DİYANET İŞLERİ BAŞKANLIĞI
BİLİŞİM KAYNAKLARI BİLGİ VE SİSTEM GÜVENLİĞİ YÖNERGESİ (*)

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönergenin amacı, Diyanet İşleri Başkanlığı bünyesinde bulunan bilişim kaynaklarının kullanımına yönelik usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönerge, Başkanlık merkez ve taşra teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle Başkanlık bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları kapsar.
*

Dayanak

MADDE 3- (1) 633 sayılı Diyanet İşleri Başkanlığının Kuruluş ve Görevleri Hakkında Kanun hükümlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönergede geçen;

a) Başkanlık: Diyanet İşleri Başkanlığını,

b) Bilişim kaynakları: Elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılımı, donanımı, araç ve gereçlerini,

c) E-posta: İnternet üzerinden bilgisayarlar aracılığıyla bilgi alışverişini sağlamak için kullanılan elektronik haberleşme sistemini,

ç) Firma personeli: Sözleşme, plan ve şartnamelere uygun biçimde bir işi/projeyi yapmayı üstlenen, bu amaçla işgücü, malzeme ve ekipman sağlayarak gerekli yöntemle istenen işi/projeyi tamamlamayı taahhüt eden resmi veya özel kurum veya kuruluş personelini,

d) Konuk: Başkanlık bünyesinde kullanmış olduğu bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemleri üzerinde yetkilendirilmemiş olan Başkanlık personeli dışındaki kişiler ile görev yeri dışında çalışan Başkanlık personelini,

e) Kullanıcı: Başkanlık bünyesinde yer alan bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemlerinden yararlanan tüm Başkanlık personeli ile Başkanlık bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları,

f) Paydaş: Ortak çalışma yapılan kurum veya kuruluşları,

g) Personel: Başkanlık merkez teşkilatı ile il ve ilçe müftülükleri çalışanlarını,

ğ) Sistem yöneticisi: Uygulama ve/veya donanımdan sorumlu personeli,

h) Yüklenici firma: Sözleşme, plan ve şartnamelere uygun biçimde bir işi/projeyi yapmayı üstlenen, bu amaçla işgücü, malzeme ve ekipman sağlayarak gerekli yöntemle istenen işi/projeyi tamamlamayı taahhüt eden resmi veya özel kurum veya kuruluşu,

ifade eder.

---

* 21/09/2012 tarihli ve 100 sayılı Başkanlık onayı ile yürürlüğe konulmuştur.

İKİNCİ BÖLÜM
Sorumluk ve Genel Kurallar

Sorumluluk

MADDE 5- (1) 5651 sayılı Kanun ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla, Başkanlıkça uygun görülen sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtları, ajanlı veya ajansız iz toplama yöntemleri kullanılarak toplanır ve en az 6 ay süreyle Başkanlıkça saklanır.

(2) Başkanlık 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; 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.

(3) Bu Yönerge kapsamında bilgi ve sistem güvenliğinin planlı, sorunsuz, güvenli ve disiplin içinde gerçekleştirilmesinden Başkanlık bilişim sistemlerinden yararlanan tüm Başkanlık personeli birinci derecede görevli ve sorumludur. Bu Yönerge kapsamında olup teknolojik değişikliklere ya da Başkanlığın genel politikasındaki ve hizmetlerindeki değişikliklere göre bu politikada gerekli düzenlemeler Başkanlıkça yapılır ve resmi internet sayfasında "Bilgi ve Sistem Güvenliği Politikaları" adı altında yayımlanır. Tüm Başkanlık personeli yayınlanan "Bilgi ve Sistem Güvenliği Politikaları" nı takip etmekle yükümlüdür.

(4) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve bu Kanuna ek olarak çıkarılan yönetmeliklere göre; internet kullanım hizmeti veren her kurum, kendi sunucuları üzerinden giden ve gelen tüm trafik bilgilerini (hangi IP adresinden, hangi adrese, hangi kullanıcı tarafından erişim yapıldığı gibi bilgiler) kayıt altına almak zorundadır. Bu nedenle kullanıcı; kişilik hakları saklı kalmak üzere internet ağı üzerindeki gelen ve giden tüm trafik bilgilerinin önceden kendisine haber vermeye gerek duyulmadan kayıt ve kontrol edilebileceğinden, bu bilgilerin istatistik ve raporlama amaçlı olarak kullanılabileceğinden haberdar olmak zorundadır.

Genel kurallar

MADDE 6- (1) Kurumun bilgi ve haberleşme sistemleri ve donanımları, internet, e-posta, bilgisayarlar ve bileşenleri dahil olmak üzere, kurum işlerinin yürütülmesi için kullanılmalıdır.

