T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Bilgi İşlem Dairesi Başkanlığı

Sayı : 54944620- 10472 06/02/2019
Konu : Bilgi Güvenliği Politikaları Yönergesi

BAKANLIK MAKAMINA

Ulaştırma ve Altyapı Bakanlığı'nın görevleri ve konumu itibariyle 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 gerçekleştirmek amacıyla "Bilgi Güvenliği Politikaları Yönergesi" hazırlanmıştır.

Bu Yönerge, Ulaştırma ve Altyapı Bakanlığı'na bağlı merkez ve taşra teşkilatında bulunan bütün birimlerdeki personelin bilgi sistemlerinin kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Bu hususlar doğrultusunda; 04.10.2013 tarih ve 22851706-706/608 sayılı Makam oluru ile yürürlüğe giren "Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi Güvenliği Politikaları Yönergesi"nin yürürlükten kaldırılması ve ekteki **"Ulaştırma ve Altyapı Bakanlığı Bilgi Güvenliği Politikaları Yönergesi"**nin onayı ile Bakanlığımızda uygulanmasına başlanmasını takdir ve tensiplerinize arz ederim.

Ekler:
1) Bilgi Güvenliği Politikaları Yönergesi (19 Sayfa)

İbrahim KOLCU
Daire Başkanı V.

Uygun görüşle arz ederim.
21../01./2019

Dr. Ömer Fatih SAYAN
Bakan Yardımcısı

OLUR
06../02./2019

Mehmet Cahit TURHAN
Bakan

Hakkı Turayliç Caddesi No: 5 06338 Emek / Çankaya / ANKARA
Telefon: (0 312) 203 12 03
E-posta: bdb@uab.gov.tr
Internet Adresi: www.uab.gov.tr

Ayrıntılı bilgi alınacak kişi:
Nejdet GÖKKAYA
Şube Müdürü

ULAŞTIRMA VE ALTYAPI BAKANLIĞI
BİLGİ GÜVENLİĞİ POLİTİKALARI
YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

Madde 1- (1) Bu yönergenin amacı; Ulaştırma ve Altyapı Bakanlığı'nın sahip olduğu elektronik ortam ve bilgilerinin 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, Ulaştırma ve Altyapı Bakanlığı Merkez ve Taşra teşkilatında bulunan birimlerdeki çalışanların bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Hukuki Dayanak

Madde 3- Bu Yönerge, 01.11.2011 tarihli ve 28102 sayılı Resmi Gazetede yayımlanan 655 sayılı Kanun Hükmünde Kararnamenin 34 üncü maddesine, 1 Numaralı Cumhurbaşkanlığı Kararnamesinin, Onaltıncı Bölüm Ulaştırma ve Altyapı Bakanlığı 497. Maddesinin ç) bendine, 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanununa dayanılarak 26.12.2007 tarihli ve 26738 sayılı Resmi Gazetede yayımlanan "Kamu İç Kontrol Standartları Tebliği", 23.05.2007 tarihli ve 26530 sayılı Resmi Gazetede yayımlanan 5651 sayılı kanunun 6. maddesine dayanılarak hazırlanmıştır.

Tanımlar

Madde 4- (1) Bu yönergede geçen;

Bakan	: Ulaştırma ve Altyapı Bakanını,
Bakanlık/Kurum	: Ulaştırma ve Altyapı Bakanlığını,
Başkanlık	: Bilgi İşlem Dairesi Başkanlığını,
Ağ Güvenlik Yöneticisi	: Ağ Sistemlerinden Sorumlu Uzman Yöneticiyi,
Sistem Yöneticisi	: Bilgi Sistemleri Yöneticisini,
Bilgi Güvenliği Yöneticisi	: Bilgi Güvenliği Uzman Yöneticisini,
Veritabanı Yöneticisi	: Veritabanı Sistemlerinden Sorumlu Yöneticiyi,
Güvenlik Politikaları Yöneticisi	: Bilgi Güvenliği Politikaları Yöneticisini,
Kullanıcı	: Bakanlık Bilgi Sistemlerini Kullanan tüm kişileri,
Sunucu	: İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini,
İstemci	: Sunucuların verdiği hizmeti alan bilgisayar sistemini,
	ifade eder.

