BİLGİ SİSTEMLERİ YÖNETİMİNE İLİŞKİN USUL VE ESASLAR TEBLİĞİ
(VII-128.10)

(13/3/2025 tarihli ve 32840 sayılı Resmi Gazetede yayımlanmıştır.)

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1- (1) Bu Tebliğin amacı, 2 nci maddede sayılan Kurum, Kuruluş ve Ortaklıkların bilgi sistemlerinin yönetimine ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Aşağıdaki Kurum, Kuruluş ve Ortaklıklar, bu Tebliğ hükümlerine uymakla yükümlüdürler:

a) Borsa İstanbul A.Ş.,

b) Borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri,

c) Emeklilik yatırım fonları,

ç) İstanbul Takas ve Saklama Bankası A.Ş.,

d) Merkezi Kayıt Kuruluşu A.Ş.,

e) Portföy saklayıcısı kuruluşlar,

f) Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.,

g) Sermaye piyasası kurumları,

ğ) Halka açık ortaklıklar,

h) Türkiye Sermaye Piyasaları Birliği,

ı) Türkiye Değerleme Uzmanları Birliği,

i) Kripto Varlık Hizmet Sağlayıcılar.

(2) Birinci fıkrada sayılan Kurum, Kuruluş ve Ortaklıklardan, 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununun 136 ncı maddesi uyarınca banka ve sigorta şirketleri ile 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanunu uyarınca finansal kiralama, faktoring, finansman ve tasarruf finansman şirketlerinin bilgi sistemlerinin, kendi özel mevzuatlarında belirlenen ilkeler çerçevesinde yönetilmesi, bu Tebliğde öngörülen yükümlülüklerin yerine getirilmesi hükmündedir.

Dayanak

MADDE 3- (1) Bu Tebliğ, 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununun 128 inci maddesinin birinci fıkrasının (h) bendine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4- (1) Bu Tebliğde geçen;

a) API: Bir yazılımın başka bir yazılımda tanımlanmış işlevleri kullanabilmesi için oluşturulmuş uygulama programlama ara yüzünü,

b) Bilgi güvenliği ihlali: Bilgi sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını, siber olayı,

c) Bilgi sistemleri: Bilginin işlendiği, iletildiği ve saklandığı yazılım, donanım ve iletişim altyapısı ile bunlarla etkileşimde bulunan insan kaynağı, faaliyet ve süreçlerin tümünü,

ç) Bilgi varlığı: Kurum, Kuruluş ve Ortaklıkların Kanundan ve Kanuna ilişkin alt düzenlemelerden kaynaklanan görevlerini yerine getirmeleri esnasında kullandıkları veri ile bunların üretildiği, işlendiği, iletildiği ve saklandığı donanım ve yazılım unsurlarını,

d) Birincil sistemler: Kurum, Kuruluş ve Ortaklıkların Kanundan ve Kanuna ilişkin alt düzenlemelerden kaynaklanan görevlerini yerine getirmeleri için gerekli bilgilerin elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamını,

e) Bütünlük: Bilginin doğruluğu ve tamlığını koruma özelliğini,

f) Çok faktörlü kimlik doğrulama: Kimlik doğrulama işleminin; kişinin bildiği, kişinin sahip olduğu veya kişinin biyometrik karakteristiği olan doğrulama faktörleri arasından iki veya daha fazla farklı faktörün kullanılarak gerçekleştirilmesini,

g) Denetim izi: Bilgi sistemleri aracılığıyla gerçekleşen işlemlerin ve bilgi güvenliği ihlal olaylarının başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtlar ile bu kayıtlar üzerinde yapılan işlemleri gösteren kayıtları,

ğ) Erişilebilirlik: Bilginin yetkili kullanıcı, uygulama veya sistem tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini,

h) Gizlilik: Bilgi sistemlerine ve bilgiye sadece yetkili kullanıcı, uygulama veya sistem tarafından erişilebilmesini,

ı) Güvenli alan: Bilgi işleme, iletişim ve depolama donanımlarını barındıran alanı,

i) Hassasiyet: Kurum, Kuruluş ve Ortaklıkların bünyesinde saklanan, müşterilere ait olan ve üçüncü kişilerce ele geçirilmesi halinde ilgili kişinin zarar görmesine, dolandırılmasına ya da sahte işlem yapılmasına sebep olabilecek verinin niteliğini,

j) 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 ve Kanuna ilişkin alt düzenlemelerde Kurum, Kuruluş ve Ortaklıklar için tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan birincil sistemin tüm yedeklerini,

k) Kanun: 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununu,

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

m) Kontrol: Bilgi sistemleri süreçleriyle ilgili olarak gerçekleştirilen ve iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların belirlenmesi, engellenmesi ve düzeltilmesine ilişkin yeterli derecede güvence oluşturmayı hedefleyen politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,

n) Kripto varlık hizmet sağlayıcı: Platformları, kripto varlık saklama hizmeti sağlayan kuruluşları ve kripto varlıkların ilk satış ya da dağıtımı dâhil olmak üzere kripto varlıklarla ilgili olarak hizmet sağlamak üzere belirlenmiş diğer kuruluşları,

o) Kritiklik: Bilgi varlığının, Kurum, Kuruluş ve Ortaklıkların iş hedeflerine ulaşmasındaki önemini veya gerekliliğini belirten niteliğini,

ö) Kullanıcı: Kurum, Kuruluş ve Ortaklıkların bilgi sistemlerinde kendisi adına hesap açılan Kurum, Kuruluş ve Ortaklıklar personelini, dışarıdan hizmet sağlayıcının personelini veya Kurum, Kuruluş ve Ortaklıkların müşterisini,

p) Kurul: Sermaye Piyasası Kurulunu,

r) Kurum, Kuruluş ve Ortaklıklar: 2 nci maddede sayılan kurum, kuruluş ve ortaklıkları,

s) Kurumsal SOME: SOME Tebliği kapsamında Kurum, Kuruluş ve Ortaklıklar tarafından kurulan Kurumsal Siber Olaylara Müdahale Ekibini,

ş) Platform: Kripto varlık alım satım, ilk satış ya da dağıtım, takas, transfer, bunların gerektirdiği saklama ve belirlenebilecek diğer işlemlerin bir veya daha fazlasının gerçekleştirildiği kuruluşları,

t) Politika: Kurum, Kuruluş ve Ortaklıkların hedef ve ilkelerini ortaya koyan ve yönetim kurulu veya üst yönetimi tarafından onaylanmış dokümanı,

u) Prosedür: Süreçlere ilişkin işlem ve eylemleri tanımlayan dokümanı,

ü) Saklama kuruluşu: Kripto varlık saklama hizmetinde bulunmak üzere Kurulca yetkilendirilmiş kuruluşu,

v) Sektörel SOME: SOME Tebliği kapsamında Kurul bünyesinde kurulan Sektörel Siber Olaylara Müdahale Ekibini,

y) Sermaye piyasası kurumları: Kanunun 35 inci maddesinde sayılan kurumları,

z) SOME Rehberi: Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanmış en güncel "Kurumsal SOME Kurulum ve Yönetim Rehberi" dokümanını,

aa) SOME Tebliği: 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği,

bb) Süreç: Bir işin yapılış ve üretiliş biçimini oluşturan sürekli işlem ve eylemleri,

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

çç) USOM: Bilgi Teknolojileri ve İletişim Kurumu bünyesinde yer alan Ulusal Siber Olaylara Müdahale Merkezini,

dd) Üçüncü taraf: Kurum, Kuruluş ve Ortaklıklar ile müşteriler dışında kalan gerçek veya tüzel kişileri,

ee) Üst yönetim: Yönetim kurulu tarafından belirlenen kişi ya da grubu, yönetim kurulu tarafından belirleme yapılmadığı durumlarda ise Kurum, Kuruluş ve Ortaklıkların en üst yetkilisini,

ff) Varlık sahibi: Bilgi varlıklarına yönelik güvenlik gereksinimlerini belirleyen ve bu gereksinimlere uyumu gözeterek bilgi varlığının idamesi ve güvenliğinden sorumlu olan kişi veya birimi,

ifade eder.

İKİNCİ BÖLÜM
Bilgi Sistemlerinin Yönetilmesi

Bilgi sistemleri yönetiminin oluşturulması ve hayata geçirilmesi

MADDE 5- (1) Bilgi sistemlerinin yönetimi, kurumsal yönetim uygulamalarının bir parçası olarak ele alınır. Kurum, Kuruluş ve Ortaklıkların operasyonlarını istikrarlı, rekabetçi, gelişen ve

güvenli bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejilerinin iş hedefleri ile uyumlu olması sağlanır, bilgi sistemleri yönetimine ilişkin unsurlar yönetsel hiyerarşi içerisinde yer alır ve bilgi sistemlerinin güvenlik, performans, etkinlik, doğruluk ve sürekliliğini hedefleyerek doğru yönetimi için gerekli finansman ve insan kaynağı tahsis edilir. Bu amaçla oluşturulan bilgi sistemleri stratejisi ilgili taraflara duyurulur. Bilgi sistemleri stratejisinin iş hedefleriyle uyumu gözetilir ve gerektiğinde iyileştirici faaliyetler uygulanır.

(2) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemlerinin yönetimine ilişkin kontrolleri tesis eder, bunlara ilişkin politika, prosedür ve süreçleri yazılı hale getirir, düzenli olarak gözden geçirerek iş alanında gerçekleşen değişiklikler veya teknolojik gelişmeler doğrultusunda günceller, yönetim kurulu veya üst yönetim tarafından onaylanmasını ve ilgililere duyurulmasını sağlar.

(3) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri yönetimi konusunda rol ve sorumlukları belirleyerek yazılı hale getirir. Üst yönetim tarafından görevler ayrılığı ilkesi çerçevesinde görevlendirmeler yapılır.

Bilgi güvenliği politikası

MADDE 6- (1) Bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik olarak bilgi güvenliği politikası üst yönetim tarafından hazırlanır ve yönetim kurulu tarafından onaylanır. Onaylanan bilgi güvenliği politikası personele ve ilgili diğer taraflara duyurulur.

(2) Bilgi güvenliği politikası, bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin, sorumlulukların belirlenmesini ve görev tanımlarının yapılmasını, hedeflerin belirlenmesini, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini, değerlendirilmesini ve gözetimini kapsar.

(3) Bilgi güvenliği politikası yılda en az bir defa gözden geçirilir; iş ihtiyaçları, değişen tehdit ve risklere göre güncellenir.

Üst yönetimin gözetimi ve sorumluluğu

MADDE 7- (1) Bilgi güvenliği politikasının ve bilgi sistemleri stratejisinin uygulanması üst yönetim tarafından gözetilir. Bilgi güvenliği politikası kapsamında bilgi sistemleri kontrollerinin etkin, yeterli ve uyumlu bir şekilde tesis edilmesi, değerlendirilmesi ve gözetimi yönetim kurulunun sorumluluğundadır.

(2) Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projeler üst yönetim tarafından gözden geçirilir ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanır. Kritik projelerin Kurum, Kuruluş ve Ortaklıkların iç kaynaklarıyla veya dışarıdan hizmet alımı yoluyla gerçekleştirilmesine bakılmaksızın personel uzmanlığının, projelerin teknik gereksinimlerini karşılayabilecek nitelikte olması esastır. Bu yapıyı desteklemek üzere oluşturulacak yönetsel rol ve sorumluluklar açıkça belirlenir.

(3) Kurum, Kuruluş ve Ortaklıkların üst yönetimi, bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder. Üst yönetim, asgari olarak aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

a) Bilgi güvenliği politikalarının ve tüm sorumlulukların yılda en az bir kez gözden geçirilmesi ve onaylanması.

b) Bilgi sistemlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetimi sürecinin oluşturulması.

c) Bilgi güvenliği ihlallerinin takip edilmesi ve yılda en az bir kez değerlendirilmesi.

