T.C.
İÇİŞLERİ BAKANLIĞI
BİLGİ GÜVENLİĞİ POLİTİKALARI
YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

MADDE 1 - (1) Bu yönergenin amacı; İçişleri Bakanlığı'nın görevlerine ve bilgi teknolojilerinin gereklerine uygun olarak bilgilerin ve bilgi varlıklarının muhafaza edilmesi ve paylaşımında gerekli güvenlik tedbirlerinin alınması, kurum içinden veya dışından oluşabilecek muhtemel tehdit ve saldırılardan korunmasını, Bakanlık hizmetlerinin güvenli, doğru ve hızlı olarak gerçekleşmesini sağlamaktır.

Kapsam

MADDE 2 - (1) Bu yönerge, İçişleri Bakanlığı merkez ve taşra teşkilatında Bakanlık bilgi sistemlerini kullanan personelin, kurumsal ve kişisel bilgi güvenliği ilke, standart ve kuralları ile sorumluluk ve cezai esaslarını kapsamaktadır.

Dayanak

MADDE 3 - (1) Bu Yönerge, 10/07/2018 tarih ve 30474 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin (Kararname Numarası: 1) 508'inci ve 267'nci maddesine, 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununa, 4/5/2007 tarih ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununa, 5/12/1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanununa, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununa, 22/5/2003 tarihli ve 4857 sayılı İş Kanununa, 06/07/2019 tarih ve 30823 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelge 2019/12'ye, dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu yönergede geçen;

a) Ağ güvenlik duvarı: Bakanlık ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazları,

b) Akıllı kart: Bünyesinde elektronik yonga bulunduran; bir okuyucu ile eşleştiği zaman farklı uygulamalar için gerekli işlem gücüne sahip olabilen plastik kartları,

c) Bakan: İçişleri Bakanını,

ç) Bakanlık: İçişleri Bakanlığını,

d) Bakanlık Bilgi Sistemleri: Bakanlığın bilişim faaliyetlerini gerçekleştirmek için Bilgi İşlem Dairesi Başkanlığı'nca yönetilen donanım, yazılım, ağ ve internet unsurları ile bunları kullanan personelden oluşan, bilgiyi toplama, muhafaza etme ve analiz ederek sonuca ulaşma gayelerini güden birbiri ile ilişkili ve uyumlu unsurlar bütünü,

e) Bilgi İşlem Birim Amiri: Müstakil Bilgi İşlem Birimi'ne sahip olan kurumun bilgi sisteminden sorumlu amirini,

f) Bilgi Varlığı: Kurum için değeri olan bilgi ve bu bilgilerin bulunduğu ortamları,

g) Etki alanı: Merkezi bir sunucuda bulunan kullanıcı, makine, bilgisayar ve diğer bilgileri ayrı ayrı veya tümleşik olarak etkileyecek biçimde kurgulayabilen sistemleri,

ğ) İstemci: Sunucuların verdiği hizmeti alan bilgisayar sistemini,

h) Kimlik Doğrulama: Herhangi bir sisteme erişmeye çalışan kullanıcının iddia ettiği kullanıcı olup olmadığını kanıtlama sürecini,

ı) Kritik süreçler: Herhangi bir felaket durumunda mutlak suretle devam etmesi gereken, vatandaş odaklılık, itibari değer, kesinti maliyeti vb. etkilere göre öncelikli ve diğerlerinden daha önemli görülen bilgi işlem süreçlerini,

i) Kullanıcı: Bakanlık bilgi sistemlerini kullanan tüm kişileri,

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

k) Siber saldırı: Siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemleri,

l) Sunucu: İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini,

m) Yerel Yönetici: Tanımlandığı bilgisayar üzerinde program ekleme, kaldırma vb. işlemler ile etki alanında basılan kuralları değiştirebilen yönetici hesabını,

n) Varlık: Kuruluş için değeri olan herhangi bir şeyi

ifade eder.

İKİNCİ BÖLÜM

Bilgi Güvenliği Politikaları

İlke ve Kurallar

MADDE 5- (1) Genel hususlar:

a) Tüm Bakanlık bilgisayarları sistem merkezlerinden yönetilecek şekilde etki alanına dâhil edilir ve en güncel işletim sistemine yükseltilir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılır ve bu bilgisayarlara kablolu internet erişimi verilmez.

b) Kullanıcılara yerel yönetici hakkı verilmez. Birimlerde sorumlu bilgi işlem personeli veya yetkilendirilmiş personel ile ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ayarlar değiştirilemez ve program ekleme veya kaldırma yapılamaz.

c) Bakanlık bünyesinde oluşturulan tüm veriler Bakanlığın mülkiyetindedir. Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanamaz.

