İÇİŞLERİ BAKANLIĞI
BİLGİ GÜVENLİĞİ POLİTİKALARI
YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

MADDE 1 - (1) Bu yönergenin amacı; İçişleri Bakanlığı'nın görevi ve konumu nedeniyle bilgi çağı gereklerine paralel olarak bilgi paylaşımı ve güvenliği konularında tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmektir.

Kapsam

MADDE 2 - (1) Bu yönerge, İçişleri Bakanlığına bağlı merkez ve taşra teşkilatında bulunan bütün birimlerdeki personelin, bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Hukuki dayanak

MADDE 3 - (1) Bu Yönerge, 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanunun 33 üncü maddesine, 23.05.2007 tarih ve 26530 sayılı Resmi Gazetede yayınlanan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 6. maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu yönergede geçen;

a) Bakanlık : İçişleri Bakanlığını,

b) Bakan : İçişleri Bakanını,

c) Başkanlık : Bakanlık Bilgi İşlem Dairesi Başkanlığını,

ç) Başkan : Bilgi İşlem Dairesi Başkanını,

d) Bilişim Ağları Şube Müdürlüğü : Başkanlık Bilişim Ağları Şube Müdürlüğünü,

e) Sistem Yönetimi Şube Müdürlüğü: Başkanlık Sistem Yönetimi Şube Müdürlüğünü,

f) Bilgi Güvenliği Şube Müdürlüğü : Başkanlık Bilgi Güvenliği Şube Müdürlüğünü,

g) Bilgi İşlem Şube Müdürlüğü : Valilik Bilgi İşlem Şube Müdürlüklerini,

h) Ağ Yöneticisi : Ağ Sistemlerinden Sorumlu Uzman Yöneticiyi,

ı) Sistem Yöneticisi : Bilgi Sistemleri Yöneticisini,

i) Bilgi Güvenliği Yöneticisi : Başkanlık Bilgi Güvenliği Şube Müdürünü,

j) Veritabanı Yöneticisi : Veritabanı Sistemlerinden Sorumlu Yöneticiyi,

k)Güvenlik Politikaları Yöneticisi: Başkanlıkça Görevlendirilen Bilgi Güvenliği Politikaları Yöneticisini,

l) Kullanıcı : Bakanlık Bilgi Sistemlerini Kullanan tüm personeli,

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

n) İstemci : Sunucuların verdiği hizmeti alan bilgisayar sistemini,

ifade eder.

Yönergede kullanılan diğer teknik terim ve tanımlar, (Ek-1) tabloda gösterilmiştir.

İKİNCİ BÖLÜM

Bilgi Güvenliği Politikaları

Genel hükümler

MADDE 5 -(1) Bakanlık bilgi sistemleri hakkında genel hükümler aşağıda belirtilmiştir.

a) Tüm kullanıcı bilgisayarları sistem merkezlerinden yönetilecek şekilde yapılandırılacaktır.

b) Bilgi sistemleri, kullanıcıların kendi bilgisayarlarında standart kullanıcı yetkisi ile çalışmasını sağlayacak şekilde yapılandırılacaktır.

c) Tanımlanan istisnalar dışında tüm bilgisayarlar etki alanı içinde yer alacaktır. İstisnalar şunlardır:

1) Dizüstü bilgisayarlar,
2) Tablet bilgisayarlar,
3) Cep telefonları,
4) DMZ sunucuları

Bilgi sistemleri genel kullanım politikası

MADDE 6 - (1) Bilgi sistemlerine sahip olma ve bu sistemlerin genel kullanım kuralları aşağıda belirtilmiştir.

a) Bakanlık güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Bakanlık bünyesinde oluşturulan tüm veriler Bakanlığın mülkiyetindedir.

b) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanamaz.

c) Bakanlık, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

ç) Tüm Bakanlık bilgisayarları etki alanına dahil edilir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılır, bu bilgisayarlarla yerel ağdaki cihazlar arasında bilgi alışverişi yapılmasına izin verilmez.

d) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılamaz ve kopyalanamaz.

e) Bakanlıkta Başkanlığın bilgisi ve onayı olmadan Bakanlık ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulamaz.

f) Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilemez.

g) Bilgisayarlara lisanssız programlar yüklenemez.

h) Sadece zorunlu hallerde bilgisayar kaynakları paylaşıma açılabilir.

ı) Taşınabilir bilgisayarların çalınması, kaybolması durumunda sorumluluk kullanıcılara aittir. Kullanıcı taşınabilir bilgisayarında şifre kullanmak ve kuruma ait evrakları da şifreli olarak saklamakla yükümlüdür.

(2) Bilgi sistemleri genel yapılandırması ile ilgili kurallar aşağıda belirtilmiştir.

a) Bütün cep telefonu ve PDA cihazları Bakanlık ağları ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızılötesi, bluetooth, vb) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.

b) Kullanıcılar kendilerine tahsis edilen bilgisayarları kullanırken gerekli özeni göstermekle yükümlüdür.

Personel güvenliği politikası

MADDE 7 - (1) Personel güvenliği politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilgiye erişim hakkı verilen, bilgi güvenliği ve sistem yönetimi kadroları için personel yetkinliği ve nitelikleri kararlaştırılır.

b) Bakanlık bilgi sistemlerinde görev verilecek kişinin özgeçmişi araştırılır, beyan edilen akademik ve profesyonel bilgiler teyit edilir, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans alınır.

c) Bakanlık bilgi sistemlerinde görev verilecek Bakanlık dışı personel için ayrıca güvenlik soruşturması yapılır.

