çalışması amacını öncelikli olarak gözetir.

(2) Kuruluş, bilgi sistemlerini Kanun kapsamında yürütmekte olduğu faaliyetlerin konusu, hacmi, karmaşıklığı ve kapsamı ile uyumlu ve kişisel verilerin güvenliğine yönelik gerekli idari ve teknik tedbirlere uygun şekilde tesis eder ve teknolojik gelişmeleri de dikkate alarak günceller.

(3) Kuruluş, bilgi sistemleri yönetimine ilişkin politikaları, ana strateji ve hedefleri ile uyumlu şekilde yazılı olarak oluşturur, yılda en az bir defa olmak üzere düzenli olarak gözden geçirir ve gerekli durumlarda günceller. Bilgi sistemleri yönetimine ilişkin politikaların yönetim kurulu tarafından onaylanması zorunludur.

(4) Kuruluş, Kanun kapsamındaki faaliyetleri ile ilgili her türlü yönetim faaliyetlerini bilgi sistemleri yönetimini de kapsayacak şekilde, bütüncül bir yaklaşım içerisinde ve kurumsal yönetim uygulamaları çerçevesinde gerçekleştirir ve bilgi sistemleri yönetimine ilişkin unsurları organizasyon yapısı içerisinde, kuruluşun büyüklüğü ile faaliyetlerinin karmaşıklığını gözeterek uygun yere yerleştirir.

(5) Kuruluş, bilgi sistemleri ile ilgili olarak organizasyon yapısı içerisinde yer alan birimlerin görev ve sorumlulukları ile bu birimlerdeki personelin görev tanımlarını açık, anlaşılır ve yazılı olarak oluşturur. Bu fıkra uyarınca hazırlanan dokümanlar yönetim kurulunca onaylanır. Dokümanların uygunluğu yılda en az bir defa gözden geçirilir.

(6) Bilgi sistemlerinin yönetimi konusunda görev alan personelin kendilerine atanan görev ve sorumluluklarla ilgili farkındalıklarının oluşturulması ile görev ve sorumluluklarda meydana gelecek değişikliklerden haberdar olması sağlanır.

(7) Kuruluş, bilgi sistemleri yönetimine ilişkin görev, yetki ve sorumlulukları açıkça belirler ve bilgi sistemleri yönetimi için gerekli her türlü kaynağı sağlar.

(8) Kuruluş, bilgi sistemleri yönetimine ilişkin faaliyetlerin politika, düzenleme ve genel kabul görmüş ilgili uluslararası standartlara uyumlu olduğunu kontrol etmek üzere Yönetmeliğin 26 ncı maddesi uyarınca oluşturulan iç kontrol sisteminin içerisinde gerekli fonksiyonu oluşturur. Bu konularda çalışacak personelin gerekli deneyim ve bilgi birikimine sahip olması gerekir.

(9) Bilgi sistemleri yönetiminin bu Tebliğde yer alan hükümlere uygun şekilde yürütülmesinden kuruluşun yönetim kurulu sorumludur.

(10) Yönetmeliğin 11 inci maddesi uyarınca faaliyet izni başvurusunda bulunulduğunda, nihai onay aşamasından önce olmak üzere, bilgi sistemleri altyapısından sorumlu yöneticinin

atamasının yapılmış olması gerekir. Ataması yapılacak yöneticinin bilgi sistemleri sektöründe benzer ölçekteki proje ekiplerinde yer almış olması gerekir.

(11) Yönetmeliğin 11 inci maddesi uyarınca faaliyet izni başvurusunda bulunulduğunda, nihai onay aşamasından önce olmak üzere, bir yıllık iş planının gerektirdiği bilgi sistemleri altyapısının üretim ortamının kurulmuş olması gerekir.

Bilgi sistemlerine ilişkin risk yönetimi

MADDE 5 – (1) Kuruluş, bilgi sistemlerinin sorunsuz şekilde işlemesini tehlikeye sokabilecek tüm risklerin tespit edilmesini, ölçülmesini, izlenmesini ve etkin bir şekilde yönetilmesini sağlamak amacıyla risk yönetim çerçevesi ve yeterli araç zenginliğine sahip bir yapıyı tesis eder. Kuruluş, risk yönetim çerçevesi kapsamında riskleri yönetmek amacıyla uygulanması gereken önlemlere ilişkin usul ve esaslar ile tesis edilmesi gereken kontrolleri içerir politika, prosedür ve süreç dokümanlarını yazılı olarak oluşturur. Bu fıkra uyarınca hazırlanan dokümanlar yönetim kurulunca onaylanır.

(2) Kuruluş, tesis edeceği risk yönetim çerçevesini oluştururken, bilgi sistemlerine ilişkin riskleri ve ilgili mevzuat ile ulusal ve uluslararası standartları göz önünde bulundurur.

(3) Birinci fıkra uyarınca bilgi sistemlerine ilişkin riskler değerlendirilirken, Kuruluşun ana faaliyetleri ile diğer faaliyetleri, varsa temsilci ve dış hizmet sağlayıcıların faaliyetleri, üçüncü taraflara olan bağımlılıkları ve Kuruluşun diğer ödeme hizmeti sağlayıcıları ve ödeme sistemleri ile olan bağlantıları da göz önünde bulundurulur.

(4) Kuruluş, bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce ve yılda en az bir defa olmak üzere bilgi sistemlerine ilişkin kapsamlı bir risk değerlendirmesi yapar ve değerlendirme sonuçlarını ve bunlara ilişkin alınacak aksiyonları içerir raporu, herhangi bir değişikliğe bağlı olmadan ve her yıl Ocak ayı sonuna kadar bir önceki yıla ilişkin olacak şekilde hazırlar ve yönetim kurulu ile Bankaya sunar.

(5) Birinci fıkra uyarınca oluşturulacak dokümanlarda yer alan önlem ve kontrollerin etkin bir şekilde uygulanabilmesi için kuruluş, organizasyon yapısı, personel ve diğer kaynaklara ilişkin gerekli tedbirleri alır ve 4 üncü maddenin beşinci fıkrası çerçevesinde oluşturulacak görev tanımlarında birinci fıkra uyarınca oluşturulacak dokümanlarda yer alan önlem ve kontrollerin uygulanmasına ilişkin sorumlulukların açık bir şekilde belirlenmesini sağlar.

Bilgi sistemleri işletimi

MADDE 6 – (1) Kuruluş, tanımlanan hizmet seviyeleri çerçevesinde bilgi sistemlerinin işleyişinin güvenilirliğine, dayanıklılığına ve sürekliliğine ilişkin hedefleri yazılı olarak açıkça belirler ve bu hedefler doğrultusunda bilgi sistemlerinin işletiminin etkin ve verimli yapılabilmesi amacıyla sağlayıcı veya üretici firma desteği süren güncel yazılım sürümlerinin kullanılması da dahil olmak üzere gerekli tedbirleri alır.

(2) Kuruluş, birinci fıkra kapsamında belirlediği hedeflere uyum düzeyini yılda en az bir defa olmak üzere düzenli aralıklarla ölçer ve sonuçların yönetim kurulu tarafından değerlendirilmesini ve uyum sağlanamayan durumlarda konuyla ilgili alınacak aksiyonların belirlenmesini sağlar. Süreç sonucunda ortaya çıkan doküman her yıl için en geç takip eden yılın Ocak ayı sonuna kadar Bankaya raporlanır.

(3) Kuruluş, bilgi sistemlerini tanımlanan hizmet seviyeleri için yeterli kapasiteye sahip olacak şekilde tesis eder, kapasitenin ölçeklenebilir olmasını öncelikli olarak gözetir ve bilgi sistemlerine yönelik etkin bir kapasite yönetimi yapar.

(4) Kuruluş, bilgi sistemleri envanterinin ve konfigürasyon bilgisinin oluşturulmasını, güvenli bir şekilde saklanmasını, güncellenmesini ve üst yönetime raporlanmasını sağlar. Kuruluş, bu çalışmalar kapsamında;

a) Masaüstü, dizüstü, mobil cihazlar ve sunucular 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. Söz

konusu standart konfigürasyon bilgilerini, standart konfigürasyondan sapmaları veya standart konfigürasyondaki güncellemeleri değişiklik yönetiminin bir parçası olarak kayıt altına alır ve onay mekanizmasına tabi tutar. Güvenli standart konfigürasyonun dışında kalan her türlü değişiklik isteği için iş gereksinimi, gereksinim süresi ve bu iş gereksinimine ihtiyaç duyan iş sorumlusunun kim olduğu gibi bilgileri kayıt altına alır.

b) Masaüstü, dizüstü, mobil cihazlar ve sunucular üzerindeki işletim sistemleri için bu işletim sistemlerinin tipi, sürüm numarası, yama seviyesi ve üzerinde yüklü olan veritabanları ve uygulamaların listesini gösterecek şekilde bir yazılım envanteri oluşturur.

c) (b) bendi uyarınca oluşturulan yazılım envanterinin aynı zamanda donanım envanteri ile de entegre olmasını ve tek bir noktadan hangi donanım üzerinde hangi yazılımların olduğu bilgisinin takip edilebilir olmasını sağlar.

(5) Kuruluş, bilgi sistemleri ile ilgili yapılacak her türlü değişikliği, süreci belirlenmiş ve üst yönetimce onaylanmış değişiklik yönetimi prosedürlerine uygun olarak gerçekleştirir.

(6) Kuruluş, kurum içi geliştirme veya dış alım yoluyla bilgi sistemlerinde gerçekleştirilecek her türlü projeyi, genel kabul görmüş ilgili uluslararası standartlara ve en iyi uygulama örneklerine uygun olarak belirlemiş olduğu proje yönetimi prosedürlerine uygun olarak yürütür. Yazılım geliştirme süreçlerinde geliştirme, test ve üretim ortamlarının birbirinden ayrı olması ve görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretime geçiş süreçlerinin farklı kişiler tarafından yürütülmesi sağlanır.

(7) Kuruluş, Kanun kapsamındaki faaliyetleri ile ilgili süreç ve sistemleri, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlar ve işletir.

(8) Kuruluş, bilgi sistemleri unsurlarının sağlayıcı veya üretici firma desteği bittiğinde veya bu unsurların güncel durumları günün şartlarına göre gerekli güvenlik ve güvenilirlik seviyesini sağlayamadığında ilgili bilgi sistemleri unsurunu kullanımdan kaldırır.

Olay yönetimi ve siber olaylar

MADDE 7 – (1) Kuruluş, önceden belirlenmiş prosedürler çerçevesinde müşteri şikâyetlerini de kapsayacak şekilde olayların zamanında tespit edilmesini, makul bir süre içerisinde müdahale edilmesini, kayıt altına alınmasını, raporlanmasını, olayın potansiyel boyutunun, etkisinin, hasarının ve etkilenen müşterilerin tespit edilmesini içerecek şekilde analiz edilmesini, mümkün olan en kısa sürede ve en az hasarla bilgi sistemleri hizmetleri normal işleyişine döndürülecek şekilde çözülmesini ve olay hakkında ilgili tüm paydaşların zamanında bilgilendirilmesini sağlayacak şekilde olay yönetimi yapar.

(2) Kuruluşun müşterilerinin bir kısmının ya da tamamının olaydan etkilenmesi durumunda, müşterilerle iletişime geçilerek olay hakkında bilgi verilir ve varsa konuyla ilgili müşterilerin yapması gereken hususlar aktarılır.

(3) Kuruluş, müşterileri ve Kişisel Verileri Koruma Kurulunu, hassas müşteri verilerinin ya da kişisel verilerin sızmasına ya da ifşasına yol açan bir siber olayın yaşanması veya kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hallerinde mümkün olan en kısa süre içerisinde bilgilendirir.

(4) Kuruluş, her önemli olaydan sonra olayın ayrıntılı olarak incelenmesini, kök neden analizinin yapılmasını, etkilerinin belirlenmesini ve olaya ilişkin sorunun takibini ve raporlamasını içerecek şekilde sorun yönetimi yapar.

(5) Kuruluş, siber olayları da olay yönetimi kapsamında ele alır ve mevzuata uygun şekilde tesis edeceği siber olay yönetimi ve siber olaya müdahale süreci kapsamında Bankaya gerekli bildirimleri yapar.

(6) Kuruluş, siber olayları önemlilik düzeyine göre sınıflandırmak üzere sınıflandırma kriterlerini yazılı olarak hazırlar, gerçekleşen siber olayın bu kapsamda belirlenen önem düzeyine uygun sürede ele alınması ve çözüme kavuşturulmasına yönelik prosedürler ile

müdahale planlarını oluşturur. Müdahale planları kapsamında birinci fıkrada yer alan unsurlara ilişkin tüm süreçler ele alınır.

(7) Oluşturulan müdahale planları yılda en az bir defa düzenli olarak test edilir ve test sonuçları yönetim kuruluna raporlanır.

(8) Kuruluş tarafından siber olay yönetimi ve siber olaya müdahale süreci kapsamında yapılması gerekenlere ilişkin usul ve esaslar Banka tarafından çıkarılacak Tebliğ ile belirlenir.

Bilgi güvenliği ve bilgi güvenliği yönetimi

MADDE 8 – (1) Kuruluş, genel kabul görmüş ilgili uluslararası standartları ve en iyi uygulama örneklerini de göz önünde bulundurarak, faaliyetlerine ilişkin bilgi sistemlerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak amacıyla kural, ilke ve politikaları içeren bilgi güvenliği yönetim çerçevesi oluşturur.

(2) Kuruluş, birinci fıkra kapsamında oluşturduğu bilgi güvenliği yönetim çerçevesine uygun bir bilgi güvenliği yönetim sistemi oluşturur.

(3) Kuruluş, bilgi güvenliği yönetim sisteminin oluşturulmasına, yönetilmesine, yılda en az bir defa düzenli olarak gözden geçirilmesine ve gerekli hallerde güncellenmesine ilişkin görev, yetki ve sorumlulukları açıkça belirler.

(4) Bilgi güvenliği yönetim sistemi kapsamında her kademedeki personelin bilgi güvenliğine ilişkin görev, yetki ve sorumlulukları açıkça belirlenir ve ilgili personelin bundan haberdar olmasını sağlayacak şekilde gerekli bilgilendirmeler yapılır.

(5) Kuruluş, bilgi güvenliği yönetim sistemi kapsamında bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve raporlanmasına ilişkin gerekli mekanizmaları oluşturur.

(6) Kuruluş, güvenlik gereksinimleri doğrultusunda bilgi varlıklarına ilişkin olarak uygun kontroller tesis etmek için yönetim kurulu tarafından onaylı bir bilgi varlıkları sınıflandırma kılavuzu hazırlar. Her bir sınıftaki bilgi varlıklarına ilişkin erişim hakları ile saklama, iletme ve imha etme prosedürlerini açıkça belirler, sınıflandırma ve bununla ilgili yükümlülükler konusunda tüm personeli bilgilendirir.

(7) Kuruluş tüm bilgi varlıklarını, önem seviyesini ve yasal yükümlülükleri de dikkate alarak bilgi varlıkları sınıflandırma kılavuzuna uygun olarak sınıflandırır. Bilgi varlığının sınıfı belirlenirken gizlilik derecesi, bütünlük gereksinimi, kullanılabilirlik gereksinimi, saklama süresi ve asgari yedekleme sıklığı ile veriler özelinde hassas müşteri verisi, müşteri bilgisi ya da kişisel veri olup olmadığı gibi kriterler göz önünde bulundurulur.

(8) Bilgi güvenliği yönetim sisteminde, personelin işe başlaması, görev ve pozisyon değiştirmesi ve işten ayrılması da dahil olmak üzere personele ilişkin tüm hususlar bilgi güvenliğini etkileyen yönleriyle değerlendirilir ve gerekli tedbirler alınır.

(9) Kuruluş, bilgi güvenliği yönetim sistemi kapsamında faaliyetleri ile ilgili kendi nezdindeki her türlü donanım ile altyapının ve bunlarla ilgili fiziksel çevrenin güvenliğini sağlar. Kuruluş, faaliyetleri ile ilgili kendi nezdinde bulunmayan donanım ile altyapının ve bunlarla ilgili fiziksel çevrenin güvenliğinin sağlanması için gerekli özeni gösterir ve güvenliğin sağlandığını kontrol eder.