ç) Bakanlık bilgi varlıkları güvenliğinden Bakanlık personeli, hizmet alımı yöntemiyle çalıştırılan personel, Bakanlığa iş yapan yükleniciler ve çalışanlar sorumludur.

d) Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulamaz.

e) Kişisel olarak kullanılanlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar Bakanlık sistemlerine bağlanamaz. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak kriptolanmak suretiyle Bakanlık dışına çıkarılabilir; bu amaçla kullanılan cihazlar kayıt altına alınır.

f) Bakanlığa ait gizlilik dereceli veya kurumsal mahremiyet içeren verilere ihtiyacın ortadan kalkması durumunda, bu verilerin geri getirilemeyecek şekilde, mevzuata uygun olarak imhası gerçekleştirilir.

(2) Personel ile ilgili bilgi güvenliğine ilişkin hususlar:

a) Bakanlık bilgi sistemlerinde görev verilecek kişinin özgeçmişi araştırılır, beyan edilen akademik ve profesyonel bilgileri teyit edilir. Bakanlık personeli ve Bakanlığa hizmet verecek firma personeli için işe alım ve çalışma öncesinde güvenlik soruşturması yapılır.
b) Gizlilik derecesi yüksek olan bilgilere erişim hakkı olan çalışanlarla ve Kurumda görevli geçici personel, hizmet alımı ve yüklenici firma çalışanları ile gizlilik sözleşmesi imzalanır.
c) Bakanlık personeli sosyal medya üzerinden Bakanlıkla ilgili gizlilik dereceli veri paylaşımı ve haberleşme yapamaz.
ç) Personele bilgi güvenliği farkındalığına yönelik periyodik olarak eğitimler verilir. İşe yeni başlayan personel için bu eğitim, uyum süreci sırasında verilir.
d) Kullanıcı bilgi güvenliği ile ilgili ihlalleri veya şüphelendiği durumları, Bilgi Güvenliği Şube Müdürlüğü'ne veya yetkili amire bildirir.
e) Personel kimliği ve personelin yetkilerini belirten kartlar ve ziyaretçi kartları görülebilir şekilde (boyunda, yakasında) taşınır.

(3) Kimlik doğrulama ve yetkilendirme ile ilgili hususlar:

a) Kullanıcının yetkisi dâhilinde bilgi sistemleri üzerinde yapmış olduğu hareketleri (okuma, yazma, değiştirme, silme, giriş-çıkış vb.) izleyebilmek üzere her kullanıcıya kendisine ait benzersiz bir kullanıcı hesabı açılır.
b) İşe başlayan, ataması yapılan veya terfi alan kullanıcıların erişim hakları yeni görevine göre güncellenir ve Bakanlıktan ayrılan kullanıcıların erişim hakları derhal kaldırılır. Erişim yetkilerinin, kullanıcı hesaplarının, e-imza, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanır, varsa devam eden sorumluluklar kayıt altına alınır.
c) Bakanlık bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulamalar ve sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenir, dokümante edilir, periyodik olarak gözden geçirilir, sürekli iyileştirme ve denetim altında tutulur. Kritik süreçler, Bakanlık Bilgi İşlem Dairesi Başkanlığınca belirlenir, onaylanır ve yılda en az 2 defa gözden geçirilerek güncelliği sağlanır. Kritik süreçler tek kişi tarafından icra edilmez, yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olarak verilir.
ç) Uzaktan erişim yetkisi ilgili bilgi işlem birimi amirinin yazılı onay verdiği bilgi işlem personeline, sistemlerde yaşanabilecek acil durumlarda anında müdahale için veya diğer birimlere, onayda belirtilen görevin ifası amacıyla verilir.

(4) Fiziksel güvenlik ile ilgili hususlar:

a) Kritik bilgi varlıklarının bulunduğu binalarda ve çalışma alanlarında gerekli güvenlik tedbirleri alınır ve erişim izinleri bu doğrultuda verilir.
b) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilir. Bilgi işlem birimlerine yetkisiz erişimler engellenir. Fotokopi makinası, yazıcı vb. cihazların mesai saatleri dışında kullanımı kısıtlanır, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınır.

c) Kurumsal bilgilerin çıktı alınmasını denetim altına almak amacı ile fotokopi makinesi, yazıcı vb. cihazların mesai saatleri dışında kullanımı kısıtlanır veya ilgili Birim Amiri'nin yazılı onayıyla kapatılır, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınır.
ç) Sistem odalarına girişler çok faktörlü kimlik doğrulama yöntemi ile yapılır ve izlenir. Sistem odalarının izlenmesi ve kayıt altına alınması için kamera kayıt sistemi kullanılır.