(2) Kullanıcılar, Kurum bünyesindeki bilişim kaynaklarını, bilgisayar ağını ve interneti;

a) Kurum ağına ve haricindeki bir sisteme, ağ kaynağına veya servisine saldırı niteliğinde girişimlerde bulunmak,

b) Diğer kullanıcılara ait verileri bozmak, değiştirmek ya da zarar vermek, şifrelerini bulmaya çalışmak, dosyalarına müdahale etmek, gizlilik hakkını ihlal etmek,

c) Genel ahlak ilkelerine aykırı, her türlü materyali üretmek, barındırmak, ya da dağıtmak,

ç) Gerçek dışı, sıkıntı ve rahatsızlık verici, gereksiz endişe yaratacak, hukuki açıdan suç teşkil edecek her türlü 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) Siyasi ve ideolojik propaganda yapmak,

için kullanamaz.

(3) Kurum Bilişim Kaynakları, Temel Kullanım kapsamındaki ihtiyaçlar için hizmete sunulmaktadır. Bu kaynaklar israf amaçlı kullanılamaz.

(4) Kurum Bilişim Kaynakları,

a) İzinsiz ağ erişim cihazı (PC, PDA, vb…) dahil edilerek,

b) Kurum içi bilgi kaynaklarını (duyuru, haber, doküman vb.), yetkisiz ve/veya izinsiz olarak kişilere/kuruluşlara dağıtmak amacıyla,

c) Kurum'a ve üçüncü kişilere/kuruluşlara ait bilgilere ve kaynaklara (bilgisayar, bilgisayar ağı, yazılım ve servisler) izinsiz ve/veya yetkisiz erişim sağlamak amacıyla,

ç) Diğer kullanıcıların kaynak kullanım hakkını engelleyici faaliyetlerde bulunmak amacıyla,

d) Kaynaklara zarar verici/kaynakların güvenliğini tehdit edici biçimde,

kullanılamaz.

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

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

(7) Kullanıcı, başka kullanıcıların bilgisayarında yer alan şifrelendirilmiş paylaşım alanlarına çeşitli yöntemleri kullanarak erişemez ve bu türlü girişimlerde bulunamaz.

(8) Kullanıcı, ihtiyaç duyduğu yazılım, donanım ve lisansların kurulumu ve kaldırılması için İdare'ye başvurur. Yetkisiz kişilere yazılım, lisans ve cihaz vermez, cihazların içini açmasına ve cihaz üzerinde herhangi bir değişiklik (RAM, ekran kartı, TV kartı takılıp sökülmesi, yazılım yüklenmesi veya kaldırılması vb.) yapmasına izin vermez.

(9) Kurum Bilişim Kaynaklarında yaşanan arızalarda yetkili olmayan personel tarafından müdahale edilen bilgisayarlara teknik destek verilmez. Bu tür müdahaleler sonucunda ortaya çıkabilecek arızalar, maddi hasarlar ya da Kurumsal ağ güvenliğinin ihlaline yol açan uygulamalardan ilgili personel sorumludur.

(10) Kurum demirbaşına kayıtlı olmayan, personelin şahsi bilgisayarlarına arıza bakım ve teknik destek hizmeti sunulmaz.

(11) Kullanıcılar, Temel Kullanım kapsamında kullanımlarına tahsis edilen/mülkiyeti kendilerine ait olan kaynakların güvenliği ile ilgili kişisel önlemlerini alırlar, bu kaynaklar üzerinde yer alan bilgileri, kritik olma düzeyine göre yedekleme yaparlar.

(12) Kurum Bilişim Kaynakları, Kurum yönetiminin yetkilendirdiği makamlarca belirlenmiş kurallar ve yönergeler çerçevesinde, yetkinin veriliş amacını aşmayacak şekilde ve yapılacak her iş için uygun yetkilendirme ile kullanılır, yetki almadan değiştirilemez ve ortadan kaldırılamaz.

ÜÇÜNCÜ BÖLÜM
Bilgi ve Sistem Güvenliği Kuralları ve Politikaları

Aktif dizin hizmetleri kuralları

MADDE 7- (1) Başkanlık bünyesinde çalışmakta olan veya işe başlayan her personel ile paydaş ve konuklar için aktif dizin kullanıcı hesabı açılır.

(2) Kullanıcı, kendisine verilen "kullanıcı adı"nı ve "şifresi"ni bir başkası ile paylaşmaz ve bir başkasına kullandırmaz. Kullanıcı, "kullanıcı hesabına" ait geçici şifresini derhal değiştirerek, 9 uncu maddede yer alan şifre politikasına uygun olarak şifresini oluşturur.