ç) Personele bilgi güvenliği gereksinimleri, riskler ve güncel tehditler konusunda bilgi düzeyini artırmaya yönelik eğitimlerin rol ve sorumluluklarına uygun şekilde yılda en az bir kez verilmesi.

(4) Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen kontroller, Kurum, Kuruluş ve Ortaklıkların organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir ve işlerliğine ilişkin gözetim ve denetim süreçleri tesis edilir.

(5) Bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hususunda üst yönetime rapor veren, bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde yeterli teknik bilgiye ve en az 5 yıl tecrübeye sahip bir bilgi güvenliği sorumlusu belirlenir. Bilgi güvenliği sorumlusunun, bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevinin bulunmaması ve üst yönetime bağlı çalışması sağlanır.

(6) Asgari olarak kritik iş süreçlerini ve faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere iş sürekliliği planının bir parçası olan bilgi sistemleri süreklilik planı hazırlanır.

Bilgi sistemleri risk yönetimi

MADDE 8- (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemlerine ilişkin riskleri belirlemek, ölçmek, izlemek, işlemek ve raporlamak üzere risk yönetimi süreç ve prosedürlerini tesis eder ve güncelliğini sağlar.

(2) Bilgi sistemlerine ilişkin risklerin yönetilmesinde asgari olarak aşağıdaki hususlar değerlendirmeye alınır:

a) Bilgi teknolojilerindeki hızlı gelişmeler sebebiyle rekabetçi ortamda gelişmelere uymamanın olumsuz sonuçları, gelişmelere uyum konusundaki zorluklar ve mevzuatın değişebilmesi.

b) Bilgi sistemleri kullanımının öngörülemeyen hatalara ve hileli işlemlere zemin hazırlayabilmesi.

c) Bilgi sistemlerinde dışarıdan hizmet alımından dolayı dış hizmeti veren kuruluşlara bağımlılığın oluşabilmesi.

ç) İş ve hizmetlerin önemli oranda bilgi sistemlerine bağlı hale gelmesi.

d) Bilgi sistemleri üzerinden gerçekleştirilen işlemlerin, verilerin ve denetim izlerine ilişkin tutulan kayıtların güvenliğinin sağlanmasının zorlaşması.

(3) Bilgi sistemlerine ilişkin risk analizi, risk işleme ve gözetim süreçleri işletilir. Risk analizi yılda en az bir defa gerçekleştirilir. Bilgi sistemlerinde meydana gelecek önemli değişikliklerde tekrarlanır. Risk analizinde tüm bilgi varlıkları değerlendirmeye alınır. Risk yönetiminde asgari olarak aşağıdaki faaliyetler yerine getirilir:

a) Risk değerlendirme kriterlerinin belirlenmesi.

b) Risklerin analiz edilmesi ve risk seviyelerinin belirlenmesi.

c) Bilgi sistemleri stratejisine ve mevzuata aykırılık teşkil etmeyecek şekilde, iş ve bilgi güvenliği hedefleriyle uyumlu risk kabul kriterleri ile risk işleme seçeneklerinin belirlenmesi ve üst yönetime onaylatılması.

ç) İyileştirici faaliyetlerin gerekli iş gücü, kaynak ve zaman bilgisiyle kayıt altına alınması.

d) İyileştirici faaliyetlerin ve risk analizinin üst yönetime onaylatılması.

e) İyileştirici faaliyetlerin takibi ve bir sonraki analizde ele alınması.

(4) Bilgi sistemlerinin güvenlik açıklarına ve bilgi güvenliği tehditlerine ilişkin bilgi zamanında elde edilir, değerlendirilir ve belirlenen riske karşı uygun tedbirler alınır.

(5) Kurum, Kuruluş ve Ortaklıkların bilgi sistemleri süreçleri ve kullanıcılara sundukları hizmetlere yönelik risk analizi yılda en az bir defa gerçekleştirilir, süreç ve hizmetlerde meydana gelebilecek önemli değişikliklerde tekrarlanır.

(6) Kurum, Kuruluş ve Ortaklıkların bilgi sistemleri, bilgi güvenliğine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından yılda en az bir kez sızma testine tabi tutulur. Kurul gerekli gördüğü takdirde Kurum, Kuruluş ve Ortaklıkların sızma testi yaptırmasını isteyebilir.

(7) Sızma testinde EK-1'de yer alan usul ve esaslar uygulanır. Kurum, Kuruluş ve Ortaklıklar tarafından yaptırılan sızma testleri sonucunda hazırlanan sızma testi raporları tamamlanmasını müteakip bir ay içinde ve her durumda en geç takip eden yılın 31 Ocak tarihine kadar Kurula gönderilir. Son bildirim gününün resmi tatil gününe denk gelmesi halinde, resmi tatil gününü takip eden ilk iş günü son bildirim tarihi kabul edilir.

ÜÇÜNCÜ BÖLÜM
Bilgi Sistemleri Kontrollerine İlişkin Esaslar

Bilgi sistemleri kontrollerinin tesisi ve yönetilmesi

MADDE 9- (1) Kurum, Kuruluş ve Ortaklıkların üst yönetimi, bilgi güvenliği politikası kapsamında bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetilmesi, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin sağlanması ve bilgi sistemlerinin etkin işletimi amacıyla gerekli süreçlerin ve kontrollerin geliştirilmesini sağlar.

(2) Her sürecin sahibi, rol ve sorumlulukları açık bir şekilde tanımlanır.

(3) Süreçlerin performansının ölçülebilmesi için ölçüm kriterleri tanımlanır.

(4) Her sürecin hedef ve amaçları tanımlanır ve performansı ölçülür.

(5) Süreçler ve kontroller hakkında ilgili personelin yeterli eğitim alması sağlanır.

(6) Bilgi sistemleri süreçleri ve kontrollerine ilişkin etkinlik, yeterlilik ve uyumluluk ile öngörülen risk ya da risklerin etkisini azaltmaya yönelik faaliyetler devamlı bir şekilde takip edilir ve değerlendirilir. Değerlendirme neticesinde tespit edilen önemli kontrol eksiklikleri ve yapılan çalışmalar yılda en az bir kez üst yönetime raporlanır ve gerekli önlemlerin alınması sağlanır.

Varlık yönetimi

MADDE 10- (1) Kurum, Kuruluş ve Ortaklıklar, sahip oldukları bilgi varlıklarını belirler, bunların envanterini oluşturur güncelliğini sağlar. Envanterde varlığa ilişkin asgari olarak aşağıdaki hususlar kayıt altına alınır:

a) Tanımı.
b) Edinim tarihi, garanti ve bakım bilgisi.
c) Lisans bilgisi veya seri numarası.
ç) Konumu.
d) Sahibi.
e) Kullanıcısı.
f) Güvenlik sınıfı.
g) Yedekleme bilgisi.

(2) Bilgi varlıklarının güvenlik sınıfının belirlenmesi için bir kılavuz oluşturulur ve üst yönetimce onaylanır. Sınıflandırma esnasında asgari olarak varlıkların gizlilik, bütünlük ve erişilebilirlik gereksinimlerini, kritikliği ve hassasiyeti dikkate alınır. Her sınıftaki varlığa ilişkin temel koruma ve güvenlik önlemleri belirlenir ve yazılı hale getirilir. Sınıflandırma sürecine veriler de dâhil edilir.

(3) Taşınabilir cihaz ve ortamlar, içerdiği bilgilerin güvenlik sınıfına göre kaybolma, hırsızlık ve kopyalama gibi risklere karşı korunur. Güvenlik sınıfı yüksek bilgileri veya bu bilgilere erişim sağlayan yazılımları barındıran taşınabilir cihaz ve ortamlar izinsiz kurum dışına çıkarılmaz.

(4) Bilgi varlıklarına ilişkin uygun kullanım prosedürleri geliştirilir, yazılı hale getirilir, üst yönetim tarafından onaylanır ve ilgili personele imza karşılığı duyurulur.

(5) Kullanımdan kaldırılan donanımsal varlıklara güvenli silme veya imha işlemleri uygulanır ve kayıt altına alınır. Kullanımdan kaldırılan yazılım ve uygulamalara erişimler engellenir ve gerekirse bu yazılım ve uygulamalar arşivlenerek sistemden silinir.

(6) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri kapsamında sundukları hizmetler için hizmet envanterini oluşturur ve güncelliğini sağlar. Envanterde asgari olarak aşağıdaki hususlar kayıt altına alınır:
a) Hizmetin tanımı.
b) Kullanıcıları.
c) Sahibi.
ç) Hizmet seviyesi taahhütleri.
d) Bağımlılıkları.

(7) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri kapsamındaki süreçler için süreç envanterini oluşturur ve güncelliğini sağlar. Envanterde asgari olarak aşağıdaki hususlar kayıt altına alınır:
a) Sürecin tanımı.
b) Sahibi.
c) Girdi ve çıktıları.
ç) Bağımlılıkları.

Görevler ayrılığı ilkesi

MADDE 11- (1) Bilgi sistemleri üzerinde hata, eksiklik veya kötüye kullanım risklerini azaltmak için görev ve sorumluluk alanları ayrılır. Bu kapsamda ayrılması gereken görev ve sorumluluklar belirlenir, yılda en az bir kez gözden geçirilir ve güncelliği sağlanır.

(2) Bilgi sistemleri süreçleri tasarlanırken kritik işlemlerin tek bir personele veya dış hizmeti sunan kuruluşa bağımlı olmaması göz önünde bulundurulur.

(3) Görevlerin tam ve uygun şekilde ayrılmasının mümkün olmadığı durumlarda oluşabilecek hata, eksiklik veya kötüye kullanımı önlemeye ve tespit etmeye yönelik telafi edici kontroller tesis edilir.

Fiziksel ve çevresel güvenlik

MADDE 12- (1) Kritik bilgi sistemlerinin konumlandırıldığı veri merkezlerinin veya güvenli alanların yetkisiz fiziksel erişime, değişen ortam koşullarına, altyapı hizmeti kesintilerine ve felaketlere karşı korunması için asgari olarak aşağıdaki kontroller uygulanır:

a) Fiziksel giriş ve çıkışlar gerekçelendirilir, yetkilendirilir, kaydedilir ve izlenir. Erişim kontrol mekanizmaları devreye alınır. Erişim hakları düzenli olarak gözden geçirilir.

b) Yetkisiz giriş denemelerini anlık izleyecek mekanizmalar kurulur.

c) Kesintisiz güç kaynaklarıyla enerji beslemesi yapılır.

ç) İklimlendirme kontrolü ile uygun ortam koşullarında çalışma sağlanır.

d) Yangın, sel, deprem, patlama ve diğer doğal ya da insan kaynaklı felaketlerden kaynaklanan hasara karşı fiziksel koruma tasarlanır ve uygulanır.

e) Destekleyici altyapı hizmetlerinin (iklimlendirme, kesintisiz güç kaynağı, jeneratör, yangın söndürme sistemi ve benzeri) yılda en az bir kere olmak üzere düzenli bakımı gerçekleştirilir.

f) Kurum, Kuruluş ve Ortaklıkların personeli olmayan kurulum, bakım ve onarım hizmetlerini gerçekleştirecek kişilere çalışma öncesi gizlilik sözleşmesi imzalatılır. Bu kişilere Kurum, Kuruluş ve Ortaklıklarda bulundukları süre boyunca refakat edilir.

g) Destekleyici altyapı hizmetlerinin, uygun çalışma koşullarının dışına çıkılması halinde, alarm üretmesi ve ilgilileri bilgilendirmesi sağlanır.