(5) Parola güvenliği ile ilgili hususlar:

a) Sistemlerin üretici firmalarının tanımladığı parolalar, varsayılan veya geçici parolalar, sistemlerin ve yazılımların kurulumunu takiben derhal değiştirilir. Kullanıcılara sistem tarafından verilen parolalar ilgili sistem veya uygulamaya ilk bağlantıda değiştirilecek şekilde yapılandırılır.
b) Bütün parolalar Bakanlığa ait gizli bilgiler olarak kabul edilir. Parolalar e-posta iletilerine, herhangi bir elektronik forma ya da kâğıtlara yazılamaz. Yeni parola ve parola sıfırlama işlemlerindeki gönderilen kısa mesajlarda (SMS) geçici parolalar yer alabilir. Kullanıcı, parolalarını hiç kimseyle paylaşamaz.

(6) Ağ güvenliği ve internet erişimi ile ilgili hususlar:

a) Bakanlığın bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvarları ve vekil sunucu (proxy) üzerinden internete çıkar. İş ile ilgili olmayan, zararlı yazılım barındıran ve sosyal medya uygulamaları ile iletişim uygulamalarına (wetransfer, whatsapp web ve google drive vb.) erişimler yasaklanır. Yaptığı işin niteliğine göre bazı kullanıcılara internete çıkışta belirlenen sürelerde ayrıcalık verilebilir. İş ile ilgili olmayan ve kaynağı bilinmeyen dosyalar gönderilemez ve indirilemez.
b) İnternet erişim kayıtları 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna göre kayıt altına alınır.

(7) E-posta güvenliği ile ilgili hususlar:

a) Kullanıcı Bakanlık tarafından tahsis edilen kurumsal e-postasını sadece görevi için kullanır, şahsi işlerinde Bakanlık kurumsal e-postasını kullanamaz. Kullanıcı adı ve parolasını başka uygulamalar için kullanamaz. Kurumsal e-posta haricindeki diğer e-posta hesaplarına erişimler engellenir.
b) Kullanıcı, kendisine ait e-posta parolasının güvenliğinden, e-posta içeriğinden ve gönderdiği e-postalardan doğacak hukuki sonuçlardan sorumludur.
c) Kaynağından şüphe duyulan e-posta, e-posta ekinde gelen dosyalar ve içeriğindeki linkler kesinlikle açılmaz. Bu e-postalar herhangi bir işlem yapılmaksızın Bilgi Güvenliği Şube Müdürlüğü'ne iletilir.
ç) Kurumsal e-postalar idari soruşturma, adli soruşturma ve kovuşturma durumlarında yetkili makamlarca önceden haber verilmeksizin denetlenebilir.
d) Belirli periyotlarla kullanılmamış e-posta hesapları kullanıcıya haber verilmeden sunucu güvenliği amacıyla pasif duruma getirilir.
e) E-postaya eklenecek dosya uzantıları, çalıştırılabilir dosyalar (".exe", ".vbs" vb.) veya güvenlik açığı oluşturabilecek diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak zip veya rar formatında mesaja eklenir. Gelen e-postaların içeriğindeki veriler (ekler, linkler vb.) güvenlik taramasından geçirilir.

(8) Antivirüs ile ilgili hususlar:

a) Bakanlığın tüm istemcileri ve sunucuları kurumsal antivirüs yazılımına sahip olur ve yazılımın sürekli güncel olması sağlanır. Kullanıcı hiç bir sebepten antivirüs yazılımını bilgisayarından kaldıramaz ve ayarlarını değiştiremez.
b) İstemcilere veya sunuculara virüs bulaştığı fark edildiğinde ilgili cihazlar ağdan çıkarılır. Virüs tespit edilen ve temizlenemeyen her durum, bir güvenlik olayı olarak ele alınır, bu durum Bilgi Güvenliği Şube Müdürlüğü'ne bildirilir ve gerekli güvenlik önlemleri alınarak çözülür.

(9) Yazılım ve uygulama güvenliği ile ilgili hususlar:

a) Bakanlık bilgi işlem birimleri tarafından dağıtılan lisanslı programlar ile personelin görevi gereği kullanması gereken lisanslı uygulamalara Bilgi İşlem Dairesi Başkanlığı'nca izin verilir. Yazılım geliştirme ve temin politikalarına uygun olmayan, ulusal ve uluslararası yazılım geliştirme standartları çerçevesinde geliştirilmemiş ve Bakanlık talebi olmaksızın üretilmiş olan yazılımların kurumsal sistemler üzerine entegre edilmesine izin verilmez.
b) Bilgi sistemlerinde değişiklik yapmaya yetkili personel, yetki seviyeleri, değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenir. Sistem aksamasına sebebiyet verebilecek önemli değişiklikler gerçekleştirilmeden önce ilgili bilgi işlem birim amirine ve etkilenebilecek taraflara bilgi verilir. Değişiklikler yapıldıktan sonra etkilenen taraflar bilgilendirilir.
c) Kullanılan işletim sistemlerinin, yazılımların, cihaz ara yüzlerinin vb. uygulamaların en güncel, güvenilir ve sistemle uyumlu versiyonu kullanılır. Lisanslı programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilir.
ç) Bakanlık için temin edilecek yazılımların kullanım amacına uygun olmayan bir özellik veya arka kapı açıklığı (kullanıcıların bilgisi/ izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine dair üretici ve/veya tedarikçilerden taahhütname alındıktan sonra kullanılır.

