TEBLİĞ

Bankacılık Düzenleme ve Denetleme Kurumundan:

ÖDEME KURULUŞLARI VE ELEKTRONİK PARA KURULUŞLARININ BİLGİ SİSTEMLERİNİN YÖNETİMİNE VE DENETİMİNE İLİŞKİN TEBLİĞ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç ve kapsam

MADDE 1 – (1) Bu Tebliğin amacı, ödeme kuruluşları ve elektronik para kuruluşlarının Kanun kapsamındaki faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimine ve yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesine ilişkin usul ve esasları düzenlemektir.

Dayanak

MADDE 2 – (1) Bu Tebliğ, Kanunun 14, 18 ve 21 inci maddeleri ile Yönetmeliğin 64 üncü maddesi hükümlerine dayanılarak düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 3 – (1) Bu Tebliğde yer alan;

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

b) Bağımsız denetçi: Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından yetkilendirilmiş bağımsız denetim kuruluşlarından Kurum tarafından yayınlanan Bankalarda Bilgi Sistemleri Denetimi Yapmaya Yetkili Bağımsız Denetim Kuruluşları listesinde yer alan bağımsız denetim kuruluşunu,

c) Birincil sistemler: Kanunda 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,

ç) 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,

d) Dış hizmet sağlayıcı: Kuruluşun, Yönetmeliğin 14 üncü maddesi çerçevesinde münhasıran kendisi tarafından yapılması gerekenler dışında kalan faaliyetlerini kuruluş adına gerçekleştiren ya da gerçekleştirilmesinde kuruluşa yardımcı nitelikte hizmet veren tüzel kişileri,

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

f) Etkinlik: BSDHY'nin 7 nci maddesinde tanımlanan etkinliği,

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

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

h) Güvenli bileşen: İçinde barındırdığı gizli verilerin yetkisiz kişilerce erişilmesine, kopyalanmasına ve kendi dışına çıkarılmasına imkan vermeyen SIM kart, akıllı kart gibi bileşenleri,

ı) Güvenli kanal: Kuruluşun kendi kullanıcılarına sunduğu elektronik posta kutusu ya da kullanıcıların kimlik doğrulama gerçekleştirerek girdiği kuruluşa ait güvenli internet sayfası gibi kullanıcılara iletilmek istenen bilgilerin kaynağının kuruluş olduğunun doğrulandığı iletişim kanalını,

i) Güvenlik olayı: Bilgi sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya ihlale teşebbüste bulunulmasını,

j) Hassas ödeme verisi: Kullanıcılar tarafından ödeme emrinin verilmesinde veya kullanıcı kimliğinin doğrulanmasında kullanılan, ele geçirilmesi veya değiştirilmesi

halinde dolandırıcılık ya da kullanıcılar adına sahte işlem yapılmasına imkan verebilecek şifre, güvenlik sorusu, sertifika, şifreleme anahtarı ile PIN, kart numarası, son kullanma tarihi, CVV2, CVC2 kodu gibi kuruluşlar tarafından ihraç edilen ödeme araçlarına ilişkin kişisel güvenlik bilgilerini,

k) Hizmet noktası: Kullanıcıların, ödeme işlemi ya da elektronik para ile ilgili işlemleri kendi kendine yapabildiği ATM, kiosk gibi cihazları,

l) İkincil merkez: İkincil sistemlerin kullanıma hazır olacak şekilde tesis edildiği, herhangi bir kesinti durumunda personelin çalışmasına imkan tanıyacak ve birincil sistemlerin tesis edildiği yapı ile aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı,

m) 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 Kanunda yer alan hususlarla ilgili bütün bilgilere erişilmesini sağlayan birincil sistem yedeklerini,

n) İki taraflı kimlik doğrulama: İletişimde bulunan tarafların birbirlerinin kimliklerinden emin olmalarını sağlamak amacıyla kullanılan, iki tarafın da kendi kimliğini diğer tarafa doğruladığı kimlik doğrulama yöntemini,

o) İşlem bilgisi: Gerçekleştirilen işleme ilişkin işlemin tutarı, zamanı, işlem konusu mal veya hizmetin ne olduğu gibi kullanıcılara ait bilgileri,