ğ) Kritik bilgi sistemlerinin konumlandırıldığı veri merkezleri veya güvenli alanlar ve çevresi kameralar ile sürekli olarak izlenir ve bilgi güvenliği gereklilikleri göz önünde bulundurularak belirlenen süre boyunca görüntü kayıtları saklanır. Bu süre; Borsa İstanbul A.Ş., Merkezi Kayıt Kuruluşu A.Ş., İstanbul Takas ve Saklama Bankası A.Ş., geniş yetkili aracı kurumlar ve kripto varlık hizmet sağlayıcılar için asgari bir yıldır. Kayıt mekanizmasının 7/24 esasına göre çalışması, hareket algılama özelliğine sahip olması ve kör nokta kalmayacak şekilde kayıt alması sağlanır.

Ağ güvenliği

MADDE 13- (1) Kurumsal ağın iç ve dış tehditlere karşı korunması ve ağı kullanan sistem, veri tabanı ve uygulamaların güvenliğinin sağlanması için kontroller tesis edilir ve etkin bir şekilde yönetilir. Kurumsal ağın ve ağda bulunan bilgi sistemlerinin güvenliğinin sağlanmasında katmanlı güvenlik yaklaşımı esas alınır. Bu yaklaşımda ağ altyapısı, işletim sistemi, uygulama savunmaları şeklinde birden çok koruma katmanı bir bütünün parçası olarak tasarlanıp devreye alınır.

(2) Kurumsal ağın fiziksel ve mantıksal topolojisi; tüm alt ağları, güvenlik cihazlarını, erişim noktalarını ve bağlantı yollarını içerecek şekilde yazılı hale getirilir, güncel tutulur ve güvenli saklanır.

(3) İletişim altyapıları dinlemeye ve fiziksel hasarlara karşı korunur.

(4) Mobil cihazların kurumsal ağa erişimine ilişkin risklere yönelik güvenlik önlemleri alınır ve uygulanır.

(5) Ağ altyapısına yönelik yetkisiz erişimler engellenir ve gözetim süreçleri tesis edilir.

(6) İç kaynak yoluyla sağlanan veya dışarıdan hizmet olarak alınan her türlü ağ hizmetinin güvenlik kriterleri, hizmet düzeyleri ve yönetim gereksinimleri tanımlanır ve hizmet anlaşmalarına dâhil edilir.

(7) Uzaktan erişim hizmetinde çok faktörlü kimlik doğrulama kullanılır. Uzaktan erişim yetkilendirmeleri bilgi güvenliği sorumlusunun onayı da alınarak yapılır. Uzaktan erişim, yalnızca uygulamaları ve işletim sistemleri güncel cihazlardan yapılır. Uzaktan erişime ilişkin denetim izleri tutulur.

(8) Uzaktan erişim bağlantıları, güncel ve güvenilir kararlı sürüme sahip iletişim protokolleri ile sağlanır. İnternet üzerinden erişimlerde uçtan uca güvenli iletişim teknolojileri kullanılır. Uzaktan erişim oturumları, tanımlanan süre boyunca işlem yapılmadığında otomatik olarak sonlandırılır ve yeniden erişim sağlanması gerektiğinde kimlik doğrulama tekrarlanır.

(9) Kurumsal ağın dış ağlarla olan iletişiminde dış ağlardan gelebilecek tehditler için sürekli gözetim altında tutulan güvenlik duvarı ile ağdaki anormal aktiviteleri ve saldırı girişimlerini tespit etmek ve engellemek için günün teknolojisine uygun çözümler kullanılır. Hassas veri içeren bilgi sistemlerine, internet üzerinden doğrudan erişim engellenir.

(10) İnternet üzerinden sunulan hizmetler hizmet dışı bırakma saldırılarına karşı korunur.

(11) İç ağ bağlantı noktalarında ağ erişim kontrolü uygulanır ve sadece bağlanmasına onay verilen cihazların ağa dâhil olması sağlanır.

(12) İç ağın farklı güvenlik gereksinimlerine sahip alt bölümleri birbirinden ayrılarak denetimli geçişi temin eden kontroller tesis edilir. Bu kapsamda asgari olarak; istemciler, sunucular ve yönetimsel işlemler için ayrı alt ağlar oluşturulur. Kablolu ve kablosuz ağlar birbirinden ayrılır.

(13) Gelen ve giden ağ trafiği analiz edilir, zararlı veya olağan dışı trafik tespit edildiğinde ilgili ağ bölümü izole edilir.

(14) Bilgi güvenliği gereksinimlerine ve yasal gerekliliklere uygun olmayan internet sitelerine erişim uygun araçlarla engellenir.

(15) Ağ erişimleri beyaz liste veya kara liste yapıları kullanılarak sınırlandırılır, güvenilmeyen bağlantılar engellenir.

(16) Kablosuz ağlarda güçlü şifreleme protokolleri kullanılır. Kablosuz ağlar için kimlik doğrulama ve erişim kontrolleri uygulanır. Kimlik doğrulama işlemleri, güvenilir ve güncel protokollerle gerçekleştirilir. Misafir ağları kurumsal ağlardan ayrı tutulur, misafir ağı kullanıcılarına geçici ve kısıtlı erişim hakkı verilir.

Bilgi sistemlerinin işletimi

MADDE 14- (1) Kurum, Kuruluş ve Ortaklıklar, ihtiyaç duyulan bilgi sistemleri hizmetlerinin istenilen seviyede ve süreklilik arz edecek şekilde sunulması için gerekli kontrolleri tesis eder. Bu kapsamda sunulan her hizmetin seviyesi, iş gereksinimleriyle uyumlu olacak şekilde iş birimleri ile mutabakata varılarak belirlenir. Kullanıcıların bilgi sistemleri ile ilgili sorun ve taleplerinin kayda alınması, bunlara cevap verilmesi ve altta yatan kök sebeplerin çözülmesi için gerekli mekanizmalar kurulur.

(2) Kritik bilgi sistemleri, hizmet seviyelerine uygun performansta çalışması için sürekli gözetim altında tutulur, sistemlerin her biri için eşik değerler belirlenir ve bu değerlerin aşılması durumunda ilgili kişilere otomatik bildirim gönderilmesi sağlanır. Beklenen performans değerinin altına düşüldüğü durumlarda kök sebep araştırılır ve gerekli iyileştirici faaliyetler gerçekleştirilir.

(3) Kurum, Kuruluş ve Ortaklıkların faaliyetlerindeki olası büyüme, kullanıcı sayısındaki artış ve benzeri durumlar dikkate alınarak bilgi sistemlerinin beklenen performans düzeyinde çalışabilmesi için kapasite planlaması yapılır.

(4) Bilgi sistemlerine ilişkin güvenlik açıkları, iş süreçlerini etkilemesini önlemek amacıyla düzenli takip edilir. Güvenlik açıklarına ilişkin yayınlanan yamaların uygulanması değerlendirilir. Uygulanmasına karar verilen yamalar önce test edilir. Yama uygulanmayacağı durumlarda söz konusu riskin ele alınması için ilave kontroller tesis edilir veya ilgili bileşen kullanımdan kaldırılır. Yama uygulaması değişiklik yönetimi çerçevesinde ele alınır. Uygulanmamasına karar verilen yamalarla ilgili olarak bilgi güvenliği sorumlusuna düzenli rapor verilir.

(5) Bilgi sistemleri bileşenlerinin yaşam döngüsü boyunca tutarlı, beklenen performans, kalite ve güvenlik düzeyinde çalışmasını sağlamak için yapılandırma ayarları takip edilir. Bilgi sistemleri bileşenlerinde gerekli olmayan tüm işlevler kapatılır. Her bileşen türü için temel yapılandırma ayarları belirlenir ve uygulanır. Yeni güvenlik açıkları ortaya çıktığında veya mevcut bileşenlerde yeni sürümlere geçildiğinde yapılandırma ayarları uygunluk ve yeterlilikleri açısından gözden geçirilir. Bir bileşendeki yapılandırma ayarı değişikliğinin diğer bileşenlere olan etkisi takip edilir. Yapılandırma ayarlarındaki her türlü değişiklik gerekçesiyle beraber kayıt altına alınır ve izlenir. Tüm bileşenlerin yapılandırma ayarları yedeklenir. Yapılandırma ayarlarındaki her tür değişiklik, değişiklik yönetimi çerçevesinde ele alınır.

(6) Bilgi sistemlerinde taşınabilir ortamlara bağlantı noktaları kapatılır. Taşınabilir ortamların kullanılabilmesi için geçerli bir iş gereksiniminin olması dikkate alınır ve bilgi güvenliği sorumlusu onayı aranır.

(7) Zararlı yazılımların Kurum, Kuruluş ve Ortaklıkların bilgi sistemlerini etkilemesine karşı gerekli önlemler alınır. Bu kapsamda, zararlı yazılımı tespit edecek ve temizleyecek yazılımlar kullanılır. Bu yazılımların sürekli güncel tutulması sağlanır. Masaüstü, dizüstü ve sunucu sistemler, taşınabilir bir ortam 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.

(8) Elektronik posta hizmetinin güvenliğinin sağlanması için şifreli iletişim esastır. İnternet ortamında sahte elektronik posta gönderimini önlemeye yönelik geliştirilen etki alanı kimlik doğrulaması yöntemleri sahip olunan etki alanları için yapılandırılır ve bu yöntemler kullanılarak doğrulanmış etki alanlarından elektronik posta alınması sağlanır. Gelen ve giden bütün elektronik posta içeriği güvenlik analizinden geçirilir, zararlı yazılım ve bağlantılara erişim engellenir.

Kimlik yönetimi

MADDE 15- (1) Bilgi sistemleri üzerinden gerçekleşen işlemler için, bilgi varlığının güvenlik sınıfına uygun kimlik doğrulama yöntemleri belirlenir ve uygulanır.

(2) Kimlik doğrulama yöntemi, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde uygulanır. Kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek gerekli önlemler alınır.

(3) Kullanılan kimlik doğrulama verilerinin tutulduğu ortamların ve bu amaçla kullanılan araçların güvenliğini sağlamaya yönelik gerekli önlemler alınır. Bu önlemler asgari olarak kimlik doğrulama verilerinin güçlü şifreleme algoritmalarıyla şifrelenerek veya geriye dönüştürülmesi

mümkün olmayacak şekilde saklanması, bu veriler üzerinde yapılacak her türlü değişikliği algılayacak sistemlerin kurulması, yeterli denetim izlerinin tutulması ve güvenliğinin sağlanması hususlarını içerir. Kimlik doğrulama verilerinin aktarımı sırasında gizliliğinin sağlanmasına yönelik önlemler alınır.

(4) Belirlenen kimlik doğrulama yöntemi asgari olarak aşağıda yer alan işlevleri yerine getirir:

a) Başarısız kimlik doğrulama girişimlerinde, girişimde bulunan kişiye sistem veya kullanıcıya ilişkin bilgi verilmemesi.

b) Belirli sayıda art arda başarısız kimlik doğrulama girişimi durumunda ilgili kullanıcı erişiminin engellenmesi ve kullanıcının bilgilendirilmesi.

c) Hiçbir işlem yapılmayan oturumların belirli bir zaman aşımı süresi sonunda sonlandırılması veya kilitlenmesi, bu durumlarda oturumun açılması için kimlik doğrulamanın tekrar edilmesi.

ç) Bilgi güvenliği sorumlusu onayı olmadan aynı kullanıcı için birden fazla oturum açılmasına izin verilmemesi.

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

a) Kullanıcıların sisteme tanıtılırken belirlenen parolasının, kullanıcının sisteme ilk girişinde değiştirilmeye zorlanması.

b) Parolaların tahmin edilmesi ve kırılması zor bir karmaşıklıkta ve uzunlukta olması.

c) Parolaların düzenli aralıklarla değiştirilmeye zorlanması.

ç) Geriye dönük olarak belirli sayıda eski parolanın kullanılmasının engellenmesi.

d) Yeni kurulan sistem ve cihazlardaki varsayılan parolaların değiştirilmesi.

e) Parolaların ekran üzerinde maskelenmiş şekilde görüntülenmesi.

