T.C.

KÜLTÜR VE TURİZM BAKANLIĞI
BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu yönergenin amacı, bilginin işlenmesi süreçlerinde bilgi güvenliğinin sağlanmasına yönelik tedbir almak; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden veya dışarıdan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak; yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesinde bilgi güvenliği açısından uyulması gereken usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Bu yönerge, Bakanlık merkez ve taşra teşkilatı ile bağlı ve ilgili kuruluşlarında görev yapan tüm personel ile kendilerine herhangi bir nedenle Bakanlık bilgi ve bilgi sistemlerine erişim yetkisi verilen kullanıcıları, bilgi sistemlerini, insan kaynaklarını, fiziksel ve çevresel güvenlik sistemlerini ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım desteği sağlayıcılarını kapsar.

Dayanak

MADDE 3- (1) Bu yönerge,

- 24/3/2016 tarih ve 6698 sayılı Kişisel Verileri Korunması Kanunu,
- 4/5/2007 Tarih Ve 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

- 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu,
- 18.04.2020 tarih 31103 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 60 sayılı Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılmasına Dair Cumhurbaşkanlığı Kararnamesinin 10 uncu ve 11 inci maddeleri,
- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından 24.07.2020 tarihinde yayınlanan Bilgi ve İletişim Güvenliği Rehberi,
- 06/07/2019 tarih ve 30823 sayılı Resmi Gazetede yayımlanan 2019/12 numaralı "Bilgi ve İletişim Güvenliği" konulu Cumhurbaşkanlığı Genelgesi,
- TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı'na dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönergenin uygulanmasında;

a) Bakan: Kültür ve Turizm Bakanını,
b) Bakanlık: Kültür ve Turizm Bakanlığını,
c) Genel Müdürlük: Bilgi Teknolojileri Genel Müdürlüğünü,
ç) Kullanıcı: Bakanlık merkez ve taşra teşkilatı ile bağlı ve ilgili kuruluşlarda yer alan bilgi ve bilgi işleme tesislerine erişen tüm kişileri,
d) Bilgi: Kurum için değeri olan, korunması gereken, yazılı olarak veya bilgi sistemleri üzerinde işlenen tüm kaynakları,
e) Bilgi işleme: Veri ve bilgilerin manuel veya bir otomasyon sisteminin parçası olarak elde edilmesi, kaydedilmesi, depolanması, muhafazası, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veri ve bilgiler üzerinde gerçekleştirilen her türlü işlemi,
f) Bilgi işleme tesisi: Bilgi işlemede kullanılan her türlü sistem, servis, altyapı ve bunların konuşlandırıldığı fiziksel mekânları,
g) Bilgi güvenliği: Bilgi ve bilgi işleme tesislerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümünü,

ğ) Bilgi güvenliği yetkilisi: Kurumda bilgi güvenliği politikalarının uygulanması için yetki verilen kişiyi,

h) Bilgi güvenliği yönetim sistemi (BGYS): Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, yazılı hale getirilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününü,

ı) Bilgi sistemleri: Donanım, yazılım, veri, bilgisayar ağları ve insan unsurlarından oluşan, veri ve bilgileri toplayan, kaydeden, işleyen, dönüştüren ve yayan sistemler bütününü,

i) Sızma testi: Bilişim sistemleri üzerinde, saldırgan bakış açısıyla güvenlik zafiyetlerinin tespit edilip bulunan zafiyetlerin kullanılarak sistemlere sızılmaya çalışılması ve raporlanması işlemlerini,

j) Siber güvenlik: Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini,

k) Siber ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,

l) Siber olay: Bilgi sistemlerinde tutulan veya işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,

m) Siber olaya müdahale: Bilgi sistemlerinde tutulan veya işlenen verilerin gizlilik, bütünlük veya erişilebilirliğinde meydana gelme riski bulunan veya meydana getirilen siber olayın kaynağını, nedenlerini ve sonuçlarını tespit ederek siber olayın devam etmesini, tekrarını veya zarar vermesini önleyen çalışmaları,

n) SOME: Siber güvenliğe ilişkin belirlenen politikalara uygun şekilde faaliyet göstermek, ihtiyaç durumunda yetkili makamlarla iletişime geçmek, kayıt vb. veriyi yetkili makamlara aktarmak ve müdahalenin yapılmasına yardımcı olmak amacıyla kurulan siber olaylara müdahale ekibini,

o) SOME ekip lideri: İlgili kurumun bilgi güvenliği yönetim komisyonu tarafından görevlendirilen, kurumsal SOME faaliyetlerini yürütmekle görevli kişiyi,

ö) Sosyal mühendislik testi: Kurum çalışanlarının kişisel hesaplarının güvenliği ve bilgi güvenliği politikaları ile ilgili farkındalık seviyelerini ölçmek için yapılan, senaryoları önceden paylaşılmış kontrolleri,

p) Veri: Bilginin işlenmemiş halini,

r) Zafiyet Testleri: Kurumun Bilişim Sistemlerini oluşturan altyapı, donanım, yazılım ve uygulamalara, bir saldırganın izlemesi öngörülen yöntemler kullanılarak yapılan saldırı ve müdahaleler sonucunda güvenlik açıklarının tespit edilip bu zafiyetlerin kullanılarak sistemlere sızılmaya çalışılmasını, bu açıkların nelere sebep olabileceğinin incelenmesini ve sonuçların raporlanmasını ifade eder.