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

İKİNCİ BÖLÜM
Bilgi Güvenliği Politikaları

Bilgi Sistemleri Genel Kullanım Politikası

Madde 5- (1) Bilgi sistemlerine sahip olma ve bu sistemlerin genel kullanım kuralları aşağıda belirtilmiştir.

a) Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Kurumun bünyesinde oluşturulan tüm veriler, iş ve işlemler için Kurum tarafından kullanıma sunulan tüm bilgisayarlar, taşınabilir cihazlar (kurum bilgisi taşıyan her türlü dizüstü bilgisayar, tablet, akıllı telefon, CD, USB disk, teyp, taşınabilir sabit disk gibi veri saklayabilecek ortamlar) ve bilişim sistemleri Kurumun mülkiyetindedir.

b) Personelin kullanımı için tahsis edilmiş olan tüm bilişim sistemleri, bilgisayarlar, dizüstü bilgisayar, mobil cihazlar, tablet vb. sadece yetkilendirilmiş personel tarafından ve veriliş amaçları doğrultusunda kullanılmalıdır. Başkanlık tarafından kullanılan/kullanılabilecek yazılımlar ile kullanıcıların kısıtlanması sağlanabilir.

c) Bilişim sistemlerinde kullanıcı hesabı oluşturulması talebi personel bilgilerinin de (Sicili, Adı ve Soyadı, T.C. Kimlik Numarası ve Cep telefonu numarası) olduğu resmi yazı ile yapılmalıdır. Bu işlemden önce Personel ve Eğitim Dairesi Başkanlığı tarafından PERBİS Sisteminde ilgili personele sicil numarası (UB/GP/GGP/İP/SP) verilmiş olmalıdır.

ç) Bakanlık birimlerince hizmet alımı şeklinde dışarıya yaptırılan projelerde yerinde destek alınıyorsa ve bu destek süresi 1 (bir) haftadan uzun ise ilgili firma personeli/personelleri içinde kullanıcı hesabı oluşturulmalı ve (c) bendinde ki politika uygulanmalıdır.

d) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmamalıdır. Bu konuda ilgili politikalar dikkate alınmalıdır.

e) Kurum bilgi sistemleri kapsamında üretilen her türlü kurumsal bilgi USB Bellek, CD vb ortamlarda taşınmamalı ve saklanmamalıdır.

f) Kurum, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

g) Kurum bilgisayarları etki alanına dahil edilmelidir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi olmamalıdır.

h) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.

i) Kurumda Bilgi İşlem Dairesi Başkanlığının bilgisi ve onayı olmadan Bakanlık Ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.

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

k) Bilgisayarlara lisanssız program yüklenmemelidir.

l) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Başkanlıktan ortak alan talebinde bulunulmalıdır. Kaynakların paylaşıma açılması halinde mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

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

a) Herhangi bir Masaüstü/Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Başkanlığa haber verilmelidir.

b) Bütün bilgisayarlar, cep telefonu, tablet bilgisayarlar ve PDA (Personal Digital Assistant) cihazları kurumun ağı 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.

c) Kullanıcılar tarafından gönderilen e-postalarda gereğine göre aşağıdaki şekilde bir açıklama yer almalıdır.