(10) Kuruluş, iç ve dış ağlar arasında Kanun kapsamındaki faaliyetler ile ilgili gerçekleşen her türlü iletişim sürecinin ve ana faaliyetlerine ilişkin operasyonel işlemlerin, güvenlik kontrolleri ve araçları kullanılarak gerçekleşecek şekilde tasarlanmasını sağlar. Güvenlik kontrolleri ve araçlarının tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır ve güncel teknolojiye uygun çözümler kullanılır.

(11) Kuruluş, iç ağdan gelebilecek tehditlerin etkisini azaltmak ve iç ağın farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere ağ segmentasyonu yapar. İç ağdaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşması, farklı ağ segmentleri arasındaki veri trafiğinin güvenliği ve iç ağa sadece yetkilendirilmiş cihazların bağlanması sağlanır. Kritik ağ segmentlerine yapılan

bağlantılar düzenli olarak tespit edilerek bu bağlantıların her biri için gereksinim değerlendirmesi yapılır ve gereksiz bağlantıların sonlandırılması sağlanır.

(12) Hassas müşteri verileri veya müşteri bilgilerine sahip sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanır. Özel iç ağdaki sistemlere yalnızca vekil uygulamalar veya güvenlik duvarı cihazları üzerinden iletişim kurulur. İnternet üzerinden veya Kuruluş dış ağından görünür olan sunucu veya 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 Kuruluş iç ağına taşınması ve iç ağ IP adreslerine sahip olması sağlanır.

(13) Ağ üzerindeki kimlik ve erişim yönetimine yönelik kurulan etki alanı yönetim sunucuları gibi yapıların Kuruluşa özgü oluşturulmuş olması ve Kuruluş dışındaki başka bir etki alanı ya da benzerinin bir parçası olmaması esastır.

(14) Kuruluş, iç ağından dış ağa akan trafik içeriğini kontrol eder. Yapılacak içerik kontrolünün, zararlı IP adreslerine olan trafik akışını ve hassas müşteri verileri ile müşteri bilgilerinin 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.

(15) 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 konfigürasyonunda bulunmadığı halde açık durumda olan portların kapatılması sağlanır.

(16) Kuruluş, bilgi sistemleri ile ilgili yapılacak her türlü değişiklikte bilgi güvenliğine gereken özeni göstermekle yükümlüdür.

(17) Bilgi güvenliği yönetim sistemine ilişkin görev, yetki ve sorumluluk verilmiş olan personel, bilgi güvenliği yönetim sisteminin bilgi güvenliği konusundaki mevzuata, standartlara ve birinci fıkra kapsamında oluşturulan bilgi güvenliği yönetim çerçevesine uyum durumunu sürekli olarak izler, uyumun sağlanması için gerekli tedbirleri alır ve uyum durumunu Kuruluşun yönetim kuruluna yılda en az bir defa düzenli olarak raporlar.

(18) Kuruluş, personelin bilgi güvenliği hususlarında farkındalığını arttıracak, ilgili mevzuat ve yönergeler hakkında bilgi sahibi olmalarını sağlayacak gerekli faaliyetleri yürütür ve bu çalışmalarını belgeler.

(19) Kuruluş, telefonda verdiği hizmetlerin müşterilere sunulmasında görev alan personele sosyal mühendislik saldırıları ve bilinen diğer dolandırıcılık yöntemleri konusunda periyodik eğitimler aldırmak ve bu çalışanların güvenlik farkındalıklarını artırıcı çalışmalar yapmakla yükümlüdür.

(20) Kuruluş, internet aracılığıyla sunulan hizmetlerde, arayüzün kuruluşa ait olduğunun doğrulanmasını sağlayacak mekanizmaları tesis eder.

(21) Kuruluş, elektronik kanal üzerinden sunduğu hizmetlere ilişkin tüm yazılım ve mobil uygulamaların kaynağının kendisi olduğunun müşteri tarafından doğrulanabilmesini sağlar.

(22) Kuruluş, elektronik kanal üzerinden sunduğu hizmetlere ilişkin tüm yazılım ve mobil uygulamaların bilgi güvenliğini tehlikeye sokacak hususlar içermemesini sağlayacak önlemleri almakla ve güvenlik açıklarını giderecek gerekli yamaları ve güncellemeleri sağlamakla yükümlüdür.

(23) Kuruluş, mobil uygulamalarının kullandığı hassas müşteri verileri ile müşteri bilgilerinin, mobil uygulamanın kullanıldığı cihazda yer alan diğer yazılım ve uygulamalar tarafından erişilemez olmasını sağlayacak önlemler alır.

(24) Kuruluş, mobil uygulamalarının kullanıldığı cihazın kaybolması, çalınması, ele geçirilmesi gibi durumlarda, bu durumun müşteri tarafından kuruluşa bildirilmesini müteakip derhal cihazda bulunan hassas müşteri verileri ve müşteri bilgilerinin yetkisiz kişilerce

erişilemez olmasını sağlamakla ve bu kapsamda doğabilecek riskleri azaltmak için günün teknolojisine uygun önlemleri almakla yükümlüdür.

(25) Personelin iç ağdaki uygulama ve sistemlere kuruluşun dışından uzaktan erişim gerçekleştirmesine, ilgili kontrol mekanizmalarından geçerek işin ve günün şartlarının gerekleri doğrultusunda onaylanmadığı sürece izin verilmez. Uzaktan erişime izin verildiği durumlarda güçlü kimlik doğrulamaya dayanan güvenli bağlantı yöntemleri uygulanır, erişimlere ilişkin denetim izleri tutulur, bağlantının süresi ve bağlantının yapılabileceği cihazlar kısıtlanır ve personel belli aralıklarla kimliğini tekrar doğrulamaya zorlanır.

(26) Kuruluş, faaliyetleri ile ilgili olarak görevler ayrılığı ve görevin gerektirdiği kapsam kadar yetki prensipleri ile tutarlı etkin bir kimlik doğrulama ve erişim yönetimi yapısı oluşturmakla yükümlüdür.

(27) Kuruluş, bilgi güvenliği yönetim sisteminin etkinliğini yılda en az bir defa düzenli olarak test eder, test sonuçlarını kayıt altına alır ve üst yönetime raporlar.

(28) Kuruluş, kullanmakta olduğu veya ihtiyaç duyabileceği uygulamalar için bir beyaz liste oluşturur ve bilgi sistemleri unsurlarında sadece ihtiyaç duyulan uygulamaların yüklü olmasını sağlar, bu unsurlara beyaz liste dışındaki uygulamaların yüklenmesini ve bu uygulamaların çalıştırılmasını engelleyecek önlemleri alır.

(29) Kuruluş, bilgi sistemleri unsurları üzerinde beyaz listede yer almayan herhangi bir uygulamanın yüklü olup olmadığına yönelik düzenli olarak tarama gerçekleştirir.

(30) Kuruluş, bilgi sistemleri unsurlarını gerekli sıklıkta ve düzenli bir şekilde kontrol ederek zararlı yazılımların ve güvenlik açıklarının tespit edilmesini sağlayacak altyapıyı oluşturur.

(31) Kuruluş, e-posta sunucusuna gelen ve giden e-postaları tarayarak zararlı yazılım barındıran ya da kuruluşun iş ihtiyaçları doğrultusunda gereksiz olan eklentiler içeren e-postaları engelleyecek çözümler kullanır. Kuruluştan gönderilen e-postalar için e-posta sunucularında gönderici kimliğini doğrulayıcı teknikler kullanılır.

(32) Kuruluşun bilgi sistemleri unsurları, bu unsurlara 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 bağlanacağı bağlantı arayüzlerinin ön tanımlı olarak kullanıma kapatılarak bu tür cihazların kullanımının yalnızca iş gereksinimi olan personelle sınırlı tutulması ve harici cihazları kullanma denemesi yapılan durumların da takip edilmesi sağlanır.

(33) Personelin, zorunlu iş gereksinimi olmadıkça yerel yönetici yetkisine sahip olmasına izin verilmez. Buna yönelik bir ihtiyaç olması durumunda iş birimi ve bilgi sistemleri yöneticisinin onayını müteakip söz konusu yetkinin tanımlı ve kayıtlı prosedürler çerçevesinde ve iş bitiminde tekrar geri alınacak şekilde verilmesi sağlanır.

Veri güvenliği ve mahremiyeti

MADDE 9 – (1) Kuruluş, faaliyetlerinin yürütülmesi sırasında edindiği ve bilgi sistemleri aracılığıyla işlediği, ilettiği veya sakladığı hassas müşteri verileri ve müşteri bilgilerinin gizliliğini ve güvenliğini sağlamaya ve kuruluş dışına sızmasını önlemeye yönelik politika ve prosedürleri yazılı olarak oluşturur ve bu amaçla gerekli tedbirleri alır.

(2) Kuruluş, faaliyetleri ile ilgili olarak kullandığı bilgi sistemlerinde verilerin gizliliğini sağlayacak önlemleri alır. Verilerin gizliliğini sağlamak üzere alınan önlemlerin, verilerin gizlilik derecesine uygun olması gerekir.

(3) Hassas müşteri verileri, müşteri bilgileri ile rekabete duyarlı verilerin şifrelenmiş bir şekilde ya da güvenli bileşenlerde saklanması esastır. Kullanılacak şifreleme tekniklerinin günün teknolojisi, ulusal ve uluslararası standartlar ile uyumlu olması, veri güvenliği ve mahremiyeti konusunda makul güvence sağlaması ve güvenilirliğini yitirmemiş olması esastır.

(4) Hassas müşteri verileri, müşteri bilgileri ve rekabete duyarlı verilerin kablosuz biçimde veya internet üzerinden iletilmesi halinde, bu iletim uçtan uca güvenli iletişim ile gerçekleştirilir.

(5) Veri barındıran bilgi sistemleri unsurlarının kullanımının durdurulması durumunda, içerdikleri verilerin gizlilik derecesine uygun olarak güvenli bir şekilde gecikmeksizin imha edilmesi sağlanır.

(6) Hassas müşteri verileri, Kanun, Yönetmelik ve bu Tebliğ kapsamında izin verilen haller saklı kalmak kaydıyla, dış hizmet sağlayıcılar ve kanunlarla açıkça yetkili kılınan merciler dışındaki taraflara verilemez. Müşteri bilgileri, kanunla açıkça yetkili kılınan merciler dışındaki taraflara, ancak müşterinin paylaşım sınırları hakkında aydınlatılması ve müşterilerin açık rızasının alınması kaydıyla verilebilir. Müşterinin açık rızası, 6698 sayılı Kanuna uygun şekilde güvenli yöntemlerle alınır. Elektronik ortamdaki bir sözleşme ile alınacak onay yalnızca ilk defa oturum açılırken ve müşterinin açıkça bilgilendirilmesi kaydıyla gerçekleştirilebilir. Müşterinin bilgilerini paylaşmaya dair rıza göstermesi verilecek hizmet için bir ön şart haline getirilemez.

(7) Kanun kapsamına giren işlemler ile ilgili olarak kişisel verilerin işlenmesi faaliyetlerinde, 6698 sayılı Kanun ve bu Kanun uyarınca yapılan düzenlemelerde yer alan hükümler öncelikli olarak uygulanır ve bu hükümler kapsamında belirlenmiş olan usul ve esaslara uyulması zorunludur.

Kimlik doğrulama

MADDE 10 – (1) Kuruluş, bilgi sistemlerinde gerçekleştirilen işlemlerde kullanılmak üzere yeterli ve etkin bir kimlik doğrulama sistemi kurar. Kurulacak kimlik doğrulama sistemi çerçevesinde personele tanımlanan roller ve sorumluluklar açık bir şekilde yazılı olarak oluşturulur.

(2) Kullanılacak kimlik doğrulama tekniklerine, sekizinci fıkra hükümleri saklı kalmak kaydıyla, yapılacak risk değerlendirmesi sonucuna göre karar verilir. Risk değerlendirmesi, bilgi sistemleri üzerinden gerçekleştirilmesi planlanan işlemlerin türü, niteliği, varsa doğuracağı finansal ve finansal olmayan etkilerin büyüklüğü, işlemin gerçekleştirilmesinde kullanılan ödeme aracı, işlem çeşitleri, işleme konu verinin hassaslık derecesi, talimata dayalı düzenli ödeme olması, müşterinin işlem limitleri, işlemin karşı tarafının güvenli alıcılar listesinde olması, kimlik doğrulama tekniğinin kullanım kolaylığı ve acil duruma özgü yetkilendirme ihtiyacı dâhil olmak üzere gerekli hususlar göz önünde bulundurularak gerçekleştirilir.

(3) Kuruluş, kimlik doğrulama sisteminin bilgi sistemlerinin hangi alt unsurları için geçerli olacağını ve kimlik doğrulama sisteminde hangi alt unsur için hangi kimlik doğrulama tekniklerinin kullanılacağını açıkça belirler.

(4) Kimlik doğrulama için günün teknolojisine uygun ve güvenli bir parola politikası belirlenir. Kimlik doğrulamada kullanılacak tek kullanımlık parolaların, ihtiyaç duyulan güvenlik seviyesini sağlayacak kadar uzun olması, yetkisiz kişilerce tespit ve tahmin edilmesine ilişkin riskleri asgari düzeye indirecek yöntemleri gözetmesi ve belirli bir süre için geçerli olması gerekir.

(5) Kimlik doğrulama için kullanılacak parola, değişken parola, tek kullanımlık parola cihazı, şifreleme gizli anahtarı, akıllı kart ve işlem doğrulama kodu gibi bileşenlerin güvenliği üretim aşamasından başlayarak kullanıcıya ulaştırılmasına dek sağlanır. İşlem doğrulama kodu aracılığıyla güçlü kimlik doğrulama unsurlarından hiçbiri hakkında bilgi edinilememesi, bilinen bir işlem doğrulama kodu ile geçerli başka işlem doğrulama kodlarının türetilememesi, işlem doğrulama kodlarının taklit edilememesi sağlanır. İşlem doğrulama kodunun üretilmesinde hata meydana gelmesi ya da üretilememesi halinde, kimlik doğrulama teşebbüsünde bulunan kişi tarafından hatanın hangi kimlik doğrulama unsurundan kaynaklandığının anlaşılamamasını sağlayacak önlemler alınır.

(6) Kuruluş, kimlik doğrulama için kullanılan verilerin gizliliğinin, bütünlüğünün ve güvenliğinin sağlanarak saklanması ve aktarılması için gerekli altyapının oluşturulmasını sağlar. Kimlik doğrulama işlemleri esnasında, müşterinin bildiği kimlik doğrulama unsurları ile tek kullanımlık parola veya işlem doğrulama kodu gibi bileşenlerin, personelin dahli ve erişimi olmadan ilgili kanal üzerinden girişinin yapılması sağlanır.

(7) Kimlik doğrulamada;

a) Kullanıcıya sisteme girdiği anda önceki başarısız kimlik doğrulama teşebbüsleri hakkında bilgi verilmesi,

b) Başarısız teşebbüslerin belirli bir sayıyı aşması halinde ilgili kullanıcı erişiminin bloke edilmesi,

c) Başarısız kimlik doğrulama teşebbüsleri sonrasında, kullanıcı adının sistemde olmadığı veya parolanın hatalı girildiği gibi bilgilerin verilmemesi,

ç) Belli bir süre işlem yapılmayan veya güvenli bir şekilde çıkış yapılmadığından arka planda çalışır şekilde kalan oturumun belirli bir süre sonra sonlandırılması,

d) Birden fazla müşterinin aynı ödeme hesabını kullanmaları ya da aynı anda farklı oturumlar açabilmeleri konusunda yetkilendirildiği durumlar hariç olmak üzere, aynı müşteri için aynı anda birden fazla oturum açılmaya çalışılması durumunda buna izin verilmemesi ve müşterinin uyarılması,

gerekir.