ç) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanır.

d) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenir. Çalışanlar, kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilir.

e) Bakanlık bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılır, bu eğitimler için belirli bir bütçe ayrılır, eğitimlere katılım takip edilir ve sonuçlar değerlendirilir.

f) Çalışanların başka görevlere atanması ya da işten ayrılması durumunda işletilecek süreçler tanımlanır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanır, varsa devam eden sorumluluklar kayıt altına alınır.

Kimlik doğrulama ve yetkilendirme politikası

MADDE 8 - (1) Kimlik Doğrulama ve Yetkilendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait benzersiz bir kullanıcı ismi ile erişeceği bir kullanıcı hesabı açılır.

b) Kullanıcı hesaplarının açılmasında veya kapatılmasında referans kaynak olarak Personel Genel Müdürlüğünün bildirimleri esas alınır. İşe başlayan, ataması yapılan, terfi alan ve ayrılan kullanıcılar ile ilgili bilgiler, Başkanlığa resmi yazı ile bildirilir.

c) Kullanıcılara erişim hakları yazılı olarak tebliğ edilir. Kullanıcılardan erişim haklarını anladıklarını ve bu hakları ihlal etmeleri halinde disiplin sürecine veya yasal işleme tabi olacaklarını anladıklarına ilişkin imzalı belge alınır.

ç) Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olarak verilir. Görevler ayrımı ile kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılır. "En az ayrıcalık" ile kullanıcıların sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları sağlanır.

d) İş tanımı değişen kullanıcıların erişim hakları yeni görevine göre güncellenir ve Bakanlıktan ayrılan kullanıcıların erişim hakları kaldırılır.

e) Bakanlık sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrulusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenir ve dokümante edilir.

f) Bakanlık sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanarak dokümante edilir.

g) Bakanlık bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama

yazılımları, paket programlar, veritabanları, işletim sistemleri ve oturum açarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenir, dokümante edilir ve denetim altında tutulur.

h) Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilir ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilir.

ı) Erişim ve yetki seviyeleri Bilgi Güvenliği Şube Müdürlüğü tarafından azami 6 ayda bir defa olmak üzere gözden geçirilir.

i) Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar ve rollerin sistem kaynakları üzerindeki yetkileri uygun araçlar kullanılarak belirli aralıklarla listelenir. Bu listeler yetki seviyeleri ile karşılaştırılır. Eğer uyumsuzluk varsa dokümanlar ve yetkiler düzeltilerek uyumlu hale getirilir.

j) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulur, tekrarlanan başarısız erişim istekleri/girişimleri incelenir.

Fiziksel güvenlik politikası

MADDE 9 - (1) Fiziksel güvenlik ile ilgili kurallar aşağıda belirtilmiştir.

a) Bakanlık binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilir.

b) Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanır ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilir.

c) Kritik bilgilerin bulunduğu alanlara girişler kontrolü akıllı kartlar veya biyometrik sistemler ile yapılır ve izlenir.

ç) Kritik bilgi sistemlerinin bulunduğu bölümlerin izlenmesi ile kayıt altına alınması için kamera kayıt sistemi kullanılır. Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanır.

d) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanır.

e) Kritik sistemler özel sistem odalarında tutulur.

f) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunur, yangın ve benzeri felaketlere karşı koruma altına alınır, ısı, duman ve nem algılayıcılar bulundurulur

ve iklimlendirilmesi sağlanır.

g) Sistem odalarında yükseltilmiş taban kullanılır. Kabinet ve cihazlarda depreme karşı sabitleme yapılır.

h) Sistem odalarında meydana gelebilecek olağanüstü durumlarda sorumlu kişileri bilgilendirecek uyarı sistemleri (sms, e-posta, telefon ile aranması gibi) oluşturulur.

ı) Sistem odasına erişim hakkı verilen personele yangınla mücadele konusunda eğitimler verilmelidir.

i) Sistem odaları dikkat çekmeyecek şekilde konuşlandırılır. Sistem odalarını açık bir şekilde belirten tabela vb. yazılardan kaçınılır.

j) Sistem odalarında pencere bulunmaz. İkinci bir kapı varsa o kapıda da birinci kapıda bulunan güvenlik tedbirleri aynen uygulanır.

k) Sistem Odası yerleşim düzeni, kablolama altyapısı ve kablo kanalları dokümante edilir.

l) Sistem odası, yedekli çalışan kesintisiz güç kaynağı (UPS) ve jeneratör ile desteklenir.

m) Sistem odalarında her türlü yeme, içme yasaklanmıştır ve yangın riski oluşturan cihazlar kullanılamaz.

n) Sistem odasının ve donanımların sürekli temiz ve düzenli olmaları sağlanır.

o) Sistem odası giriş hakkı bulunmayan üçüncü kişiler (diğer Bakanlık personeli, danışman, tedarikçi firma sorumlusu, iç/dış denetçi vb.) yetkili personel nezaretinde sistem odasına girebilir. Sistem odasına yetkili personel nezaretinde giren tüm üçüncü kişiler için Bilgi İşlem Sistem Odası Ziyaretçi Defteri doldurulur ve imzalanır. Bu çalışmalar esnasında yetkili Bilgi İşlem personeli ziyaretçilerin yanında bulunur ve onlara eşlik eder.

