# AİLE, ÇALIŞMA VE SOSYAL HİZMETLER BAKANLIĞI
# BİLGİ GÜVENLİĞİ POLİTİKALARI
# YÖNERGESİ

## BİRİNCİ BÖLÜM
## Genel Hükümler

**Amaç**

**Madde 1-** (1) Bu Yönergenin amacı; Aile, Çalışma ve Sosyal Hizmetler Bakanlığının görevi ve konumu nedeniyle sahip olduğu elektronik ortam ve bilgilerinin paylaşımı ve güvenliği konularında bilgi çağı gereklerine uygun olarak 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, Aile, Çalışma ve Sosyal Hizmetler Bakanlığına bağlı merkez ve taşra teşkilatında bulunan bütün birimlerdeki personelin ve ilgili üçüncü taraf firma/personelin bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

**Hukuki Dayanak**

**Madde 3-** (1) Bu Yönerge, 10/7/2018 tarih ve 30474 sayılı Resmi Gazetede yayımlanan 1 sayılı Cumhurbaşkanlığı Kararnamesinin 65 ve 66 ncı maddelerine, 4/5/2007 tarih ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 6 ncı maddesine, 24/3/2016 tarih ve 6698 sayılı Kişisel Verilen Korunması Kanununa ve 06/07/2019 tarih ve 30823 sayılı Resmi Gazetede yayımlanan 2019/12 numaralı Cumhurbaşkanlığı Genelgesine dayanılarak hazırlanmıştır.

**Tanımlar**

**Madde 4-** (1) Bu Yönergede geçen;

| | |
|---|---|
| Ağ Güvenlik Duvarı | :Aile, Çalışma ve Sosyal Hizmetler Bakanlığı ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında Bakanlığın karşılaşabileceği sorunları önlemek üzere tasarlanan cihazları, |
| Ağ Güvenlik Yöneticisi | :Ağ Sistemlerinden Sorumlu Yöneticiyi, |
| Aktif Dizin | :Erişim ve yetkilendirme dizin sunucusunu, |
| Bakan | :Aile, Çalışma ve Sosyal Hizmetler Bakanını |
| Bakanlık | :Aile, Çalışma ve Sosyal Hizmetler Bakanlığını, |
| Bakanlık Üst Yönetimi | :Bakan ve Bakan Yardımcıları |
| Başkanlık | :Bilgi İşlem Dairesi Başkanlığını, |
| Bilgi Güvenliği Yöneticisi | :Bilgi Güvenliği ile ilgili çalışmaların yürütülmesi ve koordinasyonundan sorumlu yöneticiyi, |
| Bilgi Güvenliği Yönetim Sistemi | : Bir organizasyonun kritik bilgilerini korumak amacıyla sistematik bir yaklaşımla yönetebilme kabiliyeti kazanması için kurulan sistemi, |
| Bilgi İşleme | :Bilginin oluşturulması, değiştirilmesi, iletilmesi, saklanması ve imha edilme süreçlerini, |
| Bluetooth | : Kablo bağlantısını ortadan kaldıran kısa mesafe radyo frekansı (RF) teknolojisini, |
| DMZ | :Bakanlık iç ağı ile Bakanlık dış ağı birbirinden ayıran bölgeyi, |
| E-İmza | : 5070 Sayılı Elektronik İmza Kanunu'na göre "Başka bir elektronik veriye eklenen veya başka bir elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi", |
| Erişim Cihazı (Access Point) | :Dizüstü bilgisayar ve akıllı telefon gibi kablosuz cihazları kablosuz erişim standartları kullanarak kablolu ağa bağlayan aygıtları, |
| Etki Alanı | :Bakanlık aktif dizin yapısını, |

