T.C.
ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI
Sivil Havacılık Genel Müdürlüğü

89663468-700/E.265 20/05/2015

Sayı :
Konu : Bilgi Güvenliği Politikaları Yönergesi.

GENEL MÜDÜRLÜK MAKAMINA;

Genel Müdürlüğümüz görevlerine ilişkin 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, Genel Müdürlüğümüz ile temsilciliklerde bulunan personelin bilgi sistemlerinin kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Bilgi Güvenliği Politikalarında özellikle üzerinde durulan "bilgi güvenliği" kavramı bilginin hukuka aykırı şekilde her türlü yetkisiz erişimden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden korunması işlemidir.

Yukarıda açıklanan hususlar doğrultusunda hazırlanan Genel Müdürlüğümüz Bilgi Güvenliği Politikaları Yönergesi'nin onayı ile uygulanmasına başlanmasını takdir ve tensiplerinize arz ederim.

Faruk SUBAŞI
Daire Başkanı

Ekler: Bilgi Güvenliği Politikaları Yönergesi.

OLUR

/05/2015

Bilal EKŞİ
Genel Müdür

Gazi Mustafa Kemal Bulvarı No:128/A 06570 Maltepe ANKARA
Telefon Nu.: (0 312) 203 60 32, Belgegeçer Nu.: (0 312) 212 46 84
e-posta: , İnternet adresi: www.shgm.gov.tr

Bilgi için:
Bilgi İşlem Birimi

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ
BİLGİ GÜVENLİĞİ ESASLARI YÖNERGESİ

GENEL HÜKÜMLER

Amaç

MADDE 1- (1) Bu yönergenin amacı; Sivil Havacılık Genel Müdürlüğü‟nün 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, yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmektir.

Kapsam

MADDE 2- (1) Bu yönerge, Genel Müdürlük personeli ile mevzuat, protokol, işbirliği veya hizmet alım kapsamında Genel Müdürlük‟te çalışan kişilerin bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği, sosyal medyayı kullanma ile ilgili uyulması gereken ilke ve kuralları kapsamaktadır.

Hukuki dayanak

MADDE 3- Bu yönerge, 18.10.2005 tarih ve 25997 sayılı Resmi Gazetede yayımlanan 5431 sayılı Sivil Havacılık Genel Müdürlüğü Teşkilat ve Görevleri Hakkında Kanun ile 24.12.2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu kapsamında 26.12.2007 tarihli ve 26738 sayılı Resmi Gazetede yayımlanan "Kamu İç Kontrol Standartları Tebliği", ve 23.05.2007 tarihli ve 26530 sayılı Resmi Gazetede yayımlanan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu yönergede geçen;

Genel Müdür	: Sivil Havacılık Genel Müdürünü,
Birim	: Bilgi İşlem Birimin, ve/veya Genel Müdürlük diğer birimlerini,
Genel Müdürlük/Kurum	: Sivil Havacılık Genel Müdürlüğü‟nü,
Sistem Yöneticisi	: Bilgi İşlem Birimi Sorumlusunu,
Kullanıcı	: Genel Müdürlük Bilgi Sistemlerini kullanan tüm kişileri,
Sunucu	: İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini,
İstemci	: Sunucuların verdiği hizmeti alan bilgisayar sistemini,

ifade etmektedir.

(2) Yönergede kullanılan teknik terim ve tanımlar,

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 fıltreleme 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 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
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
Etki Alanı	: Kurum ağ yapısı (shgm.gov.tr)

şeklindedir.

BİRİNCİ BÖLÜM
Bilgi Güvenliği Esasları

Personel ve Çalışanların Uyması Gereken Kurallar

Bilgi sistemleri genel kullanım esası

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

a) Kurumun bünyesinde oluşturulan tüm veriler, tüm bilgisayarlar ve bilişim sistemleri Kurumun mülkiyetindedir.

b) Kullanıcılar bilgi sistemlerini kişisel kullanımlarında bu talimattaki esaslara uymak ve göz önünde bulundurmak zorundadırlar.

c) Kurum, bu esas çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

ç) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve bu tür programlar sistemlere yüklenmemelidir.

d) Kurumda Bilgi İşlem Biriminin bilgisi ve onayı olmadan ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.

e) Bilgisayarlara lisanssız program yüklenmemelidir.

f) Bilgisayar kaynakları gerekmedikçe paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde ise, mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

g) Dizüstü bilgisayar, tablet vb. çalınması/kaybolması halinde, bu durum en kısa zamanda birim amirine haber verilmelidir. Bilgi İşlem Birimnin haberi olmadan kullanıcılar birbirlerine bilgisayarlarını veremez, formatlayamaz.