ö) Fotokopi, yazıcı vb. türü cihazlar mesai saatleri dışında kullanıma kapatılır, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınır.

p) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilir.

Parola politikası

MADDE 10 - (1) Parola ile ilgili sistem yöneticisi tarafından uyulması gereken kurallar aşağıda belirtilmiştir.

a) Sistemlerin üretici firmalarının tanımladığı parolaları (default passwords), sistemlerin ve yazılımların kurulumunu takiben derhal değiştirilir.

b) Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) sistem yöneticisi tarafından en geç 3(üç) ayda bir değiştirilecek şekilde yapılandırılır.

c) DMZ bölgesinde çalışan sunucuların parolaları 3(üç) ayda bir değiştirilir.

ç) Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) sistem yöneticisi tarafından en geç 90 (doksan) günde bir değiştirilecek şekilde yapılandırılır.

d) Sistem yöneticileri sistem ve kullanıcı hesapları için farklı parolalar kullanır.

e) Sistem yöneticisi, kullanıcıları güçlü parola tanımlamaya zorlamak için aşağıdaki parola özelliklerini uygular. Parola,

- En az 8 haneli olmalıdır.
- İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)
- İçerisinde en az 2 tane rakam bulunmalıdır. (1, 2, 3...)
- İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,$,#,&,/,{,*,-,],=,...)
- Aynı karakterler peş peşe kullanılmamalıdır, (aaa, 111, XXX, ababab...)
- Sıralı karakterler kullanılmamalıdır, (abcd, qwert, asdf,1234,zxcvb...)
- Bu maddede belirtilen parola özellikleri gelişen teknolojiler ve güvenlik önlemleri dikkate alınarak Başkanlık tarafından değiştirilebilir.

f) Bakanlık çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılamayacak güçlü bir parolaya sahip olarak yapılandırılır.

g) Sistem, kullanıcı parolasını 15 (on beş) dakika içinde 20 (yirmi) kez yanlış girdiğinde hesabı 15 (on beş) dakika kilitli kalacak şekilde yapılandırılır.

h) Bireylerin ve grupların kimlik doğrulaması işlemi sistem yöneticisi tarafından yapılandırılır.

ı) Parolalar, şifrelenmiş olarak saklanır, metin olarak veya kolay anlaşılabilir formda saklanamaz.

i) Parolalar, kimlik doğrulama amacıyla aktarılırken şifrelenir (kriptolanır) ve verilerin aktarımı sırasında gizliliğinin sağlanmasına yönelik önlemler alınır.

(2) Parola ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.

a) Kullanıcılara başlangıçta verilen geçici parolalar ilgili sistem veya uygulamaya ilk bağlantıda değiştirilir.

b) Kullanıcı parola tanımlarken kendisine ait anlam ifade eden kelimeler kullanmamalıdır. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

c) Parolalar e-posta iletilerine, herhangi bir elektronik forma ya da kağıtlara yazılamaz.

ç) Bütün parolalar Bakanlığa ait gizli bilgiler olarak düşünülür.

d) Kullanıcı, parolalarını hiç kimseyle paylaşamaz.

e) Kullanıcı zorunlu haller dışında, kullanıcı adı ve parolasını kullanarak, birim zamanda birden çok bilgisayarda oturum açamaz.

f) Kullanıcı, Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneğini kullanamaz.

g) Kullanıcı parola güvenliği ile ilgili bir sorundan şüphelendiğinde parolasını hemen değiştirerek Bilgi Güvenliği Şube Müdürlüğüne haber verir.

(3) Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.

İnternet erişim ve kullanım politikası

MADDE 11 - (1) İnternet erişim ve kullanım politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bakanlığın bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkar.

b) Bakanlığın politikaları doğrultusunda içerik filtreleme sistemleri kullanılır. İstenilmeyen siteler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanır.

c) Bakanlığın ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılır.

ç) Yaptığı işin niteliğine göre bazı kullanıcılara internete çıkışta özel haklar verilebilir.

d) Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.

e) İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilemez ve indirilemez. Bu konuda gerekli önlemler sistem yöneticisi tarafından alınır.

f) Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilir.

g) İnternet erişim kayıtları 5651 Sayılı Kanuna göre kayıt altına alınır.

h) Kullanıcı, internet erişimi sırasında sistemde dile getirdiği tüm fikir, düşünce, ifade ve yazıların kendisine ait olduğunu, Bakanlığın hiçbir şekilde sorumlu olmadığını kabul eder.

e-Posta politikası

MADDE 12 - (1) e-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiş olup bunlar e-posta sisteminden sorumlu sistem yöneticisi tarafından uygulanır.

a) Bilgi sistemleri, e-posta hizmetleri için kullanıcılardan parola isteyecek şekilde yapılandırılır.

b) e-Posta hizmeti için kullanılan yazılım sistemleri yetkisiz erişimlere karşı korunur.

c) 6 ay süreyle kullanılmamış e-posta hesapları kullanıcıya haber verilmeden sunucu güvenliği ve veri depolama alanının boşaltılması amacıyla pasif duruma getirilir.