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

p) Kimlik tanımlayıcı: Kuruluş tarafından kimliğinin belirlenmesi ve diğer kullanıcılardan ayırt edilmesi amacıyla kullanıcıya özgülenen sayı, harf veya sembollerden oluşan kombinasyonu,

r) Kişisel bilgi: Gerçek kişi kullanıcıların adı, soyadı, T.C. kimlik numarası, pasaport numarası, vergi kimlik numarası, sosyal güvenlik numarası, kimlik tanımlayıcısı, doğum yeri, doğum tarihi, telefon numarası, adresi, elektronik posta adresi, resim, görüntü ve ses kayıtları, biyometrik veriler gibi bilinmesi halinde tek başına veya diğer bilgiler ile bir araya geldiğinde ait olduğu kişiyi belirli ya da belirlenebilir hale getiren bilgi ya da bilgi setini,

s) Kullanıcı: Ödeme hizmeti kullanıcısı ile elektronik para kullanıcısını,

ş) Kullanıcı bilgisi: Kullanıcılara ait hassas ödeme verisi, işlem bilgisi, bakiye bilgisi, kişisel bilgi ve tüzel kişi kullanıcıların kimlik tanımlayıcısı ile unvanından oluşan bilgi setinin tamamını,

t) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

u) Kuruluş: Ödeme kuruluşları ve elektronik para kuruluşlarını,

ü) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

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

y) Ödeme emri: Ödeme hizmeti kullanıcısı tarafından ödeme işleminin gerçekleşmesi amacıyla ödeme hizmeti sağlayıcısına verilen talimatı,

z) Ödeme hesabı: Ödeme hizmeti kullanıcısı adına açılan ve ödeme işleminin yürütülmesinde kullanılan hesabı,

aa) Ödeme hizmeti: Kanunun 12 nci maddesinde belirtilen hizmetleri,

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

cc) Ödeme hizmeti sağlayıcısı: Kanunun 13 üncü maddesinde belirtilen kuruluşları,

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

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

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

ff) Siber olaya müdahale: 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 olaya müdahaleyi,

gg) Temsilci: Ödeme kuruluşu ve elektronik para kuruluşunun adına ve hesabına hareket eden gerçek veya tüzel kişiyi,

ğğ) Terminal: Ödeme aracı üzerindeki bilgileri ve/veya kullanıcıya ait hassas ödeme 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 elektronik cihazı ya da yazılımı,

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

ıı) Uyumluluk: BSDHY'nin 7 nci maddesinde tanımlanan uyumluluğu,

ii) Üst yönetim: Kuruluş yönetim kurulu ile genel müdür ve genel müdür yardımcıları ve başka unvanlarla istihdam edilseler dahi, danışmanlık birimleri dışındaki birimlerin, yetki ve görevleri itibarıyla genel müdür yardımcısına denk veya daha üst konumlarda görev yapan yöneticilerini,

jj) Üye iş yeri: Vereceği mal ve/veya hizmet karşılığında kuruluş ile yapmış olduğu anlaşma çerçevesinde kuruluşun ödeme aracını kabul eden iş yerini,

kk) Yeterlilik: BSDHY'nin 7 nci maddesinde tanımlanan yeterliliği,

ll) Yönetmelik: Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmeliği,

ifade eder.

İKİNCİ BÖLÜM
Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler

Bilgi sistemleri risk yönetimi

MADDE 4 – (1) Kuruluş, üst yönetimi tarafından onaylanmış bir risk yönetim politikası çerçevesinde, faaliyetlerinde bilgi teknolojilerinin kullanılmasından kaynaklanan riskleri tespit etmek, analiz etmek, ölçmek, izlemek, kontrol etmek ve raporlamak üzere bir risk yönetim yapısı teşkil eder.

(2) Kuruluş, risk analizlerinin nasıl gerçekleştirileceğine ilişkin hazırladığı prosedürler çerçevesinde, sonuçları üst yönetime raporlanacak şekilde, yılda en az bir defa bilgi sistemlerine ilişkin genel bir risk analizi gerçekleştirir. Kuruluş, bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce olası riskleri değerlendirir ve bilgi sistemlerine ilişkin risk analizini tekrarlar.

(3) Kuruluş risk analizi yaparken, hizmetlerini sunmak için kullandığı teknoloji altyapısı, uygulama mimarisi, programlama teknikleri, dış hizmet sağlayıcılardan kaynaklanabilecek riskleri ve teknolojik gelişmeleri de dikkate alır. Bu çerçevede risk analiz ve risk yönetim metodolojisini gözden geçirerek günceller. Yapılacak risk analizinde kullanıcı bilgilerinin güvenliğini ve gizliliğini tehdit eden riskler dikkate alınır.

Bilgi güvenliği yönetim süreci

MADDE 5 – (1) Kuruluş üst yönetimi, bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarını gözetim altında tutar ve bu amaçla bilgi güvenliği politikasını oluşturur ve onaylar.

(2) Bilgi güvenliği politikası ile bilgi güvenliği yönetim sürecinin oluşturulması, sürdürülmesi ve yönetilmesine ilişkin görev ve sorumluluklar açıkça tanımlanır ve bu kapsamda bilgi güvenliği politikasına uyum durumu yılda en az bir defa yönetim kuruluna raporlanır.