ğ) Cep telefonu, tablet bilgisayarlarlar 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.

h) Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda gerekli hassasiyeti göstermeli ve E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalıdır. E-posta ile gönderilen postanın büyüklüğü 10 Mb‟ı aşmamalı ve gerektiğinde dosyalar sıkıştırılmalıdır.

İnternet erişim ve kullanım esası

MADDE 6- (1) İnternet Erişim ve Kullanım Esası ile ilgili kurallar aşağıda belirtilmiştir.

a) Uygunsuz materyal içeren yasaklı sitelere (Pornografik, Vandalizm, Satanizm, Kumar, Hack, Crack, Warez vb.) çeşitli uygulamalar kullanarak erişmek yasaktır.
b) Kullanıcının, ağ dahilindeki ya da haricindeki bir sisteme, ağ kaynağı ve servisine saldırı amaçlı (port tarama, paket dinleme vb.) zarar verecek girişimde bulunması yasaktır.
c) Mahkemeler veya kanunla yetkilendirilen makamlar tarafından yasaklanan sitelere çeşitli uygulamalar kullanarak erişmek yasaktır.

E-Posta esası

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

a) Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.
b) Genel Müdürlük ile ilgili olan gizli bilgiler ve ekleri, gönderilen mesajlarda yer almamalıdır. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için, gönderilen adres ve içerdiği bilgiler kontrol edilmelidir.
c) Kullanıcı, Kurumun e-posta sistemini kullanarak taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik faaliyette bulunamaz. Bu yönde mesajlar alındığında ise ilgili birime haber verilmelidir.
ç) Kullanıcının Genel Müdürlük sistemlerini ticari ve kâr amaçlı olarak kullanması ve bu amaçla e-posta göndermesi yasaktır.
d) Zincir mesajlar ve bu mesajların ekleri e-posta alındığında hiçbir işlem yapılmadan sistem yöneticisine haber verilmelidir.
e) Spam, zincir e-posta ve sahte e-posta gibi zararlı e-postalara yanıt yazılmamalıdır.
f) Kullanıcı, içeriği uygun olmayan e-postaları (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 mesajların yollanmasından sorumludur.

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

a) E-posta kişisel amaçlar için kullanılmamalıdır.
b) Kullanıcı, mesajlarının yetkisiz kişiler tarafından okunmasını engellemeli ve bu yüzden parola kullanılmalı, gerektiğinde de değiştirilmelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
c) Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bir işlem yapmaksızın sistem yöneticisine haber vermelidir.
ç) Kullanıcı, kurumsal mesajlarını iş akışının aksamaması için cevaplandırmalı ve kurumsal mesajlarda acil durumlar haricinde, kurumsal e-posta adresi kullanılmalıdır.
d) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru

olduğu düşünülen e-postalar bilgi işlem birimine haber verilmelidir.

e) Kullanıcı, kendilerine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren bilgi işlem birimine haber vermelidir.

f) Kurum çalışanları e-posta şifrelerini https://mail.shgm.gov.tr/owa adresinden belirlenen sürelerde yukarıdaki esaslara göre değiştirmelidirler.

Parola esası

MADDE 8- (1) Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

a) En az 8 haneli olmalıdır.
b) İçerisinde en az 1 tane harf bulunmalıdır. (a, b, c…)
c) İçerisinde en az 2 tane rakam bulunmalıdır. (1,2,3…)
ç) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^A,+,$,#,&,/,{,*,-,],=,...)
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 tercihen kullanılmamalıdır. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)
g) Kullanıcı hesaplarına ait parolalar(örnek, e-posta, web, masaüstü bilgisayar vs.) 60 günde bir değiştirilmelidir.
ğ) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

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

a) Bütün parolalar Genel Müdürlüğe ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.
b) Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlatma" seçeneği kullanılmamalıdır.

