TEBLİĞ

Bankacılık Düzenleme ve Denetleme Kurumundan:

FİNANSAL KİRALAMA, FAKTORİNG VE FİNANSMAN ŞİRKETLERİNİN BİLGİ SİSTEMLERİNİN YÖNETİMİNE VE DENETİMİNE İLİŞKİN TEBLİĞ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç ve kapsam

MADDE 1 – (1) Bu Tebliğin amacı, finansal kiralama, faktoring ve finansman şirketlerinin 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, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanununun 14 üncü maddesinin ikinci fıkrası ve 24/4/2013 tarihli ve 28627 sayılı Resmî Gazete'de yayımlanan Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Kuruluş ve Faaliyet Esasları Hakkında Yönetmeliğin 14 üncü maddesine 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 Kanununda tanımlanan açık rızayı,

b) Birincil sistemler: Kanunda yer alan hususlarla ilgili 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,

c) 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,

ç) Denetim izi: Bir operasyonel ya da finansal işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtlar ile ilgili bilgi sistemi varlığına kimin eriştiğini, erişmeye çalıştığını ve kullanıcının hangi işlemleri gerçekleştirdiğini gösteren kayıtları,

d) Dış hizmet: Kuruluşların bilgi sistemlerine ilişkin dışarıdan temin ettikleri her türlü hizmet alımlarını,

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

f) İkincil sistemler: Birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin bilgi sistemleri süreklilik planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve Kanunda yer alan hususlarla ilgili bilgilere erişilmesini sağlayan birincil sistem yedeklerini,

g) Kanun: 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Hakkında Kanunu,

ğ) KGK: Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumunu,

h) Kontrol: BSDHY'nin 4 üncü maddesinde tanımlanan kontrolü,

ı) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

i) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

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

k) Şirket: Kanunun 3 üncü maddesinde tanımlanan şirketi,

l) Üst yönetim: Şirket 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,

ifade eder.

İKİNCİ BÖLÜM

Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler

Bilgi sistemleri yönetimi

MADDE 4 – (1) Şirket, kurumsal yönetim ilkelerinin uygulandığı yönetim kurulu onaylı bir bilgi sistemleri yönetim yapısı tesis eder. Şirketin bilgi sistemlerine ilişkin stratejisinin iş hedefleri ile uyumlu olması sağlanır. Bilgi sistemlerinin güvenliği ve gerektiği şekilde yönetimi için gerekli finansman ve insan kaynağı tahsis edilir.

(2) Şirket, bu amaçla bilgi sistemlerine ilişkin politika, prosedür ve süreçlerini tesis eder. Politika, prosedür ve süreçler düzenli olarak gözden geçirilerek güncellenir. Politikalar yönetim kurulu, prosedür ve süreçler üst yönetim tarafından onaylanır. Politika, prosedür ve süreçlerin fiili olarak işlemesi sağlanır. Bu kapsamda işleyişin sağlanması için süreç sahipleri ve sorumlulukları ile kontrol noktaları tanımlanır. Bilgi sistemlerinin kendisinden beklenen

hizmetleri zamanında, doğru ve güvenilir şekilde sağlaması için gereken kontroller belirlenir ve bu kontrollerin etkinliği sağlanır.

(3) Bilgi sistemleri kullanılarak gerçekleştirilen işlemlerin kontrolü, izlenmesi ve inkar edilemezliğin sağlanması için gerekli süreç ve altyapılar tesis edilir.

(4) Şirket iç kontrol birimi yılda bir kez, yönetim kuruluna sunulmak üzere, politika ve prosedürlere uyuma ilişkin hususları da içeren mevzuata uyum değerlendirmesi raporu hazırlar.

Bilgi sistemleri risk yönetimi

MADDE 5 – (1) Şirket, faaliyetlerinde bilgi teknolojilerinin kullanılmasından kaynaklanan riskleri tespit etmek, analiz etmek, ölçmek, izlemek ve raporlamak üzere üst yönetim tarafından onaylanmış bir risk yönetim süreci oluşturur. Şirket, riskleri takip ederek gözden geçirir ve günceller. Süreç kapsamında, Tebliğin 10 uncu maddesinin birinci fıkrası uyarınca hazırlanan envanterdeki varlıklara yönelik tehditlere, riskin ortaya çıkma ihtimaline, riskin gerçekleşmesi durumunda ortaya çıkacak olası sonuçlara ve alınabilecek önlemlere ilişkin bir değerlendirmede bulunur. Şirket yapacağı risk analizinde, belirlediği her riske ilişkin; riski azaltma, riskten kaçınma, riski kabul etme veya riski transfer etme yöntemlerinden birini seçer.

