YÖNETMELİK

Bilgi Teknolojileri ve İletişim Kurumundan:

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE ŞEBEKE VE BİLGİ GÜVENLİĞİ YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç ve kapsam

MADDE 1 – (1) Bu Yönetmeliğin amacı, şebeke ve bilgi güvenliğinin sağlanmasına yönelik olarak işletmecilerin uyacakları usul ve esasları düzenlemektir.

(2) Kişisel verilerin işlenmesi ve gizliliğinin korunması, bu Yönetmelik kapsamı dışındadır.

Dayanak

MADDE 2 – (1) Bu Yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 4 üncümaddesinin birinci fıkrasının (l) bendi, 6 ncı maddesinin birinci fıkrasının (n), (ş) ve (v) bentlerine, 12 nci maddesinin ikinci fıkrasının (i) ve (j) bentlerine ve 60 ıncı maddesinin birinci fıkrasına dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 3 – (1) Bu Yönetmelikte geçen;

a) Belgelendirme kuruluşu: TS ISO/IEC 27001 veya ISO/IEC 27001 standardına göre belgelendirme yapmaküzere akredite edilmiş kurum veya kuruluşu,

b) BGYS standardı: TS ISO/IEC 27001 veya ISO/IEC 27001 standardını,

c) Bilgi güvenliği yönetim sistemi (BGYS): Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, işletmecinin yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününü,

ç) Bilgi sistemi: İşletim sistemlerinin, veritabanlarının, sunucuların, altyapının, iş uygulamalarının, kullanıma hazır ürünlerin, donanımların, yazılımların ve hizmetlerin tamamını,

d) Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliğini,

e) Donanım: Elektronik haberleşme altyapısı, bilgisayarlar, veri kaydetmek için kullanılan taşınabilir veya sabit diskleri,

f) Dos: Hizmet dışı bırakmayı,

g) Ddos: Dağıtık hizmet dışı bırakmayı,

ğ) Erişilebilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini,

h) Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da süreçler tarafından erişilememesini, kullanılamamasını, değiştirilmemesini, depolanmamasını, başka bir ortama kaydedilmemesini veya ifşa edilmemesini,

ı) IP adresi: İnternet protokol adresini,

i) İşletmeci: Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşmeşebekesi sağlayan ve alt yapısını işleten şirketi,

j) Köle bilgisayar: Herhangi bir amaçla kullanılmak üzere, zararlı yazılımlar veya kötü niyetli kişiler tarafından uzaktan yönetilen internete bağlı bilgisayarı,

k) Kritik bilgi: Değiştirilmesi, bozulması, kaybolması, kötüye kullanılması veya yetkisiz bir şekilde ifşa edilmesi durumunda şebeke ve bilgi güvenliği açısından zararlara yol açacak bilgiyi,

l) Kritik sistem: İşletmecinin kontrolü altında yer alan elektronik haberleşme altyapısı ile işlevselliğinin bozulması halinde veya maruz kalacağı etkiler neticesinde şebeke ve bilgi güvenliğini zafiyete uğratabilecek sistemleri,

m) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,

n) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

o) Risk değerlendirme: Risklerin analizi, seviyelerinin tanımlanması, derecelendirilmesi ve tahmin edilmesi ile kabul edilebilir risk seviyesinin belirlenmesini,

ö) Risk işleme: Riski azaltmaya yönelik önlemlerin seçilmesi ve uygulanması ile kabul edilen risklerin gerekçelerinin belirlenmesini,

p) Risk temelli değerlendirme: Abone sayısı, yıllık net satış, müşteri beklentileri, yasal ve düzenleyici yükümlülükler, hizmet verilen yerleşim alanları, işletilen altyapının kritikliği veya büyüklüğü gibi kriterler dikkate alınarak Kurum tarafından yapılan değerlendirmeyi,

r) Siber Güvenlik Kurulu: 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun EK 1 inci maddesinin birinci fıkrası kapsamında kurulan kurulu,

s) SOME: Siber olaylara müdahale ekibini,

ş) USOM: 20/6/2013 tarihli ve 28683 sayılı Resmî Gazete'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı'nın ekinde yer alan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 4 üncü maddesi gereğince kurulan ulusal siber olaylara müdahale merkezini,

t) Varlık: İşletmeci için değeri olan herhangi bir şeyi,

ifade eder.

(2) Bu Yönetmelikte geçen ve birinci fıkrada yer almayan tanımlar için ilgili mevzuatta yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM

Genel Hükümler

İlkeler

MADDE 4 – (1) Bu Yönetmeliğin uygulanmasında aşağıda belirtilen temel ilkeler gözetilir:

a) İşletmecilerin yükümlülüklerinin belirlenmesinde, şebeke ve bilgi güvenliğinin sağlanmasına yönelik tedbirlerin tespitinde ve uygulanmasında mümkün olduğu ölçüde risk temelli değerlendirmelerin yapılması.

b) Tüketici haklarının korunması.

c) Hizmet kalitesinin yükseltilmesi.