Antivirüs esası

MADDE 9- (1) Antivirus esası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kullanıcı antivirüs yazılımını bilgisayarından kaldırmamalıdır.
b) Antivirüs güncellemeleri antivirüs sunucusu ile yapılmalıdır. Sunucular internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılmalıdır.
c) Kullanıcılar bilinmeyen veya şüpheli kaynaklardan (müzik, video vb) dosya indirmemelidir.
ç) Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.
d) Optik Media ve harici veri depolama cihazları antivirüs kontrolünden geçirilmelidir.

Sosyal medya kullanım esası:

MADDE 10 (1) Sosyal medya kullanımı ile ilgili kurallar aşağıda belirtilmiştir.

a) Kullanıcılar sosyal paylaşım sitelerindeki kişisel hesaplarında, Kurum ile ilgili mesleki ünvanlarını, adreslerini ve resmi e-posta adreslerini kullanmamalıdırlar.

b) Kurumla ilgili gerçekleştirilen çalışmalar veya yaşanan gelişmeler ile ilgili herhangi bir paylaşımda bulunulmamalıdır.
c) Kurumun resmi mail adresleri paylaşılmamalı ve üyelik için de kullanılmamalıdır.
ç) Kullanıcı, sosyal paylaşım sitelerinde Genel Müdürlüğümüz sosyal paylaşım veya web sitelerinde yayımladıkları bilgileri olduğu hali ile iletebilir veya yayımlayabilir.

Genel Müdürlük birimlerinin sorumlulukları;

MADDE 11 (1): İnsan Kaynakları Müdürlüğü, Genel Müdürlüğe yeni başlayan tüm personele bu yönergeyi tebliğ etmek, ayrılacak personelin ayrılma işlemi yapılmadan tüm parolalarının ve sisteme erişiminin iptal edildiğinin Sistem Yöneticisinden teyidini almakla yükümlüdür.

(2) Birim amirleri, personel dışındaki tüm çalışanlara ve bölümlerinde çalışan stajyerlere bu yönergenin Birinci Bölümündeki Personel ve Çalışanların Uyması Gereken Kuralları bildireceklerdir.

(3) Hizmet alımları şartnamelerinde ve sözleşmelerinde Genel Müdürlüğümüzde çalışanların bu yönergenin Birinci Bölümündeki Personel ve Çalışanların Uyması Gereken Kurallara uyacakları yer almalıdır.

ÜÇÜNCÜ BÖLÜM
Bilgi Güvenliği Esasları

Bilgi İşlem Biriminin Uyması Gereken Kurallar

Bilgi sistemleri genel kullanım esası

MADDE 12- (1) Bilgi sistemlerine sahip olma ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir.

a) Kurum, bu esas çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
b) 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.

E-Posta esası

MADDE 13- (1) E-Posta ile ilgili esaslar aşağıda belirtilmiştir.

a) Kurumsal e-postalar gerekli görülen yerlerde Genel Müdürün onayıyla Bilgi İşlem Birimi Sorumlusu tarafından haber vermeksizin denetlenebilir.
b) Kurum, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.
c) 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 esası

MADDE 14- (1) Parola Esası ile ilgili genel esaslar aşağıda belirtilmiştir.

a) Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) 60 günde bir değiştirilmelidir.
b) Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.
c) Kullanıcı, parolasını başkası ile paylaşmaması, kağıtlara ya da elektronik ortamlara

yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.

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

d) Bir kullanıcı adı ve parolası, birden fazla bilgisayarda kullanılmamalıdır.

(2) Uygulama Geliştirme Standartları

a) Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.

b) Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.

c) Parolalar, şifrelenmiş olarak saklanmalıdır.

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

Antivirüs esası

MADDE 15- (1) Antivirus esası ile ilgili esaslar aşağıda belirtilmiştir.

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

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

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

Belgelendirme esası

MADDE 16- (1) Belgelendirme Esası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilişim sisteminin yapısı ile 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.

İnternet erişim ve kullanım esası

MADDE 17- (1) İnternet erişim ve kullanım esası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvarları üzerinden internete bağlanmalıdır. 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 esasları 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.