(2) Şirket risk analizi yaparken, hizmetlerini sunmak için kullandığı teknoloji altyapısını, uygulama mimarisini, sistem üzerinde tutulan verinin kritikliğini, dış hizmet sağlayıcılardan kaynaklanabilecek riskleri ve teknolojik gelişmeleri dikkate alır. Yapılacak risk analizinde kullanıcı bilgilerinin güvenliğini ve gizliliğini tehdit eden riskler dikkate alınır.

(3) Şirket, bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce olası riskleri değerlendirir; veri kaybını, hizmet kesintisini ve ilave riski önlemeye yönelik tedbirleri alır.

(4) Şirket, yılda bir kez üst yönetime sunulmak üzere bilgi sistemlerine ilişkin öngörülen risk ve tehditleri içeren risk değerlendirme raporu hazırlanmasını sağlar.

Bilgi güvenliği yönetimi

MADDE 6 – (1) Şirket, bilgi güvenliğine ilişkin süreci tesis eder. Yönetim kurulu onaylı Bilgi Güvenliği Politikası içerisinde bilgi güvenliğine ilişkin süreci, rolleri ve sorumlulukları belirler.

(2) Şirket, bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemleri tesis eder.

(3) Şirket, bilgi sistemleri üzerinde edinilen, saklanan, iletilen, işlenen verileri güvenlik hassasiyet derecelerine göre sınıflandırır ve her sınıf için uygun düzeyde güvenlik kontrolü tesis eder.

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

(5) Şirket, dışarıdan gelecek bir siber saldırıya karşı gerekli önlemleri alır ve 2 yılda bir sızma testi yaptırır.

(6) Şirket, bilgi güvenliği hususunda personelin farkındalığını arttıracak bilgilendirme veya çalışmalar yapar.

(7) Şirket, yılda bir kez yönetim kuruluna sunulmak üzere; yetkisiz erişim teşebbüslerini, bilgi güvenliği sürecine uyum durumunu, bilgi güvenliği ihlaline ilişkin olayları içeren güvenlik ihlalleri raporu hazırlanmasını sağlar.

Yetkilendirme ve erişim kontrolü

MADDE 7 – (1) Şirket, veritabanlarına, uygulamalara ve sistemlere erişim için uygun bir yetkilendirme ve erişim kontrolü tesis eder. Görev ve sorumluluklar göz önünde bulundurularak, gerekli olan en kısıtlı yetki ve erişim hakkı verilir. Yetkiler ve erişim hakları en az yetki prensibi açısından asgari yılda bir kez gözden geçirilir. Sistem, servis ve veriye sadece gerekli yetkiye sahip kullanıcı, taraf ve sistemlerin erişimi mümkün kılınır.

(2) Şirket, veritabanlarına, uygulamalara ve sistemlere yapılan yetkisiz erişim teşebbüslerini kayıt altına alır ve gözden geçirir.

(3) Şirket, sunmakta olduğu hizmetlerin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesi aşamalarında, görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlar. Süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından girilmesi, yetkilendirilmesi ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir.

(4) Geçici yetkilendirmeler için yetkilendirmenin yapılacağı şartlar ve geçerli olacağı süre belirlenir. Geçici yetkilendirmeye ilişkin ilave iz kaydı tutulur.

(5) Şirket veya dış hizmet sağlayıcı bünyesinde görev yapan çalışanların görevlerinin sonlanması durumunda ilgili tüm yetkilendirmeler ivedilikle sonlandırılır.

Kimlik doğrulama

MADDE 8 – (1) Bilgi sistemleri üzerinde gerçekleşen işlemler için işlemlerin türü, niteliği, bir ihlal halinde oluşabilecek kayıplar, işlem çeşidi ve verinin hassasiyet derecesi dikkate alınarak uygun bir kimlik doğrulama mekanizması kurulur. Aynı kullanıcı hesabının birden fazla kişi tarafından kullanılması engellenir.