(10) Kriz, acil durumlar ve iş sürekliliği ile ilgili hususlar:

a) Acil durum ve felaket senaryoları (deprem, yangın, sel, elektrik kesilmesi, siber saldırı vb.) oluşturulur. Acil durum ve felaket anlarında nelerin yapılması gerektiği, hangi otoritelerle iletişim kurulacağı (iletişim bilgileri) belirlenerek yazılı hale getirilir. Kriz veya acil durum sorumluları atanır, yetki ve sorumlulukları belirlenerek dokümante edilir. Bu dokümanın sürekli güncel ve aktif durumda olması sağlanır.
b) Kriz veya acil durumlarda Bakanlık içi işbirliği gereksinimleri tanımlanır. Kriz veya acil durumlar için görevlendirilen personel bu durumlarda yapacağı çalışmaları öğrenmesi ve zamanı geldiğinde uygulayabilmesi için eğitim alır ve yılda en az bir defa tatbikat yaparak oluşan sonuçlara göre dokümanları günceller.
c) Bilgi sistemlerinde kesinti sürelerini ve veri kayıplarını en az düzeye indirmek için, kurumsal veriler düzenli olarak yedeklenir. Doğru ve eksiksiz şekilde alınan yedekler olası bir felaket anında etkilenmeyecek bir ortamda bulundurulur.

(11) Teknik destek ve bakım ile ilgili hususlar:

a) Bakanlık sistemlerinin tamamının (donanımlar, cihazlar, uygulama yazılımları, paket yazılımlar, işletim sistemleri vb.) periyodik bakımları yapılır. Bunun için eğer hizmet satın alınmışsa, hizmet alınan firmalar ile bakım öncesi gerekli anlaşmalar (iş ve gizlilik) yapılır.

Firma teknik destek elemanlarına bakım yaparken ilgili Bakanlık personeli eşlik eder ve firma elemanlarının bu yönergeye ve ilgili diğer mevzuata uygun davranmaları sağlanır.

b) Sistem bakımlarının ve Bakanlık personelinin yapmış olduğu her türlü değişikliklerin ilgili politika ve standartlar kapsamında belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için yılda en az bir defa sızma testi, uygunluk ve güvenlik testleri yapılır.

c) Bakım ve teknik destek hizmetleri öncelikli olarak yurtiçi firmalardan sağlanır. Yerinde teknik desteğin yeterli olmaması ve sorunun çözülememesi durumunda yapılan işlemler kayıt altına alınır ve kullanılan ürünün üretici firmasından uzaktan destek almak için birim amirinden yazılı onay alınarak çalışmalara başlanır. Bu çalışmalar esnasında gerekli güvenlik tedbirleri alınarak her aşamada firma personelinin yapmış olduğu işlemler izlenir.

ÜÇÜNCÜ BÖLÜM

Çeşitli Hükümler

Cezai Hükümler

MADDE 6 – (1) Bu yönergede belirtilen yetki ve sorumluklarını yerine getirmeyen ve Bakanlık bilgi sistemlerinde güvenlik zafiyetine sebep olan personel hakkında 5237 sayılı Türk Ceza Kanunu, 657 sayılı Devlet Memurları Kanunu, 4857 sayılı İş Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 5846 sayılı Fikir ve Sanat Eserleri Kanunu, 6698 sayılı Kişisel Verilerin Korunması Kanununa ve ilgili diğer mevzuatın ilgili hükümlerine göre işlem yapılır.

Değiştirilen ve Yürürlükten Kaldırılan Hükümler

MADDE 7 – (1) 20/2/2012 ve 9/9/2013 tarihli Bakanlık Onayı ile yürürlüğe giren İçişleri Bakanlığı Bilgi Güvenliği Politikaları Yönergesi yürürlükten kaldırılmıştır.

Yürürlük

MADDE 8 – (1) Bu yönerge Bakan onayı ile yürürlüğe girer.

Yürütme

MADDE 9 – (1) Bu yönerge hükümlerini Bakan yürütür.

OLUR

…/…/2020

Süleyman SOYLU

Bakan