"Bu elektronik posta ve onunla iletilen bütün dosyalar; göndericisi tarafından alması amaçlanan; yetkili gerçek ya da tüzel kişinin kullanımı içindir. Eğer söz konusu yetkili alıcı değilseniz bu elektronik postanın içeriğini açıklamanız, kopyalamanız, yönlendirmeniz ve kullanmanız kesinlikle yasaktır ve bu elektronik postayı derhal silmeniz gerekmektedir. T.C. Ulaştırma ve Altyapı Bakanlığı bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda herhangi bir garanti vermemektedir ve hiçbir hukuksal sorumluluğu kabul etmemektedir. Bu nedenle bu bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından ve saklanmasından sorumlu değildir. Bu mesajdaki görüşler yalnızca gönderen kişiye aittir ve T.C. Ulaştırma ve Altyapı Bakanlığı'nın görüşlerini yansıtmayabilir. Bu e-posta bilinen bilgisayar virüslerine karşı taranmıştır. Ancak yollayıcı, bu e-posta mesajının - virüs koruma sistemleri ile kontrol ediliyor olsa bile - virüs içermediğini garanti etmez ve meydana gelebilecek zararlardan doğacak hiçbir sorumluluğu kabul etmez."

ç) Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı, ek dosyalar eklenecekse en fazla 25 MB boyutunda ek dosyalar eklenmeli ve mümkünse dosyalar sıkıştırılmalıdır. Bu boyuttan fazla gönderilecek veya alınacak dosyalar için Kurumun Bulut Sistemi kullanılmalıdır.

Belgelendirme Politikası

Madde 6- (1) Belgelendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilişim sisteminin yapısı ile ilgili bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.

b) İş akışları uygun şekilde belgelenmelidir.

c) Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.

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.

E-Posta Politikası

Madde 7- (1) E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.

a) Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.

b) Bakanlık ile ilgili olan gizli bilgiler, gönderilen mesajlarda yer almamalıdır. Buna kapsamı içerisine iliştirilen öğeler de dahildir. Mesajların, gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

c) Kullanıcı, Kurumun e-posta sistemini taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajlar göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında ilgili birime haber verilmelidir.

ç) Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalı ve e-posta gönderilmemelidir.

d) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, ilgili birime haber verilmelidir.

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

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

g) 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 mesajları yollamaktan sorumludur.

ğ) Kullanıcı parolaları, en az 8 karakterden oluşmalı ve parolalarının içinde; 4 karmaşıklığın (büyük harf, küçük harf, rakam ve özel karakter (@,^A,+,$,#,&,/,{,*,-,],=...)) en az 3 tanesi bulunmalıdır.

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

a) E-posta kişisel amaçlar için kullanılmamalıdır.

b) Kullanıcı, mesajlarının, yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden parola kullanılmalı ve kullanılan parola en geç 45 günde bir değiştirilmelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

c) Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın ilgili birime/başkanlığa haber vermelidir.

ç) Kullanıcı, kurumsal mesajlarını, kurum iş akışının aksamaması için cevaplandırmalı ve kurumsal mesajlarda kişisel e-posta adresleri değil kurumsal e-posta adresi kullanılmalıdır.

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

e) Kurum e-posta adresleri ile kişisel sosyal medya ve kurumla alakalı olmayan hiçbir siteye abone olunmamalıdır.

f) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar ilgili birime haber verilmelidir.

g) 6 ay süreyle kullanılmamış e-posta adresleri kullanıcıya haber vermeden sunucu güvenliği için pasif hale getirilmelidir.

h) Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren Başkanlığa haber vermelidir.

(3) E-posta adresleri kurumsal kimlik kılavuzuna uygun şekilde tanımlanmalıdır.

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

(5) Kullanıcı, e-postalarına erişirken, POP3, SMTP, HTTP vb kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanmamalıdır.

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

(7) Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar antivirüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenmelidir.

Parola Politikası

Madde 8- (1) Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

a) Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) en geç 6(altı) ayda bir değiştirilmelidir.

b) Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 45(kırk beş) günde bir değiştirilmelidir.

c) Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.

ç) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

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

e) Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları kolayca kırılamayacak güçlü bir parolaya sahip olmalıdır.

f) Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

(2) Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

a) Parola en az 8 haneli olmalıdır.

b) İçerisinde en az 1'er tane büyük ve küçük harf bulunmalıdır (A,a, B,b C,c.).

c) İçerisinde en az 1 tane rakam bulunmalıdır (1, 2, 3...).