(3) Kuruluş üst yönetimi, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi için yeterli kaynağı tahsis eder ve güvenlik politikasıyla uyumlu olacak şekilde gerekli güvenlik kontrollerinin tesis edilmesini sağlar. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik

katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır.

(4) Üst yönetim, bilgi güvenliği yönetim süreci kapsamında;

a) Bilgi güvenliği politikasının ve tüm sorumlulukların yılda en az bir defa gözden geçirilmesini, güncellenmesini ve onaylanmasını,

b) Bilgi sistemleri ve bilgi sistemleri üzerinde işlenen, saklanan ve iletilen verilerin güvenlik hassasiyet derecelerine göre sınıflandırılmasını ve her bir sınıf için uygun düzeyde güvenlik kontrollerinin tesis edilmesini,

c) Güvenlik alanındaki güncel gelişmeler, yeni tehditler ve zafiyetlerin takip edilmesini, gerekli yazılım güncellemelerinin ve yamaların uygulanmasını,

ç) Bilgi güvenliği ihlaline ilişkin olayların izlenmesini ve periyodik olarak değerlendirilmesini,

d) Kuruluşun bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırılmasını,

e) Bilgi güvenliği hususunda hem kurum içinde hem de kullanıcılar ve üye işyerleri nezdinde farkındalığı artıracak çalışmaların gerçekleştirilmesini,

sağlar.

Güvenlik olay yönetimi

MADDE 6 – (1) Kuruluş, güvenlikle ilişkili kullanıcı şikayetlerini de kapsayacak ve bilgi güvenliği yönetim süreci ile entegre olacak şekilde gerçekleşen güvenlik olaylarının ele alınmasına ve takibine yönelik bir güvenlik olay yönetimi ve siber olaylara müdahale süreci oluşturur. Bu süreç kapsamında, Kurum tarafından belirlenen usul ve esaslar çerçevesinde, gerekli yönetim yapısının oluşturulması ve güvenlik olaylarının Kuruma ve ilgili yönetim birimlerine raporlanması sağlanır.

Veri gizliliği, güvenliği ve yetkilendirme

MADDE 7 – (1) Kuruluş, sunmakta olduğu hizmetlerin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesi aşamalarında, görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlar. Bu kapsamda süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından girilmesi, yetkilendirilmesi ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir.

(2) Sistemlere, servislere ve verilere ilişkin yetkilendirme düzeyi ve erişim haklarının ilgili unsurlara atanmasında gerekli olan en düşük yetkinin ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınır. Atanan yetkilerin görevler ayrılığı prensibiyle tutarlı olması bakımından periyodik olarak gözden geçirilmesi ve güncellenmesi sağlanır.

(3) Kuruluş, kendi kurumsal ağı dışındaki ağlarla iletişimde bulunduğu hallerde bu dış ağlardan gelebilecek tehditler için ağ kontrol güvenlik sistemlerini tesis eder. Kuruluş, dış ağdan iç ağına yapılacak erişimleri kontrol altında tutmak, ayrıca, iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere, gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan bir veya birden fazla güvenlik duvarı kullanır.

(4) İnternet aracılığıyla sunulan hizmetlerde, kullanıcının işlem gerçekleştirdiği internet sayfasının kuruluşa ait olduğunun doğrulanmasını sağlayacak teknikler kullanılır.

(5) 15 inci maddenin birinci fıkrasında belirtilen hükümler saklı kalmak kaydıyla, hassas ödeme verilerinin şifrelenmiş bir şekilde ya da güvenli bileşenlerde saklanması esastır.

(6) Hassas ödeme verilerinin ve kişisel bilgilerin kablosuz biçimde veya internet üzerinden iletilmesi halinde, bu iletim uçtan uca güvenli iletişim ile gerçekleştirilir.

(7) Kullanılacak şifreleme tekniklerinde, güncel durum itibariyle literatürde kabul görmüş ve güvenilirliğini yitirmemiş algoritmalar temel alınır. Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanılabileceği zaman zarfında kırılamayacak şekilde uzun seçilir. Geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılabilirliği engellenir.

(8) Kuruluş, mobil cihazlar üzerinde çalışan uygulamalarının kullandığı hassas ödeme verilerinin, aynı mobil cihaz üzerindeki diğer uygulamalar ve devam etmekte olan işlemler tarafından erişilemez olmasını sağlamak amacıyla günün teknolojisine uygun kontroller tesis eder.

(9) Kuruluş, kullanıcılarına sağladığı mobil uygulamaları barındıran mobil cihazların, güvenli bileşenlerin ya da ödeme araçlarının kaybolması ya da çalınması halinde bunlar üzerindeki hassas ödeme verilerinin erişilemez olmasını sağlamak amacıyla günün teknolojisine uygun kontroller tesis eder.

