



T.C  
HAZRO KAYMAKAMLIĞI  
İlçe Milli Eğitim Müdürlüğü

Sayı : 46201035-703.03-E.10849637

23.10.2015

Konu : İnternet ve Bilgi Güvenliği

..... MÜDÜRLÜĞÜNE

İlgi : İl Milli Eğitim Müdürlüğünün 23.10.2015 tarih ve 10813960 sayılı yazısı

İl Milli Eğitim Müdürlüğünün İnternet ve Bilgi Güvenliği ile ilgili yazısında Belirttiği üzere:Bilgi İşlem Dairesi Başkanlığının İnternet ve Bilgi Güvenliği ile ilgili ilgi (a) sayılı yazılarında, "2014 yılında yapılan iyileştirmelerle MEB ADSL VE MEB VDSL hızları güncellenmiştir. İlçe Milli Eğitim Müdürlükleri, Resmi Kurumlar ve Okullarımızda MEB ADSL /VDSL hattı kullanılması zorunludur. Her ne şekilde olursa olsun ( kişisel, okul aile birliği vb.) ADSL, 3G vb. hat kullanmak yasaktır. İhtiyaç durumunda 2. MEB ADSL hattı temin edilebilir. Aksi davranış tespit edilen personel veya kurum hakkında gerekli yasal süreç başlatılacaktır.Halka hizmet veren kurumlar ( Hizmetiçi Eğitim Enstitüsü, Öğretmenevi ve Halk Eğitim Merkezi) idari işlemler haricinde kapsam dışında tutulabilir. Resmi kurumlarımızın kullandıkları ADSL, 3G ve benzeri hatlar; adres bilgisi, abonelik gibi bilgilerle operatörlerden sorgulanarak kontrol edildiği" belirtilmektedir.

Bu durumda olan Okul/Kurumlarımızın ivedi olarak MEB ADSL /VDSL hattı dışındaki hatlarını iptal etmeleri hususunda;

Gereğini rica ederim.

Şahin SURMUŞ  
İlçe Milli Eğitim Şube Müdürü

Ek:İl MEM Yazısı (10 Sayfa )

Güvenli Elektronik İmza  
Aslı ile Aynıdır

23 / 10 / 2015

Hüriyet Mah. Şehitlik Cad. Hükümet Konağı Kat:3  
Elektronik Ağ: www.meb.gov.tr  
e-posta: hazro21@meb.gov.tr

Ayrıntılı bilgi için :Mehmet SAVUK Memur  
Tel: (0412)6712008  
Faks: (0412)6712407



T.C.  
DİYARBAKIR VALİLİĞİ  
İl Millî Eğitim Müdürlüğü

Sayı : 43289121-703.03-E.10813960  
Konu: İnternet ve Bilgi Güvenliği

23.10.2015

**İVEDİ**

..... KAYMAKAMLIĞINA  
( İlçe Millî Eğitim Müdürlüğü )

İlgi:a) Milli Eğitim Bakanlığı Bilgi İşlem Dairesi Başkanlığının 10.07.2015 tarih ve 49473396/703.03/7180248 sayılı yazısı.

b) 13.07.2015 tarih ve 43289121-703.03-E.7226234 sayılı yazımız.

İlgi (b) sayılı yazımızın ekinde gönderilen Bakanlığımız Bilgi İşlem Dairesi Başkanlığının İnternet ve Bilgi Güvenliği ile ilgili ilgi (a) sayılı yazılarında, "2014 yılında yapılan iyileştirmelerle MEB ADSL VE MEB VDSL hızları güncellenmiştir. İlçe Milli Eğitim Müdürlükleri, Resmi Kurumlar ve Okullarımızda MEB ADSL /VDSL hattı kullanılması zorunludur. Her ne şekilde olursa olsun ( kişisel, okul aile birliği vb.) ADSL, 3G vb. hat kullanmak yasaktır. İhtiyaç durumunda 2. MEB ADSL hattı temin edilebilir. **Aksi davranış tespit edilen personel veya kurum hakkında gerekli yasal süreç başlatılacaktır.** Halka hizmet veren kurumlar ( Hizmetiçi Eğitim Enstitüsü, Öğretmenevi ve Halk Eğitim Merkezi) idari işlemler haricinde kapsam dışında tutulabilir. Resmi kurumlarımızın kullandıkları ADSL, 3G ve benzeri hatlar; adres bilgisi, abonelik gibi bilgilerle operatörlerden sorgulanarak kontrol edildiği" belirtilmektedir.

Bu durumda olan Okul/Kurumların ivedi olarak MEB ADSL /VDSL hattı dışındaki hatlarını iptal etmeleri hususunda;

Bilgilerinizi ve gereğini rica ederim.