İKİNCİ BÖLÜM
Sorumluluk ve Genel Kurallar

Sorumluluk

MADDE 5-(1) 5651 sayılı kanun ve TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla, Genel Müdürlük tarafından uygun görülen sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtları, ajanlı veya ajansız iz toplama yöntemleri kullanılarak toplanır ve ilgili kanun ve yönetmeliklerde belirtilen süre boyunca Genel Müdürlük tarafından saklanır. Bu nedenle kullanıcı, kendisine ait kişisel verilerin gizli kalması ve korunması kaidesiyle, kurum ağı üzerinden gelen ve giden tüm trafik bilgilerinin önceden kullanıcıya haber verilmeksizin Genel Müdürlük tarafından kayıt ve kontrol edilebileceğini, bu bilgilerin istatistik, raporlama ve inceleme amaçlı olarak kullanabileceğini bilir ve kabul eder.

(2) Bakanlık personelinin, çocukların cinsel istismarına, müstehcenliğe, şiddet ve intihara yönlendirmeye, uyuşturucu ve uyarıcı madde kullanımını özendirmeye yönelik internet sitelerine girmesi, sohbet oturumları açarak kuruma ait gizli bilgileri paylaşması, oyun oynaması, devlet büyüklerine hakaret etmesi; sosyal medya, gazete, forum ve benzeri sitelerde kurumu küçük düşürücü ve kamuoyunu yanıltmaya yönelik yorumlar yapması, özel hayatına ilişkin suç oluşturabilecek nitelikteki bilgi ve işlemleri kurum internet hattı üzerinden yapması ile ilgili cezai ve hukuki sorumluluğu kendisine aittir. Genel Müdürlük yukarıda belirtilen davranışları tespit etmeye ve önlemeye yönelik erişim politikaları belirler ve uygular.

(3) Bu Yönerge kapsamında bilgi ve sistem güvenliğinin planlı, sorunsuz, güvenli ve disiplin içinde gerçekleştirilmesinden Bakanlık bilişim sistemlerinden yararlanan tüm Bakanlık

personeli birinci derecede görevli ve sorumludur. Bu Yönerge kapsamında olup teknolojik değişikliklere ya da Bakanlığın genel politikasındaki ve hizmetlerindeki değişikliklere göre bu politikada gerekli düzenlemeler Genel Müdürlük tarafından yapılır ve Genel Müdürlük resmî internet sayfasında "Bilgi Güvenliği Politikaları'" adı altında yayımlanır. Tüm Bakanlık personeli yayınlanan Bilgi Güvenliği Politikaları'nı takip etmekle ve bu politikalara uymakla yükümlüdür.

(4) Genel Müdürlük, yasal hükümler çerçevesinde bilişim kaynaklarını ve bunlarla gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak inceleme ve denetleme hakkını saklı tutar.

(5) Bakanlık bilişim kaynaklarında meydana gelen arızalara yetkisiz personel tarafından müdahale edilemez. Edilmesi sonucunda ortaya çıkabilecek arızalar, maddi hasarlar ya da kurumsal ağ güvenliğinin ihlaline yol açan uygulamalardan ilgili personel sorumludur.

(6) Bakanlık uygulamaları ve sistemlerinde yetkili bir kullanıcı, hiçbir sebepten uygulama ve veri tabanlarında yer alan kişisel bilgileri (ad, soyad, T.C. kimlik numarası, adres, telefon numarası, e-posta adresi vb.) diğer kamu kurumları ve 3. şahıslar ile paylaşamaz. Gerekli görüldüğü zaman bu bilgilerin paylaşımı için Genel Müdürlükten talepte bulunulur. Genel Müdürlüğün uygun gördüğü durumlarda, bilgiler yasal sınırlar içerisinde ilgili kamu kurum ve kuruluşları ile paylaşılır.

(7) Kullanıcı, kurumun kritik bilgisinin ortaya çıkmasına veya kurum servislerinin ulaşılamaz hale gelmesine sebep olabilecek tüm eylemlerden kaçınır.

(8) Kurum ağı ve bu ağı kullanan her kullanıcı ve cihaz ile ilgili her türlü erişim, güvenlik ve yönetim politikaları Genel Müdürlük tarafından belirlenir ve uygulanır. Bu ağ üzerindeki trafik, ilgili erişim kanunu çerçevesinde gelen ve giden yönünde kayıt edilip incelenebilir ve raporlanabilir.

(9) Genel Müdürlük, kurum ağının kesintisiz, verimli ve güvenlik politikalarına uygun kullanılabilmesi için, belirlenen erişim politikası düzenlemelerini uygular.

Genel Kurallar

MADDE 6-(1) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar veremez, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunamaz, içeriğini izinsiz olarak değiştiremez.

(2) Kullanıcı, bilgi teknolojileri kapsamındaki herhangi bir kaynağı, kendisinden başka hiç kimse adına ve yararına kullanamaz veya bir başkasının kullanımına izin veremez.