(10) Kuruluş tarafından kullanıcılarına sunulan her türlü yazılım ya da mobil uygulamanın kaynağının ilgili kuruluş olduğunun doğrulanabiliyor olması sağlanır. Kuruluş bu yazılımların, kullanıcı güvenliğini tehlikeye sokacak herhangi bir kod içermemesini sağlamakla, güvenlik açıklarını giderecek gerekli yamaları ve güncellemeleri yayınlamakla yükümlüdür.

Denetim izlerinin oluşturulması

MADDE 8 – (1) Kuruluş, kullanıcı bilgilerine gerçekleştirilen fiziksel veya mantıksal erişimler ile yetkisiz erişim teşebbüslerine ve bilgi sistemleri dahilinde gerçekleşen ödeme işlemleri veya elektronik para ile ilgili tüm işlemlere ilişkin etkin bir denetim izi kayıt sistemi tesis eder. Denetim izlerinin yeterli detayda ve açıklıkta tutulması esastır.

(2) Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin teknikler kullanılır. Kayıt sisteminin her türlü yetkisiz değişiklik ve müdahalelere karşı korunmasına yönelik önlemler alınır ve kuruluş personelinin kendi faaliyetlerine ilişkin denetim izlerine müdahalesi engellenir. Denetim izi kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(3) Kullanıcı bilgilerinin sorgulanması işlemleri de birinci fıkra kapsamındadır.

(4) Denetim izlerinin içeriğinde aşağıdaki bilgilerin tutulması sağlanır:

a) Kuruluş personeli aracılığı ile gerçekleştirilen ödeme işlemlerinde veya elektronik para ile ilgili işlemlerde işlemi gerçekleştiren personelin kim olduğunu gösterir bilgi.

b) Kullanıcısı belli olmayan ödeme araçlarıyla gerçekleştirilen işlemler hariç olmak üzere, kullanıcılara ait kimlik tanımlayıcısı.

c) Ödeme aracıyla gerçekleştirilen işlemler için ödeme aracını ayırt edici bilgi.

ç) Yapılan işlemlerin tutarı ve zaman bilgisi.

(5) Denetim izleri asgari 3 yıl süreyle denetime hazır bulundurulacak şekilde saklanır.

(6) Denetim izlerinin, yeterli güvenlik düzeyine sahip ortamlarda korunması ve yedeklerinin alınması suretiyle, yaşanacak olası felaketler sonrasında da erişilebilir olmaları temin edilir.

(7) Bilgi sistemlerine ilişkin dış hizmet alınması halinde, kuruluş dış hizmet sağlayıcı tarafından tutulan denetim izlerinin kendi standartlarına uygunluğunu ve bu denetim izlerinin kendisi tarafından erişilebilir olmasını temin eder.

(8) Denetim izlerinin tutulması, kuruluşun belge ve kayıtların saklanmasına ilişkin ilgili düzenlemelerde yer alan diğer yükümlülüklerini ortadan kaldırmaz.

Kimlik doğrulama

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

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

(3) Kuruluş, tesis edeceği sistemler ve geliştireceği uygulamalarda kullanıcılarına ve personeline ait kimlik doğrulama bilgilerinin gizliliğine ve güvenliğine yönelik gerekli önlemleri alır. Bu önlemler asgari olarak kimlik doğrulama bilgilerinin, veritabanlarında şifreli olarak muhafaza edilmesi, kimlik doğrulama amacıyla aktarılırken şifrelenmesi, yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunması, bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli denetim izlerinin tutulması ve bu denetim izlerinin güvenliğinin sağlanması hususlarını içerir.

(4) Hassas ödeme verilerine erişim sağlandığı durumlarda ve Yönetmeliğin 58 inci maddesine göre düşük değerli olmayan ödeme işlemleri ile 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanuna ilişkin yükümlülükler kapsamında kimlik tespitinin zorunlu olduğu işlemlerin elektronik ortamda gerçekleştirildiği hallerde söz konusu işlemlerin başlatılmasında; birbirinden bağımsız en az iki bileşenden oluşan bir kimlik doğrulama mekanizması kullanılır. Bu iki bileşen; kişinin “bildiği”, “sahip olduğu” veya “biyometrik bir karakteristiği olan” unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Bileşenlerin bağımsız olması, bir bileşenin ele geçirilmesinin diğer bileşenin güvenliğini tehlikeye atmamasını ifade eder. Bileşenlerin kimlik doğrulama bilgisinin gizliliğini koruyacak nitelikte ve kullanıcıya özgü olması, biyometrik bir bileşenin kullanıldığı durumlar haricinde bileşenlerden en az birinin tek kullanımlık olması ve bu tek kullanımlık bileşen için gerekli olan en kısa geçerlilik süresinin belirlenmesi esastır.