| | |
|---|---|
| Firmware | :Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımları, |
| Güvenli Kanal | :Güçlü bir şifrelemeden oluşan iletişim kanalını, |
| HTTP | :Bir kaynaktan dağıtılan ve ortak kullanıma açık olan bilgi sistemleri için uygulama seviyesindeki iletişim kuralını, |
| HTTPS | : Bir kaynaktan dağıtılan ve ortak kullanıma açık olan bilgi sistemleri için uygulama seviyesindeki güvenli iletişim kuralını, |
| IP | :Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adresi, |
| IPSec | :Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlamayı, |
| İstemci | :Sunucuların verdiği hizmeti alan bilgisayar sistemini, |
| İntranet | :Kuruluş içindeki bilgisayarları, yerel ağları (LAN) ve geniş alan ağlarını (WAN) birbirine bağlayan, çoğunlukla TCP/IP tabanlı bir ağı, |
| Kızılötesi | : Işık tayfında kırmızı bölümün ötesindeki alanda yayılmış durumda ısı ışınlarının oluşturduğu, gözle görülemeyen ışınımı, |
| Kullanıcı | :Bakanlık Bilgi Sistemlerini kullanan tüm kişileri, |
| MAC Adresi | :Bir ağ cihazının tanınmasını sağlayan kendisine özel adresi, |
| Portal | :Birden çok içeriği bir arada bulunduran alanı, |
| RADIUS | :Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolünü, |
| RDP | :Remote Desktop Protocol / Uzak Masaüstü Protokolünü, |
| Risk | :Bakanlığın bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörleri, |
| Sahte E-posta | :Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasa dışı yoldan) erişmeyi, |
| Siber Olay | :Bilişim sistemleri üzerinde gerçekleşen olayları, |
| Sistem Yöneticisi | :Bilgi Sistemleri Yöneticisini, |
| SOME | :Aile, Çalışma ve Sosyal Hizmetler Bakanlığı Siber Olaylara Müdahale Ekibini, |
| Son Kullanıcı | :Bir yazılım veya donanımın en son halini kullanan kullanıcıları, |
| Spam | :Yetkisiz ve/veya istenmeyen reklam içerikli e-postaları, |
| SSH (Secure Shell) | :Ağ üzerinde bulunan bir sunucuya bağlanmaya ve bağlanılan sunucu üzerinde komut çalıştırma, dosya transferi gibi işlemleri gerçekleştirmeye olanak sağlayan uzak sunucu bağlantı protokolünü, |
| SSL | :Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolünü, |
| Sunucu | :İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini, |
| Şifreleme | :Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritmayı, |
| Uygulama Sunucusu | :Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımını, |
| Uzaktan Erişim | :İnternet, telefon hatları veya kiralık hatlar vasıtası ile Bakanlığın ağına erişilmesini, |
| Varlık Sahibi | :Varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi ya da kişileri, |
| Veri tabanı | :Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğunu, |
| Veri sorumlusu | : 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi |

| | |
|---|---|
| Veritabanı Yöneticisi | :Veritabanı Sistemlerinden Sorumlu Yöneticiyi, |
| VLAN | :Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubunu, |
| VPN | :Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknolojiyi, |
| Yedekleme | :Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritabanı'nın başka bir yere kopyalanması işlemini, |
| Yetkilendirme | :Çok kullanıcılı sistemlerde sistem yöneticisi tarafından, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesini, |
| Zincir E-posta | :Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesini, |
| X.509/LDAP | :Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir internet protokolünü, |
| Web | : WWW, Web, ya da W3 (World Wide Web), yazı, resim, ses, film, gibi pek çok farklı yapıdaki verilere kompakt ve etkileşimli bir şekilde ulaşmamızı sağlayan sistemini, |

ifade eder.

## İKİNCİ BÖLÜM
## Bilgi Güvenliği Politikaları

**Bilgi Güvenliği Politikası**

**Madde 5-** (1)İş hedeflerine ulaşmak için kurumun değerli bilgi birikimini oluşturan ve paydaşlara katma değer sağlayan bilgi varlıkları çeşitli ortamlarda üretilmekte, paylaşılmakta ve saklanmaktadır. Bakanlık iş süreçleri büyük ölçüde bu bilgilerin işlendiği bilgi ve iletişim sistemlerine bağımlıdır.

Bakanlık bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini temin etmek için uyulması gereken temel kurallar iş bu yönergede tanımlanmıştır. Ayrıca Bilgi Güvenliği Yönetim Sistemi kapsamında oluşturulan diğer alt politikalarda ve prosedürlerde de uyulması gereken diğer kurallar tanımlanmıştır.

**Bilgi Sistemleri Genel Kullanım Politikası**

**Madde 6-** (1) Bilgi sistemlerine sahip olma ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir.

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

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

c)Hukuki olarak yetkilendirilmiş kişiler ve Bakanlık denetim birimleri ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

ç)Bakanlık bilgisayarları etki alanına dâhil edilmelidir.

d)Bilgisayarlarda oyun, eğlence, kumar vb. kişisel kullanıma yönelik programlar çalıştırılmamalı ve kopyalanmamalıdır.

e)Bakanlıkta Bilgi İşlem Dairesinin bilgisi ve onayı olmadan Bakanlık ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.

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

g)Bilgisayarlara lisanssız program yüklenmemelidir.