Mehmet OĞUZ  
Vali a.  
Milli Eğitim Müd. Yrd.

DAĞITIM :

—17 İlçe Kaymakamlığına  
(İlçe Millî Eğitim Müdürlüğü)

T.C.  
MİLLÎ EĞİTİM BAKANLIĞI  
Bilgi İşlem Grup Başkanlığı

Sayı : 49473396/703.03/861980

27/02/2014

Konu: İnternet ve Bilgi Güvenliği.

- İlgi: a) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,  
b) 11.04.2012 tarihli ve 565 sayılı Millî Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi.

Bakanlık olarak, 5651 sayılı Kanun gereği, bilgi güvenliği kapsamında, sistem ve kullanıcı bazlı güncel politikalar uygulanmaktadır. Bilginin gizlilik, erişilebilirlik ve bütünlük özelliklerini muhafaza etmeye, bilginin geçtiği yerlerin nasıl sınıflandırılacağına ve nasıl koruma altına alacağına dair çözümler oluşturulmaktadır.

Temel amaçlarımızdan biri, hizmet verdiğimiz tüm kesimler için, güvenli ve kesintisiz ağ hizmetini sağlamaktır. Bu amaçla; gerçekleşmesi olası tehditlere karşı, iç ağdaki trafiği ve internet trafiğini sağlıklı yönetebilmek için güvenlik duvarı, saldırı tespit ve koruma sistemleri, içerik filtreleme, spam analizi, antivirus vb. ürün ve uygulamaları kullanılmaktadır.

11 Nisan 2012 tarihinde Bilgi ve Sistem Güvenliği Yönergesi çıkarılmıştır. Bu yönerge ile kurum çalışanlarımıza, sistem ve bilgi güvenliği kapsamında, uyulması gereken kurallar, olması ve olmaması gereken tasarruflar açıklanmıştır. Buna rağmen gerek Bakanlık personelimizin bir kısmı, gerekse kurum dışından kişiler, uygulanan çözümleri aşmaya yönelik tutumlarda bulunmaktadır. Bu amaçla, bilgi ve sistem güvenliği anlamında kurum politikalarını hiçe sayma, uygulanan filtreleme çözümlerini delme, gereksiz yüksek trafik oluşturma, güvensiz yazılım kullanma vb. gibi durumlar tespit edilmektedir. İlgili yönergenin 11. maddesinin 4. bendinde belirtildiği gibi "Telif hakları ve lisansları ihlal eden, Bakanlık ağında yoğun ağ trafiğine sebep olan, iki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan noktadan noktaya (Peer-to-peer - P2P) uygulamalar kullanılamaz. Dosya paylaşımı, anlık mesajlaşma programları ve yoğun ağ trafiğine sebep olan uygulamalar gerekli görüldüğünde Bakanlık tarafından filtrelenir." denilmektedir. Bu sebeple Bakanlık hattını kullanan kullanıcıların uygulanan güvenlik politika ve kuralları çerçevesinde davranmaları gerekmektedir.

Bakanlığımız olarak TTPVN Metro İnternet Projesinin hayata geçirilmesi ile birlikte İl Millî Eğitim Müdürlüklerimizde yer alan ADSL, VDSL gibi bağlantıların iptal edilerek Bakanlık hattı haricinde herhangi bir hat(ADSL, 3G, wireless vb.) kullanılması yasaklanmıştır. Ancak İl Millî Eğitim Müdürlüklerimiz bünyesinde kurum, şahsi veya benzeri yöntemlerle ADSL, VDSL, 3G, wireless gibi bağlantıların yapıldığı tespit edilmiştir. İlgili yönergenin 11. Maddesinin 6.bendinde "Kurum ağına sistem yöneticisinin bilgisi dışında herhangi bir aktif ağ cihazı eklenemez." denilmektedir.

---

Bu belge, 5070 sayılı Elektronik İmza Kanununun 5 inci maddesi gereğince güvenli elektronik imza ile imzalanmıştır

Bu sebeple İl Millî Eğitim Müdürlüğü bünyesinde yer alan Bakanlık hattı haricindeki tüm internet hatlarının (ADSL, VDSL 3G, Wireless vb.) acilen iptal edilmesi, gelecekte Bakanlığın ilgili birimlerinin bilgisi olmadan bu ve benzeri bağlantılara izin verilmemesi ile belirtilen bağlantıları iptal ettirmeme konusunda ısrarcı davranış sergileyen personel veya kurum hakkında gerekli yasal süreç başlatılması gerekmektedir.