ç) Sistem, kullanıcılar e-postalarına erişirken, POP3, SMTP, HTTP vb. kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanmayacak şekilde yapılandırılır.

d) Bakanlık, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.

e) Kullanıcılar tarafından gönderilen e-postalarda içeriği Başkanlık tarafından belirlenen bir açıklama metni yer alır.

f) Mesaj filtreleme önlemlerinin alınması sistem yöneticisi tarafından yapılır.

(2) e-Posta ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.

a) Kullanıcı, kendisine verilen parolayı en kısa zamanda değiştirir.

b) Kullanıcı, hesaplarına ait parolaları ikinci bir şahsa veremez.

c) Kullanıcı, e-postalarında açık bir şekilde şifre yayınlayamaz.

ç) Bakanlık ile ilgili olan gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamı içerisine, iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilir.

d) Kullanıcı, kurumsal e-postalarının, Bakanlık dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.

e) Kullanıcı, e-posta erişimi için kullanılan donanım/yazılım sistemlerine yetkisiz erişimlere karşı gerekli tedbirleri alır.

f) Kullanıcı, kullanıcı adı/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Bilgi Güvenliği Şube Müdürlüğüne haber vermelidir.

g) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Bilgi Güvenliği Şube Müdürlüğüne haber verilmelidir.

h) Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren şifresini derhal değiştirmeli ve Bilgi Güvenliği Şube Müdürlüğüne haber vermelidir.

ı) Kullanıcı, Bakanlığın e-posta sisteminden ya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları gönderemez. Bu tür özelliklere sahip bir mesaj alındığında ise Bilgi Güvenliği Şube Müdürlüğüne haber verilir.

i) Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.

j) Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) gönderemez.

k) Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçlar ile e-posta gönderilemez.

l) Spam, zincir e-posta, sahte e-posta ve her türlü çalıştırılabilir dosya içeren zararlı e-postalar alındığında başkalarına iletilmeyip, Bilgi Güvenliği Şube Müdürlüğüne bildirilir ve spambildir@icisleri.gov.tr adresine incelenmek üzere gönderilir.

m) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılamaz.

n) Kullanıcı, e-posta ile gönderdiği büyük boyutlu dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olmalı ve mümkünse dosyaları sıkıştırmalıdır.

(3) Kurumsal e-postalar yetkili kişilerce hukuksal açıdan gerekli görülen yerlerde önceden haber vermeksizin denetlenebilir.

Antivirüs politikası

MADDE 13 - (1) Antivirüs politikası ile ilgili sistem yöneticisi tarafından uyulması gereken kurallar aşağıda belirtilmiştir.

a) Bakanlığın tüm istemcileri ve sunucuları antivirüs yazılımına sahip olur. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak antivirüs yazılımı yüklenmeyebilir.

b) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkarılır.

c) Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli çalışmaların yapılmasından sorumludur.

ç) Tüm sunucu ve kullanıcı bilgisayarları düzenli olarak virüs taramasından geçirilir ve bu sebeple sunucu ve kullanıcı bilgisayarlarında gerekli ayarlamalar yapılır. Tarama sonuçları ilgili sistem yöneticisi tarafından takip edilir.

d) Antivirüs güncellemeleri antivirüs sunucusu ile yapılır. Sunucular internete sürekli bağlı olur, sunucuların veri tabanları otomatik olarak güncellenir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılır.

e) Etki alanına dâhil olmayan kullanıcı bilgisayarları istisnai bilgisayarlar olarak belirlenmiştir. Antivirüs güncellemeleri sorumluluğu bu bilgisayarların kullanıcılarına ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticisi bu kullanıcı bilgisayarlarını ağdan çıkartır.

f) İstemci yazılımı aktif tarama özelliği açık olacak şekilde tanımlanır ve bilgisayara yazılan tüm veriler ile tüm veri giriş medyalarının (CD, flash disk, taşınabilir disk vb.) taramadan geçmesi sağlanır.

g) Virüs tanımları yüklenemeyen bilgisayarları tespit etmek için, tüm bilgisayarlardaki antivirüs tanımlarının son güncellenme tarihi günlük olarak ilgili sistem yöneticisi tarafından yönetim konsolu aracılığıyla kontrol edilip Bilgi Güvenliği Yöneticisine raporlanır.

h) İstemci antivirüs yazılımı üzerindeki parametrelerin kullanıcılar tarafından yazılımın etkisini azaltacak şekilde değiştirilmesine izin verilmeyecek şekilde yapılandırılır.

ı) Virüs tespit edilen ve temizlenemeyen her durum, bir güvenlik olayı olarak ele alınır, bu durum Bilgi Güvenliği Şube Müdürlüğüne bildirilir ve Güvenlik Olayları Yönetimi Prosedürü çerçevesinde çözümlenir.

i) Sistem yöneticileri, virüslere yönelik düzenli bilgi toplamak amacıyla ilgili grup listelerine üye olur ve bu konularda bilgi veren web sitelerini düzenli olarak ziyaret eder.

j) Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüsleri barındıran e-postalar antivirüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenir.

(2) Antivirüs ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.

a) Kullanıcı hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldıramaz.

b) Bilinmeyen veya şüpheli kaynaklardan dosya indirmemelidir.

c) Kullanıcı şüphelendiği tüm durumlarda Bilgi İşlem Birimlerini veya Bilgi Güvenliği Şube Müdürlüğünü haberdar eder.

