AİLE VE SOSYAL HİZMETLER BAKANLIĞI
BİLGİ GÜVENLİĞİ POLİTİKALARI
YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

Madde 1 – (1) Bu Yönergenin amacı; Aile 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 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;

a. Ağ Güvenlik Duvarı: Aile ve Sosyal Hizmetler Bakanlığı ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında Bakanlığın karşılaşabileceği sorunları önlemek üzere tasarlanan cihazları,
b. Aktif Dizin: Erişim ve yetkilendirme dizin sunucusunu,
c. Bakan: Aile ve Sosyal Hizmetler Bakanını
ç. Bakanlık: Aile ve Sosyal Hizmetler Bakanlığını,
d. Bakanlık Üst Yönetimi: Bakan ve Bakan Yardımcılarını,
e. Genel Müdürlük: Bilgi Teknolojileri Genel Müdürlüğünü,
f. Bilgi Güvenliği Yöneticisi: Bilgi Güvenliği ile ilgili çalışmaların yürütülmesi ve koordinasyonundan sorumlu yöneticiyi,
g. Bilgi Güvenliği Yönetim Sistemi: Bir organizasyonun kritik bilgilerini korumak amacıyla sistematik bir yaklaşımla yönetebilme kabiliyeti kazanması için kurulan sistemi,
ğ. Bilgi İşleme: Bilginin oluşturulması, değiştirilmesi, iletilmesi, saklanması ve imha edilme süreçlerini,
h. Bluetooth: Kablo bağlantısını ortadan kaldıran kısa mesafe radyo frekansı (RF) teknolojisini,
ı. BTGM: Bilgi Teknolojileri Genel Müdürlüğünü,

ı. DMZ: Bakanlık iç ağı ile Bakanlık dış ağı birbirinden ayıran bölgeyi,
j. 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",
k. Erişim Cihazı (Access Point): Dizüstü bilgisayar ve akıllı telefon gibi kablosuz cihazları kablosuz erişim standartları kullanarak kablolu ağa bağlayan aygıtları,
l. Etki Alanı: Bakanlık aktif dizin yapısını,
m. Güvenli Kanal: Güçlü bir şifrelemeden oluşan iletişim kanalını,
n. HTTP: Bir kaynaktan dağıtılan ve ortak kullanıma açık olan bilgi sistemleri için uygulama seviyesindeki iletişim kuralını,
o. HTTPS: Bir kaynaktan dağıtılan ve ortak kullanıma açık olan bilgi sistemleri için uygulama seviyesindeki güvenli iletişim kuralını,
ö. IP: Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adresi,
p. 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,
r. İstemci: Sunucuların verdiği hizmeti alan bilgisayar sistemini,
s. İntranet: Kuruluş içindeki bilgisayarları, yerel ağları (LAN) ve geniş alan ağlarını (WAN) birbirine bağlayan, çoğunlukla TCP/IP tabanlı bir ağı,
ş. Kızılötesi: Işık tayfında kırmızı bölümün ötesindeki alanda yayılmış durumda ısı ışınlarının oluşturduğu, gözle görülemeyen ışınımı,
t. Kullanıcı: Bakanlık Bilgi Sistemlerini kullanan tüm kişileri,
u. Portal: Birden çok içeriği bir arada bulunduran alanı,
ü. RADIUS: Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolünü,
v. Risk : Bakanlığın bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörleri,
y. Sahte E-posta: Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasa dışı yoldan) erişmeyi,
z. Siber Olay: Bilişim sistemleri üzerinde gerçekleşen olayları,
aa. Sistem Yöneticisi: Bilgi Sistemleri Yöneticisini,
bb. SOME: Aile ve Sosyal Hizmetler Bakanlığı Siber Olaylara Müdahale ekibini,
cc. Son Kullanıcı: Bir yazılım veya donanımın en son halini kullanan kullanıcıları,
çç. Spam: Yetkisiz ve/veya istenmeyen reklam içerikli e-postaları,
dd. 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,
ee. SSL: Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolünü,
ff. Sunucu: İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini,
gg. Şifreleme: Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritmayı,
ğğ. Uygulama Sunucusu: Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımını,
hh. Uzaktan Erişim: İnternet, telefon hatları veya kiralık hatlar vasıtası ile Bakanlığın ağına erişilmesini,
ıı. Varlık Sahibi: Varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi ya da kişileri,