(6) Kritik sistem ve uygulamalarda birbirinden bağımsız çok faktörlü kimlik doğrulama mekanizması kullanılır. Faktörlerin bağımsız olması, bir faktörün ele geçirilmesinin diğer faktörün güvenliğini tehlikeye atmamasını ifade eder. Kullanıcının sahip olduğu faktörün kullanıcıya özgü olması ve taklit edilememesi esastır.

(7) Ayrıcalıklı kullanıcı hesapları çok faktörlü kimlik doğrulama mekanizması ile kullanılır.

(8) Kritik sistem ve uygulamalarda kimlik doğrulama süreçlerinde gerçekleşen başarılı ve başarısız işlemlere ilişkin denetim izi tutulur.

(9) Kullanıcı hesaplarına yönelik olarak kilitli hesaplar, devre dışı bırakılmış hesaplar, parola geçerlilik süresini aşan hesaplar ve parola son kullanma süresi hiçbir zaman dolmayacak şekilde ayarlanmış hesaplar için otomatik olarak rapor üreten yöntemler kullanılır ve bu raporlar gerekli önlemleri alması için ilgililere iletilir.

Erişim yönetimi

MADDE 16- (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemlerine erişim ve uygulamaların kullanımı için uygun erişim kontrollerini tesis eder. Kullanıcılara verilecek yetki düzeyinin belirlenmesinde görev ve sorumluluklar göz önünde bulundurularak gerekli olacak en düşük yetkinin atanması ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınır. Yetki ve sorumluluklar görevler ayrılığı ilkesi ile tutarlı olur. Erişim yönetiminde rol tabanlı erişim kontrolünün uygulanması esastır.

(2) Tüm yetkiler yılda en az bir defa ilgili bilgi varlığının sorumlusu tarafından gözden geçirilir. Gerekli bir iş gereksinimi olmayan yetkiler iptal edilir.

(3) Kullanıcılara hesap açma, yetkilendirme ve erişim haklarına yönelik diğer işlemler görevler ayrılığı ilkesi kapsamında onay sürecine bağlanır. Erişim haklarına ilişkin gerçekleştirilen tüm işlemlerin denetim izleri tutulur ve düzenli olarak gözden geçirilir.

(4) Görev değişikliği veya istihdamın sonlanması durumunda yapılacaklar yazılı hale getirilir ve bu kapsamda yapılan işlemler kayıt altına alınır. Bu durumlarda mevcut yetkiler gözden geçirilir ve gerekmeyen yetkiler ivedilikle iptal edilir.

(5) Bilgi sistemlerinde ortak veya varsayılan hesapların kullanılması, zorunlu olduğu durumlar haricinde engellenir, kullanılması gereken durumlarda bu hesapları kullananlara sorumluluk atamaya yönelik kontroller tesis edilir ve bu hesaplarca gerçekleştirilen işlemlerin denetim izi tutulur.

(6) Bilgi sistemleri kullanıcılarına zorunlu olmadıkça yerel yönetici hakları verilmez. Yapılacak işin gerektirdiği durumlarda ise ancak bilgi güvenliği sorumlusunun onayı ile söz konusu haklar verilir.

(7) Bilgi sistemlerinde ayrıcalıklı yetkileri gerektirecek iş ve işlemler için ayrı hesaplar açılır. Bu hesaplarca gerçekleştirilen işlemlerin denetim izi tutulur.

(8) Ayrıcalıklı kullanıcı hesapları ile yapılan erişimleri de kapsayacak şekilde anormal veya beklenmedik erişim girişimlerini tespit edecek ve erken uyarı oluşturacak mekanizmalar tesis edilir.

(9) Acil durumlara özgü yetkilendirmeler geçici olarak yapılır ve bu yetkilendirme süresince gerçekleştirilecek işlemlerin takibine imkân verecek denetim izlerinin tutulması sağlanır.

İşlemlerin, kayıtların ve verilerin bütünlüğü

MADDE 17- (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli önlemleri alır. Bütünlüğü sağlamaya yönelik önlemler verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsayacak şekilde tesis edilir. Bilgi sistemlerine ilişkin dışarıdan hizmet alınan kuruluşlar nezdinde gerçekleşen işlemler için de aynı yaklaşım gösterilir.

(2) Kritik işlemler, kayıtlar ve verilerde meydana gelebilecek bozulmaları saptayacak ve zamanında gerekli bildirimleri yapacak teknikler kullanılır.

Veri gizliliği

MADDE 18- (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemleri alır. Gizliliği sağlamak üzere yapılacak çalışmalar asgari olarak aşağıda belirtilen hususları içerir:

a) Verilerin güvenlik sınıfına uygun şekilde korunması.

b) Verilere erişim haklarının kişilerin görev ve sorumlulukları çerçevesinde belirlenmesi, erişimlerin kayıt altına alınması, bu kayıtların yetkisiz erişim ve müdahalelere karşı korunması.

c) Hassas verilerin tüm ortamlarda şifrelenerek saklanması, iletilmesi ve yedeklenmesi.

ç) Veri gizliliğini sağlamada şifreleme tekniklerinin kullanılması durumunda, güvenilirliği ve sağlamlığı ispatlanmış algoritmaların kullanılması; geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılmasının engellenmesi, verinin ve operasyonun önem düzeyine göre anahtarların değiştirilme sıklıklarının belirlenmesi ve anahtarların güvenli saklanması.

(2) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlere ilişkin üretilen, iletilen, işlenen ve saklanan verilerin kasten veya yanlışlıkla Kurum, Kuruluş ve Ortaklıklar dışına sızmasını önlemeye yönelik olarak güvenlik sınıfına uygun önlemleri alır.

(3) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri aracılığıyla edindiği veya sakladığı kişisel verilerin gizliliğini sağlamaya yönelik kontrolleri tesis eder ve bunların gerektirdiği önlemleri alır.

(4) Saklama süresi sona eren verilerin bulundukları tüm ortamlardan güvenli ve geri döndürülemez şekilde silinmesi sağlanır ve yapılan işlemler kaydedilir.

(5) Kurum, Kuruluş ve Ortaklıklar, kişisel verilerin korunması ve işlenmesine yönelik gerekli tedbirleri alır. Bu maddede yer almayan durumlarda 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili diğer mevzuat hükümleri uygulanır.

Bilgi sistemlerine ilişkin dışarıdan hizmet alımı

MADDE 19- (1) Kurum, Kuruluş ve Ortaklıkların üst yönetimi tarafından, bilgi sistemleri kapsamında dışarıdan hizmet alımının doğuracağı risklerin yeterli düzeyde değerlendirilmesine, yönetilmesine ve dışarıdan hizmet sağlayıcı kuruluşlarla ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak bir gözetim mekanizması tesis edilir. Tesis edilecek gözetim mekanizması asgari olarak aşağıda belirtilen hususları içerir:

a) Dışarıdan alınan bilgi sistemleri hizmeti kapsamındaki tüm sistem ve süreçlerin, Kurum, Kuruluş ve Ortaklıkların kendi risk yönetimi, bilgi güvenliği ve müşteri mahremiyeti ilkelerine uygun olması.

b) Kurum, Kuruluş ve Ortaklıkların verilerinin dışarıdan hizmet sağlayan kuruluşa aktarılmasının gerekli olduğu durumlarda, söz konusu kuruluşun bilgi güvenliği konusundaki ilke ve uygulamalarının en az Kurum, Kuruluş ve Ortaklıkların uyguladığı düzeyde olması.

c) Dışarıdan alınan bilgi sistemleri hizmetine ilişkin hususların Kurum, Kuruluş ve Ortaklıkların iş sürekliliği göz önünde bulundurularak düzenlenmesi ve gerekli önlemlerin alınması.

ç) Dışarıdan alınan bilgi sistemleri hizmetlerinde ölçme, değerlendirme, raporlama, güvenlik ve yetkilendirme gibi süreçlerde nihai sorumluluğun ve karar alma gücünün Kurum, Kuruluş ve Ortaklıklarda olması.

d) Dışarıdan alınan hizmetin, Kurum, Kuruluş ve Ortaklıkların yasal yükümlülüklerini yerine getirmelerini ve etkin biçimde denetlenmelerini engelleyici nitelikte olmaması.

e) Dışarıdan hizmet sağlayacak kuruluşa karar verilmeden önce kuruluş bünyesinde söz konusu hizmeti istenilen kalitede gerçekleştirebilecek düzeyde teknik donanım ve altyapı, mali güç, tecrübe, bilgi birikimi ve insan kaynağı bulunup bulunmadığı ile dış hizmet sağlayıcı kuruluşa yönelik yoğunlaşmaların ve hizmet çıkış stratejisinin belirlenerek hizmetin ikame edilebilirliğine ilişkin hususları da dikkate alacak şekilde değerlendirme çalışması yapılması ve hazırlanacak teknik yeterlilik raporunun üst yönetimin onayına sunulması.

f) Dışarıdan alınan hizmetlere ilişkin; hizmetin kapsamının, hizmet alınan kuruluşun iletişim bilgilerinin, hizmetin geçerlilik süresinin, hizmetin seviyesinin ve kritiklik durumunun yazılı hale getirilmesi.

(2) Kurum, Kuruluş ve Ortaklıkların üst yönetimi; dışarıdan alınan kritik hizmetlerin erişilebilirliğini, performansını, kalitesini, bu hizmet kapsamında gerçekleşen güvenlik ihlalleri ile dış kaynak yoluyla hizmet sağlayan kuruluşun güvenlik kontrollerini, finansal koşullarını ve

sözleşmeye uygunluğunu yakından takip etmek için yeterli bilgi ve tecrübeye sahip sorumluları belirler. Bu sorumlular, yılda en az bir defa olmak üzere bu maddede sayılan hususları içeren bir değerlendirme raporu hazırlar ve üst yönetime sunar.

(3) Dışarıdan hizmet alımına ilişkin koşul, kapsam ve her türlü diğer tanımlama, dış hizmeti sağlayan kuruluşça da imzalanmış olacak şekilde sözleşmeye bağlanır. Hizmet sözleşmeleri asgari olarak aşağıdaki hususları içerir:

a) Hizmet seviyelerine ilişkin tanımlamalar.

b) Hizmetin sonlandırılmasına ilişkin koşullar ve hizmetin sonlanması durumunda Kurum, Kuruluş ve Ortaklıklara ait tüm verinin Kurum, Kuruluş ve Ortaklıklara teslimi ve hizmet sağlayıcı kuruluş bünyesinde güvenli ve geri döndürülemez şekilde imhasına ilişkin yükümlülükler.

c) Hizmetin beklenmedik şekillerde sonlandırılması veya kesintiye uğraması durumunda uygulanacak yaptırımlar.

ç) Kurum, Kuruluş ve Ortaklıkların bilgi güvenliği politikası dâhilinde önem arz eden konulara ilişkin gereklilikler ile hizmet sırasında ve hizmetin sonlanmasından itibaren hizmet sağlayıcı kuruluşun, Kurum, Kuruluş ve Ortaklıklar hakkında edindiği bilgileri gizli tutması konusunda yükümlülükler.

d) Sözleşme kapsamında üretilecek ürün bulunması halinde, ürünün sahipliğini, fikri ve sınai mülkiyet haklarını da göz önünde bulundurarak düzenleyen hükümler.

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

f) Hizmet sağlayıcı kuruluşun, sermaye piyasası mevzuatı kapsamında Kurum, Kuruluş ve Ortaklıklar, Kurul veya Kurulca uygun görülecek diğer kuruluşlar tarafından talep edilecek bilgileri istenen zamanda ve nitelikte sağlamasına ilişkin yükümlülüğü ve Kurulun ve Kurulca uygun görülecek diğer kuruluşların sözleşme kapsamında sunulan hizmet ile ilgili olarak hizmet sağlayıcı bünyesindeki gerekli gördüğü her türlü bilgi, belge ve kayda erişim hakkı.

g) Hizmet sağlayıcı kuruluşun bünyesinde gerçekleşen güvenlik ihlali veya veri sızıntısı gibi olayların derhal Kurum, Kuruluş ve Ortaklıklara bildirilmesini sağlayacak hükümler.