ç) Ulusal düzenleme ile ulusal ve/veya uluslararası standartların dikkate alınması.

d) Güvenlik ile kullanılabilirlik arasında denge kurulması.

e) Azami ölçüde milli kaynakların kullanılması.

İşletmecilerin yükümlülükleri

MADDE 5 – (1) İşletmeciler şebeke ve bilgi güvenliği ile ilgili olarak üçüncü bölümde yer alan hükümler kapsamında temel tedbirleri almakla yükümlüdür.

(2) Aşağıdaki yetkilendirme tiplerine sahip işletmecilerden yıllık net satışları Kurul Kararı ile belirlenen değer ve üzerinde olanlar, birinci fıkrada belirtilen yükümlülüklerin yanı sıra, dördüncü bölümdeki hükümler kapsamındaşebeke ve bilgi güvenliğinin sağlanmasına ilişkin ilave tedbirleri almakla yükümlüdür.

a) Altyapı işletmeciliği hizmeti.

b) Çeşitli telekomünikasyon hizmetleri (imtiyaz sözleşmesi).

c) GMPCS mobil telefon hizmeti.

ç) GSM/IMT-2000/UMTS (imtiyaz sözleşmesi).

d) Hava taşıtlarında GSM 1800 mobil telefon hizmeti.

e) İnternet servis sağlayıcılığı.

f) Sabit telefon hizmeti.

g) Sanal mobil şebeke hizmeti.

ğ) Uydu haberleşme hizmeti.

h) Uydu ve kablo tv hizmetleri (görev sözleşmesi).

(3) Kurul gerekli görmesi halinde işletmecilerin ilgili yükümlülüklerinde farklılaştırma yapabilir.

ÜÇÜNCÜ BÖLÜM

Şebeke ve Bilgi Güvenliğinin Sağlanmasına İlişkin Temel Yükümlülükler

BGYS'nin kurulması, kapsamı ve yönetimi

MADDE 6 – (1) İşletmeci, yetkilendirmesine ilişkin tüm hizmetleri ve kritik sistemleri kapsayacak şekilde

BGYS kurar.

(2) İşletmeci BGYS'nin kurulması, uygulanması ve sürekliliğinin sağlanması amacıyla bir yönetim mekanizmasıişletir.

BGYS politikası

MADDE 7 – (1) İşletmeci, yönetimi tarafından onaylanmış bir bilgi güvenliği yönetim sistemi politikasıtanımlar, dokümante eder, tüm çalışanlarının ve ilgili tarafların söz konusu politikaya ilişkin farkındalığını sağlar.

(2) Bilgi güvenliği yönetim sistemi politikası asgari olarak aşağıdaki hususları içerir:

a) İşletmeci açısından bilgi güvenliğinin tanımı, genel amaçları ve kapsamı.

b) Yönetimin bilgi güvenliği hedeflerinin yerine getirilmesi ve ilgili faaliyetlerin desteklenmesine ilişkin taahhüdü.

c) Risk değerlendirmesine ilişkin esasları.

ç) Varlıkların sınıflandırılması.

d) Uygulanan güvenlik politikaları, prosedürleri, kuralları, prensipleri ve standartları hakkında genel bilgileri.

Bilgi güvenliği grubu ve faaliyetleri

MADDE 8 – (1) Bilgi güvenliği faaliyetleri, işletmecinin yönetimi tarafından yetkilendirilmiş temsilcilerin katılımıyla oluşturulan bir grup marifetiyle veya işletmecinin kaynaklarının elvermediği durumlarda bir yönetici tarafından koordine edilir.

(2) Bilgi güvenliği grubu faaliyetleri aşağıdaki hususları kapsar:

a) Faaliyetlerin, BGYS politikasına uygun olarak yürütülmesinin sağlanması.

b) BGYS politikasına ilişkin uygunsuzluklarda yapılacak işlemlerin tanımlanması.

c) Bilgi güvenliğine ilişkin metot ve prosedürlerin onaylanması.

ç) Bilgiye ve bilgi sistemlerine yönelik tehditlerin ve açıkların belirlenerek çözüm yollarının tanımlanması.

d) Bilgi güvenliğinin sağlanması amacıyla alınan tedbirlerin uygulanması ve yeterliliğinin değerlendirilmesi.

e) Bilgi güvenliği farkındalığının artırılmasına yönelik eğitimlerin ve çalışmaların planlanması ve uygulanması.

f) Bilgi güvenliği olaylarının izlenmesi ve gözden geçirilmesi sonucunda elde edilen verilerin değerlendirilmesi ve uygun önlem ve faaliyetlerin belirlenmesi.

g) BGYS dokümanlarının güncel şekilde tutulması.