Donanım ve yazılım envanteri oluşturma politikası

MADDE 14 – (1) Donanım ve yazılım envanteri oluşturma ile ilgili kurallar aşağıda belirtilmiştir.

a) Başkanlığın hizmet verdiği kapsamda Varlık Envanteri Bilgi Güvenliği Şube Müdürlüğü koordinatörlüğünde oluşturulur.

b) Bakanlığın bütün masaüstü ve dizüstü bilgisayarları, ağ cihazları, sunucuları, bilgisayar ağına bağlanan bütün kablosuz erişim cihazları, ağ arabirim kartları ve diğer bütün bilgi sistemleri ekipmanları ile lisanslı yazılımlar ve Bakanlık bünyesinde oluşturulan bütün yazılım projeleri kayıt altına alınarak Varlık Envanterine eklenir.

c) Oluşturulan envanter tablosunda kullanıcı bilgisayarlarına ait şu bilgiler bulunur: sıra no, bilgisayar adı, bölüm, marka, model, seri no, özellikler, ek aksamlar, işletim sistemi, garanti süresi.

ç) Sunuculara ait bilgilerin yer aldığı tablo oluşturulur. Bu tabloda, sunucuların isimleri, ip adresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personel(ler)in isimleri ve telefon numaraları bilgileri yer alır.

d) Sunucuların bilgileri sistem yöneticileri sorumluluğunda şekli ve içeriği Başkanlık tarafından belirlenen tablolarda tutulur ve güncellenir.

e) Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer alır.

f) Veritabanı sistemleri envantere eklenir.

g) Bu tablolar merkezi bir web sunucuda tutulur ve belirli aralıklarla güncellenir. İlgili siteye girişler güvenlik politikaları çerçevesinde yapılır.

h) Envanter bilgileri sık sık kontrol edilir. Bu şekilde bilgi eksikliğinin yol açacağı kayıp ve maliyetlere engel olunmalıdır.

Ağ yönetim politikası

MADDE 15 – (1) Ağ yönetim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.

b) Ağ bağlantıları ağ yöneticisi tarafından düzenli olarak takip ve kontrol edilir.

c) Erişimine izin verilen ağlarda, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilir ve yetkisiz erişimle ilgili tedbirler alınır.

ç) Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlantısı sağlanır.

d) Sınırsız ağ dolaşımı engellenir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde yapılandırılır, ihtiyaçlara göre Bilişim Ağları Şube Müdürlüğünce serbest bırakılabilir.

e) Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınır.

f) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınır ve kayıtlar tutulur.

g) Ağ erişimi, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılır. Bakanlık kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılır ve ağlar arasında geçiş güvenlik duvarları üzerinden sağlanır.

h) Uzaktan erişim, müdahale, sorun çözme ve yapılandırma amacıyla kullanılacak portların güvenliği sağlanır.

ı) Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.

i) Bakanlık bilgisayar ağına yönelik dokümantasyon (ağ adresleri, yapılandırma, tasarım bilgileri, vb.) hiçbir şekilde üçüncü kişiler ile paylaşılmaz ve bu kişilerin erişebileceği

mantıksal ve fiziksel alanlarda saklanmaz.

j) Sistem tasarımı ve geliştirilmesi yapılırken Başkanlık tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.

k) İnternet trafiği, MADDE 11'de belirtilen İnternet Erişim ve Kullanım Politikasında anlatıldığı şekilde izlenebilmelidir.

l) Ağ cihazları görevler dışında başka bir amaç için kullanılamaz.

m) Ağ cihazlarının yapılandırılması Bilgi Güvenliği Yöneticisi tarafından veya Bilgi Güvenliği Yöneticisinin denetiminde yapılmalı ve değiştirilmelidir.

Ağ cihazları güvenlik politikası

MADDE 16 – (1) Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Etki alanına dahil edilen bilgisayarlara yerel yönetici hakkı (local) verilemez. Ağ cihazları kimlik tanımlama için LDAP, RADIUS, TACAS+ gibi protokollerden birini kullanmalıdır.

b) Ağ cihazlarına erişimler için IP kısıtları getirilir ve sadece ağ yöneticisi tarafından erişilir. Ağ cihazlarına erişimler güvenli kanallar (SSH, IPSec, vb.) üzerinden yapılır.

c) Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması Bakanlık içinde yapılır.

ç) Ağ cihazları üzerinde kullanılmayan tüm servisler kapatılır.

d) Bakanlığın standart olan SNMP community string'leri kullanılır. Bu bilgi sadece yetkilendirilmiş kişiler tarafından bilinir.

e) İhtiyaç duyulduğu zaman erişim listeleri eklenir.

f) Yönlendirici ve anahtarlar Bilişim Ağları Şube Müdürlüğü ve Bilgi İşlem Şube Müdürlükleri yönetiminde kullanılır.

g) Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin dışında üretim ortamına taşınmalıdır.

h) Ağ cihazları üzerindeki tüm yapılandırma değişikliği ve yönetici hareketlerinin log kayıtları tutulur.

ı) Ağ cihazlarında yer alan yapılandırma bilgileri Ağ Yöneticisinin erişebildiği bir dosya sunucusu üzerinde yedeklenir.

i) Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

j) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları) ve cihazların portları etiketlenir.

k) Her bir yönlendirici ve anahtar Başkanlıkça içeriği belirlenen bir uyarı yazısına sahip olur.