(2) Kimlik doğrulamada kullanılacak parolaların geçerlilik süresinin, karmaşıklığının ve uzunluğunun günün teknolojisine ve işlemin niteliğine uygun olması sağlanır.

(3) Şirket, kimlik doğrulamada inkar edilemezliği sağlar. Tüm kullanıcılara ait kimlik doğrulama bilgilerinin gizliliğine ve güvenliğine yönelik gerekli önlemleri alır. Parola gibi kritik öneme sahip veriler günün teknolojisine uygun şekilde şifreli veya matematiksel olarak geri döndürülmesi mümkün olmayan yöntemlerle muhafaza edilir, aktarılırken şifrelenir ve yetkisiz erişimlere karşı güvenliği sağlanır.

(4) Donanım ve yazılımlara ait kurulumda tanımlanmış varsayılan şifreler değiştirilir. Yeni şifreler güvenli bir şekilde saklanır.

(5) Başarısız kimlik doğrulama teşebbüslerinin belirli bir sayıyı aşması halinde erişim engellenir ve engellemenin kullanıcı adından veya paroladaki bir hatadan kaynaklandığı şeklinde gereksiz bilgi verilmez.

(6) Kimlik doğrulamada, önceden izin verilen durumlar hariç olmak üzere, aynı kullanıcıya ait birden fazla oturum açılması engellenir ve kullanıcıya birden fazla oturum açtığı konusunda uyarı verilir. Belli bir süre işlem yapılmayan oturumun sonlandırması sağlanır.

(7) Dış hizmet sağlayıcılarında görevli personelin şirket sistemlerine uzaktan erişimi esnasında yapılacak kimlik doğrulama, en az şirket personeli ile aynı seviyede güvenlik sağlanarak yapılır.

Denetim izlerinin oluşturulması

MADDE 9 – (1) Şirketin faaliyetlerine ilişkin etkin bir denetim izi mekanizması tesis edilir. Şirket faaliyetlerine ve müşterilere ilişkin bilgilere erişilmesi, sorgulanması, bunlara yönelik erişim yetkilerinin verilmesi veya değiştirilmesine yönelik işlemler ve bunlara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları tutulur.

(2) Şirketin, web servisleri, uygulama programlama arayüzü ya da benzeri metotlarla diğer kurum/kuruluşlar nezdinde tutulan hassas veriler ile kişisel verilere ilişkin yaptıkları sorgulamalar ve bu sorgulamaları hangi amaçla yaptıklarına ilişkin iz kayıtları da denetim izi kapsamındadır. Şirket, sorguladığı verinin amacı dışında kullanımının önüne geçmek için gerekli tedbirleri alır.

(3) Denetim izlerinin, bütünlüğünün bozulmasına, değiştirilmesine imkan vermeyecek şekilde ve raporlanabilir bir formatta tutulması esastır. Denetim izleri, işleme ilişkin olarak; tarih, zaman, uygulama bilgisi, kullanıcı adı, hangi bilginin sorgulandığı, değiştirildiği şeklinde detay bilgileri içerir.

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

(5) Sistem ve veritabanlarında, ayrıcalıklı yetkiye sahip veya yönetici hesapları ile yapılan erişimler kontrol altına alınır, ilave iz kayıtları tutulur. Denetim izlerinin bulunduğu sistemlerde yönetici hesapları dahil hiçbir kullanıcının kayıtlar üzerinde değişiklik yapabilmesine izin verilmez.

(6) Bilgi ve belge saklamaya ilişkin diğer mevzuat hükümleri saklı kalmak kaydıyla denetim izleri asgari 3 yıl süreyle denetime hazır bulundurulur ve yedek alınması suretiyle, yaşanacak olası felaketler sonrasında da erişilebilir olmaları temin edilir.

(7) Şirket, dış hizmet sağlayıcıdan aldığı hizmet kapsamında; dış hizmet sağlayıcı tarafından tutulan denetim izlerinin kendi standartlarına uygunluğunu ve denetim izlerinin kendisi tarafından erişilebilir olmasını temin eder.