(3) Kullanıcının Başkanlıkça 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. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.

(4) Her bir kullanıcı, bilgisayarda kendi "kullanıcı adı" ve "şifresi" 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) Merkezdeki her bir son kullanıcı, etki alanı üyesi olmalıdır. Etki alanında olmayan kullanıcıların internet erişimleri engellenir.

E-posta işlemleri kuralları

MADDE 8- (1) Kurum e-posta kaynakları; öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalır.

(2) Kullanıcı kendisine ait e-posta parolasının güvenliğinden ve kendi kullanıcı hesaplarıyla gerçekleştirdiği tüm e-posta işlemlerinden sorumludur.

(3) Kullanıcılar, elektronik ileti (e-posta) hesaplarına ait kullanıcı adı ve şifresinin sadece kendisinde olması gerektiğini, bu türden özel gizlilik ve güvenlik bilgilerini başkası ile paylaşmayacağını veya şifresinin üçüncü kişilerce ele geçirilmesi durumunda kendisi tarafından şifre değişikliği yapmak ve gerekli tedbirleri almak zorundadır.

(4) Kurum e-posta kaynakları; uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.

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

(6) Kurum e-posta kaynakları; rastgele ve alıcının istemi dışında "zincir e-postalar", reklam, aldatma, karalama, hakaret, tehdit gibi istenmeyen mesajlar (SPAM iletiler) göndermek için kullanılamaz.

(7) Kurum e-posta kaynakları; her türlü yasadışı ya da genel ahlaka aykırı bilgi ve belgeleri, bir virüs veya başka bir zararlı unsur içeren mesajları iletmek için kullanılamaz.

(8) Kurum e-posta kaynakları; lisansı olmayan hiçbir yazılımın alınması, gönderilmesi veya saklanması için kullanılamaz.

(9) Kullanıcıların tüm e-posta hesaplarında; tanınmayan e-postaların açılması, eklentilerinde (attachment) bulunan dosya veya programların indirilip çalıştırılması kaynaklı oluşabilecek güvenlik sorunlarının sorumluluğu kullanıcıya aittir. Bu itibarla kullanıcı tanımadığı kişilerden gelen özellikle eki (attachment) olan e-postaları önce zararlı kodlara ve virüslere karşı taramadan geçirmek ve mümkünse silmek zorundadır.

(10) Kurum, yasal hükümler çerçevesinde e-posta sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.

(11) Güvenlik ve performans açısından e-posta eklenti boyutu en fazla 10 MB olmalıdır.

(12) Kullanıcının e-posta kutusunun üzerinde aşağıdaki limitler uygulanır.

a) E-posta kutusu boyutu 500 MB'ı geçtiğinde kullanıcı uyarılır.

b) E-posta kutusu boyutu 550 MB'ı geçtiğinde kullanıcı e-posta gönderemez.

c) E-posta kutusu boyutu 600 MB'ı geçtiğinde kullanıcı e-posta gönderemez ve alamaz.

(13) Kullanıcı mail hesapları için öngörülen kotadan dolayı bir problem yaşamaması için mail hesabında mail büyüklüğü fazla olan mailleri barındırmamalı, gereksiz iletileri silmelidir.

(14) Başka bir kullanıcının posta sunucusu (mail server) veya posta hesabı ilgili kişinin açık izni olmadan mesaj gönderme amacıyla kullanılamaz.

(15) 90 gün süreyle kullanılmayan e-posta adresleri kullanıcıya haber verilmeden ilgili sunucu güvenliği ve veri depolama alanının boşaltılması için kapatılır ve ilgili kullanıcının dosyaları silinir.

Şifre politikası

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

(2) Kullanıcının şifrelerini belirlerken dikkat edeceği kurallar şunlardır:

a) Şifreler en az 8 karakter olmalıdır.

b) Şifreler küçük harf, büyük harf, rakam ve simgelerin kullanıldığı karışık yapıda olmalıdır.

c) Şifrelerin Başkanlıkça belirlenecek sayıda hatalı girilmesi sonucu, kullanıcı hesabı Başkanlığın politikalarına bağlı olarak kilitlenebilir. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.

ç) Şifreler en geç 3 ayda bir değiştirilir.

d) "Yönetici/Admin" kullanıcı şifreleri sadece sistem yöneticilerinde olur, kesinlikle son kullanıcılarla ve yüklenici firmalarla çalışıldığı zaman firma personeliyle paylaşılmaz.

e) Şifreler herhangi bir kişi ile paylaşılmaz.