ç) İçerisinde en az 1 tane özel karakter bulunmalıdır (@, !,?,^,+,$,#,&,/,{,*,-,],=,...).

d) Aynı karakterler peş peşe kullanılmamalıdır (aaa, 111, XXX, ababab...).

e) Sıralı karakterler kullanılmamalıdır (abcd, qwert, asdf,1234,zxcvb...).

f) Kullanıcıya ait anlam ifade eden kelimeler içermemelidir (Kullanıcı adı, sicil numarası, aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.).

(3) Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

a) Bütün parolalar Bakanlığa ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.

b) Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola

hatırlama" seçeneği kullanılmamalıdır.

c) Parola kırma ve tahmin etme operasyonları (testleri) belli aralıklar ile yapılmalıdır.

ç) Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilmelidir.

(4) Uygulama Geliştirme Standartları

a) Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.

b) Parolalar, metin olarak veya kolay anlaşılabilir formatta saklanmamalıdır.

c) Parolalar, şifrelenmiş olarak saklanmalıdır.

ç) En az RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

d) Uygulamalarda kullanıcının her uygulama için ayrı parola girmesinden kaçınılmalı, parola girişi mümkün mertebe güvenilir tek giriş uygulamaları ile sağlanmalıdır.

Antivirus Politikası

Madde 9- (1) Antivirus Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurumun tüm istemcileri ve sunucuları antivirus yazılımına sahip olmalıdır (Sistem yöneticileri tarafından antivirüs yazılımı kullanımına ihtiyaç duyulmayan sunucular hariç).

b) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalı, virüs temizliğinden sonra tekrar etki alanına alınmalıdır.

c) Sistem yöneticileri, antivirus yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.

ç) Kullanıcı hiç bir sebepten dolayı antivirus yazılımını bilgisayarından kaldırmamalıdır.

d) Antivirus güncellemeleri antivirus sunucusu/sunucuları ile yapılmalıdır. Antivirüs sunucuları internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak antivirus sunucusu tarafından antivirus güncellemeleri yapılmalıdır.

e) Haklı bir gerekçe ile etki alanı dışında tutulması gereken kullanıcı talebi olması durumunda; her türlü maddi/manevi oluşabilecek zararların kişi ve amiri tarafından kabul edildiğini beyan eden form doldurularak Başkanlığa teslim edilmelidir. Bu tip kullanıcıların her türlü güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartmalıdır.

f) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.

g) Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.

ğ) Optik Media ve harici veri depolama cihazları antivirus kontrolünden geçirilmelidir.

h) Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

İnternet Erişim ve Kullanım Politikası

Madde 10- (1) İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır (Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır).

b) Kurumun politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.

c) Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.

ç) Kurumun ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır. İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.

d) Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.

e) Ancak yetkilendirilmiş kişiler internete çıkarken (Mümkünse Kurumun normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla) bütün servisleri kullanma hakkına sahip olabilir.

f) Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemeli, internet üzerinden TV, radyo ve video izlenmemeli/dinlenmemelidir.

g) İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmemelidir. Bu konuda gerekli önlemler alınmalıdır.

ğ) Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilmelidir.

Sunucu Güvenlik Politikaları

Madde 11- (1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurumda bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel sorumludur.

b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılmalıdır.

c) Sunuculara ait bilgilerin yer aldığı tablo oluşturulmalıdır. 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 personelin isimleri ve telefon numaraları bilgileri yer almalıdır.

ç) Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.

(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.

a) Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri Başkanlık talimatlarına göre yapılmalıdır.

b) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

c) Servislere erişimler, kaydedilmeli ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.

ç) Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir. Antivirüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır. Güncellemelerde değişiklik

yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve test mekanizmasından geçirilmeli, sonra uygulanmalıdır. Bu çalışmalar için yetkilendirilmiş personel olmalıdır.

d) Sistem yöneticileri mümkün olduğu ölçülerde 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.