(3) Kullanıcı, başka kullanıcıların bilgisayarında yer alan şifreli veya şifreli olmayan paylaşım alanlarına veya dosyalara çeşitli yöntemleri kullanarak erişemez ve bu türlü girişimlerde bulunamaz.

(4) Kullanıcı, emeklilik, işten ayrılış, görev değişikliği gibi nedenler ile çalışmalarının sonlanması durumunda, kendisinde bulunan bilgisayar, yazıcı, disk ve benzeri tüm donanım ve malzemeleri, tüm yazılım ürünleri ve kodları ile bilişim sistemleri kullanımına yönelik tüm şifreleri içeren Bakanlığın tüm bilişim varlıklarını iade eder. Kullanıcının bilgi ve bilgi işleme olanaklarına erişim hakları kaldırılır, hesapları kapatılır.

(5) Yüklenici firma personeli, ancak sistem yöneticisi nezaretinde ve kontrolünde çalışma yapar. Firma personeli tarafından yapılacak çalışmalara nezaret edecek kurum personeli, en az firma personeli kadar konusunda uzman personel arasından seçilir ve sistem birimi yöneticisinin onayı ile kayıt altına alınır. Bu kurallara uyulmadığı zaman doğacak problem ve zararlardan ilgili yüklenici firma sorumludur. Nezaret eden kurum personeli yapılan çalışmaları kayıt altına alır ve herhangi bir olumsuzluk durumunda bu olumsuzluğu açıklayıcı rapor sunmak zorundadır.

(6) Bilgi güvenliğini etkileyen arızalar mümkün olan en kısa sürede, uygun yönetim kanalları kullanılarak Genel Müdürlüğe rapor edilir.

(7) Gizlilik içeren bilgiler ile kişisel veriler, E-Devlet kapsamında protokol yapılarak bilgi paylaşımı yapılan veya kanunen yetkili sayılan merciler dışında hiçbir kişi, kurum ya da kuruluş ile paylaşılmaz.

(8) Gizlilik içeren bilgilerin paylaşımı ile ilgili yapılacak protokoller Bakanlık merkez birimlerince veya Bakanlıkça yetkilendirilen taşra teşkilatı birimlerince yapılır.

ÜÇÜNCÜ BÖLÜM

Bilgi ve Sistem Güvenliği Kuralları ve Politikaları

Bakanlık Ağı Kuralları

MADDE 7-(1) Bakanlık bünyesinde çalışmakta olan veya işe başlayan veya görevlendirilen her personel ile paydaş ve konuklar için aktif dizin kullanıcı hesabı açılır. Kurum dışından görevlendirilen personel, paydaş ve konukların kullanımı için bağlı oldukları birimde görev yapan birim amiri veya yetkili personel tarafından görevlendirme yazısı ile birlikte kullanıcı hesabı açılması talebinde bulunulur. Görevli personel bu hesaptan sorumludur ve görevlendirme süresinin sonunda ilgili hesabın kapatılması için Genel Müdürlüğe, ilgili birim tarafından bildirimde bulunulur.

(2) Kullanıcı, kendisine verilen "kullanıcı adı" ve "şifresi"ni bir başkası ile paylaşmaz ve bir başkasına kullandıramaz. Kullanıcının, "kullanıcı hesabına" ait geçici şifresini derhal değiştirerek, Genel Müdürlük tarafından belirlenen şifre politikasına uygun olarak şifresini oluşturur.

(3) Kullanıcının, Genel Müdürlük tarafından belirlenecek periyotlarla "kullanıcı şifresini" değiştirmesi gerekir. Kullanıcı şifresini yenilemeyen veya kullanıcı şifresini üst üste birkaç kez hatalı giren kullanıcının, kullanıcı hesabı geçersiz kılınır ve iletişim ağına giriş izni otomatik olarak kaldırılır. Kullanıcının başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.

(4) Her bir kullanıcı, bilgisayarda kendi kurum etki alanında yer alan "kullanıcı adı" ve "şifre" ile oturum açarak çalışır. Çalışması biten kullanıcı, oturumu veya bilgisayarını kapatarak bilgisayara başkalarının fiziksel erişimini engeller. Bilgisayar başından kısa süreli ayrılmalarda bilgisayar oturumunu kilitler.

(5) İlgili hesabın amacı dışında kullanılması ve bu hesaptan doğabilecek zararların sorumluluğu, hesabı kullanan kullanıcıya aittir.

(6) Bakanlık ağındaki her bir son kullanıcı ve bilgisayar, etki alanı üyesi olmalıdır. Etki alanında olmayan kullanıcı veya bilgisayarın internet erişimleri engellenir.

E-Posta İşlemleri Kuralları

MADDE 8-(1) Kullanıcı, tüm resmî yazışmalarında e-posta adresi olarak, Genel Müdürlük tarafından kendisine tahsis edilen veya çalıştığı birime ait olan kendisine zimmetli kurumsal e-posta adresini kullanır. Bunun dışındaki e-posta servislerini resmî işlerde kullanamaz. E-postalar personel tarafından arşivlenir.