Temiz masa - temiz ekran politikası

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

(2) Personel, bilgisayarını belli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlar.

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

(4) Personel, bilgisayarındaki, USB belleğindeki, harici diskindeki ve benzeri veri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. USB veya harici diske gizli/önemli verilerin konulması gerekiyorsa kriptolanarak/şifrelenerek saklanır.

Ağ ve internet kullanımı

MADDE 11- (1) İnternet ağı eğitim, bilimsel araştırma, teknik gelişme, teknoloji transferi, bilimsel teknik ve kültürel bilginin yayılması gibi profesyonel amaçlar içindir.

(2) Kurum internet kaynakları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi, için kullanılır. Ayrıca, kurum adına araştırma ve planlama, kurumun iş ve işlemleri için yapılacak olan bütün işler için kullanılır.

(3) Kurum çıkarlarıyla çakışmadığı sürece internet kaynaklarının kişisel kullanımına İdarenin onayı ile izin verilmektedir.

(4) Kurum internet kaynakları kullanılırken ilgili yasa ve düzenlemelere uymak zorundadır.

(5) Kullanıcılar kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bunun için kullanıcılar kimlik bilgilerini uygun şekilde saklamak ve başkaları ile paylaşmamak zorundadır.

(6) Kurum internet kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.

(7) Resmi kurum işlerinin yürütülmesi dışında sohbet guruplarına, forumlara, elektronik haber gruplarına katılmak yasaktır.

(8) Kurumun kritik bilgisinin ortaya çıkmasını veya kurum servislerinin ulaşılamaz hale gelmesini sağlayacak tüm aktiviteler yasaktır.

(9) Kurumun internet kaynakları onaylanmamış veya ticari hiçbir yazılımın dağıtılması, indirilmesi veya yüklenilmesi için kullanılamadığı gibi Lisansı alınmamış hiçbir üründe kullanılamaz veya yüklenemez.

(10) İndirilen tüm yazılımlar kullanılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmelidir.

(11) Kurum, yasal hükümler çerçevesinde internet sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.

(12) Kurumsal ağ güvenliği açısından tehlike yaratabilecek nitelikte zararlı olduğu tespit edilen internet adreslerine erişim tüm kullanıcılar için engellenmektedir. Kullanıcılar tarafından bu tür engellemelerin kaldırılması konusunda İdare'ye talepte bulunulmayacaktır.

(13) Kurumsal ağa dâhil edilecek bilgisayar ve diğer cihazlar Kurum'un belirlediği standartlara göre kullanılacak ve tüm personel bu standartlara uyacaktır.

(14) Kurumsal ağa bağlı tüm bilgisayarların ve bunlar üzerindeki verilerin güvenliğini tehlikeye sokacak şekilde güvenlik ihlali yaratılmaması, kurumsal ağ trafiğinin olumsuz yönde etkilenmemesi, sistem kaynaklarının gereksiz şekilde tüketilerek ağ üzerinden kullanılan uygulama yazılımlarının veri tabanı sunucuları ile iletişiminin olumsuz yönde etkilenmemesi için, tüm kullanıcılar;

a) İnternet üzerinden kendi bilgisayarlarına özel yazılım, oyun, film, mp3 vb. materyalleri indirmezler,

b) İnternet üzerinden canlı televizyon ve radyo yayınları izlenemez/dinlenemez,

c) Web kamera vb. görüntüleme araçları kullanılamaz,

ç) Resmi işlemler dışında internet üzerinden interaktif uygulamalar kullanılamaz,

d) Kurumsal ağ üzerindeki bilgisayarlara yetkisi olmayan kişilere erişim izni verilemez,

e) Ağ kaynağına veya servisine saldırı amaçlı (DOS saldırısı, port/network taraması, paket dinleme, ağ izleme v.b. uygulamalar ile IP (internet protokol numarası) değiştirme vb. işlemler.) zarar verecek girişimlerde bulunamazlar.

(15) Kullanıcılar ağ ve internet hizmetinin verilmesini sağlayan donanıma (switch, kablo, duvar prizi, vb.) hiçbir şekilde müdahale edemez ve ayarlarını değiştiremezler. İdarenin bilgisi ve onayı olmadan networke switch, hub ya da kablosuz erişim cihazı dahil edilemez.

(16) Kullanıcıların Kurum merkezindeki bilgisayarlardan Kurumsal ağ dışında cep telefonu, 3G modem, vb. cihazları kullanarak internete çıkmaları yasaktır.

(17) 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.