Sunucu güvenlik esasları

MADDE 18- (1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurumda bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personeller sorumludur.
b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personeller 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 personellerin isimleri ve telefon numaraları bilgileri yer almalıdır.
ç) Tüm bilgiler, sistem yöneticisinin belirlediği kişiler tarafında güncel tutulmalıdır.

(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.

a) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
b) Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.
c) Sistem yöneticileri „Administrator“ ve „root“ gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.
ç) Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL,IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
d) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN“larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
e) Sunucular üzerinde lisanslı veya güvenliği test edilmiş yazılımlar kurulmalıdır.
f) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

(3) Sunucu gözlemleme kuralları aşağıda belirtilmiştir.

a) Aylık full backuplar en az 1 yıl saklanmalıdır.
b) Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanmalıdır.
c) Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları vb.) çalıştırılmamalıdır.
ç) Kayıtlar, sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.
d) Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.
e) Kayıtlar, sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.
f) Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.
g) Denetimler, Bilgi İşlem Birimi tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.

(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.

Ağ cihazları güvenlik esası

MADDE 19- (1) Ağ cihazları güvenlik esası ile ilgili kurallar aşağıda belirtilmiştir.

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

b) Ağ cihazları kimlik tanımlama için LDAP, RADIUS veya TACAS+ protokollerinden birini kullanmalıdır.
c) Kurumun standart olan SNMP community stringleri kullanılmalıdır. Bu bilgi sadece yetkilendirilmiş kişiler tarafından bilinmelidir.
ç) Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin/mesai saatleri dışında üretim ortamına taşınmalıdır.
d) Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.
e) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlenmelidir.

Ağ yönetim esası

MADDE 20- (1) Ağ yönetim esası ile ilgili kurallar aşağıda belirtilmiştir.

a) Ağ cihazları 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, 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) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.
f) 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.
g) Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.
ğ) Bilgisayar ağına bağlı bütün bilişim makinelerinde (bilgisayar, tablet, vb.) kurulum ve yapılandırma parametreleri, Kurumun güvenlik esas ve standartlarıyla uyumlu olmalıdır.
h) Sistem tasarımı ve geliştirilmesi yapılırken Kurum tarafından onaylanmış olan ağ arayüzü ve protokolleri kullanılmalıdır.
ı) İnternet trafiği, İnternet Erişim ve Kullanım Esası ile ilgili standartlarda anlatıldığı şekilde izlenebilmektedir.
i) Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. Şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.
j) Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.
k) Ağ cihazları yapılandırması bilgi işlem birimi denetiminde yapılmalı ve değiştirilmelidir.
l) Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

Uzaktan erişim esası

MADDE 21- (1) Uzaktan erişim esası 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, PPTD, L2TP vs. protokollerinden birini seçmelidir.
b) Uzaktan erişim güvenliği denetlenmelidir.
c) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

ç) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.
d) Mobil hatlar 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 gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

Kablosuz iletişim esası

MADDE 22- (1) Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.

(2) 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. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.
c) Cihaza erişim için güçlü bir parola kullanılmalı ve erişim parolaları varsayılan ayarda bırakılmamalıdır.
ç) Varsayılan SSID isimleri kullanılmamalı ve SSID yayan cihaz içerisinde kurumla ilgili bilgi olmamalıdır. (Kurum, ilgili bölüm, çalışanların ismi vb.)
d) Radyo dalgalarının binanın dışına taşmamasına özen gösterilmeli ve bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.
e) Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Kurum kullanıcı adı ve parola bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Kurum kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.
f) Erişim cihazları üzerinden gelen kullanıcılar firewall üzerinden ağa dâhil olmalıdırlar.
g) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Kurumun 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 esası

MADDE 23- (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 vb.)
b) Envanter bilgileri sık sık kontrol edilmeli ve bu şekilde bilgi eksikliğinin yol açacağı kayıp ve maliyetlere engel olunmalıdır.