Bilgi sistemleri varlıklarının yönetimi

MADDE 10 – (1) Bilgi sistemleri unsurları olan donanım, yazılım ve verinin yönetimine ilişkin olarak süreç tesis edilir. Şirket bilgi sistemleri varlık envanterini aşağıdaki çerçevede oluşturur:

a) Donanım envanteri: Donanım envanteri, kurumsal ağa bağlı olup olmadığına bakılmaksızın; üzerinde şirkete ait bilgi bulunduran, bilginin görüntülenmesine, iletilmesine ve çıktı alınmasını sağlayan tüm fiziksel cihazları ve manyetik ortamları içerir. Kurumsal kaynaklara erişmek ve işlem yapmak için personelin kullandığı kişisel cihazlar da envantere dahil edilir. Envanterde, asgari olarak donanımın türü, markası, modeli, alım tarihi, envantere giriş ve çıkış tarihi, fiziksel lokasyonu, üzerinde bulunan uygulamalar ile konfigürasyon veya diğer değişiklikleri yapmaya yetkililer, sahiplik bilgisi, yedeğinin olup olmadığı, kritiklik düzeyi bilgileri yer alır.

b) Yazılım envanteri: Kurumsal olarak kullanılan ve şirket donanımları üzerinde bulunan, aktif olarak hizmet verip vermediğine bakılmaksızın tüm yazılımları içerir. Bu yazılımlar haricinde, şirket tarafından uzaktan kullanılan yazılım hizmetleri ve kurumsal kaynaklara erişmek için kullanılan kişisel cihazlardaki ilgili uygulamalar da envantere dahil edilir. Envanterde, asgari olarak versiyon, eriştiği veri, üzerinde çalıştığı donanım, geliştirme ortamı, kritiklik düzeyi bilgileri yer alır.

c) Veri envanteri: Şirketin bilgi sistemleri üzerinde bulunan faaliyetleri kapsamındaki verileri içerir. Envanterde, asgari olarak, bulunduğu veritabanı, yedeğinin alınıp alınmadığı, yedeğin mantıksal adresi, veriyi kullanan uygulamalar, kimin erişebildiği, verinin kritiklik düzeyi bilgileri yer alır.

(2) Bilgi sistemleri varlık envanteri güncel olarak takip edilir, son 3 yıla ait envanter kayıtları saklanır. Envanterden çıkarılan donanımların şirkete ait bilgi taşımaması için gerekli tedbirler alınır.

(3) Şirket bilgi sistemleri üzerinde yer alan yazılımların güncelliğini sağlar. Bunun için yama yönetimi ile ilgili süreç tesis edilerek güncel yamalar takip edilir. Kullanılan yazılımların önceki versiyonları güvenli şekilde saklanır.

(4) Üretim ortamında kullanılan yazılımların test ortamında test edilip onaylanan versiyon ile aynı olması sağlanır ve üretim ortamındaki değişiklikler ilgili yönetici onayı alınarak gerçekleştirilir. Bu amaçla, üretim ortamına

erişim kısıtlanır, ihtiyaç halinde geçici süreyle verilen yetkiler kayıt altına alınır. Yazılım ve veritabanı değişiklikleri sistemsel olarak izlenebilir hale getirilirek kayıt altına alınır, manuel müdahale en aza indirilir.

(5) Şirket bilgi sistemlerinin fiziksel güvenliğinin sağlanması amacıyla;

a) Bilgi sistemlerinin bulunduğu alanın güvenliğini sağlar, alanın içeriden ve dışarıdan gelebilecek tehditlerden korunması için gerekli tedbirleri alır.

b) Sistem odasına giriş ve çıkışlar kontrol altına alınır, giriş ve çıkışa ilişkin bilgiler kişiyi tanımlamaya ilişkin bilgileri de içerecek şekilde kayıt altına alınır.

c) Birincil, ikincil sistem odaları ve girişlerini kamera ile izlenir hale getirir. İlgili kayıtları en az 6 ay saklar.

Bilgi sistemleri süreklilik planı

MADDE 11 – (1) Şirket, faaliyetlerini ve önemli iş fonksiyonlarını destekleyen bilgi sistemleri servislerinin sürekliliğini sağlamak üzere yönetim kurulu tarafından onaylanmış bir bilgi sistemleri süreklilik planı hazırlar.