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

(19) Kullanıcılar;

a) Kurum sunucuları üzerinde kendisine tahsis edilen kullanıcı adı, şifre ve IP (Internet Protocol) adresi kullanılarak gerçekleştirilen her türlü etkinlikten,

b) Kendisine tahsis edilen bilgisayar üzerinde bulundurduğu belge, doküman, yazılım gibi her türlü kaynağın içeriğinden,

c) Bilişim sisteminin kullanımı hakkında yetkili makamlar tarafından talep edilen bilgilerin doğru ve eksiksiz verilmesinden,

ç) Kurum tarafından sağlanan güvenlik programlarının aktif olarak kullanılmasından ve güncellenmesinden,

d) Bilişim sisteminin kullanım kurallarına, kanun ve yönetmelikler ile Başkanlığın tabi olduğu mevzuata uygun olarak kullanımından,

sorumludur.

(20) İki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan Peer-to-peer (P2P) dosya paylaşım programları ile download edilen film, mp3 ve lisanssız yazılımlar, telif haklarını ihlal etmekle kalmayıp, download esnasında yüksek bant genişliği tutarak ağ kullanımına kaynak bırakmamakta ve trafikte yavaşlamaya neden olmaktadır. Bu sebeple kullanıcılar, bilgisayarlarında bu tür yazılımları bulunduramaz ve dağıtımını yapamazlar.

(21) Dosya transferleri Kurum sunucuları üzerinden hizmet verilen resmi e-postalara eklenmek suretiyle veya kurumsal ağ paylaşımları ile gerçekleştirilecektir.

(22) Dosya paylaşımı, anlık mesajlaşma programları ve yoğun ağ trafiğine sebep olan uygulamalar gerekli görüldüğünde Kurum tarafından filtrelenir.

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

(24) Kurum ağına idarenin bilgisi dışında herhangi bir aktif ağ cihazı eklenemez.

(25) Kullanıcılar, kişisel bilişim kaynaklarını kurum ağında idareden izin almadan kullanamaz.

(26) Kurum merkezinde çalışmakta olan veya işe yeni başlayan her personel için aktif dizin kullanıcı hesabı açılır. Aktif dizin üyesi olmayan bilgisayarlara teknik destek hizmeti verilmeyecektir.

(27) Kullanıcı, kendisine verilen "kullanıcı adı"nı ve "şifresi"ni bir başkası ile paylaşmaz ve bir başkasına kullandırmaz.

(28) Kullanıcının Kurumca 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. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.

(29) Her bir kullanıcı, bilgisayarda kendi "kullanıcı adı" ve "şifresi" ile oturum açarak çalışır. Çalışması biten kullanıcı, oturumu veya bilgisayarını kapatarak bilgisayara başkalarının fiziksel erişimini engeller. Bilgisayar başından kısa süreli ayrılmalarda bilgisayar oturumunu kilitler.

(30) Merkezdeki her bir son kullanıcı, ağa dahil olarak etki alanı üyesi olmalıdır. Kurum kurumsal ağ güvenliğinin sağlanabilmesi için ağa dâhil olmayan, etki alanında bulunmayan bilgisayarlar internet erişimi, güvenlik ve antivirüs yazılımları vb. ağ hizmetlerinden faydalanamayacaktır.

DÖRDÜNCÜ BÖLÜM
Çeşitli Hükümler

Yaptırım ve uygulama

MADDE 12- (1) Kurum Bilişim Kaynaklarının genel kurallara aykırı etkinlikler dâhilinde kullanılması durumunda;

Kurum gerçekleştirilen eylemin;

a) Yoğunluğuna,

b) Kaynaklara veya kişi / kurumlara verilen zararın boyutuna,

c) Tekrarına göre aşağıdaki işlemlerin bir ya da birden fazla maddesini, sıra ile ya da sırasız uygulayabilir;

I. Kullanıcı sözlü ve/veya yazılı olarak uyarılır.

II. Kullanıcıya tahsis edilmiş Kurum Bilişim Kaynakları sınırlı veya sınırsız süre ile erişime kapatılabilir.

III. Kurum bünyesindeki idari soruşturma mekanizmaları harekete geçirilebilir.

IV. Adli yargı mekanizmaları harekete geçirilebilir.

Hüküm bulunmayan hususlar

MADDE 13- (1) Bu Yönergede hüküm bulunmayan hususlarda ilgili diğer mevzuat hükümlerine göre işlem yapılır.

Yürürlük

MADDE 14- (1) Bu Yönerge onaylandığı tarihte yürürlüğe girer.

Yürütme

MADDE 15- (1) Bu Yönerge hükümlerini Diyanet İşleri Başkanı yürütür.