ğ) Kurum, Kuruluş ve Ortaklıkların, dışarıdan hizmet sağlayan kuruluşun sözleşme kapsamındaki faaliyetlerini izleme ve değerlendirmesine ilişkin esaslar.

h) Dışarıdan hizmet alımına konu edilen bir faaliyet konusunda, ilgili mevzuatta Kurum, Kuruluş ve Ortaklıklar için yükümlülükler getirilmesi halinde, bu yükümlülüklerin dışarıdan hizmet sağlayan kuruluş tarafından da yerine getirilmesinin sağlanacağına ilişkin hükümler.

(4) Kritik olmayan hizmetler, hizmet sözleşmelerinde birinci, ikinci ve üçüncü fıkralarda belirlenen hususların yer almasının imkân dâhilinde olmadığı durumlarda standart sözleşmeler ile alınabilir ve bu durumun gerekçesi yazılı hale getirilir.

(5) Dışarıdan hizmet sağlayan kuruluşlara verilen erişim hakları özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılır, gerekiyorsa ek kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim türü, erişilecek verinin hassasiyeti ile erişimin bilgi güvenliği üzerindeki etkileri dikkate alınır. Erişim hakları, işin gerektirdiği en az yetkiyi içerir ve gerekirse zamana bağlı olarak tanımlanır. Alınan hizmetin sonlanması durumunda ilgili tüm erişim hakları iptal edilir.

(6) Kurum, Kuruluş ve Ortaklıklar, faaliyetlerinin tamamı veya bir bölümü için bulut hizmeti kullanabilir. Bulut hizmeti alımı, kullanımı ve yönetimi, dışarıdan hizmet alımı olarak

değerlendirilir. Bulut hizmeti kapsamında 27 nci maddenin birinci fıkrasında belirlenen yükümlülükler dikkate alınır.

(7) Dışarıdan alınan yazılım, donanım, işletim sistemi veya bu bileşenlerin bir ya da birkaçını barındıran cihaz/sistemlerin, mevcut güvenlik önlemlerini aşarak erişim sağlamak üzere özel olarak tasarlanan ve/veya kasıtlı olarak dâhil edilmiş boşluklar veya güvenlik açıklarını barındırmadığına yönelik taahhütname; dağıtıcı, tedarikçi veya üreticiden alınır.

Müşterilerin bilgilendirilmesi

MADDE 20- (1) Kurum, Kuruluş ve Ortaklıklar tarafından elektronik ortamda sunulan hizmetlerden yararlanacak müşteriler; sunulan hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir. Bu kapsamda; söz konusu hizmetlere ilişkin risklerin etkisini azaltmaya yönelik olarak benimsenen bilgi güvenliği ilkeleri ve bu risklerden korunmak için kullanılması gereken yöntemler, müşterilerin dikkatine sunulur. Bu bilgilendirmenin yapıldığının ispatı Kurum, Kuruluş ve Ortaklıkların sorumluluğundadır.

(2) Bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı müşterilerin yaşayabileceği sorunların takip edilebileceği ve müşterilerin şikâyetlerini ulaştırmalarına imkân tanıyacak mekanizmalar oluşturulur. Şikâyet ve uyarılar değerlendirilerek aksaklıkları giderici çalışmalar yapılır.

Üçüncü taraflarla bilgi değişimi

MADDE 21- (1) Üçüncü taraflara Kurum, Kuruluş ve Ortaklıkların bilgi sistemine erişim hakkı verilmeden önce gerekli güvenlik gereksinimleri tanımlanır ve uygulanır. Kurum, Kuruluş ve Ortaklıkların bilgi içeren ortamları, üçüncü taraflar ile yapılan veri aktarımları sırasında gerçekleşebilecek kötüye kullanım veya bozulmaya karşı korunur. Bu kapsamda yapılan çalışmalar yazılı hale getirilir ve veri aktarımlarına ilişkin denetim izi tutulur.

(2) Kurum, Kuruluş ve Ortaklıkların birinci fıkra kapsamında alacağı tedbirler Kurulun bilgi alımı, denetim ve gözetim faaliyetlerine engel teşkil edemez.

Kayıt mekanizmasının oluşturulması

MADDE 22- (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri üzerindeki riskleri, sistem veya faaliyetlerinin karmaşıklığını ve kapsamının genişliğini göz önünde bulundurarak bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizması tesis eder. Bu kapsamda asgari olarak kritik bilgi sistemlerine ve Kurum, Kuruluş ve Ortaklıkların faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemler ile hassas verilere erişilmesine, bunların sorgulanmasına, görüntülenmesine, kopyalanmasına, değiştirilmesine yönelik işlemler ve kritik bilgi varlıklarına yönelik erişim yetkilerinin verilmesine, değiştirilmesine ve geri alınmasına yönelik işlevler ile bu varlıklara yönelik yetkisiz erişim teşebbüslerine ilişkin denetim izleri tutulur. Bu sayede, bilgi sistemleri dâhilinde gerçekleşen ve Kurum, Kuruluş ve Ortaklıkların faaliyetlerine ait kayıtlarda değişiklik ve silmeye sebep olan işlemlere ilişkin denetim izlerinin yeterli detayda ve açıklıkta kaydedilmesi temin edilir. Kayıt mekanizmasının yetkisiz sistem ve kullanıcı erişimlerine karşı korunmasına yönelik önlemler alınır.

(2) Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır. Denetim izlerinin bütünlüğü düzenli olarak gözden geçirilir ve olağan dışı durumlar üst yönetime raporlanır.

(3) Denetim izlerinde asgari olarak aşağıdaki bilgiler tutulur:

a) Yapılan işlemlerin türü ve niteliği.

b) İşlemi gerçekleştiren uygulama.

c) İşlemi gerçekleştiren kişinin kimliği.

ç) Yapılan işlemlerin zamanı.

d) İşlemin sonucu.

e) Erişilen sistem, ara yüz ya da dosya adı.

(4) Denetim izleri asgari 5 yıl saklanır. Denetim izlerinin yeterli güvenlik düzeyine sahip ortamlarda korunması ve yedeklerinin alınması suretiyle, yaşanması muhtemel olumsuzluklar sonrasında da öngörülen süre için erişilebilir olmaları temin edilir. Bunun yanı sıra, denetim izlerinin alınması ve saklanmasında kullanılan araç veya yöntemler gözetim altında tutulur. Denetim izi mekanizmasında bir aksaklık yaşandığında ilgili kişilerin otomatik olarak uyarılması sağlanır.

(5) Kullanıcılar, bilgi sistemleri üzerindeki aktivitelerinin kaydının tutulduğu konusunda bilgilendirilir.

(6) Denetim izlerinin tutulması, ilgili diğer mevzuat hükümleri gereği Kurum, Kuruluş ve Ortaklıkların tabi olduğu mevzuattaki belge saklanmasına ilişkin yükümlülüklerini değiştirmez.

(7) Denetim izleri sürekli gözetim altında tutulur. Olağan dışı durumlar için otomatik uyarı mekanizması kurulur ve ilgililere bildirim yapılır. Bu bildirimlerin her biri üzerinde inceleme yapılır ve sonuçlar kayıt altına alınır.

(8) Dışarıdan alınan hizmetler için de bu madde kapsamında denetim izi tutulması ve Kurum, Kuruluş ve Ortaklıklar tarafından erişilebilmesi sağlanır.

(9) Denetim izleri merkezi bir kayıt yönetim sistemi aracılığıyla izlenir ve analiz edilir. Olası güvenlik olaylarının erken tespiti için korelasyon kuralları tanımlanır ve uyarı mekanizmaları oluşturulur.

(10) Kritik faaliyetlerin gerçekleştiği bilgi sistemlerinin yöneticileri ile bu sistemlere ilişkin denetim izlerini yöneten kişiler ayrıştırılır.

Zaman senkronizasyonu

MADDE 23- (1) Kurum, Kuruluş ve Ortaklıkların bilgi sistemlerinde kullandıkları zaman bilgisi tek bir referans kaynağına göre senkronize edilir. Zaman bilgisi atomik saatler vasıtasıyla temin edilir.

Bilgi güvenliği ihlali

MADDE 24- (1) Kurum, Kuruluş ve Ortaklıklar, bünyelerinde gerçekleşen her türlü bilgi güvenliği ihlalinin veya bilgi sistemlerine ilişkin tespit edilen güvenlik açıklarının yönetilmesini sağlayacak kontrolleri tesis eder. Bu kapsamda tüm personel, rol ve sorumlulukları hakkında bilgilendirilir. Gerçekleşen ihlal veya tespit edilen güvenlik açığı mümkün olan en kısa sürede kayda alınır ve gerekli işlemler yapılır.

(2) Bilgi güvenliği ihlal olaylarının veya güvenlik açıklarının değerlendirilmesi için kriterler belirlenir. Bu kriterler asgari olarak kritik operasyonların ve hizmetlerin olası kesinti süresi, veri sızıntısı kapsamında çalınan kayıt veya etkilenen hesap sayısı, etkilenen kullanıcı sayısı, kesinti süresince ve ileriye dönük toplam gelir kaybı, ihlal edilen hizmet seviyesi anlaşmalarının oranı ölçütlerini içerir ve bu süreç yazılı hale getirilir.

(3) Bilgi güvenliği ihlal olaylarına müdahale planı hazırlanır ve üst yönetim tarafından onaylanır. Planda asgari olarak;

a) Olaya müdahale ekibinin rolleri, sorumlulukları ve iletişim bilgileri,

b) Olay, güvenlik açığı veya tehdit bildiriminin kim tarafından ve nasıl yapılabileceği,

c) Kurum içi ve kurum dışı iletişim esasları,

ç) Güncel tehdit ve muhtemel siber olayların her biri için; olayın değerlendirilmesi, ilgili tarafların bilgilendirilmesi, olaya cevap verilmesi, kurtarma, raporlama, öğrenme ve iyileştirme aşamaları,

yer alır.

(4) Yaşanan olayın, kritik operasyonları kesintiye uğratacak veya veri sızıntısıyla sonuçlanacak potansiyelde belirlenmesi durumunda derhal Kurul, müşteriler ve ilgili diğer kurumlar bilgilendirilir.

(5) Olay sonrası, olaya ilişkin alınan kararlar, olayın etkilediği bilgi sistemleri ve iş süreçleri, olaya cevaben gerçekleştirilen tüm işlemler, olayın kök sebebi, görev alan kişiler, harcanan zaman, maliyet ve işgücü miktarı kayda alınarak siber olay müdahale raporu hazırlanır ve üst yönetime iletilir. Olaydan kritik sistemler veya hassas verilerinin etkilenmesi durumda hazırlanan rapor derhal Kurula iletilir.

(6) Olay müdahale süreciyle ilgili personelin yetkinlik, deneyim ve bilgisinin eğitim programları ile artırılması sağlanır.

(7) Yasal işlemler için kanıtların bütünlüğünün bozulmadan toplanması ve korunması için kontroller tesis edilir.

(8) Olay müdahale planının etkinliğini ve güncelliğini temin etmek üzere yılda en az bir kez test yapılır ve test sonuçları üst yönetime raporlanır.

(9) Sektörel SOME tarafından, Kurumsal SOME kurulmasına karar verilen Kurum, Kuruluş ve Ortaklıkların bünyesinde Kurumsal SOME kurulur ve SOME Tebliğinde belirtilen usul ve esaslara göre çalışır. Kurumsal SOME üyelerinin iletişim bilgileri USOM tarafından belirlenen yöntem ile USOM'a bildirilir ve güncelliği sağlanır.