(2) Kullanıcı, kurum saygınlığını zedeleyecek ve/veya başkalarını taciz edecek kurum içi veya kurum dışı e-posta gönderemez. E-Posta adresini internet üzerinde herhangi bir siteye kurumsal amaçlar dışında abone olmak için kullanamaz.

(3) Kullanıcı, Genel Müdürlük tarafından kendisine veya çalıştığı birime tahsis edilen e-posta adresini, sohbet (chat) yapmak için kullanmaz.

(4) Kullanıcı, hesabını ticari ve kar amaçlı olarak kullanamaz. Çok sayıda kullanıcıya toplu halde reklam, tanıtım, duyuru ve benzeri amaçlı e-posta gönderemez ve zincir e-posta, sahte e-posta ve benzeri zararlı e-postalara yanıt yazamaz.

(5) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmaz, derhal silinir ve kurum güvenliği açısından şüpheli e-postalar Genel Müdürlüğe bildirilir.

(6) Kullanıcı, kendisine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludur. Şifresinin başkası tarafından bilindiğini fark ettiği anda şifresini değiştirip Genel Müdürlüğe durumu haber vermekle yükümlüdür.

(7) Güvenlik ve performans açısından e-posta eklentilerinin toplam boyutu hiçbir durumda Genel Müdürlüğün belirlediği boyut değerinden fazla olamaz.

(8) Resmî işler için Bakanlık resmî e-posta hesapları dışında hiçbir e-posta adresine veri toplanamaz. Bu e-postalara cevap verilmez.

(9) Genel Müdürlük sistem ve kullanıcı güvenliğini sağlamak amacıyla gelen giden e-postalar için politika belirleyebilir ve uygulayabilir.

(10) Genel Müdürlük kişisel verilerin korunması ve gizli kalması kaidesiyle gelen giden e-postalara ait istatistiki bilgileri kayıt edebilir ve inceleyebilir.

(11) Gerekli görülmesi halinde Genel Müdürlük kullanılan e-posta sistemleri üzerinde her türlü değişikliği yapma hakkına sahiptir.

(12) Usulsüz kullanıldığı tespit edilen veya spam, virüs yayarak sistem ve kullanıcıların güvenliğini tehdit eden e-posta hesapları devre dışı bırakılır. Kullanan hakkında gerekli yasal işlem başlatılır.

(13) Bakanlık birimlerinin talebiyle oluşturulan e-posta gruplarının üyelerinin güncel olmasından ilgili birim sorumludur. Birimin kapanması, isminin değişmesi, faaliyetin bitmesi vb. nedenlerle işlevini kaybeden e-posta grubunun kapatılması veya grup üyelerinde ekleme, çıkarma yapılması gibi değişiklik taleplerini Genel Müdürlüğe bildirir. Bildirimlerin zamanında yapılmaması ihtimaline karşılık sistemde tanımlı e-posta hesapları taranır ve Genel Müdürlük tarafından belirlenen süre boyunca kullanılmayan e-posta hesapları herhangi bir uyarı yapılmaksızın pasif hale getirilir.

(14) Sorumlusu ilgili birim tarafından atanmayan, birim e-posta hesapları anonim olarak kullanılamaz.

Şifre Politikası

MADDE 9- (1) Kullanıcı, kurumda kullanılan ve belirli bir şifre ile girilmesi zorunlu olan her türlü uygulama için şifre belirler. Varsayılan şifreler kullanılamaz.

(2) Kullanıcının şifrelerini belirlerken dikkat edeceği kurallar şunlardır:

a) Şifreler en az 8 (sekiz) karakter olmalıdır.
b) Şifreler küçük harf, büyük harf, rakam ve simgelerin kullanıldığı karışık yapıda olmalıdır.
c) Şifrelerin Genel Müdürlük tarafından belirlenecek sayıda hatalı girilmesi sonucu, kullanıcı hesabı Genel Müdürlüğün politikalarına bağlı olarak kilitlenebilir. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.
ç) Şifreler en geç üç ayda bir değiştirilir.
d) "Yönetici/Admin" kullanıcı şifreleri yalnızca ilgili sistemin yöneticilerinde bulunur. Son kullanıcı ve yüklenici firma personeliyle paylaşılmaz.
e) Şifreler hesap sahibinden başka bir kişi ile paylaşılamaz, şifre değişikliği işlemlerinde başkasının hesabı ile ilgili Genel Müdürlükten yardım talebinde bulunulamaz.

Temiz Masa - Temiz Ekran Politikası

MADDE 10- (1) Sistemlerde kullanılan şifreler, masaüstü veya ekran üstü gibi herkes tarafından görülebilecek yerlere yazılmaz.

(2) Personel bilgisayarını belli bir süre kullanılmadığı zaman, ekran kilidinin otomatik olarak devreye gireceği şekilde ayarlanır ve masa başından kısa süreli ayrılmalar dâhil ctrl+alt+delete tuşlarına aynı anda bastıktan sonra, kilitle seçeneğini seçerek bilgisayar kilitlenmelidir.

(3) Kullanıcı, gizli bilgi içeren evrakı ağ üzerinden paylaşmaz, gizli bilgi içeren atık evrakı imha eder.