Kriz / Acil durum esası

MADDE 24- (1) Acil durum esası ile ilgili kurallar aşağıda belirtilmiştir.

a) Acil durum sorumluları atanmalı, yetki ve sorumlukları belirlenmeli ve dökümente edilmelidir.
b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalı ve olumsuz 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, uzaktan kopyalama, yerel kopyalama ve pasif sistem çözümleri hayata geçirilmeli ve 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 esaslar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
g) Bir güvenlik ihlali yaşandığında ilgili birime bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
ğ) Acil durumlarda bilgi işlem birimi sorumlusuna erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmelidir. Ayrıca zararın tespit edilerek, önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
h) Bilgi işlem birimi sorumlusu tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

Fiziksel güvenlik esası

MADDE 25- (1) Fiziksel Güvenlik ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurum binasının 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 altyapılarının oluşması sağlanmalıdır.
c) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi, güvenlik görevlileri gözetiminde gerçekleştirilmelidir.
ç) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
d) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.
e) Kritik sistemler özel sistem odalarında tutulmalıdır.
f) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalı ve iklimlendirilmesi sağlanmalıdır.
g) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

Kimlik doğrulama ve yetkilendirme esası

MADDE 26- (1) Kimlik doğrulama ve yetkilendirme esası ile ilgili kurallar aşağıda belirtilmiştir.

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

edilecektir.

b) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve dokümente edilecektir.
c) Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletimim sistemleri ve logon olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, dokümente edilmeli ve denetim altında tutulmalıdır.
ç) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
d) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız erişim istekleri/girişimleri incelenmelidir.
e) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
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. Uyumsuzluk durumunda, dokümanlar ve yetkiler düzeltilerek uyumlu hale getirilmelidir.

Veritabanı güvenlik esası

MADDE 27- (1) Veritabanı 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) Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.
d) Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme esasları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedekler düzenli olarak kontrol altında tutulmalıdır.
e) Yedekleme planları dokümante edilmelidir.
f) Yedekli disk üniteleri üzerinde tutulan log kayıtları 1 yıl süre ile saklanmalıdır.
g) Veritabanı erişim esasları "Kimlik Doğrulama ve Yetkilendirme" esasları çerçevesinde oluşturulmalıdır.
ğ) Hatadan arındırma ve bilgileri yedekten alma kuralları "Acil Durum Yönetimi" esaslarına uygun olarak oluşturulmalı ve dokumante edilmelidir.
h) Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
ı) Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında 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) Veritabanı sunucusu sadece ssh, rdp, ssl ve veritabanının orijinal yönetim yazılımına açık olmalı; ftp, telnet, vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır. Ancak ftp, telnet vb. açık metin şifreli bağlantılar veri tabanı sunucudan dışarıya yapılabilir.
m) Uygulama sunucularından veritabanına login vb. şekilde erişememelidir.
n) Veritabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılmalı ve root veya admin şifresi, tanımlı kişi/kişilerde olmalıdır.
o) Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.

ö) Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.
p) Veritabanı yöneticiği yetkisi sadece bir kullanıcıda olmalıdır.
r) Veritabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
s) Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmeli ve veritabanı sunucularına ancak yetkili kullanıcılar erişebilmelidir.
ş) Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapamamalı ve istekler arayüzden sağlanmalıdır. (Örnek; Kullanıcıların tablolardan "select" sorgu cümleciklerini yazarak sorgulaması vb.)
t) Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması)
u) Bütün şifreler düzenli aralıklarla değiştirilmeli ve detaylı bilgi için şifreleme esasına uyulmalıdır.
ü) Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları, uygulama sunucuları için de geçerlidir.

Değişim yönetim esası

MADDE 28- (1) Değişim yönetim esası 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) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.
d) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
e) Teknoloji değişikliklerinin Kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir.

Bilgi sistemleri yedekleme esası

MADDE 29- (1) Bilgi sistemleri yedekleme esası 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 bilgilerini ve kurumsal veriler düzenli olarak yedeklenmelidir.
b) Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde/farklı disk sistemlerinde yedekler alınmalıdır.
c) Veriler bilgi işlem odalarından farklı odalarda veya binalarda güvenli bir şekilde offline ortamlarda en az 1 (bir) yıl süreyle saklanmalıdır.
ç) Kurumsal kritik verilerin saklandığı veya sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.
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 edilmelidir.
e) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmakla birlikte bu konuyla ilgili sorumluluklar tanımlanmalıdır.

f) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
g) Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dâhil 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 periydik 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 dâhilinde tamamlanması gerekmektedir.
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 içerisinde ne zaman yapılacağı, hangi aşamalarla yedeklerin yükleneceği ve yükleme aşamasında sorunların çıkması halinde nasıl geri dönüleceği belirlenmelidir. Yedekleme ortamları ile yedekleme testlerinin ne şekilde yapılacağı hususu açıklık getirilerek hazırlanmalı ve işbirliği periyodik olarak gözden geçirilmelidir.