(5) Kullanıcının ilk defa oturum açtığı durum haricinde, ödeme aracının ve kimlik doğrulama aracının kullanıcıya ulaştırılmasında kullanılan telefon numarası ve adres gibi bilgiler ile kullanıcı tarafından tanımlanan güvenli alıcılar listesinin ve tek bileşenli kimlik doğrulama kullanılarak yapılabilecek işlem listesinin değiştirilmesi, dördüncü fıkrada belirtilen iki bileşenli kimlik doğrulama kullanılarak gerçekleştirilir.

(6) 5549 sayılı Kanuna ilişkin yükümlülükler saklı kalmak üzere, dördüncü ve beşinci fıkralara göre iki bileşenli kimlik doğrulama ile gerçekleştirilmesi gereken işlemler için kullanıcının sözleşme ile ya da güvenli yöntemlerle onayının alınması veya ödeme işleminin güvenli alıcılar listesindeki bir alıcı ile gerçekleştirilmesi halinde iki bileşenli kimlik doğrulama uygulanması zorunlu değildir. Elektronik ortamdaki bir sözleşme ile alınacak onay yalnızca ilk defa oturum açılırken ve kullanıcının açıkça bilgilendirilmesi kaydıyla gerçekleştirilebilir.

(7) Kuruluş üst yönetiminin birinci fıkra kapsamında yaptığı risk değerlendirmesi sonucunda alınan karar neticesinde, kuruluşun dördüncü ve beşinci fıkralara uygun

olarak iki bileşenli kimlik doğrulama mekanizması sunmaması ya da altıncı fıkraya uygun olacak şekilde bir kullanıcı onayı bulunmadan iki bileşenli kimlik doğrulama kullanılmaksızın işlem gerçekleştirilmesi halinde, gerçekleştirilen işlemlerin kullanıcı tarafından yetkilendirilmiş olduğunu ispat yükümlülüğü kuruluşa aittir. Kullanıcısı belli olmayan ödeme araçları için bu ispat yükümlülüğü aranmaz.

(8) Kullanıcılara uygulanan kimlik doğrulamada kullanılacak parolaların yönetilmesi için günün teknolojisine uygun ve güvenli bir parola politikası belirlenir.

(9) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasında kullanılacak parola, değişken parola, tek kullanımlık parola cihazı, şifreleme gizli anahtarı, akıllı kart ve işlem doğrulama kodu gibi bileşenlerin üretim aşamalarından başlayarak kullanıcıya ulaştırılmasına kadar geçen sürecin tamamı boyunca güvenliği sağlanır.

(10) Kimlik doğrulama mekanizmasının;

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

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

c) Hiç bir işlem yapılmayan hareketsiz oturumlar için veya kullanıcının mobil uygulamadan güvenli bir şekilde çıkış yapmadan ayrılması nedeniyle bu uygulamanın arka planda çalışır şekilde kalması halinde oturumu belirli bir süre sonra sonlandırması,

ç) Birden fazla kullanıcının aynı ödeme hesabını kullanmaları ya da aynı anda farklı oturumlar açabilmeleri konusunda yetkilendirildiği durumlar hariç olmak üzere, aynı kullanıcı için aynı anda birden fazla oturum açılmaya çalışılması durumunda buna izin vermemesi ve kullanıcıya uyarı vermesi,

gerekir.

Bilgi sistemleri süreklilik planı

MADDE 10 – (1) Kuruluş, faaliyetlerini ve önemli iş fonksiyonlarını destekleyen bilgi sistemleri servislerinin sürekliliğini sağlamak üzere bilgi sistemleri süreklilik planı hazırlar. Bu plan üst yönetim tarafından onaylanır.

(2) Planın hazırlanması sürecinde, bilgi sistemleri varlıklarının ve tutulan verilerin önem düzeyi değerlendirilerek her bir servis için kabul edilebilir kesinti süreleri belirlenir ve bu süreler içinde servislerin tekrar erişime açılabilmesini sağlayacak kurtarma prosedürleri geliştirilir.

(3) Plan kapsamında ikincil merkez tesis edilir. Veri ve sistem yedekleri ikincil merkezde kullanıma hazır bulundurulur.

(4) Plan, kuruluşun bilgi sistemleri sürekliliğini etkileyecek olay ya da değişikliklerden sonra gözden geçirilerek güncellenir.

(5) Planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa ikincil merkez üzerinden testler yapılır, testlere varsa dış hizmet sağlayıcılar da dahil edilir, test sonuçları üst yönetime raporlanır ve bu sonuçlara göre plan güncellenir.

Bilgi sistemlerine ilişkin dış hizmet alım sürecinin yönetimi

MADDE 11 – (1) 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.

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

a) Hizmet seviyelerine ilişkin tanımlamalar.

b) Hizmetin sonlanma koşulları.