(8) Müşteriler tarafından elektronik kanal üzerinden yapılan ve finansal sonuç doğuran veya finansal sonuç doğurmayan işlemlerde, düzenlemelerde açıkça aksine imkan tanınmadığı sürece güçlü kimlik doğrulama kullanılması esastır. Güçlü kimlik doğrulama esnasında müşterinin sahip olduğu bileşenin müşteriye özgü olması ve taklit edilememesi esastır. Kimlik doğrulamada T.C. Kimlik Kartının kart PIN'i veya biyometrik veri ile birlikte kullanılması veya güvenli elektronik imzanın kullanılması hallerinde bu fıkranın gerekleri yerine getirilmiş sayılır. Kuruluşun mobil uygulamasının kontrolünde olmayıp cihaz üreticisi kontrolünde olan parola, PIN ya da biyometrik veriler, bu fıkra kapsamında güçlü kimlik doğrulama unsurları olarak kullanılamaz.

(9) 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanuna ilişkin yükümlülükler kapsamında, 22 nci maddeye göre sözleşme kurulması sonrasında kimlik tespiti gerektiren müteakip ödemeler elektronik kanaldan başlatıldığında, güçlü kimlik doğrulama yöntemi kullanılır.

(10) Ödeme aracının ve kimlik doğrulama aracının müşteriye ulaştırılmasında kullanılan telefon numarası ve adres gibi bilgilerin, müşteri tarafından tanımlanan güvenli alıcılar listesinin ve tek bileşene dayalı kimlik doğrulama kullanılarak yapılabilecek işlem listesinin değiştirilmesinde güçlü kimlik doğrulama yöntemi kullanılır.

(11) Hassas müşteri verilerine erişim sağlandığında veya düzenli ödeme talimatı verilirken güçlü kimlik doğrulama yöntemi kullanılır.

(12) 5549 sayılı Kanuna ilişkin yükümlülükler saklı kalmak üzere, dokuzuncu fıkraya göre güçlü kimlik doğrulama ile gerçekleştirilmesi gereken işlemler için müşterinin sözleşme ile ya da güvenli yöntemlerle onayının alınmış olması ve ödeme işleminin güvenli alıcılar listesindeki bir alıcı ile gerçekleştirilmesi halinde güçlü kimlik doğrulama uygulanması zorunlu değildir.

(13) Müşteri tarafından gerçekleştirilecek finansal işlemler için kuruluş tarafından müşteri onayını almak üzere işlem doğrulama kodu üretilir ve işlem bilgisi ile birlikte müşteriye sunularak müşteri onayı alınır. Finansal sonuç doğurmayan işlemler için ise işlem doğrulama kodu kullanılıp kullanılmayacağına kuruluş tarafından yapılacak ikinci fıkrada belirtilen risk değerlendirmesine göre karar verilir ve işlem doğrulama kodu kullanılmayan işlemlerle ilgili olarak gerçekleştirilen işlemin müşteri tarafından yapıldığını ispat etme yükümlülüğü kuruluşa ait olur. Tek bileşene dayalı kimlik doğrulama yapıldığında, işlem doğrulama kodunun kimlik

doğrulamada kullanılandan farklı bir bileşen oluşturacak şekilde müşteriye onay için sunulması ile güçlü kimlik doğrulama yerine getirilmiş kabul edilir.

(14) Kuruluşun bu madde uyarınca gerekli hallerde güçlü kimlik doğrulama mekanizması sunmaması halinde, gerçekleştirilen işlemlerin müşteri tarafından yetkilendirilmiş olduğunu ispat yükümlülüğü kuruluşa aittir.

(15) Anonim ön ödemeli araçlarla ilgili işlemlerde güçlü kimlik doğrulama zorunluluğu yoktur.

(16) Müşterinin kimliğini tespit etmeye yarayan ve resmi kimlik belgesi yerine geçen belgeler üzerinde yer alan bilgiler ile anne kızlık soyadı, elektronik kanallar üzerinden sunulan Kanun kapsamındaki faaliyetlerin sunulması esnasında hiçbir aşamada kimlik doğrulama amacıyla kullanılamaz. Kimlik doğrulamada müşterinin bildiği bileşen olarak bir güvenlik sorusunun kullanılması durumunda, güvenlik sorusunun resmi kimlik belgesi yerine geçen belgeler üzerinde yer alan bilgilerden birine ilişkin olmaması ve cevabının müşterinin kendisi tarafından belirleniyor olması gerekir.

(17) Bir kimlik doğrulama bileşeninin bir müşteri ile ilk defa ilişkilendirilmesi uzaktan gerçekleştirilecekse, ilişkilendirme güvenli yöntemlerle ve güçlü kimlik doğrulama gerçekleştirilerek yapılır.

(18) Kuruluş, Kanun kapsamında gerçekleştirilen işlemler için inkâr edilemezliği sağlayacak teknolojik ve hukuki altyapıyı oluşturur.

(19) Kuruluş, bilgi sistemlerinin kullanımında oturum güvenliğini sağlayacak tedbirleri ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemleri alır.

(20) Kuruluş güçlü kimlik doğrulama kapsamında müşterisinin tercih ettiği kimlik doğrulama bileşenlerinin farklı bileşen sınıflarına ait olmasını temin eder. Kuruluş, güçlü kimlik doğrulama sürecinde müşterinin sahip olduğu bileşen sınıfı olarak SMS OTP ya da SMS ile işlem doğrulama kodu kullanabilir. Kuruluşun mobil uygulamasını yükleyerek etkinleştirmiş olan müşterinin güçlü kimlik doğrulaması kapsamında oturum açılması ya da oturumun devamında herhangi bir işlemin doğrulanması için SMS OTP ya da SMS ile işlem doğrulama kodu kullanılması halinde bu faktör güçlü kimlik doğrulamada müşterinin sahip olduğu bileşen olarak sayılamaz. Kuruluşun mobil uygulamasının ilk kurulumu, etkinleştirilmesi, yeniden etkinleştirilmesi aşamalarında ya da kuruluşun mobil uygulamasının kullanılamaz hale gelmesi durumunda güçlü kimlik doğrulama kapsamında müşterinin sahip olduğu bileşen olarak SMS OTP ile ya da SMS ile işlem doğrulama kodu kullanılması bu fıkra hükmüne aykırılık teşkil etmez.

(21) Kimlik doğrulama esnasında SMS teknolojisinin kullanılması durumunda, kuruluş, elektronik haberleşme işletmecileriyle SIM kart değişikliği gerçekleştirmiş veya numara taşıma yoluyla elektronik haberleşme işletmecisini değiştirmiş müşterileri tespit edebilmek için gerekli altyapıyı oluşturur ve bu tür değişiklikler yapmış müşteriye, yapılan değişikliğe ilişkin müşterinin açık teyidi alınmadığı sürece, değişikliğin yapıldığı tarihten itibaren 90 gün boyunca elektronik kanallar üzerinden gerçekleşecek işlemler kapsamında yapılacak kimlik doğrulamada SIM karta dayalı bir yöntem kullanılamaz. Aksi durumda gerçekleştirilen her türlü işlem için gerçekleştirilen işlemin müşteri tarafından yapıldığını ispat etme yükümlülüğü kuruluşa aittir.

(22) Güçlü kimlik doğrulamada kullanılacak müşterinin bildiği bileşenin, mobil uygulama veya internet tarayıcısı tarafından hatırlanarak veya başka lokal kimlik doğrulama yöntemlerine bağlanarak otomatik olarak gönderilmemesi gerekir ve müşterinin bildiği bileşenin müşteri tarafından girilmesi zorunlu tutulur.

(23) İnternet şubesinde kimlik doğrulama işlemi gerçekleştirilirken, oturum açılmadan önce, müşteri tarafından güçlü kimlik doğrulama ile önceden belirlenmiş olan bir karşılama mesajının veya resminin, müşteriye gösterilmesi sağlanır.

(24) İnternet şubesinde güçlü kimlik doğrulama işlemi gerçekleştirilirken, müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanacak şekilde işlem doğrulama kodu üretilir. İşlem doğrulama kodunun, müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanmasının mümkün olmadığı hallerde, yirminci fıkra hükümleri saklı kalmak kaydıyla, müşteriye SMS ile doğrulama kodu iletilebilir.

(25) Mobil uygulama için tanımlanan uygulama PIN'inin veya kimlik doğrulama unsuru olarak belirlenmiş olan müşteriye ait bir biyometrik verinin müşteriye özgü bir şifreleme anahtarına erişmek üzere kullanılması ve bu şifreleme anahtarı yoluyla müşteriyle ilintili biricik bir bilginin kuruluş nezdinde çevrim içi olarak doğrulanması halinde, güçlü kimlik doğrulama yerine getirilmiş kabul edilir.

(26) Mobil uygulamanın etkinleştirilerek müşterinin sahip olduğu bir kimlik doğrulama unsuru olarak kullanılması şartıyla, müşterinin yalnızca mobil uygulama aracılığıyla müşteri ve hesap bilgilerini görüntülemek istemesi, ödemenin göndereni ve alıcısının aynı olması, müşterinin talimatına istinaden gerçekleştirilen düzenli bir ödeme olması, ödeme işleminin daha önce tanımlanmış güvenli alıcılar listesindeki bir alıcı ile gerçekleştirilmesi ve kuruluşun ikinci fıkrada belirtilen risk değerlendirmesi sonucunda bu yönde karar verdiği, bu madde başta olmak üzere ilgili düzenlemelerde güçlü kimlik doğrulamanın kullanılmasının zorunlu tutulmadığı diğer ödeme işlemleri esnasında ilave bir kimlik doğrulama unsuruna gerek kalmadan tek bileşene dayalı kimlik doğrulama sekizinci fıkraya aykırılık teşkil etmez. Tek bileşene dayalı kimlik doğrulama yapılan bu işlemlerle ilgili olarak gerçekleştirilen işlemin müşteri tarafından yapıldığını ispat etme yükümlülüğü kuruluşa ait olur. Müşterinin mobil uygulamada ilk defa oturum açması veya güçlü kimlik doğrulama ile açtığı son oturumun üzerinden 90 günden daha fazla bir süre geçmiş olması halinde, güçlü kimlik doğrulamaya tabi tutulması esastır.

(27) Finansal olmayan işlemler dahil olmak üzere telefon ile gerçekleştirilecek işlemlerde güçlü kimlik doğrulama uygulanması esastır. Güçlü kimlik doğrulama uygulanmadan telefon aracılığıyla hizmet vermek üzere müşteriyi karşılayan personelin 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.

(28) Kayıp, çalıntı ve dolandırıcılık gibi riskli işlem bildirimi durumunda, personele bağlanan müşterilerin kimlik doğrulaması yapılmaksızın personelin bilmesi gerektiği kadar müşteri bilgisine erişebilmesi sağlanır ve gerekli güvenlik önlemleri alınır.

(29) Telefon bağlantısı olmaksızın ya da bağlantının sonlanması halinde kayıp, çalıntı ve dolandırıcılık gibi riskli işlem bildirimi haricinde müşteriye ilişkin herhangi bir işlem gerçekleştirilemez.

(30) Müşterinin telefon kanalıyla, elektronik kanallarda kullandığı kimlik doğrulama veya telefon bilgilerinde değişiklik gerçekleştirmek istemesi halinde bu değişikliğin personelin dahli ve erişimi olmadan otomatik sistemler üzerinden gerçekleştirilmesi sağlanır.

(31) Müşterinin telefon ile aranmasının gerektiği durumlarda, arama gerçekleştirilmeden önce telefonun başka bir numaraya yönlendirilmemiş olduğuna ilişkin kontroller işletilir.

(32) Banka, bu maddede düzenlenen kimlik doğrulama kuralları bakımından istisna getirmeye veya ilave güvenlik önlemleri ihdas etmeye yetkilidir.

Erişim yönetimi

MADDE 11 – (1) Kuruluş, personelin sisteme dâhil olan ağlara, alt sistemlere, uygulamalara, verilere ve fiziksel ortamlara erişimine ilişkin yetki ve sınırlandırmaları, personelin görev, yetki, sorumluluk ve ayrıcalıkları kapsamında işin gerektirdiği bilgiye erişimine imkân verecek şekilde açıkça belirler ve yetkisiz erişimleri engellemek üzere gerekli tedbirleri alır.

(2) Kuruluş, uygulanacak erişim kontrollerini ve atanacak yetkileri açık bir şekilde belirler ve yazılı olarak oluşturur. Bilgi sistemlerine erişim yetkisi olan kişilerin bu yetkileri yılda en az bir defa düzenli olarak gözden geçirilir.

(3) Erişim yönetimi kapsamında oluşturulacak kuralların görevler ayrılığı prensibini gözetmesi ve 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 suiistimalleri önlemeye yönelik risk azaltıcı veya telafi edici ilave kontroller tesis edilir.

(4) Erişim yönetimi kapsamında yetkilendirmelerin, personelin görev ve sorumlulukları göz önünde bulundurularak, sadece ihtiyaç duydukları kapsam ve süre ile sınırlı olacak şekilde yapılması esastır.

(5) Kuruluş, erişim yönetimi kapsamında olağandışı saatlerde yapılan girişleri, normal giriş sürelerine ilişkin aşımları, genel olarak çalışılan bilgisayar dışındaki bir bilgisayardan gerçekleştirilen işlemleri takip ederek olağandışı durumları tespit edebilmek ve uzun süredir hiç bir aktivite göstermeyen pasif hesapları tespit ederek artık bu yetkiye ihtiyaç duyulmaması durumunda yetkiyi kaldırabilmek için gerekli önlemleri alır.

(6) Erişim yönetimi kapsamında mümkün olduğu ölçüde ayrıcalıklı yetkiler tanımlanmaması esastır. Ayrıcalıklı yetkilerin tanımlanması durumunda ise bu tür yetkilerin sadece mutlak suretle ihtiyaç duyulması durumunda atanması ve sadece ihtiyaç duyulan konularla sınırlı olacak şekilde kullanılması, bu yetkilerin kullanımı esnasında kimlik doğrulama ile birlikte ilave güvenlik kontrollerinin tesis edilmesi, bu tür yetkilerin ortaklaşa kullanımının engellenmesi ve ortak kullanım gerektiren durumlarda yetkiyi kullanan kişilere sorumluluk atayacak tekniklerin kullanılması esastır.

(7) Acil durumlara özgü yetkilendirmeler geçici ve tüm süreç kayıt altına alınarak yapılır.

(8) Personelin görev ve pozisyon değiştirmesi ve işten ayrılması da dâhil olmak üzere personele ilişkin tüm değişiklikler sonrasında, erişim yönetimi kapsamında gerekli değişiklikler gecikmeksizin yapılır.

(9) Kuruluş, bilgi sistemleri üzerinde işlem yapma yetkisi bulunan tüm personel için biricik tanımlama kodları belirler ve zorunlu olmadığı müddetçe ortak veya ön tanımlı hesaplar kullanılmaz. Ortak veya ön tanımlı hesapların kullanımının zorunlu olduğu durumlarda ise bu hesaplar ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edilir.

(10) 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 gerekenlerle sınırlandırılır, erişim yetkileri yılda en az bir defa düzenli olarak gözden geçirilir ve güncellenir.

(11) Onuncu fıkra kapsamında yetkilendirilenler dışında kalan personel, ziyaretçi, dış hizmet sağlayıcı çalışanı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimleri onay mekanizmasına tabi tutulur, veri merkezindeki çalışmaları boyunca faaliyetleri yakından izlenir ve kendilerine refakat edilir.

(12) Veri merkezlerine ve sistem odalarına yapılan fiziksel erişimlerin denetim izleri tutulur. Bu alanlarda kör nokta içermeyecek ve en az bir yıl süreyle kayıt saklayacak şekilde kamera kayıt sistemleri kullanılır. Kamera kayıt sistemleri tarafından kaydedilen görüntülerin farklı bir yerleşkede yedeklenmesi sağlanır. Herhangi bir uyuşmazlık veya şüpheli durum halinde ilgili kayıtların saklama süresi söz konusu durum giderilinceye kadar uzatılır.