Varlık yönetimi sınıflandırması

MADDE 9 – (1) İşletmeci, sahip olduğu varlıkları ve bu varlıkların sorumlularını dokümante ederek bir varlık envanteri oluşturur. Birçok varlığın belirli bir fonksiyonu yerine getirmek üzere birlikte kullanıldığı karmaşık bilgi

sistemleri tek bir varlık olarak kabul edilebilir.

(2) Varlık envanteri asgari olarak varlığın adı, tipi, yeri, yedekleme bilgisi, kuruluş açısından değeri, varlık sorumlusu ve varsa lisans veya kimlik bilgisini içerir. Mevzuata uyum ve Kuruma karşı sorumluluk, varlık sorumlusundan bağımsız olarak işletmeciye aittir.

(3) İşletmeci, bilgi güvenliği ihtiyaçlarını karşılayacak şekilde varlıklarının gizlilik sınıfını; kritiklik derecesi, yasal gereksinimler ve verinin hassasiyeti kriterlerine göre belirleyerek varlıklarını uygun biçimde etiketler.

(4) Her bir gizlilik sınıfı için erişim, kullanım, depolama, iletim, imha, paylaşım ve dağıtım kuralları işletmeci tarafından belirlenir.

(5) Varlık envanteri yazılım, donanım, personel gibi envanteri oluşturan varlıklarda değişiklik olması durumunda güncellenir.

Risk değerlendirme ve işleme

MADDE 10 – (1) İşletmeci, bilgi güvenliğine ilişkin tehditlerin tanımlanmasını, söz konusu tehditlerin gerçekleşme olasılıklarını ve oluşturabilecekleri olumsuz sonuçları niteleyen ve risklerin sınıflandırılmasını içerecekşekilde yılda en az bir defa risk değerlendirmesi yapar.

(2) Risk değerlendirmesi sonuçları dikkate alınarak risklerin kabul edilme kriterleri tanımlanır.

(3) Tüm riskler için bir risk işleme kararı alınır. Risk işleme kararı,

a) Riskin azaltılmasına yönelik tedbirlerin uygulanması,

b) Belirlenen kabul edilme kriterleri çerçevesinde riskin kabul edilmesi,

c) Riskin oluşmasına neden olan faaliyetlerin durdurularak riskten kaçınılması,

ç) Riskin sigorta, sözleşme ve anlaşma gibi yöntemlerle diğer ilgili taraflara aktarılması

şeklinde olur.

(4) Risk değerlendirme ve işleme metotları dokümante edilir ve bu metotlara göre yapılan işlemler kayıt altına alınır.

İş sürekliliği

MADDE 11 – (1) İşletmeci, yetkilendirmesine ilişkin tüm hizmetlerin ve kritik sistemlerin doğal afetler,çevresel tehditler, kazalar, donanım arızaları, kasti eylemler veya siber saldırılar sonucunda kesintiye uğramasınıönlemek ve sahip olduğu varlıklarda oluşabilecek kayıpları en aza indirmek amacıyla iş sürekliliği planları yapar ve uygular.

(2) Planlarda asgari olarak; iş süreçlerini kesintiye uğratabilecek olayların tanımları, söz konusu olayların gerçekleşmesi durumunda yapılacak faaliyetler, her bir faaliyetten sorumlu personel, planın devreye alınması için gerekli koşullar, plan kapsamında kullanılacak ekipman ve malzeme yer alır.

(3) Planlar tatbikat, simülasyon gibi tekniklerle her yıl test edilir ve test sonuçları kayıt altına alınır. Test sonuçlarına göre ya da planları etkileyebilecek yazılım, donanım, personel değişiklikleri gibi durumlarda iş sürekliliği planları güncellenir.

Bilgi güvenliği ihlal olaylarının ve güvenlik açıklarının yönetimi

MADDE 12 – (1) Bilgi güvenliği ihlal olaylarının ve güvenlik açıklarının mümkün olduğunca kısa sürede raporlanmasını sağlamak üzere bir raporlama ve geri bildirim mekanizması kurulur.

(2) Hazırlanacak raporlar asgaride, olayın gerçekleşme zamanını, niteliğini ve olaydan etkilenen varlıkların neler olduğunu kapsar.

(3) Raporlanan bilgi güvenliği olaylarına en kısa sürede müdahale edilerek ihlal ve güvenlik açıklarının giderilmesi amacıyla yapılması gereken işlemleri ve bu işlemlerin sorumlularını içeren prosedürler tanımlanır.

(4) Gerçekleşen bilgi güvenliği ihlal olaylarına ilişkin bilgiler kayıt altına alınır, değerlendirilir ve BGYS'ningeliştirilmesi amacıyla yapılan çalışmalarda girdi olarak kullanılır.

İç denetim

MADDE 13 – (1) İşletmeci bu Yönetmelikte belirtilen yükümlülüklerini yerine getirmek amacıyla yaptığıfaaliyetleri ve işletmekte olduğu BGYS'yi iki yılda en az bir defa iç denetim yaparak denetler veya bu hizmeti veren taraflara denetlettirir. İç denetimlerde denetçilerin kendi çalışmalarını denetlememeleri sağlanır.