Oluşması muhtemel bilişim suçlarının önüne geçebilmek amacıyla yukarıda belirtilen çalışmaların acilen tamamlanarak, birimlerinizde çalışan personelin, sözü edilen ilgili Kanun ve Yönerge doğrultusunda tekrar bilgilendirilmesi hususunda;

Bilgilerinizi ve gereğini rica ederim.

Yusuf TEKİN

Bakan a.

Müsteşar

DAĞITIM:

B Plânı.

---

Bu belge, 5070 sayılı Elektronik İmza Kanununun 5 inci maddesi gereğince güvenli elektronik imza ile imzalanmıştır

Atatürk Blv. 06648 Kızılay/ANKARA  
Elektronik Ağ <http://bigb.meb.gov.tr>  
e-posta: bigb@meb.gov.tr

Ayrıntılı bilgi için: M. KARADAĞ - Şb. Müd.  
Tel : (0 312) 413 11 82  
Faks: (0 312) 417 50 09

**T.C.**  
**MİLLÎ EĞİTİM BAKANLIĞI**  
**Bilgi İşlem Dairesi Başkanlığı**

**Sayı :** 49473396/703.03/7180248

10.07.2015

**Konu:** İnternet ve Bilgi Güvenliği

İlgi: a) Bilgi İşlem Dairesi Başkanlığının 27/02/2014 tarihli ve 49473396/703.03/861980 sayılı yazısı.

b) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.

c) 11.04.2012 tarihli ve 565 sayılı Millî Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi.

Bakanlık olarak, temel amaçlarımızdan biri, hizmet verdiğimiz tüm kesimler için, güvenli ve kesintisiz ağ hizmetini sağlamaktır. Bu amaçla; gerçekleşmesi olası tehditlere karşı, iç ağıdaki trafiği ve internet trafiğini sağlıklı yönetebilmek için güvenlik duvarı, saldırı tespit ve koruma sistemleri, içerik filtreleme, spam analizi, antivirus vb. ürün ve uygulamaları kullanılmaktadır.

11 Nisan 2012 tarihinde ilgi (c) de yer alan Bilgi ve Sistem Güvenliği Yönergesi çıkarılmıştır. Bu yönerge ile kurum çalışanlarımıza, sistem ve bilgi güvenliği kapsamında, uyulması gereken kurallar, olması ve olmaması gereken tasarruflar açıklanmıştır. Bilgi ve sistem güvenliği anlamında kurum politikalarını hiçe sayma, uygulanan filtreleme çözümlerini delme, gereksiz yüksek trafik oluşturma, güvensiz yazılım kullanma vb. gibi durumlar oluşabilmektedir. İlgi yönergenin 11. maddesinin 4. bendinde belirtildiği gibi “Telif hakları ve lisansları ihlal eden, Bakanlık ağına yoğun ağ trafiğine sebep olan, iki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan noktadan noktaya (Peer-to-peer - P2P) uygulamalar kullanılamaz. Dosya paylaşımı, anlık mesajlaşma programları ve yoğun ağ trafiğine sebep olan uygulamalar gerekli görüldüğünde Bakanlık tarafından filtrelenir.” denilmektedir. Bu sebeple Bakanlık TTPVN ve MEB ADSL hattını kullanan kullanıcıların ( İl ve İlçe Müdürlükleri, Resmi Kurumlar, Okullar ) uygulanan güvenlik politika ve kuralları çerçevesinde davranmaları gerekmektedir.

Oluşturulan bilgi güvenliği politikaları gereği başta merkez teşkilatlarımız olmak üzere bakanlığımız üzerinden hizmet alan tüm alt kurumlarımız bu politikalara tabidir. Bu anlamda merkez teşkilatlarda bulunan kullanıcılarımızın kaçınması gereken hususlar şu şekilde sıralanabilir: Kurumsal ağ dışında bağımsız bir internet hattına veya başka bir ağa katılmak, (ADSL, VDSL, wireless, 3G, vb.) kurum içinde kullanılan kullanıcı adı ve şifre bilgilerinin üçüncü kişilerle paylaşmak, çeşitli proxy programları ile meb güvenlik hizmetlerini atlatmaya çalışmak, farklı yazılımlar veya donanımlar yardımı ile meb sistemlerine, kurumsal ağ altyapısına saldırmak ve verilen hizmetleri kesintiye uğratmak veya uğratmaya çalışmak.