Güvenlik açıkları ve ihlalleri

MADDE 12 – (1) Kuruluş, bilgi güvenliği yönetim çerçevesi ile uyumlu bir şekilde, bilgi sistemlerine yönelik olası güvenlik ihlallerinin araştırılmasını, güvenlik ihlallerinin önlenmesi için alınması gereken uygun tedbirlerin belirlenmesini, güvenlik ihlalinin gerçekleşmesi halinde ihlalin tespit edilerek zamanında müdahale edilebilmesi için gerekli tedbirlerin

alınmasını, gerçekleşen güvenlik ihlallerinin ve tespit edilen güvenlik açıklarının değerlendirilerek kayıt altına alınmasını sağlar.

(2) Kuruluş, sahip olduğu ve sistemle ilişkili olan tüm sunucular ile iletişim ağını ilk işletime alınmadan önce ve sonrasında düzenli aralıklarla yılda en az altı defa zafiyet taramasından geçirir.

(3) Kuruluş, bilgi sistemlerinin, bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından, gerçekleşebilecek iç ve dış tehditleri kapsayan senaryolar doğrultusunda yılda en az bir defa düzenli olarak sızma testine tabi tutulmasını sağlar.

(4) Sızma testleri EK-5'te yer alan usul ve esaslar çerçevesinde uygulanır.

(5) Kuruluş, olası ve gerçekleşmiş güvenlik ihlallerinin değerlendirilmesi ile zafiyet taraması ve sızma testleri sonucunda tespit ettiği öncelikli bulguları, bulguların önem derecelerini, birlikte oluşturabilecekleri riskleri, tespit edildiği varlıkların değerini ve sızma testi raporlarında yer alan önerileri dikkate alarak mümkün olan en kısa süre içerisinde giderir ve bu bulgular giderilinceye kadar uygun koruyucu tedbirlerin alınmasını sağlar. Bulguların makul bir süre içerisinde giderilmesi, bu amaçla oluşturulan ve kuruluş yönetim kurullarınca onaylanan bir eylem planı çerçevesinde takip edilir. Alınan tedbirlerin tespit edilmiş olan güvenlik açığını giderdiği veya güvenlik açığından kaynaklanan riskleri kabul edilebilir düzeye indirdiği kontrol edilir.

(6) Kuruluş, gerçekleşen güvenlik ihlallerini, sızma testinin sonuçlarını ve tespit edilen kritik güvenlik açıklarını, bunların giderilmesine yönelik alınan tedbirleri ve sonuçlarını içeren raporu yılda en az bir defa Bankanın uygun gördüğü yöntemle Bankaya sunar.

(7) Kuruluş, gerçekleşen güvenlik ihlalleriyle ilgili delilleri en az on yıl süreyle güvenli bir şekilde muhafaza eder.

Denetim izlerinin oluşturulması

MADDE 13 – (1) Kuruluş, müşteri bilgileri ve bilgi sistemlerine gerçekleştirilen fiziksel veya mantıksal erişimler ile yetkisiz erişim teşebbüslerine ve bilgi sistemlerinde gerçekleşen Kanun kapsamındaki faaliyetler ile ilgili yapılan işlemlerin takibine imkân verecek şekilde denetim izi kayıt sistemi oluşturur.

(2) Denetim izleri, ayrıntılı incelemeye ve taramaya imkân verecek, denetime hazır, gizliliği, bütünlüğü, güvenliği sağlanarak yedekli bir şekilde ve zaman damgalı olarak en az on yıl süreyle saklanır.

(3) Denetim izi kayıt sisteminde tutulacak kayıtlar asgari olarak, erişimin veya işlemin niteliğine göre;

a) İşlemin türü ve işlemin ayırt edici tanımlayıcısı,

b) İşlem tutarı, işlem tarihi, işlem saati,

c) Anonim ön ödemeli araçlar ile gerçekleşen işlemler hariç olmak üzere müşteri tanımlayıcı bilgisi,

ç) Personelin, aracı personelin ve dış hizmet sağlayıcı çalışanının kimlik bilgisi,

d) Erişimin veya işlemin gerçekleştiği uygulama bilgisi,

e) Kaydı oluşturan işlem ya da olayla birlikte, gerçekleştirilen değişikliğin ne olduğunu gösteren bilgi,

hususlarını içerir.

(4) Personelin kendi faaliyetlerine ilişkin denetim izlerine müdahalesi engellenir.

(5) Kuruluşun, web servisleri, API ya da benzeri metotlarla diğer kurum veya kuruluşlar nezdinde tutulan verilere ilişkin yaptığı sorgulamalar ve bu sorgulamaları hangi amaçla yaptığına ilişkin denetim izleri de bu madde kapsamında değerlendirilir.

(6) Denetim izleri güvenilir ortamlarda yedeklenir ve ihtiyaç duyulması halinde 24 saatten fazla olmayacak şekilde makul bir sürede bu yedeklerden geri dönüş sağlanarak inceleme yapılmasına imkân verecek şekilde kuruluş nezdinde saklanır.

(7) Denetim izi kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(8) Herhangi bir nedenden denetim izi kayıt sisteminin durması halinde, denetim izi kayıt sistemi tekrar devreye alınana kadar herhangi bir işlemin gerçekleşmesine izin verilmez.

(9) Bilgi sistemleri konusunda kuruluş tarafından dış hizmet alınması halinde, dış hizmet sağlayıcının denetim izi kayıt sisteminin bu madde hükümlerine uygunluğundan kuruluş sorumludur.

(10) Telefonla verilen hizmetlerde müşterinin gerçekleştirdiği işlemlere ilişkin ses kayıtları için bu maddede belirtilen hükümler uygulanır. Ses kayıtlarının güvenilir delillerin elde edilmesine imkan verecek ve sorumlulukların açıkça belirlenmesini sağlayacak nitelik ve kalitede olması esastır.

Bilgi sistemleri süreklilik planı

MADDE 14 – (1) Kuruluş, Yönetmeliğin 30 uncu maddesi uyarınca oluşturulan iş sürekliliği planının bir parçası olarak bilgi sistemleri süreklilik planı hazırlar.

(2) Bilgi sistemleri süreklilik planı;

a) İş sürekliliği planı ile uyumlu olacak şekilde belirlenecek bilgi sistemleri süreklilik hedeflerini ve bu hedeflere ulaşmayı sağlamak üzere oluşturulacak yedekleme ve hatadan kurtarma prosedürleri ile kullanılacak kaynakları,

b) Planın hayata geçmesini gerektiren olayın kaynağını, yarattığı hasarı, potansiyel boyutunu ve etkisini, etkilediği tarafları tespit etmeye ve tespitlerin ilgili yönetim birimlerine ulaştırılmasını sağlamaya yönelik süreçleri,

c) Planın hayata geçirilmesine ilişkin karar alma süreciyle ilgili kriter ve prosedürler ile plan devreye girdiğinde rol alacak kişi veya grupların görev, yetki ve sorumluluklarını,

ç) İlgili paydaşlar ile iletişim yöntemini,

d) Plan kapsamında verilen kararların ve hayata geçirilen eylemlerin kayıt altına alınma yöntemini,

içerir.

(3) Bu madde uyarınca hazırlanacak bilgi sistemleri süreklilik planı kapsamında, bilgi sistemleri unsurlarının ve bunlar üzerinde bulunan verilerin önem düzeyi değerlendirilerek her bir unsur için kabul edilebilir kesinti süreleri ile kabul edilebilir veri kayıpları belirlenir ve belirlenen bu limitler doğrultusunda unsurlara ilişkin kurtarma prosedürleri geliştirilir.

(4) Kuruluş, bilgi sistemleri süreklilik planı kapsamında gerekliliklerin ortadan kalkmasının ardından ikincil merkezden birincil merkeze herhangi bir kayıp olmadan geri dönüşün sağlanmasına yönelik prosedürleri hazırlar.

(5) Kuruluş, bilgi sistemleri süreklilik planının etkinliğini yılda en az bir defa düzenli olarak test eder. Test, faaliyetlerin bir günlük işleyişinin ikincil merkez üzerinden sorunsuz bir şekilde gerçekleştirilmesini de kapsar. 15 inci maddenin dördüncü fıkrası uyarınca ikincil merkezi bulunmayan kuruluşlar testlerini uzaktan çalışma şeklinde icra edebilir. Kuruluş, bu testleri temsilci ve şubeleri ile bilgi sistemlerine bağlantısı bulunan diğer kuruluşları ve üçüncü taraf hizmet sağlayıcıları da dâhil edecek şekilde planlar.

İkincil merkez, ikincil sistem ve veri yedekleme merkezi

MADDE 15 – (1) Kuruluş, faaliyetlerinin kesintisiz devam etmesini sağlamak amacıyla ikincil merkez ve sistemleri kurmak ve bunları dönemsel olarak test etmek zorundadır.

(2) İkincil sistemlerin tasarımının, acil ve beklenmedik durumlar karşısında birincil sistemlerde yaşanabilecek sorunların yedek sistemlerde de yaşanmasını engelleyecek şekilde yapılmasına özen gösterilir.

(3) Kuruluş, acil ve beklenmedik durumlar sonucunda birincil sistemde bulunan verilerin kaybının önlenmesi amacıyla veri yedekleme merkezi oluşturmakla yükümlüdür. Veri yedekleme merkezi, veriye yetkisiz erişim riskleri dikkate alınarak tasarlanır ve asgari olarak birincil sistemlerle aynı seviyede güvenlik özellikleri içerir.

(4) Kuruluş, acil ve beklenmedik durumların ortaya çıkması nedeniyle birincil merkezin kullanılamaz hale gelmesi durumunda faaliyetlerinin kesintisiz devam etmesini sağlamak amacıyla birincil merkezden farklı bir yerde ikincil bir merkez oluşturur, bu durumlarda görev alacak acil durum personelini ve bunların görevlerini belirler ve acil durum personelinin bu merkezde çalışabilmesi için gerekli önlemleri alır. İkincil merkezin, acil durum personelinin yedek sistemleri ve veri yedekleme merkezlerini de etkin bir şekilde kullanabilmesini sağlayacak şekilde tasarlanması şarttır. Uzaktan çalışma imkanlarının olması ve acil ve beklenmedik durumların ortaya çıkması nedeniyle birincil merkezin kullanılamaz hale geldiği hallerde faaliyetlerinin kesintisiz devam etmesini sağlayacak önlemleri almış olmak kaydıyla ikincil merkez oluşturulması şartı uygulanmayabilir.

(5) İkincil merkezin, ikincil sistemlerin ve veri yedekleme merkezinin yeri, acil ve beklenmedik durumların yedekleri birincil sistem ve merkezlerle aynı anda ve oranda etkilemesini engelleyecek şekilde belirlenir.

Bilgi sistemlerine ilişkin dış hizmet alım sürecinin yönetimi

MADDE 16 – (1) Kuruluş, bu maddede yer alan şartlar ile Kanun ve ilgili alt düzenlemelerin gerektirdiği yükümlülüklerin yerine getirilmesi bakımından, bilgi sistemleri yönetimi, içerik tasarımı, erişim, kontrol, güncelleme, bilgi ve rapor alma gibi fonksiyonlarda karar alma gücünün ve sorumluluğun kuruluşta olması şartıyla bilgi sistemlerinin bütünü veya bir kısmı için dış hizmet alımı yapabilir.

(2) Kuruluş üst yönetimi, bilgi sistemleri kapsamında dış hizmet alımına ilişkin olarak, söz konusu hizmetin dış hizmet alımı yoluyla gerçekleştirilmesinin kuruluş açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve dış hizmet sağlayıcı ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak yeterli bir gözetim yapısı oluşturur. Bu kapsamda kuruluş üst yönetimi, dış hizmet alımı yoluyla gerçekleştirilen servisler için asgari olarak; servisin erişilebilirliğini, performansını, kalitesini, bu servis kapsamında gerçekleşen güvenlik ihlali olayları ile dış hizmet sağlayıcının güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu takip eder ve yılda bir kez yönetim kuruluna raporlar. Performans göstergesi olarak asgari düzeyde bu maddenin dokuzuncu fıkrasında belirtilen dış hizmet alım sözleşmesinde yer alan hizmet seviyesi tanımları kullanılır.

(3) Kuruluş, bilgi sistemlerine ilişkin konularda dışarıdan hizmet alımı yolunu seçtiğinde aşağıdaki kurallar geçerlidir:

a) Kuruluşun ve kuruluş üst yönetiminin sorumluluğu devam eder.

b) Kuruluşun ilgili taraflara karşı yükümlülükleri devam eder.

c) Kanun ve Yönetmelik kapsamında kuruluşa faaliyet izni verilmesi ve faaliyet izninin sürdürülmesi konusunda kuruluşun uyacağı koşullarda herhangi bir değişiklik olmaz.

(4) Kuruluş, birinci fıkra uyarınca dışarıdan hizmet aldığında;

a) Dış hizmet sağlayıcı kuruluşun seçiminde gerekli özeni göstermekle,

b) Dışarıdan hizmet alımını, iç kontrol ve risk yönetim çerçevesinin kalitesini düşürmeyecek ve Bankanın kuruluşa ilişkin denetim faaliyetlerinin etkinliğini azaltmayacak şekilde yapmakla,

c) Dış hizmet alımına ilişkin hususları iş sürekliliği planını da göz önünde bulundurarak düzenlemekle,

ç) Dış hizmet sağlayıcı kuruluşun yükümlülüklerini sözleşme ile netleştirmekle,

d) Dışarıdan hizmet alımının doğuracağı ilave riskleri göz önünde bulundurarak bu riskleri etkin bir şekilde yönetmek için gerekli önlemleri almakla,

e) Dış hizmet alımlarında kendisine, personeline ve müşterilerine ilişkin verilerin gizliliği ve güvenliği için gerekli önlemleri almakla,

f) Dış hizmet alımının, planlananın dışında sonlanması veya kesintiye uğraması durumlarına ilişkin risklerin yönetilmesine uygun bir çıkış stratejisinin belirlenmesini sağlamakla,

yükümlüdür.

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

(6) Kuruluş dış hizmete konu edilen faaliyetler bakımından dış hizmet sağlayıcının işlemlerinden sorumludur.

(7) Kuruluş her türlü veriyi işlemek, saklamak ve iletmek için bir dış hizmet olarak yurt içinde tesis edilmiş bulut bilişim hizmetlerini kullanabilir. Ancak hassas müşteri verilerini, rekabete duyarlı verileri, kişisel verileri veya müşteriyle ilintilendirilebilir ve onu belirli ya da belirlenebilir kılan her türlü bilgiyi işleyecek, saklayacak ve iletecek şekilde bulut bilişim hizmetinin alınması, bu dış hizmetin ancak sadece kuruluşa tahsis edilmiş donanım ve yazılım kaynakları üzerinden sunulduğu özel bulut hizmet modeli ile alınması halinde mümkündür. Banka tarafından uygun görülen dış hizmet sağlayıcılar tarafından sunulması durumunda kuruluş, sadece ödeme hizmeti sağlayıcılarına veya bilgi sistemlerine ilişkin faaliyetleri ilgili mevzuat çerçevesinde yetkili bir otorite tarafından düzenlenen ve denetlenen diğer kredi kuruluşları veya finansal kuruluşlara tahsis edilmiş donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal olarak her ödeme hizmeti sağlayıcısına özgü ayrı kaynağın atandığı topluluk bulutu hizmet modeliyle dış hizmet alabilir. Topluluk bulutu hizmetinin, kuruluşun ana ortağı, iştiraki veya ana ortağının iştiraki olan ve bilgi sistemlerine ilişkin faaliyetleri ilgili mevzuat çerçevesinde yetkili bir otorite tarafından düzenlenen ve denetlenen bir kredi kuruluşu veya finansal kuruluş tarafından verilmesi, sadece ana ortak, iştirakleri ve ana ortağın iştiraklerine tahsis edilmiş donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal ayrıma gidilerek kuruluşa özgü ayrı bir kaynak atanması koşuluyla bu fıkra hükümlerine aykırılık teşkil etmez. Kuruluşun müşteri verisi içermeyen test ve geliştirme ortamları ve sistemleri için gerekli güvenlik tedbirlerini alarak bulut bilişim hizmeti alması halinde bu fıkra hükmü uygulanmaz.

(8) Dış hizmet sağlayıcılara verilecek erişim, işin gerektirdiği bilgiyle sınırlandırılır.