ğ)Bilgisayar kaynakları paylaşıma açılmamalıdır.

h) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar vermemeli, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunmamalı, kaynakların içeriğini izinsiz olarak değiştirmemelidir.

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

a)Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda bağlı olunan birime haber verilmelidir.
b)Bütün cep telefonu, tablet vb. mobil cihazlar Bakanlığın ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızılötesi, bluetooth, vb.) özellikleri aktif halde olmamalıdır ve mümkünse güncel anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.
c)Kullanıcılar tarafından gönderilen e-postalarda Aile, Çalışma ve Sosyal Hizmetler Bakanlığı sorumluluk reddini ifade eden açıklayıcı metin yer almalıdır.
ç)Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. Büyük boyutlu dosyalar e-posta ile gönderilmemelidir. Bu tür dosyalar Bakanlığın dosya paylaşım sistemi üzerinden iletilmelidir. E-posta ile gönderilen dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalıdır.
d) Doğrudan çalıştırılabilir dosyalar e-posta ile iletilmemelidir.

**Son Kullanıcı Güvenliği Politikası**
**Madde 7-** (1) Son Kullanıcı Güvenliği Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.
a)Bakanlık intranet uygulamalarını kullanan kullanıcılar, sistemlere etki alanları dâhilinde kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanmalıdır.
b)Her bir son kullanıcının yalnızca bir adet kullanıcı hesabı olmalıdır.
c)Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir.
ç)Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı 5651 sayılı kanuna uygun olarak kayıt altına alınmalıdır.
d)Güvenlik zafiyetlerine karşı, son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır.
e)Son kullanıcılar bilgisayarlarındaki ve sorumlusu oldukları cihazlardaki verilerden kendileri sorumludur.
f)Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka bilgisayarlar ekranlarını kilitlemelidir.
g)Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde harici veri depolama cihazları (e-imza ve kart okuyucusu, bellek ve/veya harici hard disk gibi taşınabilir medya araçları) bırakmamalıdır.
ğ)Son kullanıcılar, mesai bitiminde bilgisayarlarını ve çevre donanımlarını (yazıcı, monitör, hoparlör...) kapatmalıdır.
h)Bakanlık, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulayabilir.
ı)Bakanlık, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişikleri merkezi grup politikalarıyla engelleyebilir.
i)Temiz masa, temiz ekran ilkesi benimsenmeli ve hayata geçirilmelidir.
j)Kullanıcılar, Bakanlık mevcut envanteri haricindeki donanımları Bakanlık bilgisayarlarında kullanmamaya özen göstermelidir.
k)Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
l)Dosya paylaşım alanı ihtiyacı olması durumunda sadece Bakanlığın dosya sunucusu üzerinden yetkilendirilmiş personele erişim izni verilmelidir. Bunun dışında paylaşım yapılmamalıdır.

**Parola Politikası**
**Madde 8-** (1) Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.
a)Yönetici ve kullanıcı yetkisine sahip hesaplara ait parolalar en geç 90 (doksan) günde bir değiştirilmelidir. Parola yenileme işlemi esnasında son 3 parola ile aynı olmayan bir parola girilmelidir.
b)Sistem yöneticilerinin, sistem ve kullanıcı hesapları farklı olmalıdır.
c)Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir ve otomatik parola anımsama seçenekleri işaretlenmemelidir.
ç)Kullanıcı, parolasını başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazması durumunda güvenliğini sağlamalıdır.

d)Kullanıcıya ilk verilen veya sıfırlanması istenilen parolalar "geçici parola" olarak verilir ve ilk oturum açılışında değiştirilmelidir.
e)Kritik sistemlere ve ağ cihazlarına erişim için sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Bunun mümkün olmadığı durumlarda varsayılan parolalar değiştirilmelidir.
f) Genel kural olarak, parola girilen web adresleri HTTPS protokolü kullanmalıdır.
(2) Kullanıcı, güçlü bir parola oluşturmak için, aşağıda belirtilen maddelere uymalıdır.
En az 3 tanesine uyulması zorunlu olanlar:
a)En az 8 haneli olmalıdır.
b)İçerisinde en az 1 tane küçük ve 1 tane büyük harf bulunmalıdır. (a, b, A,B ..)
c)İçerisinde en az 1 tane rakam bulunmalıdır. (1, 2, 3...)
ç)İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,$,#,&,/,{,*,-,],=,...)
Uyulması tavsiye edilenler:
d)Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, bbbb ...)
e)Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)
f)Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli, doğum tarihi, adres, telefon 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)Güvenlik testleri sırasında parola kırma ve tahmin etme operasyonları bilgi güvenliği yetkililerince yapılabilir. Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilir. Tahmin edilen veya kırılan parolalar üçüncü kişilerle paylaşılamaz.
(4) Uygulama Geliştirme Standartları;
a)Bireylerin ve/veya grupların kimlik doğrulaması işlemini desteklemelidir.
b)Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.
c)Parolalar, şifrelenmiş olarak saklanmalıdır.
ç)Uygulama geliştirme standartları en az RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