(10) Bünyesinde Kurumsal SOME kurulan Kurum, Kuruluş ve Ortaklıklarda bilgi güvenliği ihlallerine ilişkin gerçekleştirilen faaliyetlere yönelik yıllık olarak SOME Rehberinde belirtilen Kurumsal SOME Faaliyet Raporu düzenlenir, üst yönetime raporlanır. Hazırlanan rapor takip eden yıl 31 Ocak tarihine kadar Türkiye Sermaye Piyasaları Birliği üyelerince Birlik aracılığıyla, diğer Kurum, Kuruluş ve Ortaklıklarca doğrudan Kurula iletilir. Son bildirim gününün resmi tatil gününe denk gelmesi halinde, resmi tatil gününü takip eden ilk iş günü son bildirim tarihi kabul edilir. Raporda, Kurumsal SOME Rehberinde belirtilenlerin yanı sıra asgari olarak aşağıdaki unsurlara da yer verilir:

a) Yaşanan olaylara cevaben yapılan tüm müdahaleler.

b) Otomatik yollarla tespit edilen ve yanıtlanan olayların sayısı ve türleri.

c) Bir tehdit aktörünün bilgi sistemleri ortamında bulunduğu süre (bir saldırganın tespit edildiği andan itibaren varlığının en erken kanıtına kadar geçen süre).

ç) Kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı performans metrikleri açısından değerlendirmeler.

Bilgi sistemleri edinimi, geliştirilmesi ve bakımı

MADDE 25- (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri edinimi, geliştirilmesi ve bakımı süreçlerinde gerekli kontrolleri tesis eder. Bu kontroller Kurum Kuruluş ve Ortaklıkların kendi bünyesinde geliştirilecek, değiştirilecek veya dışarıdan hizmet alımıyla edinilecek her türlü bilgi sistemini kapsar.

(2) Geliştirilecek, değiştirilecek veya dışarıdan hizmet alımıyla temin edilecek bilgi sistemlerinin fonksiyonel gereksinimleri ile tasarım, geliştirme ve test aşamalarının her biri için teknik ve güvenlik gereksinimleri yazılı hale getirilir. Uygulama güvenliği ve erişilebilirlik gereksinimleri belirlenirken Kurum, Kuruluş ve Ortaklıkların belirlemiş olduğu veri güvenlik sınıflandırması ve riskler göz önünde bulundurulur.

(3) Geliştirilecek, değiştirilecek veya dışarıdan temin edilecek bilgi sistemleri yapısının Kurum, Kuruluş ve Ortaklıkların ölçeği, faaliyetlerinin ve sunulan ürünlerin niteliği ve karmaşıklığı ile uyumlu olması zorunludur.

(4) Alınan hizmetin kritikliği, riskliliği ve tedarikçinin iş dışı kalması olasılığı dikkate alınarak yazılımı dış bir firma tarafından geliştirilen ve kaynak kodu tedarik edilemeyen uygulamalar için üçüncü tarafların da katılımıyla bir yazılım saklama sözleşmesi yapılır.

(5) Bilgi sistemlerinde gerçekleştirilecek büyük ölçekli geliştirme, değişiklik veya edinim süreçleri, proje yönetim faaliyetleri çerçevesinde yürütülür. Gerçekleştirilecek projeler Kurum, Kuruluş ve Ortaklıkların üst yönetimi tarafından onaylanır. Proje ile ilgili ilerleme raporları belirli periyotlarda üst yönetime sunulur.

(6) Yazılım geliştirme yaşam döngüsünün tüm aşamalarını kapsayacak şekilde güvenli yazılım geliştirme prosedürü oluşturulur.

(7) Bilgi sistemlerinde yapılacak önemli güncellemelerin veya değişikliklerin iş süreçlerini aksatmaması ve bilgi güvenliği riski oluşturmaması için güncelleme veya değişikliklere ilişkin planlama, test ve uygulama adımları detaylı olarak ele alınır.

(8) Yazılım geliştirme süreçlerinde görev alan personelin güvenli yazılım geliştirme konusunda eğitim alması sağlanır.

(9) Geliştirme, test ve gerçek ortamlar yetkisiz erişim ve değişim riskine karşı birbirinden ayrılır. Test ortamındaki veriler, müşteri bilgilerini içermeyecek ve gerçek ortamdaki işlemlerle uyumlu olacak şekilde belirlenir.

(10) Bilgi sistemleri gerçek ortamda kullanıma alınmadan önce kabul kriterleri belirlenir, hazırlanacak bir plana göre fonksiyonel, teknik ve güvenlik gereksinimleri testlerine tabi tutulur, gerçek ortama alınması onay sürecine bağlanır. Kritik uygulamalar gerçek ortama alınmadan önce güvenlik testlerinden geçirilir, tespit edilen bulgular giderilir.

(11) Gerekli hallerde değiştirilmiş veya yeni geliştirilmiş sistemin gerçek ortamda kullanıma alınmadan önce belirli bir olgunluk seviyesine ulaşana kadar eski sistemle beraber çalıştırılmasına devam edilir. Bu şekilde paralel işletimin mümkün olmadığı durumlarda ise değiştirilmiş veya yeni geliştirilmiş sistem belirli bir olgunluk seviyesine ulaşana kadar eski sistem veri kayıpsız olarak devreye alınabilir halde tutulur.

(12) Uygulama geliştiricilerin zorunlu olmadıkça gerçek ortama erişimleri engellenir. Gerekmesi durumunda, bilgi güvenliği sorumlusunun onayı alınarak ve yapılan tüm işlemlerin denetim izleri tutularak kısıtlı süreyle erişim sağlanır.

(13) Uygulama geliştirme sürecinde sürüm kontrol aracı kullanılır, kaynak kodlarda yapılan değişiklikler gerekçesi ile sürüm kontrol aracına yansıtılır.

Uygulama güvenliği

MADDE 26- (1) Kurum, Kuruluş ve Ortaklıklar, uygulamaların güvenli çalışmasını temin etmek amacıyla kontroller geliştirir. Bu kontroller girdi ve çıktı denetimini, hataların ele alınmasını, güncellemeleri, erişim denetimini, mobil uygulama ve API işletimine özgü konuları içerir ve asgari olarak kritik uygulamalarda ele alınır.

(2) Uygulamalarda veri girişlerinin tam, doğru ve geçerli şekilde yapılması, veri üzerindeki işlemlerin doğru sonuçlar üretmesi sağlanır, veri ve işlem kaybı, verinin yetkisiz değiştirilmesi ve kötüye kullanımı önlenir. Bu kapsamda; girdi doğrulama ve filtreleme mekanizmaları tesis edilir. Girdiler zararlı içerikleri engellemek üzere doğrulanır. Girdilerin önceden belirlenen uzunluk ve format gereksinimlerine uygunluğu sağlanır.

(3) Uygulamaların ürettiği çıktıların bütünlüğü sağlanır.

(4) Uygulamaların ürettiği hata mesajları, sistem güvenliğini tehlikeye atmayacak ve veri sızdırma riski yaratmayacak şekilde yapılandırılır.

(5) Uygulamalarda meydana gelen; gizlilik, bütünlük ve erişilebilirliği olumsuz yönde etkileyebilecek hatalar için kayıt tutulur ve gözetimi sağlanır. Bu kapsamda normalden sık tekrarlanan hatalar tespit edildiğinde ilgili kişilere otomatik bildirim gönderilir.

(6) Kimlik doğrulama verileri, kişisel ve finansal veriler ile benzeri hassas verilerin çerezlerde saklanması engellenir.

(7) Veri güvenliğini sağlamak amacıyla; çerezler asgari sürelerde tutulur, kalıcı çerezlerin tutulma süresi güvenlik gereksinimlerine uygun olarak sınırlandırılır. Oturum çerezleri, oturum kapanışında otomatik olarak silinir.

(8) Çerezler her oturumda kullanıcıya özel olacak şekilde üretilir. Çerez değerlerinin her kullanıcı için benzersiz olması ve oturum açma sırasında yeniden üretilmesi sağlanır.

(9) Uygulamalarda geçici veya misafir kullanıcı erişimleri belirli süreler için sağlanır ve bu erişimler süre dolduğunda devre dışı bırakılır.

(10) API erişimlerinde, kimlik doğrulama ve yetkilendirme için güvenli protokoller kullanılır. Erişim talepleri belirteç (token) bazlı doğrulanır ve kullanıcı kimlik bilgileri korunur. Zorunlu olmadıkça hassas verilerin API aracılığıyla iletilmesi engellenir.

(11) API erişimlerinde aşırı yüklenme ve kötüye kullanım girişimlerine karşı trafik yönetimi yapılır. Bu kapsamda talep sınırlandırma ve yavaşlatma mekanizmaları kullanılır.

(12) Uygulamaların oturum zaman aşımı süresi, uygulamanın kritikliğine göre belirlenir. Bu sürenin aşımında oturum otomatik olarak sonlandırılır ve kullanıcı yeniden giriş yapmaya zorlanır.

(13) Uygulamanın kaynak kodlarının kötü amaçlı kullanım ve müdahalelere karşı korunaklı olması sağlanır.

(14) Uygulamalarda, kullanıcı tarafından gönderilen tüm girdilerde kötü amaçlı içeriklerin tespit edilmesi ve engellenmesine yönelik kontroller tesis edilir ve bu amaçla koruma çözümleri kullanılır.

(15) Uygulamalara yüklenen dosyaların güvenliğini sağlamak amacıyla dosya türü, boyutu ve içeriği kontrol edilir. Olası tehditlere karşı dosyalar, güncel zararlı yazılım imzalarına ve tehdit veri tabanlarına göre taranır, tespit edilen şüpheli dosyalar otomatik olarak karantinaya alınır veya yüklenmesi engellenir. Yüklenen dosyaların yalnızca yetkili kişilerce erişilebilmesi ve güvenliği sağlanır. Erişimlerin denetim izi tutulur.

(16) Mobil uygulamanın ilk kurulumu, aktifleştirilmesi veya kullanılamaz hale gelmesi durumları hariç olmak üzere, mobil uygulamayı yükleyerek aktif hale getiren müşterilere, oturum açma veya oturum sırasında gerçekleştirilen işlemlerin doğrulaması amacıyla SMS yoluyla tek kullanımlık parola gönderilmez ve bu yöntem kimlik doğrulama faktörü olarak kullanılmaz.

(17) Uygulamalarda SMS yoluyla tek kullanımlık parola gönderilmeden önce, müşterinin SIM kart değişikliği yapıp yapmadığı veya numara taşıma yoluyla elektronik haberleşme işletmecisini değiştirip değiştirmediği Türkiye'deki mobil haberleşme operatörleriyle sağlanan entegrasyon aracılığıyla kontrol edilir ve değişiklik yapıldığının belirlenmesi durumunda müşteri tarafından bu değişiklik teyit edilmediği sürece sunulacak hizmetlerde SIM karta dayalı kimlik doğrulama faktörünün kullanılması engellenir. Değişiklikler teyit edilirken iki faktörlü kimlik doğrulama yöntemlerinin kullanılması esastır. İki faktörlü kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü Kurum, Kuruluş ve Ortaklıklara aittir.

(18) Uygulamalarda kritik işlemler için ek kimlik doğrulama adımları uygulanır. Müşterilere, varsayılan ve müşteri tarafından güncellenebilecek erişim kısıtlamaları, günlük işlem limitleri, güvenli alıcılar listesi gibi ilave güvenlik önlemleri sunulur. Güvenlik önlemlerinin tanımlanması, güncellenmesi veya değiştirilmesinin çok faktörlü kimlik doğrulama sonrasında gerçekleştirilmesi esastır.

(19) Kimlik ve işlem doğrulama amacıyla müşterilere kullandırılacak tek kullanımlık parolaların, tahmin edilmesi zor olacak şekilde yeterli uzunlukta, rastgele, değişken ve eşsiz olarak üretilmesi ve yalnızca belirli bir süre boyunca geçerli olacak şekilde tasarlanması sağlanır.

(20) Kritik uygulamalarda, kullanıcılara uygulama üzerindeki aktif oturumlar hakkında bilgilendirme yapılır ve aktif oturumların sonlandırılabilmesi için gerekli işlevsellik sağlanır.