(9) Dış hizmet alımına ilişkin sözleşme, asgari olarak aşağıdaki hususları içerir:

a) Hizmetin kapsamına ve hizmet seviyelerine ilişkin tanımlamalar ile kuruluşun ve dış hizmet sağlayıcının hak ve yükümlülükleri.

b) Hizmetin sonlanma koşulları ile hizmetin sona ermesi durumunda dış hizmet sağlayıcının dış hizmet sunarken elde ettiği veri, bilgi, belge ve kayıtları imha etmesine ilişkin hükümler.

c) Dış hizmet sağlayıcının ve kuruluşun bilgi sistemleri süreklilik planı kapsamında yükümlülükleri.

ç) Dış hizmet alımı kapsamındaki tüm sistem ve süreçlerin kuruluşun kendi risk yönetimi, güvenlik ve gizlilik politikalarına uygun olmasını sağlayacak hükümler.

d) Sözleşmeye konu ürün ve hizmetlerin sahipliği ve fikri mülkiyet haklarına ilişkin hükümler.

e) Sözleşmede dış hizmet sağlayıcılar için yükümlülük teşkil eden hükümlerin, alt yükleniciler ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler.

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

g) Kuruluşun tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde dış hizmet sağlayıcı kuruluşlar için de uygulanmasını sağlayacak hükümler.

ğ) Dış hizmet alımı kapsamındaki faaliyetlerin kuruluş bünyesinde gerçekleştirilmesi durumunda, bağımsız denetim açısından hangi denetimlere tabi tutulması öngörülüyorsa, kapsam daraltılmasına gidilmeden aynı denetimlere tabi tutulmasını sağlayacak hükümler.

h) Dış hizmet sağlayıcıların, gerçekleştirdiği faaliyetlere ilişkin olarak Bankaca 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 tüm sistem ve şifreleri incelemeye hazır bulundurmak ve işletmekle yükümlü olduğuna ilişkin hükümler.

ı) Banka, kuruluş ve bağımsız denetim kuruluşunun, dış hizmet alınan konuyla ilgili olarak dış hizmet sağlayıcıdan her türlü bilgi ve belgeyi talep etme yetkisinin bulunduğuna ilişkin hükümler.

i) Bankanın talimatı ile kuruluşun bilgi sistemleri üzerinde gerçekleştirilmesi gereken değişikliklerin, alınan hizmet kapsamında dış hizmet sağlayıcı tarafından talimat süresi içerisinde yerine getirilmesini sağlayacak hükümler.

j) Dış hizmet alımı yoluyla gerçekleştirilen işlemlere ilişkin bilgi, belge ve kayıtların mülkiyetinin kuruluşa ait olduğuna ve kuruluşa ait bilgi, belge ve kayıtların gizliliğine ilişkin hükümler.

k) Sözleşme hükümlerinin herhangi bir nedenle ihlali durumunda izlenecek prosedürlere ilişkin hükümler.

(10) Kuruluş, Kanun kapsamında sunmakta olduğu hizmetlere yönelik reklam hizmeti almak istediği arama motoru, sosyal medya platformu gibi sağlayıcıların kuruluş adına verilen sahte reklamları engellemeye yönelik tedbirleri alıp almadığını kontrol eder ve uygun tedbirleri almayan sağlayıcılardan reklam hizmeti alamaz. Kuruluş, 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. Kuruluşun bu kapsamda reklam hizmeti almak üzere anlaştığı aracı firmalar ile yapılan sözleşmeler için de bu fıkra hükümleri geçerlidir.

(11) Banka, kuruluşun dışarıdan hizmet almasının sistemin sorunsuz işleyişini olumsuz etkilediği kanaatine varması veya hizmeti sağlayan kuruluşun Bankanın kuruluşun denetimi ile ilgili faaliyetlerini engellemesi durumlarında, kuruluştan dış hizmet alımını durdurmasını istemeye yetkilidir.

Müşterilerin bilgilendirilmesi ve internet sitesi

MADDE 17 – (1) Kuruluş tarafından sunulan hizmetlerden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir. Kuruluş, sunmakta olduğu hizmetlere ilişkin riskler ve tehditler hakkında müşterilerini uyarır ve bu hususlarda müşteri farkındalığı oluşturulması için azami özen gösterir.

(2) Birinci fıkra kapsamında asgari olarak aşağıdaki hususlar müşterinin bilgisine sunulur:

a) Kuruluş tarafından müşterilere sunulan cihazlar, yazılımlar ya da mobil uygulamalar ile ödeme araçları ve hassas müşteri verisinin güvenli bir şekilde kullanımına ilişkin yönlendirici talimatlar.

b) Kuruluş tarafından müşterilere sunulan cihazlar, yazılımlar ya da mobil uygulamalar ile ödeme araçları ve hassas müşteri verisinin kaybedilmesi, çalınması, silinmesi ya da değiştirilmesinin gerekmesi gibi durumlarda müşterilerin takip etmesi gereken adımlar.

c) Sunulan hizmetlerin taşıdığı riskler ile bu hizmetlere ilişkin koşullar; müşterilerin ve kuruluşun hakları ve sorumlulukları.

ç) Dolandırıcılık şüphesi ya da hizmetin alınması sırasında herhangi bir problemle karşılaşılması halinde yapılması gerekenlere ilişkin yönlendirici talimatlar, müşterilerin takip etmesi gereken adımlar.

(3) Müşteriler, ödeme hizmetlerinde iki saatten daha uzun süreli bir kesinti, planlı bakım ve değişiklik gibi durumlarda önceden bilgilendirilir.

(4) Bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı müşterinin yaşayabileceği sorunların takip edilebileceği ve müşterilerin şikâyetlerini ulaştırmalarına imkân tanıyacak mekanizmalar oluşturulur. Şikâyetlerin en kısa sürede değerlendirilerek çözümlenmesi; bu kapsamda oluşturulacak şikâyet birimleri veya çağrı merkezlerinde müşteriyi karşılayacak menülerde elektronik kanal üzerinden sunulan hizmete ilişkin yaşanan dolandırıcılık vakalarının iletilmesi işleminin ana menüde ve ilk sıralarda müşterinin dikkatine sunulması ve bu kapsamda kuruluşa ulaştırılan bildirimlerin en kısa sürede giderilmesine yönelik gerekli çalışmaların yapılması sağlanır.

(5) Kuruluş, müşterinin işlem bilgilerini ve bakiye bilgilerini takip edebilmesine olanak sağlar. Bu bilgilerin kuruluşca sunulan elektronik kanallar kullanılarak takip edilebilmesi için müşterilere gerekli yönlendirmeler yapılır. Bu kapsamda, kuruluşun elektronik ortamda müşterilerine ileteceği hassas müşteri verisi veya müşteri bilgisi içeren her türlü ekstre, dekont, hesap özeti gibi belgelerin, kuruluşça sunulan elektronik kanallar üzerinden sağlanması esastır. Müşterinin talep etmesi durumunda bu belgelerin, müşterinin belirttiği iletişim veya elektronik posta adresine hassas müşteri verisi içermeyecek şekilde gönderilmesi sağlanır.

(6) Kuruluşun internet sitesinde kuruluşun ticaret unvanı, iletişim bilgileri, genel müdürlük adresi ile Bankanın iletişim bilgilerine yer verilir. Kuruluşun internet sitesinde Bankanın iletişim bilgileri verilirken, Bankanın iletişim bilgileri, farkındalık ve bilinilirlik anlamında kuruluşun iletişim bilgilerinin önüne geçecek şekilde konumlandırılamaz.

(7) Kuruluş, müşteriye özel duyuru, uyarı ve benzeri sürekli bilgilendirme ihtiyaçlarını müşteri ile önceden mutabık kaldığı güvenli bir kanal üzerinden gerçekleştirir. Bu kanal üzerinden gelmeyen bilgilere itibar edilmemesi konusunda müşteriler bilgilendirilir.

(8) Erişilen internet sitesinin kuruluşa ait olduğunun doğrulanmasını sağlayacak teknikler kullanılır.

(9) Bu Tebliğ ve Yönetmelik kapsamında tanımlanmış olan müşterilerin bilgilendirilmesi için gerekli her türlü bilgi ve açıklama, kuruluşun internet sitesi üzerinden müşteri erişimine daima açık tutulur.

(10) Sunulan ödeme hizmetleri, bu hizmetlerin erişime açık olduğu gün ve saatler ile hizmetlere ilişkin diğer koşullar, sunulan hizmetlerin doğurabileceği riskler, bu risklerden korunmak için müşterilerin kullanması gereken yöntemler, müşteri farkındalığını artıracak yönlendirici güvenlik kılavuzları ile bu hizmetlerden yararlanacak müşterilerin sorumluluk ve haklarına ilişkin hususlar ile Yönetmelik kapsamında müşterilere yapılması gereken diğer genel bilgilendirmelere internet sitesinde yer verilir.

(11) Sunulan hizmetlere ilişkin bilgi ve açıklamaların açık ve anlaşılır olması, internet sitesinde dikkat çekici bir yere yerleştirilmesi gerekir ve ilgili ödeme hizmetinden yararlanmaya başlamadan önce müşterilerin bunları en az bir kere tam olarak okunabilir şekilde görüntülemesini garanti edecek şekilde yönlendirmeler ile sistemsel kısıtlamalar uygulanması sağlanır.

(12) Kuruluş tarafından elektronik kanal üzerinden sunulan Kanun kapsamındaki hizmetlerde, 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 müşterinin bilgisine sunulması ve müşterinin bunları onaylaması halinde söz konusu işlemlerin gerçekleştirilmesi temin edilir.

(13) Kuruluş, yapacağı pazarlama faaliyetleri, reklâmlar veya yayınlarda, müşterilerine sunmakta olduğu herhangi bir hizmetin mutlak manada güvenli olduğu veya bu hizmetlerde hiçbir güvenlik riskinin bulunmadığı izlenimini ve bilgisini verecek ifadeler kullanmaktan kaçınır.

(14) Kuruluş Kanun kapsamında sunduğu hizmetler için bu Tebliğ kapsamında yapılması gereken bilgilendirmelerin, hizmetin verildiği platformdan ya da müşterinin hizmeti alırken kullandığı cihazdan kaynaklanan nedenlerle bilgilendirme olanakları açısından yetersiz kalması durumunda, müşterinin söz konusu bilgilere farklı kanallar üzerinden ulaşması için gerekli yönlendirmeleri yapar.

Elektronik sertifikalar

MADDE 18 – (1) Kuruluş internet sitesinin kimliğinin doğrulanması ve 23 üncü maddedeki veri paylaşım servisleri kapsamında tarafların güvenli bir şekilde tanımlaması amacıyla 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda açıklanan elektronik sertifikaları kullanır.

(2) Elektronik sertifikada Banka tarafından raporlama yaparken kullanması için kuruluşa verilen kod ve kuruluşun türüne dair bilgiler yer alır.

Yüksek riskli işlemlerin takibi

MADDE 19 – (1) Kuruluş, sahtekârlık ya da dolandırıcılık amaçlı işlemler ile mali suç kapsamında değerlendirilebilecek işlemleri tespit etmek ve önlemek amacıyla işleme taraf müşteriler ile temsilciler, işyerleri ve insansız hizmet noktalarından gerçekleştirilen tüm işlemler için takip mekanizmaları tesis eder. Bu kapsamda şüpheli veya yüksek riskli işlemleri detaylı olarak değerlendirir. Kuruluş, gerçekleşen işlemlere yönelik işleme taraf işyeri ve sunduğu hizmete yönelik etkin bir takip yürütmekle sorumludur. Bu kapsamda kuruluş, işyerine yönelik risk değerlendirme çalışması yapmak, işyerinin sunduğu hizmetin sosyal mühendislik faaliyetlerine konu olmadığı ve belirtilen hizmet ile gerçekte sunulan hizmetin uyumluluğu konusunda bilgi sahibi olmak, hizmetlere ilişkin yoğun müşteri şikâyeti olması durumunda risk değerlendirmesini gözden geçirerek gerekli tedbirleri almaktan sorumludur.

(2) 5549 sayılı Kanuna ilişkin yükümlülükler saklı kalmak üzere kuruluş, olağan dışı, şüpheli ya da yüksek riskli işlemlerin gerçekleştirildiğini tespit etmesi halinde telefon ya da SMS gibi uygun yöntemlerle müşterilerin en kısa sürede uyarılmasını sağlar. Müşteriye kısa sürede ulaşılabilecek bir iletişim bilgisinin kuruluş ile paylaşılmamış olması halinde bu fıkra hükmü uygulanmaz.

(3) Düşük değerli olan ödeme işlemlerinin kısa bir süre içinde sıklıkla gerçekleştirilmesi ya da düşük değerli ödeme aracının kısa bir süre içinde sıklıkla kullanılması yüksek riskli işlem olarak değerlendirilir.

(4) Kuruluş, Kanun kapsamında elektronik kanallar üzerinden sunduğu hizmetlerle ilgili olarak 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 ödeme işleminin tutarı ve bu tutarlara göre müşterinin, fiziki ortamlarda gerçekleştirilen tüm işlemlerde, elektronik kanallar üzerinden gerçekleştirilen işlemlerde ise müşterinin onay vermesi durumunda 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.

d) Mümkün olması durumunda, müşterinin ve müşterinin ödeme yaptığı veya fon transfer ettiği tarafların daha önce sahtekârlık amaçlı veya dolandırıcılık kapsamına giren ödeme işlemleri gerçekleştirip gerçekleştirmediğine ilişkin kayıtlar.

e) T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu tarafından yayımlanan rehberlerde yer alan şüpheli işlem tipleri kapsamında uygun görülen senaryolar.

(5) Kuruluş, yüksek riskli işlemleri filtreleyerek değerlendirir ve bu filtrelere takılan müşterileri daha yakından takip eder.

(6) Kuruluş, yürütmekte olduğu risk yönetimi faaliyetleri kapsamında, kuruluş tarafından Kanun çerçevesinde sunulan hizmetlerin, yasa dışı bahis başta olmak üzere yasa dışı faaliyetlerde kullanılıp kullanılmadığının tespiti için sosyal medya ve çevrim içi platformlar dâhil gerekli araştırmaların yapılması ve bu tür işlemlerin önlenmesi için uygun tedbirlerin alınmasını sağlar.

(7) Altıncı fıkra uyarınca alınacak tedbirler kapsamında kuruluş bu işten doğrudan sorumlu olacak yeterli sayıda personeli görevlendirir ve;

a) Görevlendireceği personel tarafından sosyal medya ve çevrim içi platformlar başta olmak üzere yasa dışı bahis ve benzeri yasa dışı faaliyetlerin gerçekleşmesine imkân tanıyan sanal mecralarda kuruluş üzerinden para transferi yapılmasına ilişkin yer alan linkler kullanılarak kuruluş nezdinde hangi kişilerin, hesapların, kartların, işyerlerinin yasa dışı faaliyetlerde kullanıldığının tespit edilmesini,

b) Tespit edilen müşterilere ödeme hizmeti sunulmasının ivedi olarak sonlandırmasını, bu müşterilere para gönderen veya bu müşteriler tarafından para gönderilen kişilerin, hesapların, kartların, işyerlerinin de tespit edilerek yakın takibe alınması ve yasa dışı bahis başta olmak üzere yasa dışı faaliyetlerde kullanıldığına veya rol aldığına ilişkin şüphe oluşması durumunda bu müşterilere de ödeme hizmeti sunulmasının sonlandırılmasını,

c) (a) bendinde yer alan adımların, yasa dışı bahis ve benzeri yasa dışı faaliyetlerin gerçekleşmesine imkân tanıyan sanal mecralarda kuruluş üzerinden para transferi yapılmasına ilişkin diğer kişilerin, hesapların, kartların, işyerlerinin kullanılmadığına ilişkin makul görüş oluşuncaya kadar tekrarlanmasını,

ç) Bu madde uyarınca tespit edilen kişilerin, hesapların, kartların, işyerlerinin ve bunlarla ilgili olarak gerçekleştirilen tüm işlemlerin kayıt altına alması, kayıt altına alınan söz konusu müşterilerin ve bu müşteriler üzerinden gerçekleşen işlemlerin Bankaya ve yasa dışı işlemin mahiyetine bağlı olarak başta T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu olmak üzere ilgili kamu otoritelerine raporlanmasını,

d) Kontrolü yapılan ve yasa dışı bahis ve benzeri yasa dışı faaliyetlerin gerçekleşmesine imkân tanıdığı tespit edilen sanal mecraların da kayıt altına alınarak Bankaya ve T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kuruluna bildirilmesini,

sağlar.