**E-Posta Politikası**
**Madde 9-** (1) E-Posta ile ilgili kullanım kuralları aşağıda belirtilmiştir.
a)Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.
b)Bakanlığa ait "gizlilik" içeren bilgiler e-posta ve eklerinde bulunmamalıdır.
c)Kullanıcılar, Bakanlığın e-posta sistemini taciz ve suiistimal etmemelidir, küçük düşürücü, hakaret edici veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Bakanlık Siber Olaylara Müdahale Ekibine (some@ailevecalisma.gov.tr) adresine iletilmelidir.
ç)Kurumsal iletişim gerektiren durumlarda Kurumsal e-posta adresleri kullanılmalıdır. Kullanıcılara tahsis edilen Bakanlık e-posta hesabının güvenliğinden kullanıcılar sorumludur. Bu e-posta hesapları Bakanlık işlerinin gerçekleştirilmesi için kullanılmalı, iş dışı konularda kullanılmamalıdır.
d)Kaynağı bilinmeyen oltalama (phishing), kullanıcı kodu/parolasını girmesini isteyen, zincir mesajlar, ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında açılmadan, başkalarına iletilmeden, herhangi bir işlem yapmaksızın (some@ailevecalisma.gov.tr) adresine iletilmelidir.
e)Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
f)Kullanıcılar, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
g)Kullanıcılar, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret, küfür veya iftira içeren, ahlaka aykırı mesajların gönderilmesinden sorumludur.
ğ)6 ay süreyle kullanılmamış e-posta hesapları, kullanıcıya haber vermeden sunucu güvenliği için Başkanlık tarafından pasif hale getirilmelidir.
h)Her bir kullanıcının yalnızca 1 adet e-posta hesabı olmalıdır. Grup e-postaları için kullanıcı hesabı açılmamalıdır.

ı) Kullanıcılar e-posta gönderiminde ad, soyad, iletişim bilgisi, kurum, birim adı gibi alanları içeren imza şablonu kullanmalıdır.
i) Bakanlık dışında, güvenliğinden emin olunmayan bir bilgisayar üzerinden kurumsal Web Posta Sistemi kullanılmamalıdır.
(2)Kurumsal e-postalar, resmi yazı ile gelen talepler doğrultusunda, hukuki olarak yetkilendirilmiş kişilerce tutanak altında denetlenebilir.
(3)Kullanıcıların e-postalarına erişirken, HTTP vb. kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanmamaları sağlanmalıdır. Genel kural olarak, parola girilen adreslerin HTTPS olmasına dikkat edilmelidir.
(4)Bakanlık, e-postaların Bakanlık bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.
(5)Virüs veya diğer zararlı kodlar bulaşmış olan e-postalar anti-virüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenmelidir.

**İnternet Erişim ve Kullanım Politikası**
**Madde 10-** (1) İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Kullanıcıların internet erişimlerinde firewall, anti-virüs, URL filtreleme vs. güvenlik kriterleri uygulanmalıdır.
b)Bakanlığın politikaları doğrultusunda en az kategori ve uygulama bazlı filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (terör, pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.
c)Bakanlığın ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.
ç)Kullanıcılar internete Bakanlık tarafından sağlanan kullanıcı adı/şifre (LDAP vb.) ile erişmelidir. Ayrıcalıklı erişim yetkileri ihtiyaç halinde gerekçelendirilerek Başkanlık tarafından belirli bir süre ile sınırlı olarak verilebilir.
d)Hizmet kalitesinin sağlanması amacıyla Bakanlık uygulamaları erişimde önceliklendirme yapılarak internet erişimi ve bant genişliğinde düzenleme yapılabilir.
e)İş ile ilgili olmayan dosyalar (müzik, video vs. dosyaları) gönderilmemeli, paylaşılmamalı ve indirilmemelidir. Dosya paylaşım uygulamaları kullanılmamalıdır. Bu konuda sorumluluk kullanıcıya aittir.
f)Bakanlık tarafından onaylanmamış yazılımlar internet üzerinden indirilmemelidir ve Bakanlık sistemlerine yüklenmemelidir.
g) Bakanlık içerisinden yapılan internet erişimlerinde 5651 sayılı kanun gereği Bakanlık ilgili erişim bilgilerini tutmak ve devletin ilgili mercileri tarafından istenmesi durumunda bu bilgiyi sağlamakla yükümlüdür. Bakanlık, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgileri hukuki olarak yetkilendirilmiş kişilere verebilir.