(2) İşletmeci tespit edilen uygunsuzluklarla ilgili gerekli düzeltici ve önleyici faaliyetleri yerine getirir. Denetim sonuçları ve yapılan düzeltici ve önleyici faaliyetler kayıt altına alınır.

Personel ve istihdam

MADDE 14 – (1) İşletmeci istihdam ettiği personelin, yetkilendirme kapsamında sunulan hizmetlere ilişkinşebeke ve bilgi güvenliğine, milli güvenliğe ve kamu düzenine aykırı davranışta bulunmaması için her türlü önlemi alır.

(2) İstihdam edilecek personel hakkında adli sicil kaydı belgesi istenir, muhafaza edilir ve ilgili personelin görevlendirilmesinde dikkate alınır.

(3) Bilgi güvenliğine ilişkin rol ve sorumluluklar, istihdam edilen personele işe alım sürecinde açık bir şekilde ifade edilir ve imzalattırılarak muhafaza edilir.

(4) İstihdamın sonlandırılmasında veya görev değişikliklerinde; varlıkların iadesi ve erişim haklarının kaldırılmasıveya güncellenmesi işlemlerine ilişkin, asgari olarak aşağıdaki hususları içeren bir prosedür oluşturulur, dokümante edilir ve uygulanır:

a) İlgililere istihdam sonlandırılmasında veya görev değişikliği sonrasında da devam eden bilgi güvenliğine ilişkin sorumlulukları ve yükümlülükleri.

b) İlgililerin işletmeci tarafından kendilerine söz konusu görevle ilgili tahsis edilmiş olan ekipman, yazılım, doküman, mobil cihazlar, kredi kartları ve erişim kartları da dahil olmak üzere tüm varlıkları iade etmesi ve kendilerine tanımlanmış erişim haklarının, üyeliklerin, kullanıcı hesaplarının kaldırılması.

c) İlgililerin kendi mülkiyetlerinde bulunan ekipman kullanmaları durumunda işletmeciyle ilgili tüm bilgilerin iadesi ve güvenli bir şekilde silinmesi.

Disiplin prosedürü

MADDE 15 – (1) İşletmeci, şebeke ve bilgi güvenliğine ilişkin kuralların ihlal edilmesi durumunda, ilgililere yaptırım uygulanmasını sağlamak üzere bir disiplin prosedürü oluşturur, dokümante eder ve tüm personelin konu ile ilgili farkındalığını sağlar.

Eğitim

MADDE 16 – (1) Personelin, konusunda yeterliliğe sahip ve gerekli eğitimleri almış olması, alınan eğitimlerin personelin rol ve sorumluluklarına uygun olması esastır.

(2) Tüm personelin iki yılda en az bir defa, bilgi güvenliği farkındalık eğitimi alması sağlanır.

(3) Personelin aldığı eğitimlere ilişkin kayıtlar muhafaza edilir.

Fiziksel erişim

MADDE 17 – (1) İşletmeci, bina ve tesislerinde, yetkisiz erişime ve istenmeyen fiziksel etkilere karşı gerekli tedbirleri alır.

(2) Kritik sistemlerin bulunduğu alanlara giriş ve erişim yetkisi sadece yetkili kişilerle sınırlandırılır, bu yetkiler düzenli olarak gözden geçirilerek güncellenir ve gerekli değilse iptal edilir. Kritik sistemlerin bulunduğu alanlara giriş veçıkış bilgileri takip edilir ve kayıt altına alınır. Söz konusu kayıtlar en az 2 yıl süreyle muhafaza edilir.

(3) Ziyaretçi giriş ve çıkışlarında gerekli kontroller yapılarak, tarih, saat ve kimlik gibi bilgiler kaydedilir. Ziyaretçilere yalnızca ziyaret amacına uygun giriş ve erişim yetkileri verilir. Gerekli durumlarda işletmeci personelinin refakati sağlanır.

(4) Teslimat alanları, yükleme alanları veya depo gibi üçüncü tarafların bina ve tesislere girişinin söz konusu olabileceği alanlar, kritik sistemlerin bulunduğu alanlardan ayrılır.

(5) Elektronik haberleşme altyapısını içeren bina, kule, dolap ve kutu gibi güvenlik riski oluşturabilecek altyapıbileşenlerine erişim kontrol altında tutulur ve bu bileşenler yetkisiz kişilerin kolaylıkla erişim sağlayamayacağı şekilde tesis edilir.

Çevresel tehditlere karşı korunma

MADDE 18 – (1) İşletmeci; yangın, su baskını, deprem, yıldırım, patlama ve diğer çevresel tehditlere karşıgerekli önlemleri alır.

(2) İşletmeci, bilgi sistemlerine gelen haberleşme ve elektrik hatlarının mümkün olduğunca yer altında olmasınıveya kesinti ve zarar görmesini engelleyecek şekilde korunmasını sağlar.