(4) USB bellek, harici disk vb. hafıza ünitelerinin kullanım şartlarını Genel Müdürlük belirler. Genel Müdürlük gerekli gördüğü durumlarda ilgili ünitelerin kullanımının durdurulması, sınırlandırılması veya kriptolanması/şifrelenmesi gibi uygulamaları yürürlüğe koyar.

(5) Kurumsal veriler, Genel Müdürlüğün belirttiği dosya paylaşım sisteminde depolanır. Kurum bilgisayarlarında, USB belleklerde, harici disk ve benzeri veri depolamanın mümkün olduğu ortamlardaki her türlü kurumsal ve kişisel verilerin güvenliğinden ve yedekliliğinden ilgili personel sorumludur.

Ağ ve İnternet Kullanımı

MADDE 11-(1) Tüm kullanıcılar interneti bilinçli bir şekilde kullanmak, başkalarının hakkını ihlal edici ve bilişim sisteminin işleyişini engelleyici, bozucu faaliyetlerde bulunmamakla yükümlüdür.

(2) Kullanıcı;

a) Bakanlık sunucuları üzerinde kendisine tahsis edilen kullanıcı adı, şifre ve IP adresi kullanılarak gerçekleştirilen her türlü etkinlikten,
b) Kendisine tahsis edilen bilgisayar üzerinde bulundurduğu belge, yazılım gibi her türlü kaynağın içeriğinden,
c) Bilişim sisteminin kullanımı hakkında yetkili makamlar tarafından talep edilen bilgilerin doğru ve eksiksiz verilmesinden,

ç) Bakanlık tarafından sağlanan güvenlik programlarının aktif olarak kullanılmasından ve güncellenmesinden,
d) Bilişim sisteminin; kullanım kurallarına, kanun ve yönetmelikler ile Bakanlığın tabi olduğu mevzuata uygun olarak kullanımından sorumludur.

(3) Kullanıcı, Bakanlık bünyesindeki tüm bilişim kaynaklarını;

a) Bakanlık ağına ve haricindeki bir sisteme, ağ kaynağına veya servisine saldırı niteliğinde girişimlerde bulunmak,
b) Diğer kullanıcılara ait verileri bozmak ya da zarar vermek, gizlilik hakkını ihlal etmek,
c) Yasaklanmış her türlü materyali üretmek ya da dağıtmak,
ç) Gerçek dışı, sıkıntı ve rahatsızlık verici, gereksiz endişe yaratacak materyali üretmek ve dağıtmak,
d) Başka bir kullanıcının e-posta adresini, o kullanıcının izni olmadan kullanmak,
e) Yerel, ulusal, uluslararası bilgisayarları veya hizmetleri kasıtlı olarak yetkisiz kullanmak,
f) Başkalarının telif haklarını ihlal edici konumda olan yazı, makale, kitap, film, müzik eserleri gibi materyali edinmek, yayınlamak, dağıtmak,
g) Özel yazılım, oyun, film, müzik, video vb. materyalleri edinmek, yayınlamak, kullanmak, dağıtmak,
ğ) Resmî işlemler dışındaki interaktif uygulamalara/hizmetlere erişmek,
h) Kurum dışı bulut ve depolama sistemlerine erişmek,
ı) Sosyal medya hesaplarına erişmek,
i) Siyasi ve ideolojik propaganda yapmak için kullanamaz.

(4) Telif hakları ve lisansları ihlal eden, zararlı yazılım bulunduran, Bakanlık ağında yoğun ağ trafiğine sebep olan iki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan noktadan noktaya (Peer-to-peer - P2P) uygulamaları kullanılmaz. Dosya paylaşımı, anlık mesajlaşma programları ve kurum altyapısında soruna yol açacak şekilde yoğun ağ trafiğine sebep olan uygulamalar ile güvenlik tehdidi oluşturan reklam, içerik, site, kullanıcı, yazılım, uygulama, erişim sağlayan cihazların tamamı gerekli görüldüğünde Genel Müdürlük tarafından filtrelenir veya erişime kapatılır.

(5) Zararlı veya güvenlik tehdidi oluşturan yazılım, uygulama, eklenti vb. içerik barındıran bilgisayarlar yeniden kurulum yapılmadan kurumsal ağa dâhil edilemez.

(6) Bilgisayarlara tahsis edilen IP numarası ve ortam erişim kontrolü adresi (MAC adresi) ile BIOS ayarları Bakanlık tarafından yetkilendirilmiş kişiler dışında değiştirilemez.

(7) Kurum ağına sistem yöneticisinin bilgisi dışında herhangi bir aktif ağ cihazı eklenemez.

(8) Kullanıcılar, kişisel bilişim kaynaklarını kurum ağında sistem yöneticisinden izin almadan kullanamaz.

(9) Kurum içinde hizmet veren sunucu, sistem veya kullanıcı bilgisayarlarına uzaktan erişim, zorunlu hallerde Genel Müdürlük onayı/izni alınarak verilir. Uzaktan erişim kurallarını Genel Müdürlük belirler.