(21) Kritik uygulamalarda, başarısız kimlik doğrulama teşebbüsleri hakkında ilgili kullanıcıya sisteme ilk girdiği anda bilgi verilir.

(22) Mobil uygulamaların, güvenlik güncellemelerini kullanıcılara otomatik olarak bildirmesi sağlanır. Kritik güvenlik güncellemelerinin yapılması için kullanıcılar zorlanır ve uygulamanın eski sürümleri devre dışı bırakılır.

(23) Mobil uygulamaların çalıştıkları cihaza özgü güvenlik gereksinimlerine uygunluğu sağlanır. Bu uygulamalar yalnızca gerekli cihaz izinlerini talep eder ve kullanıcıların onayı alınarak en az izinle çalıştırılır.

(24) Mobil uygulamalarda aynı kullanıcı hesabıyla birden fazla cihazda eş zamanlı oturum açılması engellenir.

(25) Müşteri kullanımına sunulan mobil uygulamaların cihaz tanıma özelliğine sahip olması sağlanır.

(26) Mobil uygulamaların çalıştığı cihazlardaki hassas verilerin güvenliğini sağlamak ve bu cihazların işletim sistemi yazılımının kırılması veya değiştirilmesi gibi hallerden kaynaklanacak risklerin azaltılması amacıyla günün teknolojisine uygun kontroller tesis edilir.

(27) Mobil uygulama kontrolünde olmayıp cihaz üreticisi kontrolünde olan parola, PIN ya da biyometrik veriler, müşterinin bildiği ya da biyometrik karakteristiği olan unsurlar olarak kabul edilmez.

Bilgi sistemleri sürekliliği

MADDE 27- (1) Kurum, Kuruluş ve Ortaklıkların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur. İkincil sistemin yeri, doğal ve çevresel felaketlere karşı birincil sistemle aynı risklere maruz kalmayacak şekilde seçilir.

(2) Bilgi sistemleri süreklilik planının geliştirilmesi ve işletilmesinde görev alacak kişiler ile rol ve sorumlulukları belirlenerek ilgili eğitimleri almaları sağlanır. Planın devreye alınması kararını verecek kişi ve durumlar yazılı hale getirilir. Bilgi sistemleri süreklilik planı üst yönetim tarafından onaylanır. Planın sadece ilgili kişiler tarafından erişilebilir olması ve güncel fiziksel kopyalarının gereken yerlerde bulundurulması sağlanır.

(3) Plan kapsamında ikincil sistem tesis edilir. İkincil sistemde, Kurum, Kuruluş ve Ortaklıkların kritik veri ve sistem yedekleri kullanıma hazır bulundurulur.

(4) Plan, iş birimleriyle gerçekleştirilen iş etki analizi sonuçlarını ve iş sürekliliği planında belirlenen hedefleri de dikkate alacak şekilde, asgari olarak kritik iş süreçlerini destekleyen bilgi sistemleri ve bunların yer aldığı konumlara yönelik hazırlanır. Planda yer alan süreçlerin her biri için kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı değerleri belirlenir. Bu çerçevede hizmetlerin tekrar kullanıma açılmasını sağlayacak alternatifli kurtarma süreç ve prosedürleri tesis edilir ve gerekli önlemler alınır.

(5) Bilgi sistemleri süreklilik planının devreye alınması durumunda gerekli olacak kapasite belirlenir ve bunu sağlayacak önlemler alınır.

(6) Bilgi sistemlerinden kaynaklanabilecek kesintilere, işlem performansını düşürecek veya iş sürekliliğini aksatacak durumlara karşı gerekli önlemler alınır.

(7) Bilgi sistemlerinin sürekliliğini sağlamak amacıyla, risk değerlendirmesi, risk azaltma ve risk izleme faaliyetleri gerçekleştirilir.

(8) Plan, iş süreçlerini veya bilgi sistemlerini etkileyecek değişikliklerden sonra veya yılda en az bir kez gözden geçirilerek güncellenir. Planın etkinliğini ve güncelliğini temin etmek üzere testler yapılır, testlere varsa dışarıdan hizmet alınan kuruluşlar da dâhil edilir ve test sonuçları üst yönetime raporlanır. Testler her yıl tekrarlanır.

(9) Kurum, Kuruluş ve Ortaklıkların, birincil sistemin tamamen devre dışı kaldığı durumlarda en geç yirmi dört saat içerisinde faaliyetlerini sürdürebilir hale gelmesi esastır.

(10) Birincil sistemin tamamen devre dışı kaldığı durumlarda Kurul derhal bilgilendirilir.

(11) İkincil sistemlerden birincil sistemlere geri dönüş prosedürleri hazırlanır.

(12) Bilgi sistemleri, iş sürekliliği planındaki önceliklere uygun olarak yedeklenir ve yedekten geri dönülmesi için gerekli süreçler bilgi sistemleri sürekliliği planına ve testine dâhil edilir. Bu kapsamda yedekleme çizelgesi hazırlanır, üst yönetime onaylatılır ve güncelliği sağlanır. Yedeklerin en az bir kopyası farklı coğrafi bir konumda saklanır. Yedeklerin güvenliğine ilişkin gerekli önlemler alınır.

(13) Yılda en az bir defa asgari olarak kritik sistemlerin yedekten geri dönme testi gerçekleştirilir ve teste katılanların bilgisi, tarih, testin detayları ve sonuçları kayıt altına alınır. Alınan yedeklerin yasal saklama süresi boyunca geri döndürülebilir olması sağlanır.

(14) Kurum, Kuruluş ve Ortaklıklar, faaliyetlerini iş sürekliliği planında belirlediği kabul edilebilir kesinti süreleri ve azami veri kaybı değerleri dahilinde sürdürmesini sağlayacak şekilde bilgi sistemlerinde gerekli altyapıyı kurar.

(15) Kurum, Kuruluş ve Ortaklıklar, kritik faaliyetlerinin çalışamaz hale gelmesini önlemek adına bilgi sistemlerinde yedekli çalışma ya da hazırda bekleme düzenleri kurar.

(16) Kurum, Kuruluş ve Ortaklıklar, bilgi güvenliği politikasının, bilgi sistemleri süreklilik planının, bilgi varlıkları envanteri ile iş sürekliliği ve güvenliği açısından önem arz eden diğer dokümanların güncel sürümlerini ve bilgi sistemleri yönetimine ilişkin parolalarını güvenli ortamlarda saklar.

Değişiklik yönetimi

MADDE 28- (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemlerini oluşturan her türlü yazılım, donanım ve altyapı bileşenlerine, dokümantasyona ve bilgiye yapılan değişiklikleri yönetebilmek amacıyla kontroller geliştirir. Bu kontroller en az aşağıdaki hususları içerir:

a) Yapılacak her türlü değişiklik için; değişikliğin sebebini, kapsamını, etkisini, içerdiği riskleri, beklenen faydasını, değişikliği yapacak kişileri, maliyetini, gerekli test ve eğitim faaliyetlerini tanımlayan kayıtlar oluşturulur.

b) Planlanan değişiklikler uygulanmadan önce bu değişikliklere yönelik detaylı bir test süreci yürütülür ve değişikliklerin güvenirliği ve işlevselliği doğrulanır, sistem ve uygulamaların yapılandırma ayarlarının ve sürümlerinin değişiklik sonrası olması gerektiği biçimde belirlendiği kontrol edilir.

c) Planlanan değişiklikler onay sürecinden geçmedikçe işleme konulmaz, ancak acil durumlarda yapılacak değişiklikler için özel bir prosedür tanımlanır ve bu şekilde gerçekleştirilen değişikliklerin belge ve kayıtlarının mümkün olan en kısa sürede tamamlanması sağlanır.

ç) Planlanan değişiklikler, devreye alınma tarihleri, test ve eğitim faaliyetleri ilgili tüm taraflara önceden duyurulur.

d) Değişikliğin uygulanmasında ortaya çıkan hatalar ve öngörülemeyen durumlarda uygulamaya alınacak geri dönüş prosedürleri ve bunlarla ilgili sorumluluklar önceden belirlenir, bu prosedürlerin mümkünse test edilmesi sağlanır.

e) Gerçekleştirilen değişikliklerin sonuçları gözden geçirilir.

f) Gerçekleştirilen, iptal edilen veya reddedilen tüm değişiklikler gerekçeleriyle birlikte kayda geçirilir ve saklanır.

İç denetim

MADDE 29- (1) Kurum, Kuruluş ve Ortaklılar, yılda en az bir kez olmak kaydıyla bilgi sistemlerine yönelik iç denetim gerçekleştirir.

(2) İç denetim faaliyeti dışarıdan hizmet alımı yoluyla icra edilemez.

(3) İç denetim faaliyeti, bilgi sistemlerinin tasarımı ve işleyişine yönelik görevi bulunmayan kişilerce gerçekleştirilir. İç denetimi gerçekleştirecek kişilerin 14/8/2014 tarihli ve 29088 sayılı Resmî Gazete'de yayımlanan Sermaye Piyasasında Faaliyette Bulunanlar İçin Lisanslama ve Sicil Tutmaya İlişkin Esaslar Hakkında Tebliğ (VII-128.7)'in 5 inci maddesinde belirtilen Bilgi Sistemleri Bağımsız Denetim Lisansına sahip olmaları zorunludur.

(4) İç denetim sonrası ulaşılan tespit ve sonuçlar bir rapor haline getirilir ve yönetim kuruluna sunulur.

(5) Bilgi güvenliği sorumlusu tarafından, iç denetim raporunda yer alan tespitlere göre yapılacaklar gerçekleştirme tarihleriyle beraber bir aksiyon planına dönüştürülür, üst yönetime onaylatılır. Aksiyon planına uyum üst yönetim tarafından takip edilir ve bir sonraki iç denetim faaliyetinde dikkate alınır.

(6) İç denetim dönemi bitiminde iç denetim faaliyet raporu hazırlanır ve yönetim kurula sunulur. Söz konusu faaliyet raporunda asgari olarak; tamamlanan, devam eden, ertelenen ve iptal edilen denetim faaliyetlerine, denetim planına uyum düzeyine, bulguların nihai durumu ile bulguların kapatılmasına yönelik olarak aksiyon planında hedef tamamlanma tarihi atanmayan, aşılan, aşma süresi bir seneden fazla uzatılan veya iptal edilen bulgulara yer verilir.

(7) Kurum, Kuruluş ve Ortaklıklar bilgi sistemleri yönetimine ilişkin olarak iç denetim gerçekleştirecek kişileri, göreve başlamalarını takiben 10 iş günü içinde Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.'ye bildirir.

DÖRDÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Muafiyetler

MADDE 30- (1) Asgari özsermaye yükümlülüğünde 2/7/2013 tarihli ve 28695 sayılı Resmî Gazete'de yayımlanan Portföy Yönetim Şirketleri ve Bu Şirketlerin Faaliyetlerine İlişkin Esaslar Tebliği (III-55.1)'nin 28 inci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerine tabi portföy yönetim şirketleri, dar yetkili aracı kurumlar, varlık kiralama şirketleri, ipotek finansmanı kuruluşları, Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği, bağımsız denetim, derecelendirme ve değerleme kuruluşları, halka açık ortaklıklar, varlık finansmanı fonları, kolektif yatırım kuruluşları, emeklilik yatırım fonları, konut finansmanı fonları 8 inci maddenin beşinci, altıncı ve yedinci fıkralarını, 10 uncu maddenin altıncı ve yedinci fıkralarını, 12 nci maddenin birinci fıkrasının (b) bendini, 13 üncü maddenin on birinci ve on üçüncü fıkralarını, 14 üncü maddenin beşinci, altıncı ve sekizinci fıkralarını, 15 inci maddenin üçüncü, altıncı, yedinci, sekizinci ve dokuzuncu fıkralarını, 16 ncı maddenin sekizinci ve dokuzuncu fıkralarını, 17 nci maddenin ikinci fıkrasını, 18 inci maddenin ikinci fıkrasını, 22 nci maddenin yedinci, dokuzuncu ve onuncu fıkralarını, 24 üncü maddenin yedinci ve sekizinci fıkralarını, 25 inci maddenin dördüncü, beşinci, altıncı ve on birinci fıkralarını, 26 ncı maddeyi, 27 nci maddenin üçüncü, dokuzuncu, onuncu, on birinci ve on beşinci fıkralarını, 28 inci maddeyi ve 29 uncu maddeyi uygulamak zorunda değildir.