Ekipman ve çalışma ortamı güvenliği

MADDE 19 – (1) İşletmeci kullandığı ekipmanın; çevresel tehditler, elektrik, su, kanalizasyon, iklimlendirme ve havalandırma sistemleri gibi destek sistemlerinin fonksiyon kaybı veya eksikliklerinden kaynaklanabilecek olumsuz etkilere ve yetkisiz erişime karşı korunması amacıyla gerekli tedbirleri alır.

Elektronik ortam yönetimi

MADDE 20 – (1) İşletmeci elektronik ortamda tutulan bilgilerin yetkisiz olarak erişilmesine, bu bilgilerin yetkisiz olarak değiştirilmesine, silinmesine ve zarar görmesine karşı gerekli önlemleri alır.

(2) Kullanımdan kaldırılması veya başka amaçlarla yeniden kullanılması planlanan ekipmanda veya elektronik ortamda yer alan kritik bilgilerin yedekleri ile birlikte geri döndürülemez şekilde silinmesi sağlanır. Silme işleminin mümkün olmaması durumunda söz konusu bilgi depolayan parçalar kullanılamaz hale getirilir.

(3) Taşınabilir ortamlardan veya mobil cihazlardan kaynaklanabilecek güvenlik zafiyetlerine yönelik tedbirler belirlenir; söz konusu ortam ve cihazlarda yer alan kritik bilgilerin yetkisiz erişim, değiştirme ve ifşa edilmeye karşıkorunması amacıyla önlemler alınır ve çalışanların bunlara uymaları sağlanır.

(4) Kritik bilgiler içeren dokümanlar veya sayısal kayıtları içeren ortamlar kullanımda olmadıkları zamanlarda

kilitli dolaplarda veya şifre koruması altında tutulur.

Şebeke güvenliği

MADDE 21 – (1) İşletmeciler, şebekelerinin tehditlerden korunması ve şebekeleri kullanan sistem ve uygulamaların güvenliğinin sağlanması amacıyla gerekli önlemleri alır.

Aboneye yönelik tedbirler

MADDE 22 – (1) İşletmeci, kendisine tahsisli bir IP adresi kullanılarak şebekesine dışarıdan paket gönderilmesini engellemeye yönelik gerekli önlemleri alır.

(2) İşletmeci, abonelerinin kendisine atanmamış bir IP adresi kullanarak paket göndermelerini engellemeye yönelik gerekli önlemleri alır.

(3) İşletmeci, abonelerini bilinçlendirmek ve gerekli önlemlerin alınmasını sağlamak amacıyla zararlı yazılımlar, köle bilgisayar ağları ve muhtemel siber tehditler ile ilgili olarak bilgilendirir.

Değişim yönetimi

MADDE 23 – (1) İşletmeci sahip olduğu kritik sistemlere ilişkin tesis, ekipman, yazılım ve prosedürlerde değişiklik yapılmasının söz konusu olduğu durumlarda uygulanmak üzere gerekli kuralları belirler.

(2) Söz konusu kurallar asgari olarak aşağıdaki hususları içerir:

a) Değişikliklerin tanımlanması ve kayıt altına alınması.

b) Değişikliklerin planlanması ve test edilmesi.

c) Değişikliklerin etkilerinin analiz edilmesi.

ç) Önerilen değişikliklerin onaylanması.

d) Değişikliklerin yetkili kullanıcılar tarafından yapılmasının sağlanması.

e) Değişikliğe ilişkin bilgilerin ilgililere bildirilmesi.

f) Başarısız değişikliklerle ve öngörülemeyen sonuçlarla karşılaşılması durumunda yapılacak işlemleri.

Görevlerin ve ortamların ayrılması

MADDE 24 – (1) İşletmeci, kritik sistemlere yetkisiz erişimin, bu sistemler üzerinde yetkisiz değişiklik yapılmasının veya bu sistemlerin yetkisiz kullanımının önüne geçilmesi amacıyla;

a) Kritik sistemlerde yapılacak işlemlerin başlatılması ve onaylanması süreçlerini birbirinden ayırır,

b) Kritik sistemlerde işlemleri gerçekleştiren kişiler ile ilgili işlemlerin kayıt dosyalarını yöneten kişileri ayrıştırır,

c) Gerçek sistemleri, geliştirme ve test ortamlarından ayırır,

ç) Yazılımların geliştirme ortamından gerçek ortama aktarılmasına ilişkin kuralları tanımlar ve dokümante eder,

d) Gerekli olmadıkça derleyici, editör ve diğer geliştirme araçlarının veya sistem araçlarının gerçek sisteme erişimine imkân vermez,

e) Geliştirme ve test kullanıcılarının gerçek sistemlere erişimine izin vermez, geliştirme ve test faaliyetlerinin test verisi üzerinden yapılmasını sağlar.

Sistem planlama ve kabulü

MADDE 25 – (1) İşletmeci, kapasite ihtiyacının karşılanması amacıyla bilgi sistemlerinde kaynak kullanımının planlanmasını yapar ve takip eder.