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 Kurumca talep edilen her tür bilgi ve belgeyi zamanında ve doğru olarak vermekle ve bunlara ilişkin her türlü elektronik, manyetik ve benzeri ortamlardaki kayıtları ve bu kayıtlara erişim ve kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifreleri incelemeye hazır bulundurmak ve işletmekle yükümlü olduğuna ilişkin hükümler.

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

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

(3) 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.

(4) Bilgi sistemlerinin bir bütün olarak veya kısmen dış hizmet alımına konu edilebilmesi ancak;

a) Kanun ve ilgili alt düzenlemelerin gerektirdiği yükümlülüklerin yerine getirilmesi bakımından yönetim, içerik tasarımı, erişim, kontrol, denetim, güncelleme, bilgi ve rapor alma gibi fonksiyonlarda karar alma gücünün ve sorumluluğun kuruluşta olması,

b) Yazılıma ilişkin fikri mülkiyet hakları saklı olmak üzere, alınan dış hizmet kapsamında oluşan tüm hesap, kayıt ve işlemlere ait her türlü bilgi ve belgenin mülkiyetinin kuruluşa ait olması,

şartıyla mümkündür.

(5) Kuruluş her türlü veriyi işlemek, saklamak ve iletmek için bir dış hizmet olarak bulut bilişim hizmetlerini kullanabilir. Ancak hassas ödeme verisini, kişisel bilgileri veya kullanıcıyla ilintilendirilebilir ve onu belirli ya da belirlenebilir kılan her türlü kullanıcı bilgisini 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.

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

Kullanıcıların bilgilendirilmesi

MADDE 12 – (1) Kuruluş tarafından sunulan hizmetlerden yararlanacak kullanıcılar; hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir. Kuruluş, sunmakta olduğu hizmetlere ilişkin riskler ve tehditler hakkında kullanıcılarını uyarır ve bu hususlarda kullanıcı farkındalığı oluşturulması için azami özen gösterir. Bu kapsamda asgari olarak aşağıdaki hususlar kullanıcının bilgisine sunulur:

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

b) Kuruluş tarafından kullanıcılara sunulan cihazlar, yazılımlar ya da mobil uygulamalar ile ödeme araçları ve hassas ödeme verilerinin kaybedilmesi, çalınması, silinmesi ya da değiştirilmesinin gerekmesi gibi durumlarda kullanıcıların takip etmesi gereken adımlar,

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

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

(2) Bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı kullanıcıların yaşayabileceği sorunların takip edilebileceği ve kullanıcıların şikâyetlerini ulaştırmalarına imkân tanıyacak mekanizmalar oluşturulur. Ulaşan şikâyetlerin en kısa sürede değerlendirilerek çözümlenmesi sağlanır.

(3) Kuruluş, kullanıcıya özel duyuru, uyarı ve benzeri sürekli bilgilendirme ihtiyaçlarını kullanıcıyla önceden mutabık kaldığı güvenli bir kanal üzerinden gerçekleştirir. Bu kanal üzerinden gelmeyen bilgilere itibar edilmemesi konusunda kullanıcılar bilgilendirilir.

(4) Kuruluş, kullanıcının işlem bilgilerini ve bakiye bilgilerini takip edebilmesine olanak sağlar. Bu kapsamda kullanıcının belirttiği iletişim veya elektronik posta adresine hassas ödeme verisi içermeyecek şekilde dekont gönderilmesi sağlanır.

(5) Kuruluşun internet sitesinde, kuruluşun ticaret unvanı, genel müdürlük adresi ve kuruluş ile Kurumun iletişim bilgilerine yer verilir. Bu madde kapsamında tanımlanmış olan kullanıcıların bilgilendirilmesine yönelik her türlü açıklama, kuruluşun internet sitesi üzerinden kullanıcı erişimine daima açık tutulur.

Kullanıcı bilgilerinin gizliliği

MADDE 13 – (1) Kuruluş, faaliyetlerinin yürütülmesi sırasında bilgi sistemleri aracılığıyla edindiği, işlediği, ilettiği veya sakladığı kullanıcı bilgilerinin gizliliği ve güvenliğini sağlamaya yönelik politika ve prosedürler oluşturur ve bunların gerektirdiği tedbirleri alır.

(2) Hassas ödeme verileri, dış hizmet sağlayıcılar ve kanunlarla açıkça yetkili kılınan merciler dışındaki taraflara verilemez. Hassas ödeme verisi dışındaki diğer kullanıcı bilgileri, kanunla açıkça yetkili kılınan merciler dışındaki taraflara, ancak paylaşım sınırları açıkça belirtilmek ve kullanıcıların önceden izinleri alınmak kaydıyla

verilebilir. Kullanıcı izni sözleşme ile ya da güvenli yöntemlerle alınır. Elektronik ortamdaki bir sözleşme ile alınacak onay yalnızca ilk defa oturum açılırken ve kullanıcının açıkça bilgilendirilmesi kaydıyla gerçekleştirilebilir.