(10) Bakanlık ağ erişimleri ve kaynakları öncelikli olarak resmî ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılır.

(11) Genel Müdürlük gerekli gördüğü durumlarda kurum içi kritik düzeydeki hizmetlere öncelik sağlamak için bant genişliği düzenleme yoluna gidebilir.

(12) Bakanlık ağında kategorisi olmayan IP adresi, içerik veya sitelere erişim izni verilmez. Erişim talepleri Başvuru Yönetim Sistemi üzerinden yapılır.

(13) Genel Müdürlük gerekli gördüğü durumlarda Bakanlığın görev alanına giren kategorilerin dışında kalan kategorilere yönelik erişimi düzenleme hakkına sahiptir.

(14) Kullanıcı, kendi kullanıcı hesaplarıyla internet üzerinden gerçekleştirdiği tüm işlemlerden sorumludur. Kimlik bilgilerini uygun bir şekilde saklar ve başkalarıyla paylaşmaz.

(15) Kurumsal ağ güvenliği açısından tehlike yaratabilecek nitelikte zararlı olduğu tespit edilen internet adreslerine erişim tüm kullanıcılar için engellenir. Kullanıcı bu tür engellemelerin kaldırılması konusunda Genel Müdürlükten herhangi bir talepte bulunamaz.

(16) Kurumsal ağ üzerindeki bilgisayarlara erişim hakkı, yetkisi olmayan kişilere verilemez.

(17) Yetkilendirilmiş kişiler ve kuruluşlar dışında, ağ kaynağına veya servisine zarar verebilecek DOS saldırısı, port/ağ taraması, paket dinleme, ağ izleme, IP değiştirme gibi kasıtlı veya kasıtsız girişimlerde bulunamaz.

(18) Bakanlık ağında Genel Müdürlük tarafından oluşturulan sertifika kullanılır. İlgili sertifikanın yüklü olmadığı cihazların ve aktif dizine eklenmeyen/yönetilemeyen cihazların ağ erişimine izin verilmez.

(19) Bakanlık ağına izinsiz kablosuz bağlantı alanı cihazı takılamaz. İzin dâhilinde takılan kablosuz bağlantı alanı cihazları şifresiz veya basit şifre ile kullanılamaz.

(20) Kurum bilişim kaynakları; ağ ve internet kaynaklarının kurum dışından kullanılmasına sebep olabilecek ya da kurum dışındaki kişi ya da bilgisayarların kendilerini kurum içerisindeymiş gibi tanıtmalarını sağlayacak (DHCP, DNS, Proxy, IP Sharer, NAT vb.) şekilde kullanılamaz.

(21) Genel Müdürlük, erişime açılacak ve kapanacak portları belirleme ve düzenleme yetkisine sahiptir. Genel Müdürlüğün belirlediği uzaktan erişim (RDP, SSH, Telnet vb.) uygulamaları dışındaki uygulamalara erişim izni verilmez. Veri tabanı sunucularının ağı kapalı devre olup internet erişimine kapalıdır.

(22) Bakanlığa ait gizli ya da açık her türlü veri Bakanlık dosya paylaşım sistemleri üzerinde barındırılır. Bakanlık'a ait olmayan herhangi bir bulut depolama sisteminde veya ortamda veri bulundurulamaz.

(23) Kurumsal ağ üzerindeki bilgisayarlarda ve sunucularda güvenlik politikalarının Genel Müdürlük tarafından belirlendiği antivirüs yazılımının kullanılması zorunludur.

(24) Bakanlık bilişim kaynaklarında ve ağında zararlı yazılım tespit edilen, saldırmaya yönelik teşebbüste bulunan ve kullanılan güvenlik sistemlerini aşmaya, atlatmaya yönelik her türlü tünel, Proxy, VPN vb. program kullanan kullanıcı veya kurumların, internet ve intranet erişimleri kesilir. İlgili durum ortadan kalkınca erişim tekrar sağlanır. Erişim politikalarını ve sistemlerini aşmaya veya bilişim sistemlerine saldırmaya yönelik girişimde bulunan kullanıcı veya kurum hakkında yasal işlem başlatılır. Ayrıca Bakanlık sistemlerine yönelik dışarıdan VPN, Proxy, tünel vb. bağlantılarla erişim sağlanması (kullanıcının kendi IP adresi yerine sahte IP adresleri üzerinden erişmesi), saldırı girişiminde bulunulması durumunda ilgili erişimler engellenir. Erişim kesintileri ile ilgili süreçler Genel Müdürlük tarafından belirlenir ve yönetilir.

Sistem Odası Güvenliği

MADDE 13- (1) Sistem odasının üstünde ıslak zeminli (tuvalet, banyo vb.) oda bulunmamalıdır. Kurulumda jeneratör, kesintisiz güç kaynağı, klima ile yangın, duman, nem ve su sensörlü algılama- önleme sistemleri tercih edilmelidir. Mevcut kurulu sistem odaları yukarıda belirtilen niteliklere göre iyileştirilmelidir. Sistem odalarının giriş ve çıkış kapılarında gerekli güvenlik önlemleri (kilit, şifre, parmak izi, kamera vb.) alınmalıdır. Sistem yöneticisinin bilgisi ve izni dışında giriş çıkışlar yapılmamalıdır. Giriş çıkışlar kayıt altına alınmalıdır.