(2) İşletmeci, yeni bilgi sistemlerinin, sistem güncellemelerinin ve yeni sürümlerin, kullanıma alınmadan önce mevcut sistemlere ve güvenlik gereksinimlerine uygunluğunun test edilmesini sağlar.

Zararlı kodlara karşı korunma

MADDE 26 – (1) İşletmeci, bilgi sistemlerinde yer alan bilgilerin ve yazılımların gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması amacıyla bilgisayar virüsleri, solucanlar, truva atları gibi zararlı kodlara karşı gerekliönlemleri alır.

(2) İşletmeci BGYS politikasına aykırı ve lisanssız yazılım kullanımına izin verilmez.

(3) Dış ağlar aracılığıyla dosya veya yazılım indirilmesi ve kullanılmasında uygulanacak güvenlik önlemleri belirlenir.

Yedekleme

MADDE 27 – (1) İşletmeci, bir felaket veya hata durumunda ihtiyaç duyulacak bilgi ve yazılımların kurtarılmasına imkân verecek şekilde yedek alınmasını sağlar.

(2) İşletmeci, yedeği alınacak sistemleri ve bu sistemlere ilişkin yedekleme periyodunu, yedekleme türünü, saklama zamanını iş ihtiyaçlarına ve yedeği alınacak sistemlerin kritiklik seviyesine uygun olacak şekilde belirler.

(3) Yedekleme işlemlerinde aşağıdaki hususlar yerine getirilir.

a) Yedek kopyaların kaydı tutulur.

b) Yedekler gerçek bilgi ve yazılımların bulunduğu yerleşkede meydana gelebilecek felaketlere maruz kalmayacak ve gerçek bilgi ve yazılımların bulunduğu yerleşkeyle aynı riskleri taşımayacak şekilde tutulur ve yedekler için gerçek bilgi ve yazılımlarla aynı düzeyde güvenlik önlemleri uygulanır.

c) Yedekler periyodik olarak test edilerek kullanıma hazır halde tutulur.

Zaman senkronizasyonu

MADDE 28 – (1) İşletmeci, bünyesinde kullanılan tüm bilgi sistemlerinin belirlenen tutarlı bir zaman kaynağına göre ayarlanmasını ve senkronize şekilde çalışmalarını sağlar.

Sistem kayıt dosyalarının tutulması

MADDE 29 – (1) İşletmeci, istenmeyen bilgi işleme faaliyetlerinin önlenmesi ve bilgi güvenliği ihlal olaylarının tanımlanması amacıyla kritik sistemleri izler ve asgari aşağıdaki hususların uygulanabilir olanlarını içeren kayıt dosyalarını en az 2 yıl süreyle tutar:

a) Kullanıcı kimlikleri.

b) Oturum açma/kapatma, veri ekleme/silme/değiştirme gibi işlemlerin tarihi, zamanı ve açıklamaları.

c) Bağlantı sağlanan ekipmanın kimliği ve yeri.

ç) Başarılı ve reddedilen sistem, veri ve diğer kaynaklara erişim girişimlerinin kayıtları.

d) Sistem ayarlarındaki değişiklikleri.

e) Kullanılan özel izinleri ve ayrıcalıkları.

f) Sistem araçlarının ve uygulamalarının kullanımı.

g) Erişilen dosyalar ve erişimin tipi.

ğ) Ağ adresleri.

h) Erişim kontrol sistemi tarafından üretilen alarmlar.

ı) Anti virüs yazılımı, güvenlik duvarı gibi güvenlik sistemlerinin aktif ve pasif hale getirilmeleri.

i) Sistem güvenlik ayarlarına ve kontrollerine ilişkin değişiklikler veya değişiklik girişimleri.

j) Sistem yöneticileri tarafından yapılan işlemler.

k) Kullanıcı veya sistem programları tarafından rapor edilen bilgi işlem ve haberleşme sistemlerine ilişkin hatalar.

(2) Sistem yöneticilerinin kendi işlemlerine ilişkin kayıt dosyalarını silmelerini veya değiştirmelerini engelleyecek önlemler alınır.

(3) Kayıt dosyaları değişikliğe ve yetkisiz erişime karşı korunur.

Kritik sistemlerde kullanıcı erişim yönetimi

MADDE 30 – (1) İşletmeci, kritik sistemlerde kullanıcıların, kendileri ile ilişkilendirilebilecek ve yaptıklarıişlemlerden sorumlu olmalarını sağlayacak nitelikte ayırt edilebilir ve eşsiz kullanıcı adı kullanmalarını sağlar.

(2) Kullanıcılara verilen erişim yetkisinin kapsamı, ilgili işin amaçlarından daha geniş olamaz.

(3) Bir hizmeti kullanmaya veya bir sisteme erişmeye yetkili tüm kullanıcı adlarının kaydı tutulur.