(8) Kuruluş tarafından yedinci fıkra uyarınca görevlendirilecek personelin sayısının kuruluşun işlem adet ve tutarları ile faaliyet gösterdiği ödeme hizmeti türleri göz önünde bulundurularak yeterli kontrol mekanizmasının sağlanmasını temin edecek şekilde belirlenmesi gerekmektedir. Banka, kuruluşun işlem adet ve tutarlarını gözeterek kuruluştan yedinci fıkra uyarınca görevlendirilecek personelin bu işe özgü olarak atanmasını istemeye yetkilidir.

(9) Münhasıran Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (g) bendinde yer alan ödeme hizmetlerini sunan kuruluşlar bu maddedeki yükümlülüklerden muaftır.

İşyerleri, temsilciler ve insansız hizmet noktaları

MADDE 20 – (1) Kuruluş, işyerleri ve temsilciler ile yapacağı sözleşmelerde;

a) Hassas müşteri verilerinin gizliliğinin ve güvenliğinin sağlanması hususunda gerekli önlemlerin alınmasına,

b) Hizmetlerin gerçekleştirilmesi için gerekli olan terminaller ve kuruluş arasındaki iletişim haricinde, kendi nezdinde hassas müşteri verisini tutmamasına, işlememesine veya kaydetmemesine,

c) Önemli bir güvenlik olayı yaşanması halinde bu durumun ivedilikle kuruluşa bildirilmesine,

ilişkin hükümlerin yer almasını sağlamakla yükümlüdür.

(2) Kuruluş, işyerleri ve temsilciler ile yapacağı sözleşmelerde yer alacak birinci fıkra kapsamındaki hükümlerin gereklerinin yerine getirildiğini gözetmekle ve gereğinin yerine getirilmediğinin anlaşılması halinde sözleşmeyi feshetmekle yükümlüdür. Müşterilerin, işyerlerinin hassas müşteri verilerini tutması, işlemesi veya kaydetmesi hususunda aydınlatılması suretiyle açık rızasının alındığı durumlarda birinci fıkranın (b) bendine uyum şartı aranmaz.

(3) Ödeme işlemlerinin veya elektronik para ile ilgili işlemlerin gerçekleştirilmesini sağlayan API, fiziki veya sanal terminaller ve insansız hizmet noktaları ile kuruluş arasında karşılıklı doğrulama ve uçtan uca güvenli iletişim olması esastır. Terminaller ve insansız hizmet noktalarında işleme tabi tutulan hassas müşteri verilerine yetkisiz fiziki veya elektronik erişim engellenir.

(4) Kuruluş, temsilcilerine güncel sahtekârlık ve dolandırıcılık yöntemleri ile 5549 sayılı Kanun kapsamında alınması gereken önlemler konusunda eğitim vermekle ve kullanıcılarını insansız hizmet noktalarının güvenli kullanımı hususunda bilgilendirmekle yükümlüdür.

(5) Kuruluş, insansız hizmet noktalarına ilişkin hırsızlık, sahtekârlık ve dolandırıcılık gibi tehditlere karşı gerekli önlemleri almakla yükümlüdür. Bu kapsamda insansız hizmet noktaları üzerine yabancı aparatlar veya kart kopyalama cihazları, sahte klavye, kamera gibi başka cihazların yerleştirilmesini önleyici ve bunları tespit edici kontroller tesis edilir.

(6) İnsansız hizmet noktaları üzerinde ön tanımlı olarak gelen her türlü parola kolaylıkla tahmin edilemeyecek şekilde değiştirilir.

(7) İnsansız hizmet noktaları ve terminallere, her türlü yetkisiz erişimi ve bunlar üzerine zararlı içerikli programların yüklenmesini engelleyecek tedbirler alınır.

(8) İnsansız hizmet noktaları ve terminallerde sağlayıcı veya üretici firma desteği olan güncel yazılım sürümleri kullanılır ve güvenlik açıklıklarını gidermek amacıyla gerekli güncellemeler vakit kaybetmeksizin yapılır.

(9) İnsansız hizmet noktalarında gerçekleştirilen işlemler için kimlik doğrulama hükümleri uygulanır; işlem tipi, sayısı ve limiti gibi hususlar dikkate alınarak şüpheli işlem gerçekleştirilmesi ihtimaline karşı kontrol ve takip mekanizması tesis edilerek gerekli bildirimlerin yapılması sağlanır.

(10) Kuruluş, insansız hizmet noktalarının bulunduğu yerlere güvenlik kamerası koyar. Güvenlik kamerası kayıtları kişilerin kimliklerinin tespit edilmesine yetecek görüntü kalitesinde en az altı ay süreyle saklanır ve kamera teçhizatının sağlıklı çalışıp çalışmadığı düzenli olarak kontrol edilir. Görüntüleme alanı bakımından insansız hizmet noktasını da kapsayan ve bu fıkradaki koşulları karşılayan bir güvenlik kamerası altyapısının varlığı durumunda ayrıca bir güvenlik kamerası kurulmaz. Kamu güvenlik ve istihbarat kurumlarının faaliyet bölgesinde bulunan insansız hizmet noktaları için güvenlik kamerası kurulma şartı, ilgili kamu güvenlik ve istihbarat kurumlarından izin alınabilmesi koşuluyla yerine getirilir.

Bilgi sistemlerine ilişkin sınırlamalar

MADDE 21 – (1) Kuruluşların birincil ve ikincil sistemleri ile veri yedekleme merkezlerini yurt içinde bulundurmaları zorunludur. Bu maddenin uygulanmasında, Yönetmeliğin 19 uncu maddesinin on üçüncü fıkrası hükümleri saklıdır.

(2) Aynı kuruluşun müşterileri ya da farklı kuruluşların müşterileri arasındaki ödeme işlemlerinin yürütülmesinde kullanılan tüm bilgi sistemleri ve bunların yedeklerinin yurt içinde bulunması esastır. Bu kapsamda dış hizmet alınması halinde, dış hizmet sağlayıcının söz konusu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de yurt içinde tutulur.

(3) Ödeme işleminin taraflarından birinin, kuruluşun müşterisi olmadığı durumlarda, kuruluş işlemin kendi tarafında gerçekleşen kısımları için bu Tebliğ hükümlerine tabidir.

Uzaktan iletişim aracı ile yürütülecek süreçler

MADDE 22 – (1) Kuruluş, uzaktan iletişim aracı ile kurulacak sözleşmelerde, Banka tarafından uygun bulunan merkezi bir yapının kullanılmaması durumunda müşteri kimliğinin doğrulanmasına imkan verecek internet tabanlı yöntemleri kullanır ve asgari olarak aşağıdaki hususları yerine getirir:

a) Kimlik tespitinin yapılabilmesi için müşteriden gerekli bilgi ve belgelerin temin edilmesi.

b) Müşteriden temin edilen bilgi ve belgelerin doğruluğunun optik karakter tanıma, NFC, kart okuyucu ve benzeri yöntemlerden en az birisi kullanılarak kontrol edilmesi ve orijinallik, bütünlük, yıpranma ile tahrif edilme durumlarına ilişkin testlerinin yapılması.

c) Müşterinin onayının kayıt altına alınması.

ç) Müşterinin video, hareketli fotoğraf, çevrim içi görüntülü görüşme ve benzeri yöntemler kullanılarak canlılık testinin yapılması ve kimliğinin doğrulanması.

d) Işık ve gürültü seviyesi, sinyal gücü ve benzeri kıstaslar açısından müşterinin cihaz ve ortam kontrolünün yapılması.

e) Müşterinin uzaktan iletişim aracı olarak kullanacağı yöntem ile ilgili iletişim bilgilerinin uygun yöntemlerle doğrulanması.

(2) Anonim ön ödemeli araçlar ve T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu tarafından belirlenen sınırlar dahilinde kimlik tespiti yapılması zorunlu olmayan ve sürekli iş ilişkisi kapsamına girmeyen tek seferlik ödeme işlemleri için gerekli bilgi, sözleşme, dekont ve benzeri belgelere ilişkin süreçlerin işletilmesi esnasında uzaktan iletişim aracı kullanılması halinde birinci fıkra hükümlerinin uygulanması zorunlu değildir.

(3) Kuruluş, ödeme hizmetinin sunulması ile ilgili bilgi ve belgeleri posta, faks, elektronik posta ve çevrim içi görüntülü görüşme benzeri yöntemler, Banka tarafından uygun bulunan merkezi bir yapı veya günün teknolojisine uygun yenilikçi diğer yöntemler ile temin edebilir.

(4) Birinci fıkra kapsamında uzaktan iletişim aracı ile yürütülen süreçler, personelin manuel müdahalesinin bulunduğu hallerde görevler ayrılığı prensibine uygun olarak, tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân verilmeyecek şekilde tasarlanır ve işletilir.

(5) Birinci fıkra kapsamında uzaktan iletişim aracı ile yürütülen süreçler, tüm adımları içerecek şekilde kayıt altına alınır ve elde edilen veriler, Kanun, Yönetmelik ve bu Tebliğ ile diğer ilgili düzenlemelere uygun bir şekilde saklanır. Uyuşmazlık durumunda, uzaktan iletişim aracı ile yürütülen süreçler esnasında Yönetmelik ve bu Tebliğde yer alan hükümlere uygun işlem tesis edildiğinin ispatından kuruluş sorumludur.

(6) Kuruluş, uzaktan iletişim aracı ile kurulacak sözleşmelere ilişkin izlenecek süreç ve prosedürleri yazılı olarak oluşturur, oluşturulan süreç ve prosedürleri yılda en az iki defa olmak üzere düzenli olarak test eder ve test sonuçlarında ortaya çıkan eksiklik, hata, zayıflık ve açıklara ilişkin olarak teknolojik ve operasyonel gereklilikler başta olmak üzere tüm önlemleri alır ve gerekli güncellemeleri yapar.

(7) Uzaktan iletişim aracı ile kurulacak sözleşmelere ilişkin izlenecek süreç ve prosedürler çerçevesinde müşterilerden alınacak belgeler, bu belgelerin doğrulanması esnasında dikkat edilecek güvenlik ve doğrulama özellikleri ile bu kapsamda kullanılacak kriterler ve müşterinin kimliğinin doğrulanması esnasında dikkate alınacak güvenlik ve doğrulama özellikleri ile bu kapsamda kullanılacak kriterler yazılı olarak dokümante edilir.

(8) Çevrim içi görüntülü görüşme yoluyla kurulacak sözleşmelerde görev alacak personel tarafından görüşme esnasında müşterinin kimlik tespitinin yapılması, doğrulanması ve sözleşmenin başka bir tarafın zoru ya da zorlamasıyla yapılmadığından emin olunabilmesi için sorulacak sorular; görüşmenin seyrine ilişkin aşamalar ve her aşamada sorulacak sorular belirlenecek şekilde yazılı olarak oluşturulur ve bu sorular güncel gelişme ve tehditler çerçevesinde düzenli olarak güncellenir.

(9) Kuruluş, çevrim içi görüntülü görüşme yoluyla kurulacak sözleşmelerde aşağıdaki şartları yerine getirmekle yükümlüdür:

a) Görüntülü görüşmenin gerçek zamanlı ve kesintisiz şekilde yapılması gerekir.

b) Görüntülü görüşme uçtan uca güvenli iletişim ile gerçekleştirilir.

c) Görüntülü görüşmenin görüntü ve ses kalitesinin, bu madde uyarınca gerekli kontrollerin etkin bir şekilde yapılmasını sağlayacak şekilde yeterli seviyede olması sağlanır ve görüşme boyunca görüntü kalitesinin istenilen seviyede olduğunu gösterecek kontroller oluşturulur. Görüntü kalitesinin ölçülmesinde asgari olarak, görüşme yapılan kişinin görsel olarak net bir şekilde görüntülenebilmesinin, sunulan belgenin beyaz ışık altında görsel olarak doğrulanabilmesinin ve sunulan belgenin tahrif edilmemiş olduğunun kontrol edilebilmesinin mümkün olmasına dikkat edilir.

ç) Görüntülü görüşme esnasında müşteri tarafından sunulan belgenin geçerliliği hususunda ya da dolandırıcılık veya sahtecilik teşkil edebilecek eylemlerden şüphe edilmesi durumunda, sözleşme kurulmadan görüşme sonlandırılır.

(10) Dokuzuncu fıkrada yer alan şartlara uyulmadığı durumlarda çevrim içi görüntülü görüşme yoluyla sözleşme kurulamaz, bu şekilde kurulan sözleşmelerde yetkilendirilmemiş, hatalı gerçekleşmiş veya benzeri sorunlu işlemlerde tüm sorumluluk kuruluşa ait olur.

(11) Kuruluş, uzaktan iletişim aracı ile kurduğu sözleşmelere taraf müşterilerini farklı bir risk profilinde izler. Bu müşterilerce yapılan işlemlerin türüne ve tutarına bağlı olarak ilave güvenlik ve kontrol yöntemleri uygulanır.

(12) Banka, ihtiyaç duyulması halinde bu madde kapsamında uygulanacak diğer usul ve esasları belirlemeye yetkilidir.

ÜÇÜNCÜ BÖLÜM
Ödeme Hizmetlerinde Kullanılan Veri Paylaşım Servisleri

Veri paylaşım servisi

MADDE 23 – (1) HHS, Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (f) ve (g) bentlerinde yer alan faaliyetler kapsamında Yönetmeliğin 59 uncu maddesinin beşinci fıkrasına uygun olarak gerekli bağlantıları yaparak veri paylaşım servislerini HBHS ve ÖBHS'ye sunar.

(2) Ödeme emri başlatma hizmetinde veri paylaşım servisinin tarafları ÖBHS ile HHS'dir.

(3) Ödeme hesabı bilgisi sağlama hizmetinde veri paylaşım servisinin tarafları HBHS ile HHS'dir.

(4) Veri paylaşım servisinde taraflar Bankanın belirlediği elektronik sertifikaları kullanır ve tarafların Bankaca yetkilendirilmiş olduğu kontrol edilir.

(5) Veri paylaşım servislerine ilişkin faaliyetlerde hassas müşteri verileri, müşteri bilgileri ve rekabete duyarlı veriler başta olmak üzere ilgili tüm verilerin gizliliği, bütünlüğü, güncelliği ve güvenliği sağlanır.

(6) Veri paylaşım servisleri, Yönetmeliğin 59 uncu maddesinde yer alan hükümler ile aynı maddenin birinci fıkrası uyarınca Banka tarafından belirlenen teknik ve operasyonel gerekliliklere uygun olarak yürütülür.

(7) Müşteri tarafından Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (f) ve (g) bentlerinde belirtilen hizmetlerle ilgili her bir bilgi talebi ve ödeme emri başlatma işlemi için ayrı ayrı onay verilir. Hesap bilgisi sağlama hizmeti için ilgili hesaplar ve bu hesaplar üzerinde tanımlanan işlemler için ise onay düzenlenen sözleşme ile de verilebilir.

Veri paylaşım servisine ilişkin HHS'nin yükümlülükleri

MADDE 24 – (1) HHS, Yönetmeliğin 59 uncu maddesi uyarınca BKM API Geçidi'ne bağlanır, nezdinde bulunan ödeme hesaplarına ilişkin Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (f) veya (g) bentlerinde yer alan ödeme hizmetlerinin sunulması için talepte bulunan tüm diğer yetkili ödeme hizmeti sağlayıcılarına gerekli altyapıyı sağlar.

(2) HHS, hesap bilgisi hizmeti ile ödeme emri başlatma hizmeti kapsamında gelen istekleri gecikmeksizin gerçekleştirir.

(3) HBHS ve ÖBHS'nin gerçekleştirdiği işlemlerde hata oluşması durumunda HHS, hatanın sebebini açıkça ilgili HBHS ve ÖBHS'ye bildirir.