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

f) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.

g) Sunucular üzerinde lisanslı veya güvenliği test edilmiş açık kaynak kodlu yazılımlar kurulmalıdır.

ğ) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

(3) Sunucu gözlemleme kuralları aşağıda belirtilmiştir.

a) Kritik sistemlerde, uygulama erişimleri kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.

b) Kayıtlara çevrimiçi olarak minimum 90 gün süreyle erişilebilmelidir.

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

d) Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.

e) Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.

f) Sunucularda port taramaları düzenli olarak yapılmalıdır. Açık olmaması gereken portlar kapatılmalıdır.

g) Yetkisiz kişilerin ayrıcalıklı hesaplara yönelik girişimlerinin kontrolü periyodik yapılmalıdır.

h) Yedekler Başkanlığın belirleyeceği bir yedekleme politikasına göre saklanmalıdır.

ı) Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.

i) Denetimler, Bilgi İşlem Dairesi Başkanlığı tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.

j) Sunucuların bilgileri yetkilendirilmiş kişi tarafından tutulmalı ve güncellenmelidir.

(4) Sunucu işletim kuralları aşağıda belirtilmiştir.

a) Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulmalıdır.

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

c) Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.

Ağ Cihazları Güvenlik Politikası

Madde 12- (1) Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.

b) Yerel kullanıcı hesapları açılmamalıdır. Ağ cihazları kimlik tanımlama için LDAP, RADIUS veya TACAS+ protokollerinden birini kullanmalıdır.

c) Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması kurumun içerisinden yapılmalıdır.

ç) Kurumun standart olan SNMP community string'leri kullanılmalıdır. Bu bilgi sadece yetkilendirilmiş kişiler tarafından bilinmelidir.

d) İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.

e) Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin/mesai saatleri dışında üretim ortamına taşınmalıdır.

f) Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.

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

h) Yönlendiriciye erişen tüm kullanıcılar uyarılmalıdır.

i) Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır.

"BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir."

Ağ Yönetim Politikası

Madde 13- (1) Ağ yönetim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Ağ cihazlarının yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrılmalıdır.

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

c) Erişimine izin verilen ağlar için ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimle ilgili tedbirler alınmalıdır.

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

d) Sınırsız ağ dolaşımı engellenmelidir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.

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

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

g) Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır. Kurum kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılmalı ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanmalıdır.

ğ) Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.

h) Bilgisayar ağına bağlı bütün bilişim makinelerinde (Bilgisayar, tablet, v.b) kurulum ve

yapılandırma parametreleri, Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.

ı) Sistem tasarımı ve geliştirilmesi yapılırken Kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.

i) İnternet trafiği ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.

j) Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.

k) Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.

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

Uzaktan Erişim Politikası

Madde 14- (1) Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar **VPN** teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamaktadır. **VPN** teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.

b) Uzaktan erişim güvenliği denetlenmelidir.

c) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

d) Firma ve personeline veya 3. şahıslara Kurum ağına uzaktan bağlanma yetkisi verilmesi için Kurumun herhangi bir birimi ile bir bilişim projesi sözleşmesi olmalı ve VPN talep formu ile gizlilik taahhütnameleri imzalanmalıdır.

ç) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

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

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

f) Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların yetkileri ve hesap özellikleri buna göre güncellenmelidir.

Kablosuz İletişim Politikası

Madde 15- (1) Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.

(2) Bütün kablosuz erişim cihazları Başkanlık tarafından onaylanmış olmalı ve Başkanlığın belirlediği güvenlik ayarlarını kullanmalıdır. Başkanlığın onayı olmadan hiçbir birim hiçbir şekilde bilgisayar ağına kablolu/kablosuz ağ cihazları takmamalıdır.