Kablosuz iletişim politikası

MADDE 17 - (1) Bakanlık bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.

(2) Bütün kablosuz erişim cihazları Bilişim Ağları Şube Müdürlüğü tarafından onaylanır ve belirlenen güvenlik ayarları kullanılır.

(3) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılır.

b) Erişim cihazlarındaki firmware'ler düzenli olarak güncellenir.

c) Cihaza erişim için güçlü bir parola kullanılır. Erişim parolaları varsayılan ayarda bırakılamaz.

ç) Varsayılan SSID isimleri kullanılamaz. SSID ayarı bilgisi içerisinde Bakanlıkla ilgili bilgi olmamalıdır, mesela Bakanlık ismi, ilgili bölüm, çalışanın ismi vb.

d) Radyo dalgalarının binanın dışına taşmamasına özen gösterilir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.

e) Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Bakanlık kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanır ve Bakanlık kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenir.

f) Erişim Cihazları üzerinden gelen kullanıcılar güvenlik duvarı üzerinden ağa dâhil olurlar.

g) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilir ve kullanıcılar tarafından Bakanlığın internet bant genişliğinin tüketilmesi

engellenir.

h) Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlandırılır.

ı) Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmalıdır.

i) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenir.

j) Kablosuz ağ ile Bakanlığın yerel ağı birbirinden ayrılmış durumda yapılandırılır.

k) Kablosuz internet kullanımında erişim kısıtlamaları uygulanır.

Uzaktan erişim politikası

MADDE 18 – (1) Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) İnternet üzerinden Bakanlığın herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vb. protokollerinden birini içermelidir.

b) Uzaktan erişim güvenliği Bilgi Güvenliği Şube Müdürlüğü tarafından denetlenir.

c) Bakanlık çalışanları bağlantı bilgilerini hiç kimse ile paylaşamaz.

ç) Bakanlık ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlantı kuramaz.

d) Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılır.

e) Bakanlık ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeleri yapılmış olmalıdır.

f) Bakanlıktan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

Sunucu güvenlik politikaları

MADDE 19 - (1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

a) Bakanlıkta bulunan sunucuların yönetiminden, sunucuyla yetkilendirilmiş, ilgili sistem yöneticileri sorumludur.

b) Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri Sistem Yönetimi Şube Müdürlüğünün talimatlarına göre yapılır.

(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.

a) Kullanılmayan servisler ve uygulamalar kapatılır.

b) Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanır.

c) Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs vb. koruma amaçlı yazılımlar sürekli güncellenir. Antivirüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve test mekanizmasından geçirilir, sonra uygulanır. Bu çalışmalar için yetkilendirilmiş bir personel görevlendirilir.

ç) Sistem yöneticileri 'administrator' ve 'root' gibi genel sistem hesapları kullanamaz. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı belirlenir.

d) Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılır.

e) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılamaz. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanır.

f) Sunucular üzerinde sadece lisanslı yazılımlar kurulur.

g) Sunucular fiziksel olarak korunmuş sistem odalarında bulundurulur.

(3) Sunucu gözlemleme kuralları aşağıda belirtilmiştir.

a) Bilgi Güvenliği Şube Müdürlüğü koordinesinde Başkanlık bünyesinde kritik sistemler belirlenir.

b) Kritik sistemlerde, uygulamalar kaydedilir ve kayıtlar aşağıdaki gibi saklanır.

1) Kayıtlara minimum 6 ay süreyle erişilir.
2) Günlük yedekler (tape backup) en az 1 ay saklanır.
3) Haftalık yedekler en az 1 ay saklanır.
4) Aylık tam yedekler (full backup) en az 12 (on iki) ay saklanır.

c) Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanır.

ç) Sunucu üzerinde zararlı yazılım (malware, spyvvare, hack programları, vvarez programları, vb.) çalıştırılamaz.

d) Kayıtlar Bilgi Güvenliği Şube Müdürlüğü tarafından değerlendirilir ve gerekli tedbirler alınır.

e) Port tarama atakları düzenli olarak yapılır.

f) Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik olarak yapılır.

g) Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli olarak takip edilir.

h) Denetimler, Bilgi Güvenliği Şube Müdürlüğü tarafından yetkilendirilmiş kişilerce yönetilir ve belirli aralıklarda yapılır.

ı) Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

Veritabanı güvenlik politikası

MADDE 20 – (1) Veritabanı güvenlik kuralları aşağıda belirtilmiştir.

a) Veritabanı işletim kuralları belirlenir ve dokümante edilir.

b) Veritabanı sistem kayıtları tutulur ve gerektiğinde Bakanlık tarafından izlenir.

c) Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilir.

ç) Veritabanı sistemlerinde tutulan bilgiler sınıflandırılır ve uygun yedekleme politikaları oluşturulur, yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli olarak alınması kontrol altında tutulur.

d) Yedekleme planları dokümante edilir.

e) Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile güvenli ortamlarda saklanır.

f) Veritabanı erişim politikaları MADDE 8'de belirtilen Kimlik Doğrulama ve Yetkilendirme politikası çerçevesinde oluşturulur.

g) Hatadan arındırma, bilgileri yedekten döndürme kuralları MADDE 24'te belirtilen Kriz / Acil Durum Politikasına uygun olarak oluşturulur ve dokümante edilir.

h) Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulur.