İşlemlerin takibi

MADDE 14 – (1) Kuruluş, sahtekarlık ya da dolandırıcılık amaçlı işlemleri tespit etmek ve önlemek amacıyla işlem takip mekanizmaları tesis eder. Bu kapsamda şüpheli veya yüksek riskli işlemlerin filtrelenmesi ve değerlendirilmesi sağlanır.

(2) İşlem takip mekanizması işleme taraf kullanıcılar ile temsilciler, üye işyerleri ve hizmet noktalarında gerçekleştirilen tüm işlemleri kapsar.

(3) Yönetmeliğin 58 inci maddesine göre düşük değerli olan ödeme işlemlerinin kısa bir süre içinde sıklıkla gerçekleştirilmesi yüksek riskli işlem olarak değerlendirilir.

(4) Kuruluş, şüpheli ya da yüksek riskli işlemlerin gerçekleştirildiğini tespit etmesi halinde telefon ya da kısa mesaj gibi uygun yöntemlerle kullanıcıların en kısa sürede uyarılmasını sağlar. Kullanıcıya kısa sürede ulaşılabilecek bir iletişim bilgisinin kuruluş ile paylaşılmamış olması halinde bu fıkra hükmü uygulanmaz.

Üye işyerleri, temsilciler ve hizmet noktaları

MADDE 15 – (1) Kuruluş, üye işyerleri ve temsilciler ile yapacağı sözleşmelerde;

a) Hassas ödeme verilerinin gizliliğinin ve güvenliğinin sağlanması hususunda gerekli önlemlerin alınmasını,

b) Hizmetlerin gerçekleştirilmesi için gerekli olan terminaller ve kuruluş arasındaki iletişim haricinde, kendi nezdinde hassas ödeme verisini tutmamasını, işlememesini veya kaydetmemesini,

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

şart koşacak hükümlerin yer almasını sağlamakla yükümlüdür.

(2) Kuruluş, üye 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. Kullanıcıların, üye işyerlerinin hassas ödeme verilerini tutmasına, işlemesine veya kaydetmesine onay verdiği durumlarda birinci fıkranın (b) bendine uyum şartı aranmaz.

(3) Ödeme işlemlerinin veya elektronik para ile ilgili işlemlerin gerçekleştirilmesini sağlayan terminaller ve hizmet noktaları ile kuruluş arasında iki taraflı kimlik doğrulama ve uçtan uca güvenli iletişim olması esastır. Terminaller ve hizmet noktalarında işleme tabi tutulan hassas ödeme verilerine yetkisiz fiziki veya elektronik erişim engellenir.

(4) Kuruluş, temsilcilerine güncel sahtekârlık ve dolandırıcılık yöntemleri konusunda eğitim vermekle ve kullanıcılarını hizmet noktalarının güvenli kullanımı hususunda bilgilendirmekle yükümlüdür.

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

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

(7) Hizmet noktaları ve terminallere, fiziksel ya da mantıksal yetkisiz erişimi ve bunlar üzerine zararlı içerikli programların yüklenmesini engelleyecek tedbirler alınır.

(8) Hizmet noktalarına ve terminallere, güvenlik açıklıklarını gidermek amacıyla gerekli güncellemeler ve yamalar yüklenir.

(9) Hizmet noktalarında gerçekleştirilen işlemler için 9 uncu maddeye uygun olarak kimlik doğrulama gerçekleştirilir; 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, hizmet noktalarının bulunduğu yerlere güvenlik kamerası koyar. Güvenlik kamerası kayıtları kişilerin kimliklerinin tespit edilmesine yetecek görüntü kalitesinde en az iki ay süreyle saklanır ve kamera teçhizatının sağlıklı çalışıp çalışmadığı düzenli olarak kontrol edilir. Görüntüleme alanı bakımından 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 hizmet noktaları için güvenlik kamerası kurulma şartı, ilgili kamu güvenlik ve istihbarat kurumlarından izin alınabilmesi koşuluyla yerine getirilir.

Bilgi sistemlerine ilişkin sınırlamalar

MADDE 16 – (1) Kuruluşların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.

(2) Aynı kuruluşun kullanıcıları ya da farklı kuruluşların kullanıcıları 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 kullanıcısı olmadığı durumlarda, kuruluş işlemin kendi tarafında gerçekleşen kısımları için bu Tebliğ hükümlerine tabidir.

(4) Ödeme işleminin taraflarından birinin hizmet sağlayıcısının yurtdışında bulunması halinde; kendi kullanıcısına karşı tüm sorumluluğun kuruluşta olması ve kuruluşun söz konusu işlemleri kendi adına ve hesabına yürütmesi kaydıyla, yurt dışında bulunan hizmet sağlayıcıdan hizmet alınabilir veya bununla işbirliği yapılabilir. Bu fıkra kapsamında alınan hizmetler ile ilgili olarak 11 inci maddede yer alan hükümler uygulanmaz.