(3) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802. lx erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.

b) Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir.

c) Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

ç) Varsayılan SSID isimleri kullanılmamalıdır. SSID yayan bilgisi içerisinde kurumla ilgili bilgi olmamalıdır (mesela kurum ismi, ilgili bölüm, çalışanın ismi vb).

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

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

f) Erişim Cihazları üzerinden gelen kullanıcılar güvenlik duvarı(Firewall) üzerinden ağa dâhil olmalıdırlar.

g) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Kurum'un tüm internet bant genişliğinin tüketilmesi engellenmelidir.

ğ) Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.

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

ı) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

Donanım ve Yazılım Envanteri Oluşturma Politikası

Madde 16- (1) Donanım ve yazılım envanteri oluşturma ile ilgili kurallar aşağıda belirtilmiştir.

a) Oluşturulan envanter tablosunda şu bilgiler olmalıdır; sıra no, bilgisayar adı, bölüm, marka, model, seri no, özellikler, ek aksamlar, işletim sistemi, garanti süresi vs.

b) Bu tablolar merkezi bir web sunucuda tutulmalı ve belirli aralıklarla güncellenmelidir. İlgili siteye girişler güvenlik politikaları çerçevesinde yapılmalıdır.

c) Envanter bilgileri sık sık kontrol edilmelidir.

Kriz / Acil Durum Politikası

Madde 17- (1) Acil Durum politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Acil durum sorumluları atanmalı, yetki ve sorumlulukları belirlenerek dokümante edilmelidir.

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

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

ç) Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.

d) Acil durumlarda sistem kayıtları incelenmek üzere saklanmalıdır.

e) Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.

f) Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.

g) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.

ğ) Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.

h) Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

Fiziksel Güvenlik Politikası

Madde 18- (1) Fiziksel Güvenlik ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurumun binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.

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

c) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilmelidir.

ç) Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılmalı ve izlenmelidir.

d) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.

e) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.

f) Kritik sistemler özel sistem odalarında tutulmalıdır.

g) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalı ve iklimlendirilmesi sağlanmalıdır.

ğ) Fotokopi, yazıcı vs. türü cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.

h) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

Kimlik Doğrulama ve Yetkilendirme Politikası

Madde 19- (1) Kimlik Doğrulama ve Yetkilendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenmeli ve dokümante edilmelidir.

b) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanmalı ve dokümante edilmelidir.

c) Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve açılış ekranları olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, dokümante edilmeli ve denetim altında tutulmalıdır.

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

d) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.

e) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız erişim istekleri/girişimleri incelenmelidir.

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

g) İstisnai durumlar dışında bakanlık bünyesindeki tüm uygulamalar için kimlik doğrulaması tek oturum açma uygulaması ile olmalıdır.

Veri tabanı Güvenlik Politikası

Madde 20- (1) Veri tabanı güvenlik kuralları aşağıda belirtilmiştir.

a) Veritabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.

b) Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.

c) Veritabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.

ç) Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.

d) Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.

e) Yedekleme planları dokümante edilmelidir.

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

g) Veritabanı erişim politikaları "Kimlik Doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.

ğ) Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil Durum Yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.

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

ı) Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.

i) Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

j) Bilgi saklama medyaları kurum dışına çıkartılmamalıdır.

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

l) Veri tabanı 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 sunucudan

dışarıya yapılabilmelidir.

m) Uygulama sunucularından veri tabanına login vb. şekilde erişilememelidir.

n) Veri tabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılmalıdır. Root veya admin şifresi, tanımlı kişi/kişilerde olmalıdır.

o) Bağlanacak kişilere kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.

p) Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.

q) Veri tabanı yöneticiliği yetkisi en fazla 2(iki) kullanıcıda olmalıdır.

r) Veri tabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.

s) Veri tabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmelidir. Veri tabanı sunucularına ancak yetkili kullanıcılar erişmelidir.

t) Veri tabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler ara yüzden sağlanmalıdır (örnek; Kullanıcılar tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmamalıdır).

u) Veri tabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir.

v) Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için Şifreleme Politikasına bakılmalıdır.

y) Veri tabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

Değişim Yönetim Politikası

Madde 21- (1) Değişim Yönetim Politikası ile ilgili kurallar aşağıda belirtilmiştir.