Bakanlığımız 2012 yılından itibaren İl Millî Eğitim Müdürlüklerini TTVPN Metro İnternet Projesine dahil etmiştir. Bu süreç ile birlikte İl Millî Eğitim Müdürlüklerimizde ve ek binalarda yer alan ADSL, VDSL gibi bağlantıların iptal edilmesi ilgi ( a) yazıda istenmiştir. Bu kapsamda İl Millî Eğitim Müdürlüklerinin Ağ alt yapıları yenilenmiş ve merkezi yönetime geçilmiştir. Son zamanlarda yapılan incelemelerde İl Millî Eğitim Müdürlüklerimiz bünyesinde kurum, şahsi veya benzeri yöntemlerle ADSL, VDSL, 3G, wireless gibi bağlantıların yapıldığı tespit edilmiştir.

Bu sebeple İl Millî Eğitim Müdürlüğü bünyesinde yer alan Bakanlık hattı haricindeki tüm internet hatlarının (ADSL, VDSL 3G, Wireless vb.) acilen iptal edilmesi, gelecekte Bakanlığın ilgili birimlerinin bilgisi olmadan bu ve benzeri bağlantılara izin verilmemesi ile belirtilen bağlantıların iptal ettirmeme konusunda ısrarcı davranış sergileyen personel veya kurum hakkında ilgi (a) da belirtilen yasal sürecin başlatılması gerekmektedir.

Ayrıca 2014 yılında yapılan iyileştirmelerle MEB ADSL VE MEB VDSL hızları güncellenmiştir. İlçe Millî Eğitim Müdürlükleri, Resmi Kurumlar ve Okullarımızda MEB ADSL /VDSL hattı kullanılması zorunludur. Her ne şekilde olursa olsun ( kişisel, okul aile birliği vb.) ADSL, 3G vb. hat kullanmak yasaktır. İhtiyaç durumunda 2. MEB ADSL hattı temin edilebilir. Aksi davranış tespit edilen personel veya kurum hakkında gerekli yasal süreç başlatılacaktır. Halka hizmet veren kurumlar ( Hizmetiçi Eğitim Enstitüsü, Öğretmenevi ve Halk Eğitim Merkezi) idari işlemler haricinde kapsam dışında tutulabilir. Resmi kurumlarımızın kullandıkları ADSL, 3G ve benzeri hatlar; adres bilgisi, abonelik gibi bilgilerle operatörlerden sorgulanarak kontrol edilmektedir.

Oluşması muhtemel bilişim suçlarının önüne geçebilmek amacıyla yukarıda belirtilen çalışmaların acilen tamamlanarak, birimlerinizde çalışan personelin, sözü edilen ilgili Kanun ve Yönerge doğrultusunda tekrar bilgilendirilmesi hususunda;

Bilgilerinizi ve gereğini arz/rica ederim.

Bilal TIRNAKÇI  
Bakan a.  
Bilgi İşlem Dairesi Başkanı

EK:

- 1.EK-1 İnternet ve Bilgi Güvenliği konulu yazı
- 2.EK-2 Bilgi ve Sistem Güvenliği Yönergesi

DAĞITIM:

A ve B Planı

**MİLLÎ EĞİTİM BAKANLIĞI**  
**BİLGİ VE SİSTEM GÜVENLİĞİ YÖNERGESİ**

**BİRİNCİ BÖLÜM**

**Amaç, Kapsam, Dayanak ve Tanımlar**

**Amaç**

**MADDE 1-** (1) Bu Yönergenin amacı, Millî Eğitim Bakanlığı bünyesinde bulunan bilişim kaynaklarının kullanımına yönelik usul ve esasları belirlemektir.

**Kapsam**

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

**Dayanak**

**MADDE 3-** (1) Bu Yönerge, 5/12/1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile 25/8/2011 tarihli ve 652 sayılı Millî Eğitim Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümlerine dayanılarak hazırlanmıştır.

**Tanımlar**

**MADDE 4-** (1) Bu Yönergede geçen;

- a) Bakanlık: Millî Eğitim Bakanlığını,
- b) Başkanlık: Bilgi İşlem Grup Başkanlığını,
- c) Bilişim kaynakları: Elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gerecini,
  - ç) E-posta: İnternet üzerinden bilgisayarlar aracılığıyla bilgi alışverişini sağlamak için kullanılan elektronik haberleşme sistemini,
  - d) 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,
  - e) Konuk: Bakanlık bünyesinde kullanmış olduğu bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemleri üzerinde yetkilendirilmemiş olan Bakanlık personeli dışındaki kişiler ile görev yeri dışında çalışan Bakanlık personelini,
  - f) Kullanıcı: Bakanlık bünyesinde yer alan bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemlerinden yararlanan tüm Bakanlık personeli ile Bakanlık bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları,
  - g) Kurum: 652 sayılı Kanun Hükmünde Kararnamenin 6 ncı ve 28 inci maddelerinde yer alan Bakanlık merkez teşkilatı ile il ve ilçe millî eğitim müdürlükleri ve bu müdürlüklere bağlı örgün ve yaygın eğitim kurumlarını,
  - ğ) Merkez: 652 sayılı Kanun Hükmünde Kararnamenin 6 ncı ve 28 inci maddelerinde yer alan Bakanlık merkez teşkilatı birimlerini,
  - h) Paydaş: Ortak çalışma yapılan kurum veya kuruluşları,
  - ı) Personel: Bakanlık merkez teşkilatı ile il ve ilçe millî eğitim müdürlükleri ve bu müdürlüklere bağlı örgün ve yaygın eğitim kurumlarındaki tüm çalışanları,
  - i) Sistem yöneticisi: Uygulama ve/veya donanımdan sorumlu personeli,
  - j) 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.