(2) Sistem odasında gürültü ve titreşime karşı yalıtım önlemi sağlanmalıdır. Bakım, kontrol ve acil durum çizelgeleri görünür bir panoda yer almalıdır. Sistem odasının periyodik olarak kontrolleri sağlanmalı ve ilgili çizelgelere işlenmelidir.

(3) Sistem odasında kesintisiz güç kaynağı ile soğutma sistemleri aktif olarak çalışmalıdır. Sistem odasında meydana gelen arıza vb. durumlarda Genel Müdürlüğe bilgi verilerek en kısa sürede arızanın giderilmesi sağlanmalıdır.

(4) Bakanlık teşkilatında yer alan sistem odalarının tasarım ve işletme süreçleri Genel Müdürlük koordinasyonunda yapılmalıdır.

DÖRDÜNCÜ BÖLÜM

Bilgi Güvenliği Yönetim Sistemi ve Temel İlkeleri

Bilgi Güvenliği Yönetim Sistemi

MADDE 14- (1) Bakanlık merkez ve taşra teşkilatı ile bağlı kuruluşlarda yer alan birimlerde, başta kuruma ait veriler olmak üzere, yazılı veya elektronik ortamda saklanan her türlü bilginin gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla BGYS tesis edilir.

(2) BGYS'nin tesis edilmesi ve etkin bir şekilde işletilmesi için, üst yönetim desteği ve katılımı zorunludur. Genel Müdürlük bilgi güvenliği ile ilgili tedbirlerin alınmasını sağlamaktan birinci derecede sorumludur.

(3) BGYS tesis edilmesi için alınması gereken tedbirler, bilgi güvenliği politikaları güvenlik ihtiyaçları dikkate alınmak suretiyle, Genel Müdürlük tarafından ayrıntılı olarak belirlenir, yazılı hale getirilir ve tüm kullanıcılara duyurulur.

(4) Bilgi güvenliği politikası ile belirlenen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar BGYS prosedürleri ile düzenlenir. Kurum personeli ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

(5) Tesis edilen BGYS için herhangi bir belgelendirme kuruluşundan sertifika alınması zorunlu değildir.

(6) Etkin bir BGYS tesis edilmesi için risk yönetimi yapılır. Tespit edilen riskler için riski azaltacak veya kaldıracak tedbirler belirlenir ve uygulanır. Risk yönetimi süreçleri süreklilik arz eder.

(7) Bilgi işleme faaliyetlerinin büyük oranda siber ortam üzerinden yapılması nedeniyle, siber güvenlik tedbirlerinin alınması için azami özen gösterilir.

(8) Bilgi güvenliğinin sağlanması için sadece siber güvenlik ile ilgili tedbirlerin alınması yeterli değildir. Personel, evrak, donanım, fiziksel ve çevre güvenliği için de güvenlik tedbirleri alınması gerekir.

(9) Kullanıcılar, BGYS kapsamında hazırlanan politikalarına uymak zorundadır ve görevlerini ifa ederken öğrenmiş oldukları bilgileri, sır saklama yükümlülüğü uyarınca süresiz olarak saklamakla yükümlüdür. Kullanıcılar, kurumun kritik bilgisinin ortaya çıkmasına veya kurum servislerinin ulaşılmaz hale gelmesine sebep olabilecek tüm eylemlerden kaçınır.

(10) BGYS politikalarına ve sır saklama yükümlülüğüne uymayanlar hakkında 657 sayılı Devlet Memurları Kanunu'nun veya iş sözleşmesinin ilgili hükümleri ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ilgili hükümleri uyarınca işlem yapılır.

Politika, Prosedür, Talimatların hazırlanması ile değişikliklerin yönetimi

MADDE 15- (1) BGYS dokümanları, planlanan zaman aralıklarında veya teknik gereklilikler ortaya çıktığında uygunluğu, elverişliliği ve etkinliğinin sürekliliğini belirlemek amacıyla Genel Müdürlükçe belirlenen personel vasıtasıyla gözden geçirilir.

(2) BGYS ile ilgili duyurular Genel Müdürlük internet sitesinde yapılır.

BGYS'nin Uygulanması ve SOME

MADDE 16- (1) BGYS dökümanlarında yer alan hususların hayata geçirilmesi ve takibi için Genel Müdürlük tarafından eylem planları hazırlanır ve yayımlanır.

(2) Bakanlık birimlerinde eylem planında belirtilen konularda çalışmalar yapılır ve neticeleri, planda belirtilecek süreçlere uygun olarak Genel Müdürlüğe bildirilir.

(3) Genel Müdürlük veri merkezinden bağımsız yönetilen, ayrı veri merkezi/sistem odası bulunan Bakanlık birimleri bünyesinde, bilgi güvenliği ve siber olaylara müdahale faaliyetlerini yürütmek ve koordine etmek üzere, Bakanlık bünyesinde oluşturulan SOME Ekibinde görevlendirilmek üzere "bilgi güvenliği yetkilisi" görevlendirilir.