(2) Borsa İstanbul A.Ş., İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği ve Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş. 29 uncu maddenin yedinci fıkrasından muaftır.

(3) Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2) hükümleri kapsamında, bilgi sistemleri bağımsız denetim zorunluluğu bulunmayan halka açık ortaklıklar, 27 nci maddenin birinci fıkrası uyarınca, birincil ve ikincil sistemlerini yurt içinde bulundurmak zorunda değildir.

(4) Platformlar, bulut hizmet sağlayıcısının yurt içinde temsilciliğinin bulunması koşulu ile müşteri emirlerinin eşleştiği ortamlar için yurt dışı bulut hizmeti kullanabilir. Her halükarda, yurt dışı bulut hizmeti sağlayıcı bünyesinde oluşan tüm kayıtlar gün sonunda yurt içindeki sistemlere aktarılır.

(5) Bağımsız denetim kuruluşları tarafından rezerv kanıt denetimi sürecinde kullanılacak araçlar için yurt dışı bulut hizmeti kullanılabilir.

(6) Kurul, bu Tebliğ kapsamında belirlenen yükümlülüklere ilişkin olarak muafiyet belirlemeye, bunların kapsamını ve içeriğini Kurum, Kuruluş ve Ortaklıklar bazında değiştirmeye yetkilidir.

Diğer hususlar

MADDE 31- (1) Bu Tebliğ hükümleri esas olmak üzere, tezgahüstü türev araç işlemi gerçekleştiren aracı kurumların bilgi işlem altyapılarına ilişkin olarak ilgili Kurul düzenlemelerinde belirlenen ilke ve esaslara uyulur.

(2) Kripto Varlık Hizmet Sağlayıcılar, bu Tebliğde yer alan hükümlere ilave olarak Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun Kripto Varlık Hizmet Sağlayıcıların bilgi sistemleri ve teknolojik altyapılarına ilişkin olarak hazırladığı dokümanda yer alan kriterlere uyar.

(3) Kurul, bu Tebliğ kapsamında belirlenen süreleri Kurum, Kuruluş ve Ortaklıklar bazında değiştirmeye yetkilidir.

(4) Kurul, bu Tebliğ kapsamında bulut hizmet sağlayıcılara ilişkin kriterleri belirlemeye yetkilidir.

Yürürlükten kaldırılan tebliğ

MADDE 32- (1) 5/1/2018 tarihli ve 30292 sayılı Resmî Gazete'de yayımlanan Bilgi Sistemleri Yönetimi Tebliği (VII-128.9) yürürlükten kaldırılmıştır.

(2) Mevzuatta, birinci fıkra ile yürürlükten kaldırılan tebliğe yapılan atıflar bu Tebliğe yapılmış sayılır.

Geçiş süresi

GEÇİCİ MADDE 1- (1) Kripto Varlık Hizmet Sağlayıcıların 27 nci maddeye 31/12/2025, 29 uncu maddenin üçüncü fıkrasına 31/12/2026 tarihine kadar uyum sağlaması gerekmektedir.

(2) Kripto Varlık Hizmet Sağlayıcılar haricindeki Kurum, Kuruluş ve Ortaklıkların ise 29 uncu maddenin üçüncü fıkrasına 31/12/2026 tarihine kadar, bu Tebliğin diğer hükümlerine ise 31/12/2025 tarihine kadar uyum sağlaması gerekmektedir.

(3) Kripto Varlık Hizmet Sağlayıcılar haricindeki Kurum, Kuruluş ve Ortaklıklar, 31/12/2025 tarihine kadar 32 nci madde ile yürürlükten kaldırılan tebliğ hükümlerine uymakla yükümlüdür.

Yürürlük

MADDE 33- (1) Bu Tebliğ 30/6/2025 tarihinde yürürlüğe girer.

Yürütme

MADDE 34- (1) Bu Tebliğ hükümlerini Sermaye Piyasası Kurulu yürütür.

EK-1

Bilgi Sistemleri Sızma Testleri Usul ve Esasları

1) Amaç: Sızma testlerinin amacı, Kurum Kuruluş ve Ortaklıkların bilgi sistemlerindeki olası güvenlik açıklarının herhangi bir sızma girişiminden daha 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
ç. E-posta Servisleri
d. Veri tabanı Sistemleri
e. Web Uygulamaları
f. Mobil Uygulamalar
g. Kablosuz Ağ Sistemleri
ğ. Dağıtık Servis Dışı Bırakma Testleri
h. Sosyal Mühendislik Testleri
ı. Bulut Sistemleri

3) Metodoloji: Sızma testleri, aşağıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek testlerden oluşur. Testler, sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder. Sızma testleri gerçekleştirilirken, bir önceki sızma testinde tespit edilen ve aksiyon alınması planlanan bulguların giderilip giderilmediğine yönelik doğrulama testleri de yapılır ve buna ilişkin tespitlere sızma testi raporunda ayrı bir başlık altında yer verilir. Sızma testleri gerçekleştirilirken, Kurum, Kuruluş ve Ortaklıklar faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol açabilecek tüm testler Kurum, Kuruluş ve Ortaklıklar ile koordineli bir şekilde planlanarak gerçekleştirilir. Sızma testleri sonrası saptanan açıklık ve bulgular, Kapsam bölümünde belirtilen ve ilişkili olduğu her bir başlık altında ayrıntılı olarak incelenerek raporlanır. Raporda kapsam bölümünde belirtilen her bir başlığa yer verilir. Sızma testleri sürecinde her bir test başlığı kapsamında saptanan açıklık ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilir. Söz konusu değerlendirmenin yapıldığına ilişkin bilgi ve birlikte değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgular da raporda yer alır. Bulgular, **"Bulgu Önem Dereceleri"** bölümünde yer verilen dereceler 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 Kurum, Kuruluş ve Ortaklıkların sorumluluğundadır. Sızma testi raporunda; raporun nihai tarihinin yazılı olması, sızma testini gerçekleştiren test ekibine ilişkin ad-soyad ve iletişim bilgilerinin de yer alması gerekir. Bununla birlikte sızma testini gerçekleştiren gerçek veya tüzel kişilere ait sızma testi konusunda ulusal veya uluslararası belgelere sızma testi raporu ekinde yer verilir.

a. Testlerin Gerçekleştirileceği Erişim Noktaları

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

i. İnternet: Kurum, Kuruluş ve Ortaklıkların İnternet üzerinden erişilebilen tüm sunucu ve servislerine İnternet üzerinden erişilerek sızma testleri gerçekleştirilir ve devamında ve detaylı sızma testleri uygulanır.

ii. Kurum, Kuruluş ve Ortaklıklar iç ağı: Kurum, Kuruluş ve Ortaklıkların iç ağında yer alan ve test kapsamında ele alınan sunuculara Kurum, Kuruluş ve Ortaklıklar 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 personel bilgisayarı profilinde bilgisayarlar 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, Kurum, Kuruluş ve Ortaklıkların web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Kurum, Kuruluş ve Ortaklıklara ait web uygulamalarının üyesi olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili güvenlik açıklarını bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

ii. Kurum, Kuruluş ve Ortaklıklar müşterisi profili: İnternet üzerinden, Kurum, Kuruluş ve Ortaklıklar'ın web servislerine erişebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. İnternet üzerinde Kurum, Kuruluş ve Ortaklıklara ait web uygulamalarının üyesi olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili güvenlik açıklarını bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

iii. Kurum, Kuruluş ve Ortaklıklar personel profili: Kurum, Kuruluş ve Ortaklıklar personelinin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili güvenlik açıklarını bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır. Kurum, Kuruluş ve Ortaklıklar personeli profili ile gerçekleştirilecek testlerde, Kurum, Kuruluş ve Ortaklıklarda çapında en yaygın olarak kullanılan personel profilinin seçilmesinin yanında, yerel yönetici (local admin) yetkisine sahip personel profilleri ile de sızma testleri gerçekleştirilir. Kurum, Kuruluş ve Ortaklıklar personel profili ile yapılan testlerde, testi yapan kişi/kuruluşa Kurum, Kuruluş ve Ortaklıklar tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilmelidir.

iv. 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 açıklık taraması/araştırması adımları ile başlar. Sistem tespiti, servis tespiti ve açıklık 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: Kurum, Kuruluş ve Ortaklıklar bilgi sistemlerinde yer alan varlıkların port taramasının gerçekleştirildiği ve dış dünyaya/genel erişime açık olan portların sunduğu servislerin tespit edilmeye çalışıldığı adımdır.

iii. Açıklık taraması/araştırması: Kurum, Kuruluş ve Ortaklıkların bileşenleri ve bu bileşenlerin sunduğu servislerin açıklık tarayıcıları ile güncel açıklıklara karşı tarandığı ve muhtemel güvenlik açıklarının belirlenmeye çalışıldığı adımdır. Bu adımda ayrıca, tespit edilen muhtemel açıklıklar için açıklık veri tabanları gibi kaynaklar kullanılarak bu açıklıkların bileşenlere ve bileşenlerin etkileşimde olduğu sistemlere güvenlik açısından etkileri araştırılır.

d. Sızma Testleri

i. İnternet üzerinden gerçekleştirilecek temel sızma testleri: Kurum, Kuruluş ve Ortaklıklar ağından bağımsız bir konumdan , Kurum, Kuruluş ve Ortaklıklar'ın internet üzerinde sahip olduğu IP ağı taranarak sistem tespiti, servis tespiti ve açıklık taraması adımları gerçekleştirilir.

ii. Kurum, Kuruluş ve Ortaklıklar iç ağından gerçekleştirilecek sızma testleri: Kurum, Kuruluş ve Ortaklıkların iç ağında sistem tespiti, servis tespiti ve açıklık taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:

- Kurum yerel ağ haritası tespiti
- Belirlenen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin gerçekleştirilmesi
- Yerel alan ağı içerisinde güvenlik açığı taraması yapılması
- Kurum yerel ağında araya girme teknikleri ile hassasiyet derecesi yüksek 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

4) Sızma Testi Sonuçlarının Takibi

Kurum, Kuruluş ve Ortaklıklar, sızma testleri sonucu tespit edilen bulguları, bulguların önem derecelerini, birlikte oluşturabilecekleri riskleri, tespit edildiği varlıkların değerini ve sızma testi raporlarında yer alan önerileri dikkate alarak, Kurum, Kuruluş ve Ortaklıklar yönetim kurullarınca onaylanan ve bu bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planı çerçevesinde takip eder. Sızma testi raporunda "Acil" ve "Kritik" olarak derecelendirilen bulgular ivedilikle kapatılır. Sızma testleri sonucu ortaya çıkan tespitler, gerekli görülmesi halinde Kurum, Kuruluş ve Ortaklıkların iç denetim planına da dâhil edilir. Aksiyon planı ve kabulüne ilişkin yönetim kurulu kararı sızma testi raporuna eklenir.

Bulgu Önem Dereceleri

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 Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Kritik	Nitelikli saldırgan tarafından Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Yüksek	Kurum, Kuruluş ve Ortaklıklar 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 açıklıklardır.
Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

Bulgu Formatı

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, EK-1'de yer verilen önem derecesi
Etkisi	Bulguda yer verilen açıklığın/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 Bileşen/Bileşenler	Bulgunun tespit edildiği bileşeni 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 sunulacak çözüm önerisi