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

b) Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.

c) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümante edilmelidir.

ç) Değişiklikler gerçekleştirilmeden önce Güvenlik Politikaları Yöneticisi ve ilgili diğer yöneticilerin onayı alınmalıdır.

d) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.

e) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.

f) Teknoloji değişikliklerinin Kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir.

Bilgi Sistemleri Yedekleme Politikası

Madde 22- (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 konfigürasyon, sistem bilgileri ve kurumsal veriler düzenli olarak yedeklenmelidir.

b) Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde/farklı disk sistemlerinde yedekleri alınmalıdır.

c) 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 edilmelidir.

d) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.

e) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.

f) Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilmemelidir.

ğ) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.

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

ı) Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

i) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.

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

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

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

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 belirlenmelidir. Yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

Personel Güvenliği Politikası

Madde 23- (1) Personel Güvenliği Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.

b) Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden veya dışından referans sorulması sağlanmalıdır.

c) Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.

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

d) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

e) İş tanımı değişen veya Kurumdan ayrılan kullanıcıların erişim hakları kaldırılmalıdır.

f) Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

g) Kurum bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.

ğ) Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılması ile ilgilidir. Bu paylaşım ile kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılmalıdır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamasıdır. Sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmalıdır.

h) Çalışanlar, işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilmelidir.

ı) Çalışanların güvenlik ile ilgili aktiviteleri izlenmelidir.

i) Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

Bakım Politikası

Madde 24- (1) Bakım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır.

b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.

c) Firma teknik destek elemanlarının bakım yaparken "Ulaştırma ve Altyapı Bakanlığı Bilgi Güvenliği Politikaları'na uygun davranmaları sağlanmalı ve kontrol edilmelidir.

ç) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" ve ilişkili standartlar uygulanmalıdır.

d) Bakım yapıldıktan sonra gerekiyorsa tüm sistem dokümantasyonu güncellenmelidir.

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 yapılmalıdır.

f) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "Ulaştırma ve Altyapı Bakanlığı Bilgi Güvenliği Politikaları" uyarınca hareket edilmelidir.

Yazılım Geliştirme Politikası

Madde 25- (1) Yazılım Geliştirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Yazılımlarda mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirmemelidir.

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

c) İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.

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

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

e) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.

f) Hazırlanan 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.

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

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

ı) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

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

j) Kişisel verilerin korunması amacıyla erişim kontrolü(görmesi gereken ve görmesi gerektiği kadar) ve veri maskeleme(veriyi bütün halde göstermemek) metodları kullanılmalıdır.

ÜÇÜNCÜ BÖLÜM
Çeşitli Hükümler

Yürürlük

Madde 26- (1) Bu Yönerge Ulaştırma ve Altyapı Bakanının onayı ile yürürlüğe girer.

Yürütme

Madde 27- (1) Bu yönerge hükümlerini Ulaştırma ve Altyapı Bakanı yürütür.

(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 kazanmak ve kişisel bilgilerine (tamamen yasadışı yoldan) erişmek
RADIUS (Remote Authentication Dial-in User Service)	Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolü
X.509/LDAP(Light weight Directory Access Protocol	Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir 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	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
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	Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokol
Firmware	Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımlar
DMZ	Kurum içi ağı ile kurum dışı ağı birbirinden ayıran bölge
Uzaktan Erişim	İnternet, telefon hatları veya kiralık hatlar vasıtası ile Kurumun ağına erişilmesi
Risk	Kurumun bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörler
Güvenli Kanal	Güçlü bir şifrelemeden oluşan iletişim kanalı
Uygulama Sunucusu	Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımıdır. Üç katmanlı uygulamaların bir parçasıdır. Bu üç katman: Kullanıcı ara yüzü (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.
Veri tabanı.	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