**Uzaktan Erişim Politikası**
**Madde 11-** (1) Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Internet üzerinden Bakanlık ağına erişen kişiler ve/veya kurumlar güvenli protokoller kullanmalıdırlar. Web tabanlı uygulama erişimleri sadece yetkili idari yöneticilere bir üst amirinin onayı ile Başkanlık tarafından verilir. Sunucu tabanlı erişimler (RDP, SSH) iş sürekliliği kapsamında ihtiyaç halinde verilir. RDP, SSH ve VPN haricinde sadece Bakanlığın belirlediği uygulama üzerinden erişim sağlanır.
b)Uzaktan erişimler Başkanlık tarafından kayıt altına alınmalıdır.
c)Bakanlık çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
ç)Bakanlık ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti-virüs yazılımı güncellemeleri yapılmış olmalıdır.
d)Bakanlık personeli haricinde üçüncü şahıslara istisnai durumlar dışında uzak erişim izni verilmemelidir.

**Kablosuz İletişim Politikası**
**Madde 12-** (1)Bakanlığın bilgisayar ağına bağlanan bütün cihazların erişim bilgileri Başkanlık tarafından kayıt altına alınmalıdır.
(2)Bütün kablosuz erişim cihazları Bilgi İşlem Dairesi Başkanlığı tarafından belirlenen güvenlik ayarlarını kullanmalıdır.

(3)Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.
a)Kablosuz cihazlar güçlü şifreleme protokolleri kullanmalıdır.
b)Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Bakanlık kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Bakanlık kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.
c)Erişim cihazları üzerinden gelen kullanıcılar ağ güvenlik duvarı üzerinden ağa dâhil olmalıdırlar.
ç)Kullanıcı bilgisayarlarında güncel anti-virüs ve işletim sistemi güvenlik duvarı yazılımları yüklü olmalıdır.
d)Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

**Anti-Virüs Politikası**
**Madde 13-** (1) Anti-virüs Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Bakanlığın tüm istemcileri ve sunucuları güncel anti-virüs yazılımına sahip olmalıdır. Ancak sunucu yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak anti-virüs yazılımı yüklenmeyebilir.
b)İstemcilere ve sunuculara zararlı yazılım bulaştığı fark edildiğinde ağ erişimi sınırlandırılabilir.
c)Bilgi İşlem Daire Başkanlığı anti-virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
ç)Kullanıcı hiç bir sebepten dolayı anti-virüs yazılımını bilgisayarından kaldırmamalıdır.
d)Harici veri depolama cihazları her kullanımda anti-virüs kontrolünden geçirilmelidir.
e)Kullanılan anti-virüs yazılımı üzerinde düzenli taramalar yapılacak şekilde konfigürasyonlar yapılmalıdır.

**İşletim Sistemleri Güvenliği Politikası**
**Madde 14-** (1) İşletim Sistemleri Güvenliği Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.
a)Bakanlık, son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar verir ve bu işletim sistemine uygun yazılım ve donanım sistemlerinin kurulumunu temin eder.
b)Bakanlık, işletim sistemlerinin güncel ve güvenli olması için yama yönetimi yapar.
c)Sunucu işletim sistemlerinde kurulumda gelen yönetici hesaplarının (Administrator, root vb.) kaba kuvvet saldırılarıyla ele geçirilmesine karşı, gerekli önlemler alınır.

**Fiziksel Güvenlik Politikası**
**Madde 15-** (1) Fiziksel Güvenlik ile ilgili kurallar aşağıda belirtilmiştir.
a)Bakanlığın 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)Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
ç)Bakanlık dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili personel gözetiminde gerçekleştirilmelidir.
d)Kritik bilgilerin bulunduğu alanlara girişler kontrolü bir şekilde yapılmalı ve izlenmelidir.
e)Her ziyaretçi için kayıt tutulmalı ve her bir ziyaretçiye bir adet ziyaretçi kartı verilmelidir.
f)Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.
g)Kritik sistemler sistem odalarında barındırılmalıdır.
ğ)Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalı ve iklimlendirilmesi sağlanmalıdır.
h)Kritik bilgi içeren ofisler ve odalar kolay erişilebilir yerlerde konumlandırılmamalıdır,
ı)Kritik bilgi içeren ofisler ve odalar için işaret, tabela vb. bulunmamasına dikkat edilmelidir,