(2) Planın hazırlanması sürecinde, bilgi sistemleri varlıklarının 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) Planda ilgili bilgi sistemleri bileşenleri sorumluları ve iş sorumluları belirtilir. Uygulanması gereken kurtarma ve geri dönüş adımları ile bu adımların hangi koşullarda uygulanacağı tanımlanır.

(4) Plan, şirketin bilgi sistemleri sürekliliğini etkileyecek olay ya da değişikliklerden sonra veya her yıl gözden geçirilerek güncellenir ve yönetim kurulu tarafından onaylanır.

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

(6) 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 yönetim kuruluna raporlanır ve bu sonuçlara göre planın güncellenmesi sağlanır.

Dış hizmet alımı ve yönetimi

MADDE 12 – (1) Bilgi sistemlerinin dış hizmete konu edilebilmesi ancak Kanun ve Kanuna ilişkin alt düzenlemelerden kaynaklanan görev ve sorumlulukların yerine getirilmesi sırasında yönetim, içerik tasarımı, erişim, kontrol, denetim, güncelleme, bilgi/rapor alma gibi fonksiyonlarda karar alma gücü ve sorumluluğunun şirkette olması ile mümkündür.

(2) Şirket üst yönetimi, bilgi sistemleri kapsamında dış hizmet alımına ilişkin olarak, söz konusu hizmetin dış hizmet alımı yoluyla gerçekleştirilmesinin şirket açısından doğuracağı riskleri değerlendirir. Bu kapsamda, şirket üst yönetimi, dış hizmet alımı yoluyla gerçekleştirilen servisler için servisin içeriğine uygun olarak; hizmet seviyesini, kalitesini ve güvenlik kontrollerini, firmanın mali yapısını da değerlendirerek hizmet alımını gerçekleştirir.

(3) Şirket bilgi sistemleri kapsamında dış hizmet alımına ilişkin asgari olarak aşağıdaki ilkeleri gözetir:

a) Dış hizmet alımı kapsamındaki tüm sistem ve süreçlerin şirketin kendi risk yönetimi, güvenlik ve gizlilik politikalarına uygunluğunun sağlanması,

b) Sözleşmeye konu ürün ve hizmetlerin sahipliği ve fikri mülkiyet haklarının belirlenmesi,

c) Dış hizmet sağlayıcılar için yükümlülük teşkil eden hükümlerin alt yükleniciler ile yapılacak olan sözleşmelerde de bağlayıcılığının sağlanması,

ç) Dış hizmet alımının, planlananın dışında sonlanmasından veya kesintiye uğramasından kaynaklanacak risklerin yönetilmesi,

d) Şirketin tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde dış hizmet sağlayıcılar için de uygulanması ve Kurul veya Kurum talimatı ile şirketin bilgi sistemleri üzerinde gerçekleştirilmesi gereken değişikliklerin, alınan hizmet kapsamında dış hizmet sağlayıcı tarafından talimat süresi içerisinde yerine getirilmesinin sağlanması,

e) Dış hizmetin alt yükleniciye devrinin şirketin izinine tabi olduğuna ilişkin hükümler, şirketin risk değerlendirmesi yapmak suretiyle yazılı olarak dış hizmet sağlayıcıya izin vermesi haricinde dış hizmetin alt yükleniciye devrinin kısıtlanması,

f) Dış hizmet alımı kapsamındaki faaliyetlerin şirket bünyesinde gerçekleştirilmesi durumunda, bağımsız denetim açısından hangi denetimlere tabi tutulması öngörülüyorsa, kapsam daraltılmasına gidilmeden aynı denetimlere tabi tutulmasının sağlanması,

g) 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 olması.

(4) Şirket, dış hizmet sağlayıcıların erişimleri için gerekli kontrolleri tesis eder. Veri ve sistem güvenliği açısından sağlanan erişimler, verilen erişim hakları ve tesis edilen kontroller düzenli olarak gözden geçirilir.