ÜÇÜNCÜ BÖLÜM
Bilgi Sistemlerinin Bağımsız Denetimi

Bilgi sistemlerinin bağımsız denetimi

MADDE 17 – (1) Bilgi sistemleri 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) Kuruluşun bilgi sistemleri denetimi ve denetim sonuçlarının Kuruma raporlanması birinci fıkradaki tanımla sınırlı olmak üzere, Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından belirlenen standartlara uygun olarak BSDHY ile belirlenen usul ve esaslar çerçevesinde, bağımsız denetçi tarafından gerçekleştirilir. Bu fıkranın uygulanmasında, BSDHY'nin 27 nci maddesinin ikinci fıkrasındaki koşul aranmaz.

(3) BSDHY ile belirlenen usul ve esaslar bu Tebliğ çerçevesinde uygulanırken BSDHY'de geçen "banka" ve "denetlenen" ibareleri kuruluşu, "bilgi sistemleri denetimi" ibaresi bu maddenin birinci fıkrasında tanımlanan denetimi ifade eder.

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

(5) Kuruluşta bilgi sistemleri denetimi iki yılda bir yapılır. Kurum, gerekli gördüğü hallerde bilgi sistemleri denetiminin kapsamını ve sıklığını farklılaştırabilir.

Yönetim beyanı

MADDE 18 – (1) Kuruluş bu Tebliğ hükümlerinin gereği olarak tesis ettiği iç kontroller hakkında denetim dönemi itibariyle güvence veren BSDHY'nin 33 üncü maddesi ve diğer alt düzenlemelerde belirtilen ve üst yönetim tarafından onaylanmış yönetim beyanını her denetim döneminde hazırlamakla yükümlüdür.

Denetim görüşünün oluşturulması ve denetim mektubu

MADDE 19 – (1) Kuruluşta gerçekleştirilen denetim sonucunda BSDHY'nin 5 inci ve 7 nci maddelerinde belirtilen hükümler ile 34 üncü maddesinde belirtilen görüş çeşitleri çerçevesinde; 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.

DÖRDÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Muafiyet ve istisnalar

MADDE 20 – (1) Kanunun sadece 12 nci maddesinin birinci fıkrasının (e) bendinde belirtilen ödeme hizmetini yürüten ödeme kuruluşu, ödeme hesabı açılmaksızın, kullanıcının fatura ödeme işlemelerini sadece ödeme kuruluşuna veya temsilcilerine gelerek yüz yüze gerçekleştirebilmesi ya da bu yöntemin yanında fatura ödeme işlemlerinin kuruluşun çağrı merkezi veya hizmet noktaları aracılığıyla gerçekleştirebilmesi halinde, bu Tebliğin sadece 13 üncü, 15 inci ve 16 ncı maddeleri hükümlerine tabidir. Bu kuruluş yapılan işlemlerle ilgili 8 inci maddenin dördüncü ve beşinci fıkralarına uygun olarak denetim izi tutar.

(2) Kanunun sadece 12 nci maddesinin birinci fıkrasının (e) bendinde belirtilen ödeme hizmetini yürüten ve kullanıcılarına internet üzerinden de hizmet sunan ödeme kuruluşları bu Tebliğin sadece 4, 5, 7, 8, 13, 14, 15 ve 16 ncı maddeleri hükümlerine tabidir.

(3) 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 3 üncü maddesinde tanımlanan üye iş yeri veya bu Tebliğde tanımlanan üye iş yeri olan ve 5464 sayılı Kanunda tanımlanan kart hamilinden ya da ödeme aracı hamilinden aldığı fonların alt anlaşma yaptığı üçüncü taraflara aktarılmasına aracılık eden kuruluşlar, sunmakta oldukları ödeme hizmetlerinin kapsamının sadece bu fıkrada belirtilen faaliyetler ile sınırlı olması kaydıyla, bu Tebliğin sadece 4, 5, 7, 8, 13, 14 ve 16 ncı maddeleri hükümlerine tabidir.

(4) Birinci, ikinci ve üçüncü fıkra kapsamındaki kuruluşlarda bağımsız bilgi sistemleri denetimi yapılmasına karar vermeye ve bu denetimin kapsam ve sıklığını belirlemeye Kurum yetkilidir.

Yürürlük

MADDE 21 – (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 22 – (1) Bu Tebliğ hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

EK-1

BİLGİ SİSTEMLERİ DENETİMİ RAPORU
Olumlu Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Denetçi Görüşü]
Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Denetçi Görüşü]
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 Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Denetçi Görüşü]
Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine 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 Denetçi Görüşü]
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