ı) Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında ilgili birim amiri bilgilendirilir.

i) Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulur ve sonrasında ilgili uygulama kontrolleri gerçekleştirilir.

j) Bilgi saklama medyaları Bakanlık dışına çıkartılmamalıdır.

k) Veritabanı dokümantasyonu güvenli şekilde saklanmalıdır.

l) İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenir.

m) Veritabanı sunucusu sadece ssh, rdp, ssl ve veritabanının orijinal yönetim yazılımına açık olmalı; bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır. Ancak ftp, telnet vb. açık metin şifreli bağlantılar veri tabanı sunucusundan dışarıya yapılabilir.

n) Uygulama sunucularından veritabanına uzaktan erişim bağlantısı (rlogin) yapılamaz.

o) Veritabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır.

ö) Arayüzden gelen kullanıcılar bir tabloda saklanmalı, bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.

p) Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmelidir.

r) Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler arayüzden sağlanmalıdır.(örnek; Kullanıcılar tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmamalıdır)

s) Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için)

ş) Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için MADDE 10'da belirtilen Parola Politikasına bakılmalıdır.

t) Veritabanına doğrudan ulaşan kullanıcılar bir tabloda saklanır, bu tablodaki kullanıcıların yaptıkları işlemler kayıt altına alınır.

u) Veritabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılır. Root veya admin şifresi tanımlı kişi/kişilerde olmalıdır.

ü) Bağlanacak kişilerin kendi adına kullanıcı adı verilir ve yetkilendirme yapılır.

v) Bütün kullanıcıların yaptıkları işlemler kaydedilir.

y) Veritabanı yönetimi birbirini yedekleyen en az iki personel tarafından yapılır.

z) Veritabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenir.

aa) Veritabanı sunucularına ancak yetkili kullanıcılar erişebilir.

Bilgi sistemleri yedekleme politikası

MADDE 21 – (1) Bilgi sistemleri yedekleme politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki yapılandırma, sistem bilgileri ve kurumsal veriler düzenli olarak yedeklenir.

b) Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak manyetik kartuş, DVD veya CD ortamında yedekleri alınır.

c) Taşınabilir ortamlar (manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından farklı odalarda veya binalarda güvenli bir şekilde saklanır. Veriler offline ortamlarda en az 2 (iki) yıl süreyle saklanır.

ç) Varlık envanterinde bulunan varlıklar kritiklik seviyelerine göre sınıflandırılır ve yedekleme ihtiyacı bakımından dokümante edilir.

d) Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilir.

e) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanır ve atamalar yapılır.

f) Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyalarının önem derecesine göre yedekleme periyotları belirlenir.

g) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik

olarak gözden geçirilmeli ve güncellenmelidir.

h) Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenir.

ı) Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilir ve temin edilir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilir.

i) Yedekleme ortamları düzenli periyotlarda test edilir ve acil durumlarda yedekleme ortamlarının kullanılması gerektiğinde güvenilir olması sağlanır.

j) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dâhilinde tamamlanması sağlanır.

k) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanır.

l) Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek bir ortamda bulundurulur.

m) Veri Yedekleme Standardı, yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği belirlenir. Yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanır ve işlerliği periyodik olarak gözden geçirilir.

n) Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı yapılır.

Yazılımı geliştirme politikası

MADDE 22 - (1) Yazılım geliştirme politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

b) Bakanlık sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

c) İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.

ç) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.

d) Bakanlık içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

e) Bakanlıkta kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.

f) Geliştirilen yazılımlar mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.

g) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

h) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

ı) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.

i) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

j) Yazılımlar sınıflandırılmalı / etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

Değişim yönetim politikası

MADDE 23 – (1) Değişim yönetim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilir.

b) Bakanlık bilgi sistemleri mevcut ve üretilen tüm hizmetler ve ürünlerin kapsamındaki uygulama yazılımı, sistem yazılımı, veritabanı ve donanım gibi altyapı yapılandırma bileşenleri ile ilgili değişiklikler kayıt altına alınır. Üretim, test, geliştirme ortamları ve felaket kurtarma merkezi bu kapsama dahildir.

c) Yazılım ve donanım envanteri kullanılarak, yazılım sürümleri kontrol edilir.

ç) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenir ve dokümante edilir.

d) Değişiklikler gerçekleştirilmeden önce Güvenlik Politikaları Yöneticisi ve ilgili diğer yöneticilerin onayı alınır.

e) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulur, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilir.

f) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanır ve ilgili yöneticiler tarafından onaylanması sağlanır.

g) Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilir.

h) Teknoloji değişikliklerinin Bakanlığın sistemlerine etkileri belirli aralıklarla gözden geçirilir ve dökümante edilir.

Kriz / Acil durum politikası

MADDE 24 – (1) Acil durum politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Acil durum sorumluları atanır, yetki ve sorumlulukları belirlenerek dokümante edilir.

b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınır. Problem durumlarında sistem kesintisiz veya makul kesinti süresi içerisinde felaket ve/veya iş sürekliliği merkezi üzerinden çalıştırılabilmelidir.

c) Bilişim sistemlerinin kesintisiz çalışmasının sağlanması için aynı ortamda kümeleme veya uzaktan kopyalama veya yerel kopyalama veya pasif sistem çözümleri hayata geçirilir. Sistemler tasarlanırken minimum sürede iş kaybı hedeflenir.