ıı. Veritabanı: Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğunu,
jj. 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 kişiyi,
kk. Veritabanı Yöneticisi: Veritabanı Sistemlerinden Sorumlu Yöneticiyi,
ll. 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,
mm. VPN: Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknolojiyi,
nn. Yedekleme: Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritabanı'nın başka bir yere kopyalanması işlemini,
oo. Yetkilendirme: Çok kullanıcılı sistemlerde sistem yöneticisi tarafından, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesini,
öö. Zincir E-posta: Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesini,
pp. X.509/LDAP: Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir internet protokolünü,
rr. 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.
(2) Bilgi Teknolojileri Genel Müdürlüğü bu yönergenin uygulanması ile ilgili olarak Bilgi Güvenliği Politikaları Kılavuzu hazırlayabilir ve gerek görmesi halinde güncelleyebilir.

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. Bakanlık kullanıcı bilgisayarları etki alanına dâhil edilir.
c. Bilgisayarlarda oyun, eğlence, kumar vb. kişisel kullanıma yönelik programlar çalıştırılması ve kopyalanması politikaya aykırıdır.

ç. Bakanlıkta Bilgi Teknolojileri Genel Müdürlüğünün bilgisi ve onayı olmadan Bakanlık ağ iletişim sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulamaz.
d. Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilemez.
e. Kurum bilgisayarlarına lisanssız program yüklenmesi politikaya aykırıdır.
f. Kurum bilgisayar kaynaklarının paylaşıma açılması politikaya aykırıdır.
g. Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar vermemeli, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunmamalı, kaynakların içeriğini izinsiz olarak değiştirmemelidir.
ğ. Bakanlık merkez ve taşra teşkilatında bilişim varlığı satın alınacağı zaman, Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi tedbirleri gereği Bilgi Teknolojileri Genel Müdürlüğü'ne görüş sorulmalı, Bilgi Teknolojileri Genel Müdürlüğü tarafından uygun bulunmayan bilişim varlıkları alınmamalıdır.
h. Bilgi Güvenliği Yönetim Sistemi, Bakanlığımızda Bilgi Teknolojileri Genel Müdürlüğü kapsamında kurulmuş olup, gerekli durumlarda kapsamın genişletilmesi ve/veya taşra birimlerinde Bilgi Güvenliği Yönetim Sistemi (BGYS) ekiplerinin kurulmasına Genel Müdürlük karar verebilir.

(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 ve BTGM'ye bilgi verilir.
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 kurum dışına gönderilen e-postalarda Aile ve Sosyal Hizmetler Bakanlığı sorumluluk reddini ifade eden açıklayıcı metin yer alır.
ç. Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır.
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 kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanır.
b. Her bir son kullanıcının görevleri gereği ihtiyaç duymadıkları sürece yalnızca bir adet kullanıcı hesabı bulunur.
c. Son kullanıcılar için erişim kuralları görevleri gereği ihtiyaç duydukları kadar yetkilendirilirler.
ç. Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı 5651 sayılı kanuna uygun olarak kayıt altına alınır.
d. Güvenlik zafiyetlerine karşı, kullanıcılar hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi 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 bilgisayar ekranlarını kilitlemelidir.

g. Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde kullandıkları harici cihazları (e-imza ve kart okuyucusu, bellek ve/veya harici hard disk gibi taşınabilir medya araçları) kontrol altında tutmalıdır.
ğ. Bakanlık, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulama yetkisine sahiptir.
h. Bakanlık, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişikleri merkezi grup politikalarıyla engeller.
ı. Temiz masa, temiz ekran ilkesi benimsenmeli ve hayata geçirilmelidir.
i. Kullanıcılar, Bakanlık mevcut envanteri haricindeki donanımları kullanırken güvenlik kriterlerine özen göstermelidir.
j. Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
k. Dosya paylaşım alanı ihtiyacı olması durumunda Bakanlık dosya paylaşım sistemleri kullanılır.
l. Gizli ve kişisel veriler Bakanlık tarafından sağlanan dosya paylaşım ve depolama alanları haricinde depolanamaz/paylaşılamaz.

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 değiştirilir. Parola yenileme işlemi esnasında son 3 parola ile aynı olmayan bir parola girilir.
b. Sistem yöneticilerinin, sistem ve kullanıcı hesapları farklı olarak tanımlanır.
c. Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir ve kritik sistemlerin bağlantıları için otomatik parola anımsama seçenekleri işaretlenmemelidir
ç. Kullanıcı, parolasını başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazması durumunda güvenliğini sağlar.
d. Kullanıcıya ilk verilen veya sıfırlanması istenilen parolalar "geçici parola" olarak verilir ve ilk oturum açılışında değiştirilir.
e. Kritik sistemlere ve ağ cihazlarına erişim için sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Bunun mümkün olmadığı durumlarda varsayılan parolalar değiştirilir.
f. Genel kural olarak, parola gibi hassas veri girilen web adresleri HTTPS protokolü kullanmalıdır. Ayrıca HTTPS sitede kullanılan sertifikanın siteyi yayınlayan kurum/şirkete ait olduğu kontrol edilmelidir.
g. Parola kriterleri gerek görüldüğü takdirde Bilgi Teknolojileri Genel Müdürlüğü tarafından sıkılaştırılabilir.
(2) Kullanıcı, güçlü bir parola oluşturmak için, aşağıda belirtilen maddelere uymalıdır. Parola en az 8 haneli olmak üzere; aşağıdaki kriterlerden (a, b, c) en az 2 tanesine uyulması zorunludur.
a. İçerisinde en az 1 tane küçük ve 1 tane büyük harf bulunmalıdır. (a, b, A,B ..)
b. İçerisinde en az 1 tane rakam bulunmalıdır. (1, 2, 3...)
c. İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,$,#,&,/,{,*,-,],=,...)
ç. 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 bilgilerin e-posta ve eklerinde bulunması politikaya aykırıdır.
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@aile.gov.tr) adresine iletilmelidir.
ç. Kurumsal iletişim gerektiren durumlarda Kurumsal e-posta adresleri kullanılır. 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@aile.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.) gönderemez.
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. Kullanıcılar e-posta gönderiminde ad, soyad, iletişim bilgisi, kurum, birim adı gibi alanları içeren imza şablonu kullanılır.
h. Bakanlık dışında, güvenliğinden emin olunmayan bir bilgisayar üzerinden kurumsal Web Posta Sistemi kullanılması politikaya aykırıdır.
(2) Kurumsal e-postalar, resmi yazı ile gelen talepler doğrultusunda, hukuki olarak yetkilendirilmiş kişilerce tutanak altında denetlenebilir.

İnternet Erişim ve Kullanım Politikası

Madde 10 – (1) İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a. Kullanıcıların internet erişimlerinde güvenlik kriterleri uygulanır.