(4) Erişim yetkileriyle ilgili imtiyazlar, yalnızca gerekli durumlarda verilir. Erişim yetkileriyle ilgili imtiyazların kullanılması durumunda;

a) İşletim sistemi, veritabanı yönetim sistemi ve uygulamalar gibi her bir sistem elemanı için erişim imtiyazlarının verilmesi gerekli olan kullanıcılar tanımlanır,

b) Erişim imtiyazları devreye alınmadan önce onaylanır ve tanınan imtiyazların kaydı tutulur,

c) Erişim imtiyazları, ilgili kişiye, mümkün olduğu ölçüde kısa süre için ve normalde

kullandıkları kullanıcıadından farklı bir kullanıcı adıyla tanımlanır.

Parola yönetimi

MADDE 31 – (1) İşletmeci, kritik sistemlerde kullanılan kullanıcı parolaları ile ilgili olarak aşağıdaki hususlarıuygular:

a) Parola atanması, mevcut parolanın değiştirilmesi veya geçici parola alınması gibi durumlarda kimlik doğrulaması yapılması,

b) Kullanıcıların belirledikleri parolaları belirli aralıklarla değiştirmeleri, fiziksel ve elektronik ortamda korunmasız olarak bulundurmamaları ve eski parolaları belirli süre yeniden kullanmamaları,

c) Sistem ve yazılımların tedarikçileri tarafından atanmış olan varsayılan parolalarının, kurulumun ardından derhal değiştirilmesi.

(2) Bu maddede belirtilen güvenlik gereksinimlerini karşılaması şartıyla
kullanıcı parolaları yerine biyometrikdoğrulama, akıllı kart gibi sistemler de kullanılabilir.

Gizlilik sözleşmeleri

MADDE 32 – (1) İşletmeci, çalışanlarıyla ve mal veya hizmet alış verişinde bulunduğu üçüncü taraflarla yapacağı sözleşmelerde gizlilik hükümlerine yer verir ve imzalanan sözleşmeleri muhafaza eder.

(2) Gizlilik hükümleri veya sözleşmeleri asgari olarak aşağıdaki hususları içerir:

a) Gizli veya korunması amaçlanan bilginin tanımı.

b) Sözleşmenin geçerlilik süresi.

c) Sözleşme şartlarının ihlali halinde tesis edilecek işlemler.

ç) İmzalayan tarafların sorumlulukları.

d) Gizli bilginin kullanılabileceği durumlar ve sözleşmeyi imzalayanların gizli bilginin kullanılmasına ilişkin hakları.

(3) İşletmecinin, çalışanlarıyla ve mal veya hizmet alış verişinde bulunduğu üçüncü taraflarla yaptığısözleşmeler bu Yönetmelik kapsamındaki yükümlülüklerine ilişkin sorumluluğunu ortadan kaldırmaz.

Sistem ve yazılım temini veya geliştirilmesi

MADDE 33 – (1) İşletmeci, temin edeceği veya geliştireceği bilgi sistemleri ve yazılımlar için uygun güvenlik gereksinimleri belirler ve uygular.

Bakım ve onarım

MADDE 34 – (1) İşletmeci, gerçekleşen arıza ve hatalar ile yapılan düzeltici ve önleyici bakım ve onarım faaliyetlerini kayıt altına alır.

(2) Bakım ve onarım faaliyetlerinin üçüncü taraflarca yapıldığı durumlarda kritik sistemlerin bulunduğu alanlara erişim izni verilen üçüncü taraf çalışanlarının giriş - çıkış tarihi ve saati ile söz konusu çalışanlar tarafından yapılan işlemler izlenir ve kayıt altına alınır.

(3) Kuruluş dışında bakım onarım faaliyetlerinin yapılması durumunda sistem ve ekipmanlarda yer alan kritik bilgilerin korunmasına yönelik önlemler alınır.

DÖRDÜNCÜ BÖLÜM

Şebeke ve Bilgi Güvenliğinin Sağlanmasına İlişkin İlave Yükümlülükler

Siber saldırılara yönelik tedbirler

MADDE 35 – (1) İşletmeciler, bünyelerinde SOME kurar ve ulusal siber güvenliğin sağlanmasına ilişkinUSOM'un ve Kurum bünyesinde kurulan sektörel SOME'nin koordinesinde ve belirlediği esaslar çerçevesinde gerekli tedbirleri alır.

(2) İşletmeci, sunucular, yönlendiriciler ve diğer şebeke elemanlarının Dos/Ddos saldırıları, zararlı yazılım yayılması gibi siber saldırılara karşı korunması amacıyla, elektronik haberleşme hizmetinin tipi de dikkate alınarak, IP adreslerinde, haberleşme portlarında ve uygulama protokollerinde; sinyal işleme kontrolü, kullanıcı doğrulama ve erişim kontrolleri gibi mekanizmalar kurar ve talep edilmesi halinde siber saldırılara karşı koruma hizmeti sunar.