**Personel Güvenliği Politikası**
**Madde 16-** (1) Personel Güvenliği Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları ilgili Başkanlık/Birim tarafından imzalanmalıdır.
b)Kurumsal bilgi güvenliği bilinçlendirme eğitimleri Başkanlık tarafından düzenlenmelidir.

c)İş tanımı değişen veya Bakanlıktan ayrılan kullanıcıların erişim haklarının kaldırılması için ivedilikle Başkanlığa bilgi verilmelidir. Birim amiri, ilgili çalışanın, Kuruma ait bilgi varlıklarını(yazılım donanım vs.) teslim etmesini sağlamalıdır.
ç)Bakanlık 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.
d)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 kullanıcılara gereğinden fazla yetki verilmemesidir. Sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmalıdır.
e)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.
f)Tüm çalışanlar, yükleniciler ve üçüncü taraflar Bakanlığın politika ve prosedürlerine uymak zorundadır.

**Sunucu Güvenlik Politikaları**
**Madde 17-** (1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.
a)Bakanlıkta bulunan sunucuların yönetiminden, ilgili sunucu üzerinde yetkilendirilmiş personel sorumludur.
b)Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılmalıdır.
c)Sunuculara ait bilgilerin yer aldığı güncel sunucu envanter bilgisi tutulmalıdır.
(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.
a)Sunucuyu kullanan birim tarafından, kullanılmayan servisler ve uygulamalar kapatılmalıdır.
b)Sunuculara yetkisiz kişilerin erişmesine engel olmak için gerekli önlemler alınmalıdır.
c)Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve anti-virüs vb. koruma amaçlı yazılımlar güncel tutulmalıdır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, hizmeti aksatmayacak şekilde kontrollü olarak yapılmalıdır.
ç)Sistem yöneticileri özel durumlar dışında 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.
d)Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
e)Sunucu ağları kullanıcı ağlarından ayrılmalıdır.
f)Sunucular üzerine lisanslı yazılımlar kurulmalıdır.
g)Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.
(3) 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 kayıt edilmelidir.

**Ağ Yönetim Politikası**
**Madde 18-** (1) Ağ yönetim politikası 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)Sınırsız ağ dolaşımı engellenmelidir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaca göre açılmalıdır.
ç)İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.

d)Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır. Kullanıcı bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılmalı ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanmalıdır.
e)Bilgisayar ağına bağlı bütün cihazlarda kurulum ve yapılandırma parametreleri, Bakanlığın güvenlik politika ve standartlarıyla uyumlu olmalıdır.
f)Ağ trafiği düzenli olarak izlenmeli ve ölçülmelidir.
(2)Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.
a) Ağ cihazlarının güncel envanter ve topoloji bilgileri tutulmalı, bu bilgilere erişim yetkileri kullanıcı listesi oluşturulmalıdır.
b)Özel durumlar haricinde yerel kullanıcı hesapları kullanılmamalıdır. Ağ cihazları kimlik tanımlama için (LDAP, RADIUS veya TACACS+ gibi) güvenli protokollerden birini kullanmalıdır.
c)Yazılım ve firmware güncellemeleri önce test edilmeli ve mesai saatleri dışında yapılmalıdır.
ç)Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.
d)Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları vb.) etiketlenmelidir.
e)Her bir yönlendirici ve anahtar *"Bu Cihaza Yetkisiz Erişimler Yasaklanmıştır. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut kayıt altına alınır. Bu politikaya uyulmamasının disiplin hukuku ve ceza hukuku açısından yaptırımı olabilir."* uyarı yazısına sahip olmalıdır. Yönlendiriciye erişen tüm kullanıcıları uyarmalıdır.
f)Cihazlara erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.
g)Yazıcı, fotokopi cihazı, faks cihazı gibi cihazların bulunduğu ağlar kritik sistemlerin bulunduğu ağlardan ayrılmalıdır

**Donanım ve Yazılım Envanteri Oluşturma Politikası**
**Madde 19-** (1) Donanım ve yazılım envanteri oluşturma ile ilgili kurallar aşağıda belirtilmiştir.
a)Oluşturulan envanter tablosunda şu bilgiler olmalıdır: seri/etiket no, donanım/yazılım adı, fonksiyonu, varsa ip adresi fiziksel yeri, sahibi vs.
b)Envanter bilgileri değişiklik olduğunda güncellenmelidir. Bu şekilde bilgi eksikliğinin yol açacağı kayıp ve maliyetlere engel olunmalıdır. Envanter bilgilerinin güncel olmaması nedeniyle yaşanabilecek kayıp ve maliyetlerden, varlık sahipleri sorumlu olacaktır.