b. Bakanlığın politikaları doğrultusunda en az kategori ve uygulama bazlı filtreleme sistemleri kullanılır. İstenilmeyen siteler (terör, pornografi, oyun, kumar, şiddet içeren vs.) yasaklanır.
c. Kullanıcılar internete Bakanlık tarafından sağlanan kullanıcı adı/şifre (LDAP vb.) ile erişim sağlar. Ayrıcalıklı erişim yetkileri ihtiyaç halinde gerekçelendirilerek Genel Müdürlük tarafından belirli bir süre ile sınırlı olarak verilir.
ç. İş ile ilgili olmayan dosyalar (müzik, video vs. dosyaları) gönderilmemeli, paylaşılmamalı ve indirilmemelidir. Dosya paylaşım uygulamaları kullanılmamalıdır. Bu konuda sorumluluk kullanıcıya aittir.
d. Genel Müdürlük tarafından onaylanmamış yazılımlar internet üzerinden indirilmemelidir ve Bakanlık sistemlerine yüklenmemelidir.
e. 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. Kuruluşlar eğer Bakanlık altyapısı dışında bir internet hizmeti alıyorsa bu hizmetin mevzuata ve 5651 sayılı kanuna uygun olarak kullanılmasından ve iz kayıtlarının tutulmasından sorumludurlar. Bakanlık, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgileri hukuki olarak yetkilendirilmiş kişilere verebilir.
f. Bakanlık etki alanına dâhil olmayan cihazlar Bilgi Teknolojileri Genel Müdürlüğü onayı olmadan internete çıkamaz. Etki alanına dâhil olmayan cihazlar için istisnai durumlarda internete çıkış izni Genel Müdürlük tarafından uygun bulunması halinde verilir.

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 Genel Müdürlük tarafından verilir.
b. Uzaktan erişimler Genel Müdürlük 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 Genel Müdürlük tarafından kayıt altına alınır.
(2) Bütün kablosuz erişim cihazları Bilgi Teknolojileri Genel Müdürlüğü tarafından belirlenen güvenlik ayarlarını kullanır.
(3) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.
a. Kablosuz cihazlar güçlü şifreleme protokolleri kullanmalıdır.
b. Bakanlık kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenir.
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 kullanıcı bilgisayarları ve sunucuları güncel anti-virüs yazılımına sahip olmalıdır.
b. Son kullanıcı bilgisayarlarına ve sunuculara zararlı yazılım bulaştığı fark edildiğinde ağ erişimi sınırlandırılır.
c. Bilgi Teknolojileri Genel Müdürlüğü anti-virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
ç. Kullanıcı bilgisayarlarından hiçbir sebepten dolayı anti-virüs yazılımını bilgisayarından kaldırmamalıdır.
d. Harici veri depolama cihazları her kullanımda anti-virüs kontrolünden geçirilir.
e. Kullanılan anti-virüs yazılımı üzerinde düzenli taramalar yapılacak şekilde konfigürasyonlar yapılır.

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. Bakanlık tarafından temin edilen kurumsal imaj dosyaları dışında kurulum yapılmamalıdır.
b. Genel Müdürlük, 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 edilir.
b. Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanır ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilir.
c. Tanımlanan farklı güvenlik bölgelerine erişim yetkileri gözden geçirilir ve güncellenir.
ç. Bakanlık dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili personel gözetiminde gerçekleştirilir.
d. Kritik bilgilerin bulunduğu alanlara girişler kontrolü bir şekilde yapılır ve izlenir.
e. Her ziyaretçi için kayıt tutulur ve her bir ziyaretçiye bir adet ziyaretçi kartı verilir.
f. Kritik sistemler sistem odalarında barındırılır.
g. Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunur, yangın ve benzer felaketlere karşı koruma altına alınır ve iklimlendirilmesi sağlanır.
ğ. Kritik bilgi içeren ofisler ve odalar için işaret, tabela vb. bulunmamasına dikkat edilir.

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 Genel Müdürlük/Birim tarafından imzalanır.
b. Kurumsal bilgi güvenliği bilinçlendirme eğitimleri Genel Müdürlük tarafından düzenlenir.
c. İş tanımı değişen veya Bakanlıktan ayrılan kullanıcıların erişim haklarının kaldırılması için Genel Müdürlüğe bilgi verilir.
ç. Bakanlık bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapar, bütçe ayırır, eğitimlere katılım sağlanmasını gözetir ve eğitim etkinliği değerlendirir.
d. Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olarak verilir. "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. Tüm çalışanlar, yükleniciler ve üçüncü taraflar Bakanlığın politika ve prosedürlerine uymak zorundadır.