Bilgi güvenliği ihlal olaylarının yönetimi

MADDE 17- (1) Bakanlık çalışanları ve vatandaşlar tarafından tespit edilen Bakanlık ile ilgili her türlü bilgi güvenliği ihlal olayı, Genel Müdürlüğe bildirilir ve raporlanır.

(2) Bildirilen olaylar, Genel Müdürlük ekipleri tarafından değerlendirilir. Bakanlık genelini ilgilendirecek şekilde iş sürekliliğine zarar veren veya durduran, acil müdahale gereken, kurum imajına zarar verebilecek ihlal olaylarına Genel Müdürlük koordinatörlüğünde işlem yapılır ve neticesi bildirim yapan kişiye/birime iletilir.

(3) Bakanlık genelini ilgilendirmeyen ve yerel olarak incelenmesi gereken hususlar, Genel Müdürlük tarafından ilgili kurumun bilgi güvenliği yetkilisine ve/veya SOME ekip liderine bildirilir ve yerinde işlem yapılması sağlanır.

(4) Genel Müdürlük, bilişim kaynaklarının yönergeye aykırı etkinlikler dâhilinde kullanılması durumunda; gerçekleştirilen eylemin; yoğunluğuna, kaynaklara veya kişi/kurumlara verilen zararın boyutuna ve tekrarına göre aşağıdaki işlemlerin bir ya da birden fazla maddesini sıra ile ya da sırasız uygulayabilir;

a) Kullanıcı sözlü veya yazılı olarak bilgilendirilir.
b) Kullanıcıya tahsis edilmiş kurum bilişim kaynakları sınırlı veya sınırsız süre ile erişime kapatılır.

c) Yönergeye aykırı kullanım halinde kullanıcı hakkında gerektiğinde idari ve adli soruşturma açılması için gerekli işlemler başlatılır.

(5) Eğer ihlal olaylarının personel tarafından kasıtlı yapıldığı anlaşılırsa 657 sayılı Devlet Memurları Kanunu gereğince personel hakkında işlem yapılır.

(6) Çeşitli kaynaklardan derlenen siber güvenlik ile ilgili tehdit, açıklık, alarm ve uyarıların duyurulması maksadıyla kullanılacak sistem Genel Müdürlük tarafından belirlenir.

Bilgi güvenliği denetimi

MADDE 18- (1) Bakanlığın bilgi güvenliği politika ve standartlarıyla ilgili tüm bilgi güvenliği denetimleri Genel Müdürlük tarafından yapılır veya yaptırılır.

(2) Genel Müdürlük, önceden makam onayı almak ve ilgili birimlere bilgi vermek şartıyla, Bakanlık merkez ve taşra teşkilatı ile bağlı ve ilgili kuruluşlara sızma ve sosyal mühendislik testleri ve zafiyet taraması gerçekleştirir.

(3) Bakanlık bağlı ve ilgili kuruluşlar ile taşra teşkilatları, önceden makam onayı almak ve ilgili birimlere bilgi vermek şartıyla, kurumsal SOME vasıtasıyla kendi bağlısı birimlerde sızma ve sosyal mühendislik testleri yapar veya yaptırır.

(4) Genel Müdürlük, bilgi güvenliği denetimi ile sızma ve sosyal mühendislik testi yapacak personelin niteliklerini belirler.

(5) Genel Müdürlük, yasal hükümler çerçevesinde bilişim kaynaklarını ve bunlarla gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak inceleme ve denetleme hakkını saklı tutar.

Bilgi Güvenliği ve SOME Eğitimleri

MADDE 19- (1) Genel Müdürlük tarafından bilgi güvenliği / siber güvenlik konularına yönelik eğitim, tatbikat, seminer, konferans, sempozyum gibi faaliyetler planlanır ve uygulanır. Ulusal ve uluslararası düzeyde planlanan benzeri etkinliklere Genel Müdürlük koordinatörlüğünde katılım sağlanabilir.

(2) Görev yapan personelin bilgi güvenliği farkındalık seviyesinin artırılması maksadıyla ihtiyaç duyulan eğitimler, Genel Müdürlük tarafından planlanır ve uygulanır.

(3) Siber güvenlik ile ilgili kurum çalışanlarını bilinçlendirmeye yönelik periyodik olarak bilgi güvenliğiyle ilgili hatırlatma e-postaları gönderilir.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Bilgi güvenliği ve standartları

MADDE 20- (1) Genel Müdürlük, bilgi güvenliği çalışmalarının standardize edilmesi ve çalışmalara sistematik bir anlayış getirilmesi için çalışır. Bu amaç ile konuya ilişkin ulusal ve uluslararası standartları kullanır, bunu belgeleyen sertifikaların temini yönünde çalışmalar yapar. Bu konuda ulusal ve uluslararası kuruluşlarla işbirliği gerçekleştirir, siber güvenlik tatbikatlarına katılım sağlar.

Yürürlük

MADDE 21- (1) Bu Yönerge onaylandığı tarihte yürürlüğe girer.

Yürütme

MADDE 22- (1) Bu Yönerge hükümlerini Kültür ve Turizm Bakanı yürütür.