(4) HHS, Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (f) ve (g) bentlerinde yer alan ödeme hizmetlerinin sunulması ile ilgili olarak, Yönetmelik, bu Tebliğ ve Yönetmeliğin 59 uncu maddesi uyarınca belirlenen teknik ve operasyonel gerekliliklere uygun şekilde geliştirmeleri yapmak, bunlara ilişkin teknik özellikleri belgelemek ve bu teknik özelliklerde yapılacak herhangi bir değişiklik konusunda ilgili tüm tarafları 3 ay öncesinde bilgilendirmekle yükümlüdür.

(5) HHS, Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (f) ve (g) bentlerinde yer alan ödeme hizmetlerinin sunulması ile ilgili olarak HBHS ve ÖBHS'lere yazılımlarını ve uygulamalarını test etmelerini sağlamak için test ortamı sağlar. Test ortamı aracılığıyla hassas müşteri verisi paylaşılmaz.

(6) Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (f) ve (g) bentlerinde yer alan ödeme hizmetlerinin, bu madde kapsamındaki hizmetlerle sınırlı olmak üzere HHS tarafından sunumu, kullanılabilirliği, performansı ve içerdiği destek hizmeti, HHS'nin müşteriye sağladığı ödeme hesabına doğrudan çevrim içi erişiminden farksız olmalıdır.

(7) HHS, Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (f) ve (g) bentlerinde yer alan ödeme hizmetlerinin sunulması ile ilgili olarak, Yönetmelik, bu Tebliğ ve Yönetmeliğin 59 uncu maddesi uyarınca belirlenen teknik ve operasyonel gereklilikler kapsamında tanımlanan temel performans göstergeleri ile hizmet seviyesi hedeflerine uyum sağlar. Performans göstergeleri ile hizmet seviyesi hedeflerine ilişkin istatistikler düzenli olarak Bankanın belirleyeceği yöntemle yayımlanır.

(8) HHS, Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (f) ve (g) bentlerinde yer alan ödeme hizmetlerinin sunulmasında müşteriye sağladığı ödeme hesabına doğrudan çevrim içi erişim için belirlediği kural ve gerekliliklere kıyasla, hizmetin amacı dışında akışlar ve pazarlama faaliyetleri gibi ek zorluklar getiremez.

Oturum özellikleri ve denetim izleri

MADDE 25 – (1) Veri paylaşım servisinin tarafları, müşteri ile olan bağlantılar da dâhil olmak üzere, uçtan uca güvenli iletişim kurar ve tüm işlemlerin takip edilebilirliğini garanti eder.

(2) Müşterinin HBHS ve ÖBHS üzerinden HHS ile kurduğu oturumlar kimlik doğrulamaya dayanır.

(3) Her oturum biricik oturum numarası ve zaman damgası içerir.

(4) Oturumdaki işlemler işlem numarası, zaman damgası ve ilgili tüm işlem verilerini içerecek şekilde kontrol alanı ölçüsünde ispat yükümlülüğüne sahip olan taraflarca güvenli ve ayrıntılı olarak kayıt altına alınır.

(5) Zaman damgası, 5070 sayılı Kanun kapsamında tanımlanan zaman damgasına dayanır.

(6) Taraflar açtıkları oturumu kısa tutmaya çalışır ve işlem biter bitmez kapatır.

Veri paylaşım servislerinde kimlik doğrulama ve işlem güvenliği

MADDE 26 – (1) Hesap bilgisi hizmetinde, müşterinin onayının alınması esnasında HHS tarafından müşteriye 10 uncu maddede belirtilen hükümlere uygun olarak güçlü kimlik doğrulama uygulanır.

(2) Ödeme emri başlatma hizmetinde, HHS tarafından 10 uncu maddede belirtilen hükümlere uygun olarak müşteriye güçlü kimlik doğrulama uygulanır ve işlem doğrulama kodu ile müşterinin onayı alınır.

(3) Ödeme emri başlatma hizmetinde HHS tarafından müşteriye güçlü kimlik doğrulama uygulanmasına ilişkin istisna veya ilave güvenlik önlemleri Banka tarafından Yönetmeliğin 59 uncu maddesi uyarınca oluşturulan teknik ve operasyonel gereklilikler kapsamında belirlenir.

Veri paylaşım servislerine ilişkin olağanüstü durum önlemleri

MADDE 27 – (1) HHS, sunduğu veri paylaşım servislerinin kesintiye uğraması durumunda alacağı önlemleri içerecek olağanüstü durum planlarını 14 üncü madde uyarınca hazırlayacağı bilgi sistemleri süreklilik planı kapsamında hazırlar.

(2) Birinci fıkra uyarınca hazırlanacak olağanüstü durum planları, HBHS ve ÖBHS'lerin bilgilendirilmesine ilişkin iletişim planları ve kullanılabilecek alternatif erişim yöntemlerini içerir.

(3) HHS, HBHS ve ÖBHS'ler veri paylaşım servislerine ilişkin önemli olayları Bankaya ivedilikle raporlar.

DÖRDÜNCÜ BÖLÜM
Bilgi Sistemlerinin Bağımsız Denetimi

Bilgi sistemlerinin bağımsız denetimi

MADDE 28 – (1) Bilgi sistemleri bağımsız denetimi; kuruluşun bu Tebliğ hükümlerine uyum durumunun tespit edilmesi amacıyla, bilgi sistemleri yönetimi kapsamında yer alan süreç, faaliyet, yazılım, donanım gibi bilgi sistemi unsurları ile bu sistem ve süreçler dâhilinde tesis edilen iç kontrollerin bağımsız denetim kuruluşları tarafından değerlendirilmesi sonucunda, söz konusu iç kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş oluşturulması ve sonuçların rapora bağlanması aşamalarından oluşan süreçtir.

(2) Birinci fıkra uyarınca kuruluşun bilgi sistemlerine ilişkin yürütülecek denetim faaliyeti Bankacılık Düzenleme ve Denetleme Kurumu tarafından yayımlanan Bankalarda Bilgi Sistemi Denetimi Yapmaya Yetkili Bağımsız Denetim Kuruluşları listesinde yer alan bağımsız denetim kuruluşlarınca yapılır. Banka, gerek görmesi durumunda kuruluş tarafından, bu listede yer alan bir bağımsız denetim kuruluşundan bu madde uyarınca bağımsız denetim hizmeti alınmamasına veya bu listede yer almayan bir bağımsız denetim kuruluşunun kuruluş nezdinde bilgi sistemleri denetimi yapabilmesine karar vermeye yetkilidir.

(3) Birinci fıkra uyarınca gerçekleştirilen denetim faaliyetleri sonucunda oluşturulacak raporun denetim dönemini izleyen yılın Şubat ayı sonuna kadar kuruluş tarafından Bankayla paylaşılması zorunludur. Banka, kuruluşun talebi üzerine gerekli gördüğü hallerde ilave süre vermeye yetkilidir. Banka, kuruluş tarafından yapılacak raporlamanın belirleyeceği yönteme uygun bir şekilde elektronik olarak yapılmasına karar vermeye yetkilidir. Banka, ihtiyaç duyması halinde bağımsız denetim faaliyetine ilişkin hususlarda bağımsız denetim kuruluşundan veya kuruluştan ilave açıklama talep edebilir.

(4) Bağımsız denetim kuruluşu, kuruluşun dış hizmet alarak gerçekleştirdiği hizmetlerin, bilgi sistemlerini nasıl etkilediğini göz önünde bulundurur, buna göre gerekli görmesi halinde denetimini dış hizmet sağlayıcılarını da kapsayacak şekilde planlar ve etkin bir denetim yaklaşımı geliştirir.

(5) Kuruluşta bilgi sistemleri denetimi iki yılda bir yapılır. Yeni faaliyet izni alan bir kuruluşa ilişkin birinci fıkra uyarınca yapılacak ilk denetim faaliyeti, kuruluşa faaliyet izni verilmesini takip eden yılı kapsayacak şekilde yürütülür. Banka, gerekli gördüğü hallerde bilgi sistemleri denetiminin kapsamını ve sıklığını farklılaştırabilir.

(6) Banka, bilgi sistemlerine ilişkin yürütülecek bağımsız denetim faaliyetlerine ilişkin ilke, usul ve esasları belirlemeye yetkilidir.

(7) 5411 sayılı Kanun kapsamındaki bankalar, Kanun kapsamındaki faaliyetleri ile ilgili olarak kullandıkları bilgi sistemlerinin bağımsız denetimi konusunda, sekizinci fıkra hükümleri saklı kalmak kaydıyla, Bankacılık Düzenleme ve Denetleme Kurumu tarafından 5411 sayılı Kanuna dayanılarak çıkarılmış olan mevzuata tabidir.

(8) Banka, gerekli durumlarda Posta ve Telgraf Teşkilatı Anonim Şirketinin ve 5411 sayılı Kanun kapsamındaki bankaların bilgi sistemlerinin Kanun kapsamındaki faaliyetleri ile ilgili olarak Kanun, Yönetmelik ve bu Tebliğ hükümleri ile Bankanın talimat ve genelgeleri çerçevesinde bağımsız denetim kuruluşlarınca denetlenmesini isteyebilir.

Yönetim beyanı

MADDE 29 – (1) Kuruluş, bu Tebliğ hükümlerinin gereği olarak tesis ettiği iç kontroller hakkında denetim dönemi itibarıyla güvence veren ve yönetim kurulu ve genel müdür tarafından onaylanmış yönetim beyanını her denetim döneminde hazırlamakla yükümlüdür.

(2) Bağımsız denetim kuruluşu, denetim görüşünü oluştururken yönetim beyanını ve bu beyana mesnet teşkil eden çalışmaları inceler. Bağımsız denetim kuruluşu, bu inceleme sonucunda beyanda eksiklik veya yanlışlık tespit ederse denetim raporunda bu tespitlere bulgu olarak yer verir.

(3) Denetlenen kuruluşun yönetim beyanını vermeyi reddetmesi durumunda, bilgi sistemleri denetimi raporunu imzalamaya yetkili kişiler şartlı görüş bildirebilir, görüş bildirmekten kaçınabilir veya 30 uncu maddenin beşinci fıkrasında belirtilen şartlar çerçevesinde denetimden çekilmek için bağımsız denetim kuruluşu yönetimine teklifte bulunabilirler. Bağımsız denetim kuruluşunun çekilme kararı alması halinde durum gerekçeleri ile birlikte kararın alındığı tarih itibarıyla en geç yedi iş günü içinde Bankaya bildirilir.

Denetim görüşünün oluşturulması ve denetim mektubu

MADDE 30 – (1) Bağımsız denetim kuruluşu tarafından kuruluşta gerçekleştirilen denetim sonucunda; olumlu, şartlı veya olumsuz görüşe varılması hallerinde, sırasıyla EK-1, EK-2, EK-3'te yer alan örneklere uygun olarak denetim mektubu düzenlenir. Görüş bildirmekten kaçınmayı gerektirecek şartların varlığı halinde ise denetim mektubu EK-4'te yer alan örneğe uygun olarak düzenlenir.

(2) Denetim raporunu imzalamaya yetkili kişiler, yapılan denetim sonucunda herhangi önemli bir kontrol eksikliğinin bulunmaması ve denetim kapsamında herhangi bir kısıtlama ya da engelleme ile karşılaşılmaması durumunda, kendilerine bağlı bağımsız denetim ekiplerinin de görüşlerini alarak, EK-1'de yer alan örneğe uygun olarak olumlu görüş bildirirler.

(3) Denetim raporunu imzalamaya yetkili kişiler, kendilerine bağlı bağımsız denetim ekiplerinin de görüşlerini alarak;

a) Yapılan denetim sonucunda en az bir önemli kontrol eksikliğiyle karşılaşmalarına rağmen, bu eksikliklerin denetlenenin bilgi sistemleri ile ödemeler alanı süreç ve sistemlerinin bütününü veya büyük bir kısmını etkilemediğini düşündükleri,

b) Görüş bildirmekten kaçınmayı gerektirecek önemde olmamakla birlikte, bilgi sistemleri denetimi faaliyetlerini sınırlayan herhangi bir hususun varlığı veya yeni tesis edilmiş bir sistem veya süreç hakkında yeterince bilgi edinememeleri veya,

c) Denetim görüşünün oluşturulması için yeterli ve uygun denetim kanıtının elde edilememesi,

durumlarında EK- 2'de yer alan örneğe uygun olarak şartlı görüş bildirirler.

(4) Denetim raporunu imzalamaya yetkili kişiler, yapılan denetim sonucunda rastlanılan önemli kontrol eksikliklerinin tek başlarına veya beraber değerlendirildiklerinde;

a) Denetlenenin bilgi sistemleri ile ödemeler alanı süreçlerinin bütününü veya büyük bir kısmını etkilediğine ilişkin kanaat edinmeleri veya,

b) Bağımsız denetim kuruluşunun denetlenen bünyesinde gerçekleştirdiği denetim sonrasında önemli bir kontrol eksikliğinin bütün önemli taraflarıyla eksik veya yanlış aktarılmasından kaynaklanan bir farklılık bulunması,

durumlarında kendilerine bağlı bağımsız denetim ekiplerinin de görüşlerini alarak, EK-3'te yer alan örneğe uygun olarak olumsuz görüş bildirirler.

(5) Denetim raporunu imzalamaya yetkili kişiler, denetim çalışmalarında karşılaşılan belirsizlik ve sınırlamaların görüş belirtilmesini engelleyecek derecede önemli olduğunu

düşündükleri durumlarda, kendilerine bağlı bağımsız denetim ekiplerinin de görüşlerini alarak, bilgi sistemleri ile ödemeler alanı süreçleri üzerindeki kontroller hakkında görüş bildirmekten kaçınabilirler. Bu durumda denetim mektubu EK- 4'te yer alan örneğe uygun olarak düzenlenir. Görüş bildirmekten kaçınma durumunda düzenlenecek raporda, kaçınmaya yol açan nedenlere ilişkin bağımsız denetim kuruluşu görüşlerine yer verilmesi şarttır.

(6) Banka, denetim görüşünün oluşturulması ve denetim mektubuna ilişkin dikkat edilmesi gereken ilke, usul ve esasları belirlemeye yetkilidir.

BEŞİNCİ BÖLÜM
Çeşitli ve Son Hükümler

Posta ve Telgraf Teşkilatı Anonim Şirketi ve bankalar ile banka ve kredi kartları

MADDE 31 – (1) Posta ve Telgraf Teşkilatı Anonim Şirketi sunduğu ödeme hizmetleri ve elektronik para ihracı ile ilgili olarak 16 ncı madde hariç olmak üzere bu Tebliğ hükümlerine tabidir.

(2) 5411 sayılı Kanun kapsamındaki bankalar sundukları ödeme hizmetleri ve elektronik para ihracı ile ilgili olarak ödeme hizmetlerinde kullanılan veri paylaşım servisleri başlıklı üçüncü bölüm ve 28 inci maddenin yedinci ve sekizinci fıkraları hariç olmak üzere bu Tebliğ hükümlerine tabi değildir.

(3) Banka ve kredi kartları ile ilgili olarak 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu ve bu Kanun uyarınca yapılan düzenlemelerde yer alan hususlara ilişkin olarak bu Tebliğin ilgili hükümleri uygulanmaz.

Yürürlükten kaldırılan tebliğ

MADDE 32 – (1) 27/6/2014 tarihli ve 29043 sayılı Resmî Gazete'de yayımlanan Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ yürürlükten kaldırılmıştır.

Geçiş hükümleri

GEÇİCİ MADDE 1 – (1) Bu Tebliğin yürürlüğe girdiği tarih itibarıyla faaliyette bulunan kuruluşlar, bu Tebliğ ile getirilen ve bu Tebliğin 32 nci maddesi uyarınca yürürlükten kaldırılan Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde daha önce yer almayan hükümlere, **(Değişik ibare:RG-25/11/2022-32024)** 28/2/2023 tarihine kadar uyumlu hale gelmekle yükümlüdür.