Sunucu Güvenlik Politikaları

Madde 17 – (1) Sunucuya sahip olma ve sunucu sahiplerinin sorumlulukları ile ilgili kurallar aşağıda belirtilmiştir.
a. Bakanlıkta bulunan sunucuların yönetiminden, ilgili sunucu üzerinde Genel Müdürlük tarafından yetkilendirilmiş personel sorumludur.
b. Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılır.
c. Sunuculara ait bilgilerin yer aldığı güncel sunucu envanter bilgisi tutulur.
(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.
a. Sunucuyu kullanan birim tarafından, kullanılmayan servisler ve uygulamalar kapatılır.
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 tutulur.
ç. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
d. Sunucular üzerine lisanslı yazılımlar kurulur.
e. Sunucular fiziksel olarak korunmuş sistem odalarında bulundurulur.
(3) Sunucu işletim kuralları aşağıda belirtilmiştir.
a. Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulur.
b. Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılır.
c. Sistem odalarına giriş ve çıkışların erişim kontrollü olması sağlanır ve kayıt edilir.

Ağ Yönetim Politikası

Madde 18 – (1) Ağ yönetim politikası ile ilgili kurallar aşağıda belirtilmiştir.
a. Ağ cihazları yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrı değerlendirilir.

b. Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılır ve güncellemeler uygulanır.
c. Sınırsız ağ dolaşımı engellenir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaca göre açılır.
ç. İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınır ve kayıtlar tutulur.
d. Kullanıcı bilgisayarlarının bulunduğu ağ, iç sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılır ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanır.
e. Bilgisayar ağına bağlı bütün cihazlarda kurulum ve yapılandırma parametrelerinin, Bakanlığın güvenlik politika ve standartlarıyla uyumlu olması gerekmektedir.
f. Ağ trafiği düzenli olarak izlenir ve ölçülür.
(2) Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.
a. Ağ cihazlarının güncel envanter ve topoloji bilgileri tutulur.
b. Özel durumlar haricinde yerel kullanıcı hesapları kullanılmamalıdır. Ağ cihazları kimlik tanımlama için güvenli protokoller kullanılır.
c. Cihazlar üzerinde kullanılmayan servisler kapatılır.
ç. Cihazlara erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.
d. Yazıcı, fotokopi cihazı, faks cihazı gibi cihazların bulunduğu ağlar kritik sistemlerin bulunduğu ağlardan ayrılır.

Donanım ve Yazılım Envanteri Oluşturma Politikası

Madde 19 – (1) Donanım ve yazılım envanteri oluşturma ile ilgili kurallar aşağıda belirtilmiştir.
a. Oluşturulan envanter tablosunda envantere ait ayırt edici ve önemli bilgiler tutulur.
b. Envanter bilgileri değişiklik olduğunda güncellenir. Envanter bilgilerinin güncel olmaması nedeniyle yaşanabilecek kayıp ve maliyetlerden, varlık sahipleri sorumlu olacaktır.
c. Satın alınan, geliştirilen, hibe yoluyla elde edilen, proje kapsamında sağlanan bilişim varlıkları ve yazılımlar Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi tedbirleri gereği Bilgi Teknolojileri Genel Müdürlüğü tarafından bildirilen envanter yönetim sistemi yazılımına aktarılmalıdır.

Kriz / Acil Durum Politikası

Madde 20 – (1) Acil Durum politikası ile ilgili kurallar aşağıda belirtilmiştir.
a. Oluşturulan acil durum senaryoları çerçevesinde acil durum sorumluları atanır, yetki ve sorumlulukları belirlenir ve yazılı hale getirilir.
b. Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınır.
c. Bilişim sistemlerinin kesintisiz çalışmasının sağlanması için sistemler tasarlanırken minimum sürede iş kaybı hedeflenir.
ç. Acil durumlarda Bakanlık içi iş birliği gereksinimleri tanımlanır.
d. Acil durumlarda sistem kayıtları incelenmek üzere saklanır.
e. Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilir.
f. Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulur.
g. Acil durumlarda bilgi güvenliği yöneticisine erişilir, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilir ve

zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülür.