**Kriz / Acil Durum Politikası**
**Madde 20-** (1) Acil Durum politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Acil durum sorumluları atanmalı, yetki ve sorumlulukları belirlenmeli ve yazılı hale getirilmelidir.
b)Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır.
c)Bilişim sistemlerinin kesintisiz çalışmasının sağlanması için sistemler tasarlanırken minimum sürede iş kaybı hedeflenmelidir.
ç)Acil durumlarda Bakanlık içi işbirliği gereksinimleri tanımlanmalıdır.
d)Acil durumlarda sistem kayıtları incelenmek üzere saklanmalıdır.
e)Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
f)Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
g)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.

**Kimlik Doğrulama ve Yetkilendirme Politikası**
**Madde 21-** (1) Kimlik Doğrulama ve Yetkilendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Bakanlık bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama ve sistemler üzerindeki kullanıcı yetkileri belirlenmeli ve denetim altında tutulmalıdır.
b)Erişim hakları tanımlanırken ihtiyacı kadar ilkesi (need to know) göz önünde bulundurulmalıdır.
c)Üçüncü tarafların tüm erişimleri kayıt altına alınmalıdır. İşi biten firmaların hesapları kapatılmalıdır.

ç)Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız erişim istekleri/girişimleri incelenmelidir.
d)Kullanıcı hareketlerini doğru bir şekilde kayıt altına almak için her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
e)Son kullanıcıların yetkileri, içinde bulundukları grup politikasına göre belirlenmelidir.

**Veri Tabanı Güvenlik Politikası**
**Madde 22-** (1) Veri tabanı güvenlik kuralları aşağıda belirtilmiştir.
a)Veri tabanı sistemleri envanteri güvenli şekilde tutulmalı, saklanmalı ve bu envanterden sorumlu personel tanımlanmalıdır.
b)Veri tabanı işletim prosedürleri belirlenmeli ve yazılı hale getirilmelidir.
c)Veri tabanı sistem olay 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 buna uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.
e)Yedekleme planları yazılı hale getirilmelidir.
f)Veri tabanı erişim politikaları "Kimlik Doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.
g)Bilgi saklama medyaları kontrolsüz olarak Bakanlık dışına çıkartılmamalıdır.
ğ)İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.
h)Veri tabanı sunucusu sadece güvenli erişim protokolleri ile erişim sağlanmalıdır.
ı)Veri tabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak Bakanlığın kasasında saklanmalı ve gereksiz yere açılmamalıdır.
i)Veri tabanı sunucusuna ancak zorunlu hallerde ayrıcalıklı erişim ("root" "admin" vb..) yetkisi ile bağlanılmalıdır. Ayrıcalıklı erişim yetkili kullanıcılar kişilerin kendi adına özel oluşturulmalı ve ortak kullanılmamalıdır.
j)Veri tabanına doğrudan bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.
k) Veri tabanına doğrudan bağlanan kullanıcıların yaptıkları işlemler kaydedilmelidir.
l)Veri tabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir.

**Değişim Yönetim Politikası**
**Madde 23-** (1) Değişim Yönetim Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri yazılı hale getirilmelidir.
b)Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.
c)İş kritik bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek sistem ve uygulamalar ilgili birim(ler) tarafından belirlenmeli ve yazılı hale getirilmelidir.
ç)Yapılacak değişiklikler öncelikle mümkünse bir test ortamında denenmelidir.
d)Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı ve güncel tutulmalıdır.
e)Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı, geri dönüş planları test edilmeli ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
f)Sistemlerde oluşacak problemlere yönelik bakım, onarım, yama, güncelleme ve değişiklikler ile ilgili çalışmalardan önce varlık sahibine ve proje paydaşlarına bilgi verilmelidir. Sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

**Bilgi Sistemleri Yedekleme Politikası**
**Madde 24-** (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)Veri yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceğinin kritiklik derecesine göre belirlenmesi ve yazılı hale getirilmesi veri sorumlularının sorumluluğundadır.
c)Yedek medyaları mümkün olduğunca verilerin oluştuğu fiziksel ortamlardan faklı yerlerde veya binalarda güvenli bir şekilde saklanmalıdır.
ç)Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
d)Son kullanıcılar kendi bilgisayarlarındaki verilerin yedeklenmesinden kendileri sorumludurlar.