(5) Şirket dış hizmet olarak bulut bilişim hizmetlerini kullanabilir. Birincil ve ikincil sistemler için bulut hizmeti, tek bir şirkete tahsis edilmiş donanım ve yazılım kaynakları üzerinden özel bulut hizmet modeliyle alınabilir. Bunun

yanında, sadece Kurumun denetimine tabi şirketlere tahsis edilmiş donanım ve yazılım üzerinde, şirketler arasında mantıksal ayrıma gidilerek topluluk bulutu hizmet modeliyle dış hizmet alınması Kurum iznine tabidir. Ayrıca, Kanuna tabi bir şirketin ana ortağı, iştiraki ve ana ortağın iştirakleriyle birlikte donanım ve yazılım üzerinde, şirketler arasında mantıksal ayrıma gidilerek kullanılması da Kurum iznine tabidir.

(6) Şirket, dış hizmet alımlarında şirketin kendisine, kullanıcılarına ve müşterilerine ait gizli bilgilerin güvenliğinin sağlanması için gerekli tedbirleri almakla yükümlüdür. Dış hizmet sağlayıcılara verilecek erişim yetkisi işin gerektirdiği bilgiyi kapsayacak şekilde sınırlandırılır. Dış hizmet sağlayıcı tarafından şirkete ve kullanıcılarına ait gizli bilgilerin korunmasına yönelik tedbirlerin alınmasını sağlamak şirketin sorumluluğundadır.

İşlem bilgilerinin gizliliği

MADDE 13 – (1) Şirket faaliyetlerinin yürütülmesi sırasında edindiği, işlediği, ilettiği veya sakladığı işlem ve müşteri bilgilerinin gizliliğini ve güvenliğini sağlamaya yönelik politika, prosedürleri oluşturur ve gerekli tedbirleri alır.

(2) Şirket, Kanunla yetkili kılınmış taraflar haricinde, müşterilerine ait her türlü bilgi ve belgeyi kişinin açık rızası olmadan, toplandığı amaçlar dışında kullanamaz veya kullanılması için başkasına aktaramaz.

(3) Şirket tarafından sunulacak bir hizmet, müşteriye ait bilgi ve belgelerin paylaşılması amacıyla açık rıza vermesi şartına bağlanamaz.

ÜÇÜNCÜ BÖLÜM
Bilgi Sistemlerinin Bağımsız Denetimi ve Diğer Hükümler

Bilgi sistemlerinin bağımsız denetimi

MADDE 14 – (1) Bilgi sistemleri denetimi; şirketin bu Tebliğ hükümlerine uyumluluğunun tespit edilmesi amacıyla, bilgi sistemleri yönetimi kapsamında yer alan faaliyet, süreç, 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) Şirketin bilgi sistemleri denetimi ve denetim sonuçlarının Kuruma raporlanması birinci fıkradaki tanımla sınırlı olmak üzere, KGK tarafından belirlenen standartlara uygun olarak BSDHY'nin denetim ile ilgili beşinci bölümünde 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 şirketi, "bilgi sistemleri denetimi" ibaresi bu maddenin birinci fıkrasında tanımlanan denetimi ve Kanun ibaresi bu Tebliğde tanımlanan Kanunu ifade eder.

(4) Bağımsız denetçi, şirketin 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) Şirkette bilgi sistemleri denetimi üç yılda bir yapılır. Bu denetimin yapılacağı şirketi, denetimin yapılacağı yılı ve raporların gönderileceği tarihi belirlemeye Kurum yetkilidir. Kurum, gerekli gördüğü hallerde bilgi sistemleri denetiminin kapsamını ve sıklığını farklılaştırabilir.

(6) Denetim görüşünün oluşturulması ve denetim mektubu; şirkette 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.

Diğer hükümler

MADDE 15 – (1) Şirket sunduğu internet hizmetleri kapsamında;

a) Müşterinin işlem gerçekleştirdiği platformun şirkete ait olduğunu garanti eden,

b) İşlemin taşıdığı risklerle uyumlu olarak gerekli kimlik doğrulama mekanizmasını sağlayan,

c) Kullanıcıları güvenlik riskleri hakkında bilgilendiren,

bir yapı tesis eder.

(2) Şirket birincil ve ikincil sistemlerini yurt içinde bulundurur. Bu kapsamda dış hizmet alınması halinde, dış hizmet sağlayıcının söz konusu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların tüm yedekleri de yurt içinde tutulur.

DÖRDÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Geçiş süreci

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

Yürürlük

MADDE 16 – (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 17 – (1) Bu Tebliğ hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

Ekleri için tıklayınız.