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 belirlenir ve denetim altında tutulur.
b. Erişim hakları tanımlanırken ihtiyacı kadar yetki ilkesi göz önünde bulundurulur. c)Üçüncü tarafların tüm erişimleri kayıt altına alınır. İşi biten firmaların hesapları kapatılır. Bu işlem için Genel Müdürlüğe ve ilgili personele bilgi verilir.
c. Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulur, tekrarlanan başarısız erişim istekleri/girişimleri incelenir.
ç. Kullanıcı hareketlerini doğru bir şekilde kayıt altına almak için her kullanıcıya kendisine ait bir kullanıcı hesabı açılır.

Veri Tabanı Güvenlik Politikası

Madde 22 – (1) Veri tabanı güvenlik kuralları aşağıda belirtilmiştir.

a. Veri tabanı sistemleri envanteri güvenli şekilde tutulur, saklanır ve bu envanterden sorumlu personel tanımlanır.
b. Veri tabanı işletim prosedürleri belirlenir ve yazılı hale getirilir.
c. Veri tabanı sistem olay kayıtları tutulur ve gerektiğinde Genel Müdürlük tarafından izlenir.
ç. Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilir.
d. Yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.
e. Veri tabanı yedekleme planları yazılı halde olmalıdır.
f. Veri tabanı erişim politikaları "Kimlik Doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulur.
g. Bilgi saklama medyaları kontrolsüz olarak Bakanlık dışına çıkartılamaz.
ğ. İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenir.
h. Veri tabanı sunucusuna sadece güvenli erişim protokolleri ile erişim sağlanır.
ı. Veri tabanı sunucusuna ancak zorunlu hallerde ayrıcalıklı erişim ("root" "admin" vb.) yetkisi ile bağlanılır. Ayrıcalıklı erişim yetkili kullanıcılar kişilerin kendi adına özel oluşturulur ve ortak kullanılamaz.
i. Veri tabanına doğrudan bağlanacak kişilerin kendi adına kullanıcı adı verilir ve yetkilendirme yapılır.
j. Veri tabanına doğrudan bağlanan kullanıcıların yaptıkları işlemler kaydedilir.

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 getirilir.
b. Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilir.
c. İş kritik bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek sistem ve uygulamalar ilgili birim(ler) tarafından belirlenir ve yazılı hale getirilir.

ç. Yapılacak değişiklikler öncelikle bir test ortamında denenmelidir.
d. Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulur ve güncel tutulması sağlanır.
e. Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanır, geri dönüş planları test edilir ve ilgili yöneticiler tarafından onaylanması sağlanır.
f. Sistemlerde oluşacak problemlere yönelik bakım, onarım, yama, güncelleme ve değişiklikler ile ilgili çalışmalardan önce varlık sahibine ve proje paydaşlarına bilgi verilir. Sonrasında ilgili uygulama kontrolleri gerçekleştirilir.

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 yedeklenir.
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 verilerin oluştuğu fiziksel ortamlardan faklı yerlerde veya binalarda güvenli bir şekilde saklanır.
ç. Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanır.
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 alınır.
b. Üreticilerden, sistemler ile ilgili bakım prosedürleri sağlanır.
c. Firma teknik destek elemanlarının bakım yaparken bu yönergeye uygun davranmaları sağlanır ve kontrol edilir.
ç. Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" ve ilişkili standartlar uygulanır.
d. Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda, bu yönerge uyarınca hareket edilir. Güvenlik açıkları Bakanlık Siber Olaylara Müdahale Ekibine (some@aile.gov.tr adresine) bildirilmelidir.
e. Bakanlık içinde firmalar tarafından bakımı ve onarımı yapılan sistemlerde, bakım işlemi yetkili bir çalışanın gözetiminde yapılır ave sistemden bilgi alınmasına engel olunması sağlanır.
f. Depolama ortamının (örn. sabit disk) bakım, onarım gibi amaçlarla Bakanlık dışına çıkarıldığı durumlar kayıt altına alınır ve firma yetkilisi tarafından imzalanır. Gerekli durumlarda firma ile gizlilik sözleşmesi imzalanır.