**Bakım Politikası**
**Madde 25-** (1) Bakım Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Bakanlık sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli bütçe ayrılmalıdır.
b)Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
c)Firma teknik destek elemanlarının bakım yaparken bu yönergeye 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 tüm sistem dokümantasyonu güncellenmelidir.
e)Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda, bu yönerge uyarınca hareket edilmelidir. Güvenlik açıkları Bakanlık Siber Olaylara Müdahale Ekibine (some@ailevecalisma.gov.tr adresine) bildirilmelidir.
f)Bakanlık içinde firmalar tarafından bakımı ve onarımı yapılan sistemlerde, bakım işlemi yetkili bir çalışanın gözetiminde yapılmalı ve sistemden bilgi alınmasına engel olunmalıdır.
g)Depolama ortamının (örn. sabit disk) bakım, onarım gibi amaçlarla Bakanlık dışına çıkarıldığı durumlar kayıt altına alınmalı ve firma yetkilisi tarafından imzalanmalıdır. Gerekli durumlarda firma ile gizlilik sözleşmesi imzalanmalıdır.

**Yazılım Geliştirme Politikası**
**Madde 26-** (1) Yazılım Geliştirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Yazılım planlama aşamasında güvenlik ihtiyaçları planlanmalıdır.
b)Yazılım Bakanlık Bilgi Güvenliği Politikalarına uygun olarak geliştirilmeli, yetkisiz kişilerin müdahale etmesi şifreleme işlemleri ile engellenmelidir.
c)Yazılım kodları dışarıdan erişime kapalı olan bir ortamda saklanmalıdır.
ç)Yazılım geliştirme, test ve uygulama ortamları ayrılmalı, her biri için özel olarak tahsis edilmiş ayrı sistemler kullanılmalıdır.
d)Yazılım geliştirme süreçleri uluslararası kabul görmüş proje yönetim mantığına uygun şekilde yazılı hale getirilmelidir. (yazılımın veri akışı ve işleme özelliklerini içeren tasarım belgesi, vb.)

## ÜÇÜNCÜ BÖLÜM
## Çeşitli Hükümler

**Yaptırım**
**Madde 27-**(1) Bu yönergeye uyulmadığının tespit edilmesi halinde, bu ihlalden sorumlu olan çalışan ya da 3. taraf için geçerli olan usul, esas ve sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır. Cezai yaptırımlarda öncelik hukuki, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere aittir.

**Üçüncü Tarafların Yönetimi**
**Madde 28-** (1) Bakanlık çalışanı olmayıp bilgi sistemleri kaynaklarına erişim sağlayan her türlü kişi üçüncü taraf olarak kabul edilir. Üçüncü taraf tanımına uyan her türlü kişi ya da kurumla yapılacak geçici ya da sürekli çalışma sözleşmelerin imzalanması güncel olarak takip edilir. Sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları hazırlanıp kurumlarla kurumsal, şahıslar ile bireysel gizlilik sözleşmeleri yapılır. Üçüncü taraf çalışanları Bakanlık politikalarına uymak zorundadır.

**Yönetimin Taahhüdü**

**Madde 29-** (1) Bakanlığın, belirlediği hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sistemini TS ISO/IEC 27001 standardına uyumlu hale getirecek şekilde kurar ve yürütür.

(2) Bakanlık Üst Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.

(3) Bakanlık Üst Yönetimi, bilgi güvenliği kapsamında yapılan çalışmalar için gerekli bütçeyi temin eder.

**Sorumluluk**

**Madde 30-**(1) Bakanlığın bütün çalışanları "Bilgi Güvenliği Politikalarını" bilmek ve uygulamak ile yükümlüdür. Aksi belirtilmedikçe 3. taraflar da bu politikaya uymakla yükümlüdür.

**Yürürlükten Kaldırılan Yönerge**

**Madde 31-** (1) Bu yönergenin imzalanmasıyla 08/07/2015 tarihli Aile ve Sosyal Politikalar Bakanlığı Bilgi Güvenliği Politikaları Yönergesi yürürlükten kalkar.

**Yürürlük**

**Madde 32-** (1) Bu Yönerge Aile, Çalışma ve Sosyal Hizmetler Bakanının onayı ile yürürlüğe girer.

**Yürütme**

**Madde 33-** (1) Bu Yönerge hükümlerini Aile, Çalışma ve Sosyal Hizmetler Bakanı yürütür.

**OLUR**

**... /... /2020**