ç) Acil durumlarda Bakanlık içi işbirliği gereksinimleri tanımlanır.

d) Acil durumlarda sistem kayıtları incelenmek üzere saklanır.

e) Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilir.

f) Acil durumlarda bilgi güvenliği yöneticisine erişilir, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilir ve zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülür.

Bakım politikası

MADDE 25 – (1) Bakım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bakanlık sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınır. Bunun için gerekli anlaşmalar yapılır ve yıllık bütçe ayrılır.

b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanır.

c) Firma teknik destek elemanlarının bakım yaparken İçişleri Bakanlığı Bilgi Güvenliği Politikaları Yönergesine uygun davranmaları sağlanır ve kontrol edilir.

ç) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak MADDE 23'te belirtilen Değişim Yönetimi Politikası uygulanır.

d) Bakım yapıldıktan sonra tüm sistem yapılandırma dokümantasyonu güncellenir.

e) Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılır.

f) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda İçişleri Bakanlığı Bilgi Güvenliği Politikaları Yönergesi uyarınca hareket edilir.

Belgelendirme politikası

MADDE 26 – (1) Belgelendirme politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bakanlığın bilişim sistemleri ile ilgili bütün iş ve işlemleri açıkça belgelenir ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda bulunur.

b) Bilişim sistemlerindeki iş akışları uygun şekilde belgelendirilir.

c) Belgeleme, tarih belirtilerek yapılır ve yedek kopyaları güvenli bir yerde muhafaza edilir.

ç) Girdi türleri ve girdi form örnekleri belgelenmelidir.

d) Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.

e) Çıktı form örnekleri ve çıktıların kimlere dağıtılacağı belgelenmelidir.

f) Programların nasıl test edildiği ve test sonuçları belgelenmelidir.

g) Bütün program değişikliklerinin detayları belgelenmelidir.

ÜÇÜNCÜ BÖLÜM

Çeşitli Hükümler

Yaptırımlar

MADDE 27 – (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, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve ilgili diğer mevzuatın ilgili hükümlerine göre işlem yapılır.

Başkanlıkça değiştirilebilecek maddeler

MADDE 28 – (1) Bu yönergenin;

5. maddesinin (1) fıkrasının c,

8. maddesinin (1) fıkrasının b, ı,

10. maddesinin (1) fıkrasının b, c, ç, e, g,

12. maddesinin (1) fıkrasının c, (2) fıkrasının l,

13. maddesinin (1) fıkrasının ı,

14. maddesinin (1) fıkrasının a, c, ç,

16. maddesinin (1) fıkrasının a, b,

17. maddesinin (3) fıkrasının a,

18. maddesinin (1) fıkrasının a,

19. maddesinin (2) fıkrasının d, (3) fıkrasının b,

20. maddesinin (1) fıkrasının e, m,

21. maddesinin (1) fıkrasının c,

Bendinde yer alan hükümleri teknolojik gelişmeler ve güvenlik ihtiyaçları dikkate alınarak Başkan onayı ile değiştirilebilir.

Yürürlük

MADDE 29 – (1) Bu yönerge Bakan onayı ile yürürlüğe girer.

Yürütme

MADDE 30 – (1) Bu yönerge hükümlerini Bakan yürütür.

OLUR

09/09/2013

Muammer GÜLER

Bakan

Tablo (Ek-1)

Kısaltmalar Tablosu

Kısaltma	Tanım
Zincir e-posta	Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesi
Spam	Yetkisiz ve/veya istenmeyen reklam içerikli e-postalar
Sahte e-posta	Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanma ve kişisel bilgilerine (tamamen yasadışı yoldan) erişme maksadıyla hazırlanmış e-posta.
RADIUS (Remote Authentication Dial-in User Service)	Sunuculara uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolü
Portal	Birden çok içeriği bir arada bulunduran alan
SSL (Secure Socket Layer)	Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolü
VPN (Virtual Private Network)	Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknoloji
IPSec (Internet Protocol Security) VPN	Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlama
Ağ Güvenlik Duvarı	Bakanlık ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazları
IP	Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adres
MAC adresi	Bir ağ cihazının tanınmasını sağlayan kendisine özel adres
SNMP (Simple Network Management Protocol)	Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokol
Firmware	Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden

Kısaltma	Tanım
	beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımlar
DMZ (Demilitarized Zone)	Bakanlık içi ağı ile Bakanlık dışı ağı birbirinden ayıran bölge
Uzaktan Erişim	İnternet, telefon hatları veya kiralık hatlar vasıtası ile Bakanlığın ağına erişilmesi
Risk	Bakanlığın bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörler
Güvenli Kanal	Güçlü bir şifreleme ile korunan iletişim kanalı
Uygulama Sunucusu	Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımıdır. Üç katmanlı uygulamaların bir parçasıdır. Bu üç katman: Kullanıcı arayüzü (GUI), uygulama sunucusu ve veritabanı sunucusu
Yetkilendirme	Sisteme giriş izni verilmesi, çok kullanıcılı sistemlerde sistem yöneticisi tarafından, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesi
Yedekleme	Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritabanının başka bir yere kopyalanması işlemi.
Veritabanı	Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğu
Şifreleme	Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritma
VLAN (Virtual LAN)	Sanal yerel ağ. Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubu
Ağ güvenlik duvarı,	Kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
PDA	Personal Digital Assistant