Personel güvenliği esası

MADDE 30- (1) Personel güvenliği esası 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 ve 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) Kurum bilgi sistemlerin 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.
g) 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.
ğ) Çalışanlar, kendi 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.

h) Çalışanların güvenlik ile ilgili aktiviteleri izlenmelidir.
ı) 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 esası

MADDE 31- (1) Bakım esası 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 Genel Müdürlük Bilgi Güvenlik Esasları"na uygun davranmaları sağlanmalı ve kontrol edilmelidir.
ç) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Esası" ile ilişkili standartlar uygulanmalıdır.
d) Bakım yapıldıktan sonra gerekiyorsa tüm sistem dokümantasyonu güncellenmelidir.
e) Sistem bakımlarının ilgili esas ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığına emin olmak için, periyodik olarak uygunluk ve güvenlik testleri yapılmalıdır.
f) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "Genel Müdürlük Bilgi Güvenlik Esasları" uyarınca hareket edilmelidir.

Yazılım geliştirme esası

MADDE 32- (1) Yazılım geliştirme esası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.
b) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısın 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) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
e) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.
f) Hazırlanan sistemler 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.

Sanal özel ağ (Vpn) esası

MADDE 33-(1) Sanal özel ağ (VPN) esası ile ilgili kurallar aşağıda belirlenmiştir.

a) Genel Müdürlüğün yetkili çalışanları ve üçüncü şahıslar (programcılar, firmalar vs) VPN‟den faydalanması durumunda herhangi bir internet servis sağlayıcısını kullanabileceklerdir.
b) VPN kullanım hakkı verilen kişiler, bu hakkın yetkisiz kişilere kullandırılmamasından sorumlu olup, gerekli tedbirleri almakla yükümlüdürler.
c) VPN konfigürasyonu mümkünse tek yönlü şifreleme/one-time password authentication (token device) veya güçlü bir uzun şifre ile yapılmalıdır.
ç) Kurum ağına bağlanıldığında, PC‟den çıkan ve giren trafik sadece VPN kanalından iletilecek ve diğer bütün trafik devre dışı bırakılacaktır.
d) Çift tünel (split tunnel-aynı anda iki vpn bağlantısı) sistemine izin verilmemeli ve sadece bir ağ bağlantısına izin verilmelidir.
e) Kurumun VPN ağ geçitlerinin kurulması ve yönetimi yetkili Bilgi İşlem personeli tarafından yapılmalıdır.
f) Kurumun ağına VPN veya başka bir yöntemle bağlanan bilgisayarlar en son güncellenmiş kurumun standardı olan, antivirüs yazılımını kullanmak zorundadılar.
g) VPN kullanıcıları hat kullanılmadığı takdirde kurumun ağından 30 dakika sonra otomatik olarak bağlantıları kesilecektir. Kullanıcı tekrar bağlanmak için logon olmak zorundadır. Ping veya diğer işlemler, network bağlantısını açık tutmak için kullanılmamalıdır.
ğ) Uzaktan erişim, güvenli kanal üzerinden yapılmalıdır. (Örnek, SSH veya IPSec kullanarak)
h) Bütün güncellemeler güvenli iletişim kanalı üzerinden yapılmalıdır.
ı) Güvenlikle ilgili olaylar loglanmalı ve sonrasında değerlendirilmelidir.

ÜÇÜNCÜ BÖLÜM
Çeşitli Hükümler

Yürürlük

MADDE 34- (1) Bu yönerge Sivil Havacılık Genel Müdürünün onayı ile yürürlüğe girer.

(2) Tüm çalışanlar, Yönergenin yürürlüğe girdiği tarihten itibaren 1 ay içerisinde parolalarını bu yönergeye uygun hale getireceklerdir.

Yürütme

MADDE 35- (1) Bu yönerge hükümlerini Sivil Havacılık Genel Müdürü yürütür.