(3) İşletmeciler Dos/Ddos saldırıları, zararlı yazılım yayılması ve benzeri siber saldırılara karşı, USOM'unkoordinesinde gerekli tüm tedbirleri almakla yükümlüdür.

(4) İşletmeci, USOM tarafından bildirilen siber saldırı kaynağının;

a) Kendi abonesi olması durumunda ilgili abonenin bilgilendirilmesi ve abone tarafından talep edilmesi halinde sunulan elektronik haberleşme hizmetinin askıya alınmasını sağlar. İşletmeci tarafından aboneye yapılan bildirim ve bildirim türü USOM'a bildirilir.

b) Başka bir işletmecinin abonesi olması durumunda, gerekli önlemlerin alınması için ilgili işletmecinin veUSOM'un bilgilendirilmesini sağlar.

Belgelendirme yükümlülüğü

MADDE 36 – (1) İşletmeci, yetkilendirmesine ilişkin tüm hizmetleri ve kritik sistemleri kapsayacak şekilde kurduğu BGYS için belgelendirme kuruluşlarından uygunluk belgesi alır ve Kuruma gönderir.

(2) İlk defa belgelendirme yükümlülüğüne tabi olan işletmeci yükümlülük durumunun değiştiği yılın sonundan itibaren bir yıl içinde uygunluk belgesi alır ve Kuruma gönderir.

(3) Birinci ve ikinci fıkralar gereğince uygunluk belgesi almış işletmeci, uygunluk belgesinin yenilenmesi, kapsamında değişiklikler yapılması gibi durumlarda, değişiklikten itibaren en geç iki ay içerisinde Kuruma bilgi vermekle yükümlüdür.

Rapor hazırlama yükümlülüğü

MADDE 37 – (1) Şebeke ve bilgi güvenliğine ilişkin rapor işletmeci tarafından her yıl Mart ayı sonuna kadar hazırlanır ve istenildiğinde Kuruma gönderilmek ve/veya Kurum tarafından yapılan denetimlerde ibraz edilmek üzere 5 yıl süreyle muhafaza edilir. Söz konusu rapor asgari olarak aşağıdaki hususları içerir:

a) 10 uncu madde kapsamında yapılan risk değerlendirme ve işleme metotlar ve bu metotlara göre yapılan işlemlerin ayrıntıları.

b) 11 inci madde kapsamında yapılan iş sürekliliği planları.

c) 12 nci madde kapsamında gerçekleşen bilgi güvenliği ihlal olaylarına ilişkin bilgiler.

ç) En son yapılan iç denetimler ile belgelendirme kuruluşu tarafından yapılan son denetimin sonuçları, rapor edilen bilgi güvenliği ihlalleri ve söz konusu ihlallere ilişkin yapılan faaliyetler.

d) Şebeke ve bilgi güvenliğinin sağlanmasına yönelik yapılan yatırımlar ve yatırım tutarları.

e) Şebeke ve bilgi güvenliğinin sağlanmasına yönelik istihdam edilen personel sayısı ve niteliği.

İhlallerin bildirilmesi yükümlülüğü

MADDE 38 – (1) İşletmeci abonelerinin %5'inden fazlasını etkileyen şebeke ve bilgi güvenliği ihlallerini ve işsürekliliğini kesintiye uğratan olayları, en kısa sürede Kuruma bildirir. Söz konusu bildirim asgari olarak; olayın gerçekleşme zamanını, niteliğini, etkisini, süresini ve alınan önlemleri içerir.

Felaket kurtarma merkezi

MADDE 39 – (1) İşletmeci bir felaket, arıza veya hata durumunda sunulan elektronik haberleşme hizmetinin sürekliliğinin veya zamanında kurtarılmasının sağlanması için, ilgili bilgi sistemlerinin ve merkezi şebeke yönetim sistemlerinin bulunduğu yerde meydana gelebilecek bir felaketten etkilenmeyecek uzaklıkta felaket kurtarma merkezi kurar veya kurulu felaket kurtarma merkezlerinden hizmet satın alır.

(2) Felaket kurtarma merkezi kurma yükümlülüğüne tabi olan işletmeci, yükümlülük durumunun değiştiği yılın sonundan itibaren iki yıl içerisinde felaket kurtarma merkezi kurar.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Denetim

MADDE 40 – (1) Kurum, işletmecilerin bu Yönetmelikte belirtilen yükümlülüklerini yerine getirip getirmediğini re'sen veya şikâyet üzerine denetler veya denetlettirir.

Yürürlükten kaldırılan yönetmelik

MADDE 41 – (1) 20/7/2008 tarihli ve 26942 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Güvenliği Yönetmeliği yürürlükten kaldırılmıştır.

(2) 20/7/2008 tarihli ve 26942 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Güvenliği Yönetmeliğine yapılan atıflar bu Yönetmeliğe yapılmış sayılır.

Yürürlük

MADDE 42 – (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 43 – (1) Bu Yönetmelik hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.