(2) Bu Tebliğin yürürlüğe girdiği tarih itibarıyla nezdinde ödeme hesabı bulunduran ve Banka Ödeme Sistemlerinde 2020 yılı içerisinde gerçekleştirilen hesaba ödeme işlemleri açısından, toplam adedine göre ilk on katılımcı arasında yer alan ödeme hizmeti sağlayıcıları, bu Tebliğin 24 üncü maddesinin birinci fıkrası kapsamında yerine getirmesi gereken yükümlülükleri **(Değişik ibare:RG-25/11/2022-32024)** 28/2/2023 tarihine kadar yerine getirir. Banka, bu süreyi, her defasında altı ayı aşmamak üzere iki kez uzatmaya yetkilidir. Nezdinde ödeme hesabı bulunduran diğer tüm ödeme hizmeti sağlayıcıları, Banka Ödeme Sistemlerinde gerçekleştirilen hesaba ödeme işlemleri açısından toplam adedine göre ilk on katılımcı arasında yer alan ödeme hizmeti sağlayıcıları için bu fıkra kapsamında Banka tarafından öngörülen sürenin tamamlanmasının ardından bu Tebliğin 24 üncü maddesinin birinci fıkrası kapsamında yerine getirmesi gereken yükümlülükleri bir yıl içerisinde yerine getirir.

(3) Bu Tebliğin 23 üncü maddesinin altıncı fıkrası kapsamında teknik gereklilikleri belirlenmiş veri paylaşım servisleri hizmetleri, **(Değişik ibare:RG-25/11/2022-32024)** 28/2/2023 tarihine kadar standart olmayan servisler kullanılarak da verilmeye devam edilebilir. Banka, bu süreyi, altı ayı aşmamak üzere uzatmaya yetkilidir.

(4) Bu Tebliğin 23 üncü maddesinin altıncı fıkrası kapsamında teknik gereklilikleri belirlenmemiş veri paylaşım servisi hizmetleri, gereklilikler belirlenınceye kadar standart olmayan servisler kullanılarak verilmeye devam edilir. Banka tarafından teknik ve operasyonel gerekliliklerin belirlenmesinin ardından bu hizmetler için de en geç bir yıl içerisinde uyum

sağlanarak, hizmetler söz konusu gerekliliklere uygun olarak yürütülmeye başlanır. Banka, bu süreyi, altı ayı aşmamak üzere uzatmaya yetkilidir.

(5) Banka tarafından bu Tebliğin 28 inci maddesinin altıncı fıkrası uyarınca gerekli düzenlemeler yapılıncaya kadar bu Tebliğ uyarınca gerçekleşecek bilgi sistemleri bağımsız denetimi çalışmaları, bu Tebliğin 28 inci maddesinin ikinci fıkrasındaki koşul hariç olmak üzere, BSDHY ile belirlenen usul ve esaslar çerçevesinde gerçekleştirilir. BSDHY ile belirlenen usul ve esaslar bu Tebliğ çerçevesinde uygulanırken BSDHY'de geçen banka ve denetlenen ibareleri kuruluşu, bilgi sistemleri denetimi ibaresi bu Tebliğin 28 inci maddesinin birinci fıkrasında tanımlanan denetimi ifade eder.

Yürürlük

MADDE 33 – (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 34 – (1) Bu Tebliğ hükümlerini Türkiye Cumhuriyet Merkez Bankası Başkanı yürütür.

	Tebliğin Yayımlandığı Resmî Gazete'nin	
	Tarihi	**Sayısı**
	1/12/2021	31676
	Tebliğde Değişiklik Yapan Tebliğlerin Yayımlandığı Resmî Gazetelerin	
	Tarihi	**Sayısı**
1.	25/11/2022	32024
2.		
3.		

EK-1

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Olumlu Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

[Bağımsız denetim kuruluşuGörüşü]
Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin

Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-2

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Şartlı Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Bağımsız denetim faaliyetine getirilen sınırlandırma ve bu nedenle denetlenemeyen süreçler, uygulamalar, kontroller; denetlenenin bilgi sistemleri üzerinde tespit edilen önemli kontrol eksiklikleri ve bu kontrol eksikliklerinin denetlenenin bilgi sistemlerinin bütününü veya büyük bir kısmını etkilememesine ilişkin görüşüne esas neden ve gerekçeler)

[Bağımsız denetim kuruluşuGörüşü]
Görüşümüze göre, yukarıda *(....ncı paragrafta)* açıklanan *husus(lar) nedeniyle,* denetlenenin bilgi sistemleri üzerinde bu *hususun/hususların* muhtemel etkileri haricinde bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin

Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-3

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Olumsuz Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetlenenin bilgi sistemleri üzerindeki kontrollerin etkin, yeterli veya uyumlu bulunmama sebepleri)

[Bağımsız denetim kuruluşuGörüşü]
Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmemiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin

Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-4

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Görüşten Kaçınma

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetçinin görüş bildirmemesinin nedenleri)

[Bağımsız denetim kuruluşuGörüşü]
Yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle ..... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde tesis edilen kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş bildirmiyoruz.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin

Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

EK-5

Bilgi Sistemleri Sızma Testleri Usul ve Esasları

1) AMAÇ

Sızma testlerinin amacı, kuruluş bilgi sistemlerinde gizlilik, bütünlük ve erişilebilirlik açısından güvenlik açıklarının istismar edilmeden önce tespit edilmesi ve düzeltilmesidir.

2) KAPSAM

Sızma testleri kapsamında gerçekleştirilecek testler asgari olarak aşağıdaki başlıkları kapsar:

a) İletişim Altyapısı ve Aktif Cihazlar
b) DNS Servisleri
c) Etki Alanı ve Kullanıcı Bilgisayarları
d) E-posta Servisleri
e) Veritabanı Sistemleri
f) Web Uygulamaları
g) Mobil Uygulamalar
h) Bulut Sistemleri
i) Kablosuz Ağ Sistemleri
j) ATM, kiosk, vb. istemleri
k) Dağıtık Servis Dışı Bırakma (DDoS) Testleri
l) Sosyal Mühendislik Testleri

3) METODOLOJİ

Sızma testleri, aşağıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek testlerden oluşur. Testler, sistem tespiti, servis tespiti ve zafiyet taraması/araştırması adımları ile başlar ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder. Bu testler sonucunda saptanan açıklar ve bulgular, Kapsam bölümünde belirtilen ilişkili her bir başlık altında ayrıntılı olarak incelenerek raporlanır. Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklar ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklar açısından da değerlendirilir ve bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklar ve bulgular da raporlanır. Bulgular, "**Bulgu Önem Dereceleri**" bölümünde yer verilen bulgu önem dereceleri kullanılarak "**Bulgu Formatı**" bölümünde tariflenen formata uygun olacak şekilde sunulur. Bu kapsamda bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmaz. Varlık değerlendirmesi yapmak ve varlıkların önem derecelerine göre aksiyon almak kuruluşların sorumluluğundadır.

Sızma testleri gerçekleştirilirken, kuruluş faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol açabilecek tüm testler kuruluş ile koordineli bir şekilde planlanarak gerçekleştirilir.

a) Testlerin Gerçekleştirileceği Erişim Noktaları

Sızma testlerinin gerçekleştirileceği asgari erişim noktaları aşağıda tanımlanmaktadır. Bu noktalardan sisteme erişildikten sonra, sızma testleri gerçekleştirilir.

i. **İnternet**: Kuruluşun internet üzerinden erişilebilen tüm sunucu ve servislerine İnternet üzerinden erişilerek sızma testleri gerçekleştirilir.
ii. **Kuruluş iç ağı**: Kuruluşun iç ağında yer alan ve test kapsamında ele alınan sunuculara kuruluş iç ağı üzerinden erişilerek sızma testleri gerçekleştirilir. Ağ ve ağ trafiği üzerinde gerçekleştirilecek testler için de bu ağ kullanılır ve testi gerçekleştirecek şahıslara kullanımı en yaygın olan çalışan bilgisayarı profilinde bilgisayarlar sağlanır.
iii. **Şube ağı**: Kuruluş şube kullanıyorsa, kuruluşun yönlendirmesi ile belirlenecek bir şubenin sahip olduğu ağ altyapısına erişim sağlanarak bu şubede bulunan sistemler, ağ altyapısı, ağ trafiği ve şube üzerinden erişilebilen diğer sistemler sızma testlerine tabi tutulur. Testi gerçekleştirecek şahıslara, şube çalışanlarının kullanmış olduğu bilgisayarlar ile aynı profilde bilgisayarlar sağlanır.
iv. **Temsilci bağlantısı**: Kuruluş temsilci kullanıyorsa, kuruluşun yönlendirmesi ile belirlenecek bir temsilciye bağlantı sağlanarak bu temsilcinin kuruluşa bağlantıda kullandığı giriş noktaları sızma testlerine tabi tutulur. Testi gerçekleştirecek şahıslara, temsilcinin bağlantıda kullandığı aynı profilde ortam sağlanır.
v. **Dış hizmet sağlayıcının bağlantısı:** Dış hizmet sağlayıcının kuruluşun bilgi sistemlerine uzaktan bağlantıda kullandığı giriş noktaları sızma testine tabi tutulur. Testi gerçekleştirecek şahıslara, dış hizmet sağlayıcının bağlantıda kullandığı aynı profilde ortam sağlanır.

b) Testlerin Gerçekleştirileceği Kullanıcı Profilleri

Sızma testlerinin sağlıklı bir şekilde gerçekleştirilebilmesi ve testlerin gerçek hayata uygun olması için, yukarıda tanımlanan erişim noktalarına bu ortamların doğasına uyacak şekilde aşağıdaki kullanıcı profilleri ile sızma testleri gerçekleştirilir.

i. **Anonim kullanıcı profili**: İnternet üzerinden, kuruluşun web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Kuruluşa ait web uygulamalarının üyesi olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
ii. **Kuruluş müşterisi profili**: İnternet üzerinden, Kuruluşun web servislerine erişebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. İnternet üzerinde kuruluşa ait web uygulamalarının üyesi olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
iii. **Kuruluş misafiri profili**: Kuruluşu ziyaret eden kişilerin misafir ağında oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
iv. **Kuruluş personel profili**: Kuruluş personelinin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır. Kuruluş personeli profili ile gerçekleştirilecek testlerde, kuruluş çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici (*ing.* local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilir. Kuruluş personeli profili ile yapılan testlerde, testi yapan kişi/kuruluşa kuruluş tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilmelidir.

v. **Diğer kullanıcı profilleri**: Sızma testlerinin, yukarıda tanımlanan diğer dört kullanıcı profiline uymayan bir kullanıcı profili ile gerçekleştirilmesi durumunda, kullanılan her bir profil için tanımlanan hak ve yetkiler bu başlık altında açıkça ifade edilir.

c) Sistem Tespiti, Servis Tespiti ve Açıklık Taraması

Sızma testleri aşağıda tanımlanan sistem tespiti, servis tespiti ve zafiyet taraması/araştırması adımları ile başlar. Sistem tespiti, servis tespiti ve zafiyet taraması/araştırması tüm bilgi sistemi varlıklarına uygulanır.

i. **Sistem tespiti**: Sunucu veya aktif/pasif ağ cihazlarının sistem/yapılandırma bilgilerinin tespit edilmeye çalışıldığı adımdır.
ii. **Servis tespiti**: Kuruluş bilgi sistemlerinde yer alan varlıkların port taramasının gerçekleştirildiği ve dış dünyaya/genel erişime açık olan portların sunduğu servislerin tespit edilmeye çalışıldığı adımdır.
iii. **Zafiyet taraması/araştırması**: Kuruluşun bilgi sistemleri unsurları ve bunların sunduğu servislerin zafiyet tarayıcıları ile güncel açıklara karşı tarandığı ve muhtemel güvenlik açıklarının belirlenmeye çalışıldığı adımdır. Bu adımda ayrıca, tespit edilen muhtemel açıklar için güvenlik açıkları veritabanları gibi kaynaklar kullanılarak bu açıkların bilgi sistemleri unsurlarına ve bu unsurların etkileşimde olduğu sistemlere güvenlik açısından etkileri araştırılır.

d) Sızma Testleri

i. **İnternet üzerinden gerçekleştirilecek sızma testleri**: Kuruluş ağından bağımsız bir yerleşkeden, kuruluşun internet üzerinde sahip olduğu IP ağı taranarak sistem tespiti, servis tespiti ve zafiyet taraması adımları gerçekleştirilir.
ii. **Kuruluş iç ağından gerçekleştirilecek sızma testleri:** Kuruluşun iç ağında sistem tespiti, servis tespiti ve zafiyet taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:
- Kuruluş yerel ağ haritası tespiti
- Belirlenen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin gerçekleştirilmesi
- Yerel alan ağı içerisinde zafiyet taraması yapılması
- Kuruluş yerel ağında araya girme teknikleri ile hassas bilgilerin elde edilmeye çalışılması
- Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırılarının gerçekleştirilmesi
- Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılması

iii. **Kuruluş şube ağından gerçekleştirilecek sızma testleri:** Kuruluş, şube kullanıyorsa, şube ağında sistem tespiti, servis tespiti ve zafiyet taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:
- Şube yerel ağ haritasının tespiti
- Şube yerel alan ağında zafiyet taraması yapılması
- Şube yerel ağında araya girme teknikleri ile hassas bilgilerin elde edilmeye çalışılması
- Ağ altyapısında bulunan aktif cihazların testlerinin gerçekleştirilmesi
- Şube personelinin bilgisayarı üzerinden oluşturulabilecek tehditlerin incelenmesi
- Elde edilen bilgiler ışığında şube ağından erişilebilen diğer sunucu ve sistemlere yönelik ele geçirme saldırılarının gerçekleştirilmesi

iv. **Temsilcinin bağlantısında gerçekleştirilecek sızma testleri:** Temsilcinin kuruluşa gerçekleştirdiği bağlantı ve giriş noktalarından kaynaklanabilecek tehditlerin incelenmesi sağlanır.

v. **Dış hizmet sağlayıcının bağlantısında gerçekleştirilecek sızma testleri:** Dış hizmet sağlayıcının kuruluşun bilgi sistemlerine uzaktan erişim için kullandığı bağlantı ve giriş noktalarından kaynaklanabilecek tehditlerin incelenmesi sağlanır.

4) BULGU ÖNEM DERECELERİ

Bulgu önem dereceleri beş kategoride ele alınır. "**Acil"**, "**Kritik"**, "**Yüksek"**, "**Orta"** ve "**Düşük"** şeklinde olan bu kategorilere ilişkin açıklamalar aşağıda yer almaktadır:

Önem Derecesi	Açıklama
Acil	Niteliksiz saldırgan tarafından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklardır.
Kritik	Nitelikli saldırgan tarafından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklardır.
Yüksek	Kuruluş dış ağından gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklardır.
Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

5) BULGU FORMATI

Kapsam bölümünde belirtilen başlıkların her biri altında raporlanacak bulguların sunuluş biçimi aşağıda yer almaktadır.

Bulgu Referans No	Rapordaki her bulguyu tekil olarak niteleyen harf/rakam dizisi
Bulgu Adı	Bulguyu özet olarak ifade eden tanımlayıcı isim
Önem Derecesi	Bulgunun, "*4. Bulgu Önem Dereceleri"* bölümünde verilen önem derecesi
Etkisi	Bulguda yer verilen açığın/eksikliğin kötüye kullanılması durumunda oluşabilecek potansiyel sonuç
Erişim Noktası	*"3.a. Testlerin Gerçekleştirileceği Erişim Noktaları"* bölümünde yer verilen testin gerçekleştirildiği erişim noktası
Kullanıcı Profili	*"3.b. Testlerin Gerçekleştirileceği Kullanıcı Profilleri"* bölümünde yer verilen testin gerçekleştirildiği kullanıcı profili
Bulgunun Tespit Edildiği Bilgi Sistemi Unsuru/Unsurları	Bulgunun tespit edildiği bilgi sistemleri unsurunu niteleyen IP Numarası, URL, Sistem, Servis, Sunucu veya Varlık adı gibi bilgiler
Bulgu Açıklaması	Bulgunun detaylı açıklaması
Çözüm Önerisi	Bulgunun giderilmesi için testi gerçekleştiren kuruluş tarafından yapılacak çözüm önerisi