Yazılım Geliştirme Politikası

Madde 26 – (1) Yazılım Geliştirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a. Yazılım planlama aşamasında güvenlik ihtiyaçları planlanır.

b. Yazılım Bakanlık Bilgi Güvenliği Politikalarına uygun olarak geliştirilir, yetkisiz kişilerin müdahale etmesi şifreleme işlemleri ile engellenir.
c. Yazılım kodları dışarıdan erişime kapalı olan bir ortamda saklanır.
ç. Yazılım geliştirme, test ve uygulama ortamları ayrılır, her biri için özel olarak tahsis edilmiş ayrı sistemler kullanılır.
d. Yazılım geliştirme süreçleri uluslararası kabul görmüş proje yönetim mantığına uygun şekilde yazılı hale getirilir. (yazılımın veri akışı ve işleme özelliklerini içeren tasarım belgesi, vb.)
e. Bakanlıkta yazılım geliştirileceği ya da temin edileceği durumda Bilgi Teknolojileri Genel Müdürlüğü'ne görüş sorulması, Genel Müdürlük onayı ve bilgisi dışında yazılım geliştirme/temini yapılmaması gerekmektedir.
f. Bakanlık merkez ve taşra kuruluşları Bilgi Teknolojileri Genel Müdürlüğünce sağlanan Bakanlığa ait web portali üzerinden yayın/paylaşım yapmalı, Bakanlık alan adlarından farklı bir web sayfası oluşturmamalı/yayınlamamalıdır.

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.

KVKK Uyum

Madde 28 – (1) Bakanlığımız, Bilgi Teknolojileri Genel Müdürlüğü kişisel verilerin korunması konusundaki yasal yükümlülüklerini tam olarak yerine getirmek ve KVKK'nın öngördüğü standartlara uyum sağlamak amacıyla kişisel verilerin saklanması ve işlenmesi sürecinde gerekli teknik ve organizasyonel önlemleri almayı, kişisel verilerin güvenliğini sağlamayı ve veri ihlallerini önlemek için gerekli tüm teknik tedbirleri almayı hedeflemektedir.

Üçüncü Tarafların Yönetimi

Madde 29 – (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 ve yapılan iş ile ilgili Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi tedbirlerine uymak zorundadır.

Yönetimin Taahhüdü

Madde 30 – (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.

(4) KVKK şeffaflık ilkesi doğrultusunda kişisel veri sahiplerine gerekli bilgilendirmeleri yapmayı ve haklarını korumak için gerekli adımları atmayı, KVKK'ya uyum politikalarının benimsenmesi konusunda sürekli destek ve teşvik sağlamayı, kamuoyunu aydınlatma yükümlüğü kapsamında ise olası veri sızıntılarında bildirmeyi taahhüt etmektedir.

Sorumluluk

Madde 31 – (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 32 – (1) Bu yönergenin imzalanmasıyla 09/01/2020 tarihli Aile, Çalışma ve Sosyal Hizmetler Bakanlığı Bilgi Güvenliği Politikaları Yönergesi Bakanlığımızda yürürlükten kalkar.

Yürürlük

Madde 33 – (1) Bu Yönerge Aile ve Sosyal Hizmetler Bakanının onayı ile yürürlüğe girer.

Yürütme

Madde 34 – (1) Bu Yönerge hükümlerini Aile ve Sosyal Hizmetler Bakanı yürütür.

OLUR

06/05/2024