## İKİNCİ BÖLÜM

### Sorumluluk ve Genel Kurallar

#### Sorumluluk

**MADDE 5-** (1) 5651 sayılı Kanun ve 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 ajanlız iz toplama yöntemleri kullanılarak toplanır ve en az 6 ay süreyle Başkanlıkça saklanır.

(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; 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 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 Başkanlıkça yapılır ve resmi internet sayfasında "Bilgi ve Sistem Güvenliği Politikaları" adı altında yayımlanır. Tüm Bakanlık personeli yayınlanan "Bilgi ve Sistem Güvenliği Politikaları" nı takip etmekle yükümlüdür.

#### 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 şifrelendirilmiş paylaşım alanlarına çeşitli yöntemleri kullanarak erişemez ve bu türlü girişimlerde bulunamaz.

(4) Kullanıcı, çalışmalarının sonlandırılması ile birlikte 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 işlem olanaklarına erişim hakları kaldırılır.

(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 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 Başkanlığa 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.

*MA*



## ÜÇÜNCÜ BÖLÜM

### Bilgi ve Sistem Güvenliği Kuralları ve Politikaları

#### **Aktif dizin hizmetleri kuralları**

**MADDE 7-** (1) Bakanlık 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 kullanıdurmaz. 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) Kullanıcı, e-posta adresi olarak, Başkanlıkça kendisine tahsis edilen adresi kullanır. Bunun dışındaki e-posta servisleri resmî işlerde kullanılmaz.

(2) 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 kullanılmaz.

(3) Kullanıcı, Başkanlık tarafından kendisine tahsis edilen e-posta adresini sohbet yapmak için kullanmaz.

(4) Kullanıcı, hesabını ticari ve kâr 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 ve derhal silinir.

(6) Kullanıcı, kendisine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludur. Şifresinin başkası tarafından tespit edildiğini fark ettiği andan itibaren Başkanlıkla temasa geçip durumu haber vermekle yükümlüdür.

#### **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 6 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 altı 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) Tüm kullanıcılar interneti bilinçli bir şekilde kullanmak, başkalarının hakkını ihlal edici ve bilişim sisteminin işleyişini engelleyici, bozucu faaliyetlerde bulunmamakla yükümlüdür.

(2) Kullanıcılar;

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 tabii olduğu mevzuata uygun olarak kullanımından sorumludur.

(3) Kullanıcılar, Bakanlık bünyesindeki bilişim kaynaklarını, bilgisayar ağını ve interneti;

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) Siyasi ve ideolojik propaganda yapmak

için kullanamaz.

(4) Telif hakları ve lisansları ihlal eden, 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 yoğun ağ trafiğine sebep olan uygulamalar gerekli görüldüğünde Bakanlık tarafından filtrelenir.

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

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

(7) Kullanıcılar, kişisel bilişim kaynaklarını kurum ağına sistem yöneticisinden izin almadan kullanamaz.

(8) Kurum içinde hizmet veren sunucu, sistem veya kullanıcı bilgisayarlarına uzaktan erişim, zorunlu hallerde sistem yöneticisinin onayı/izni alınarak yapılır.

#### **İnternet sitesi barındırma hizmeti politikası**

**MADDE 12-** (1) Bakanlığımız Kurumları ile Bakanlığımız sorumluluğunda yürütülen projelere ait internet sitelerinin barındırma hizmeti Bakanlık sunucuları üzerinden yapılır.

(2) İletişim için kurum tüzel kişiliğine ait e-posta adresi kullanılır.

(3) Kurum internet sitelerinin hazırlanmasında, güncellenmesinde ve yönetilmesinde dikkat edilecek hususlar şunlardır:

a) Bakanlık tarafından belirlenen internet sitesi standartlarına göre hazırlanır.

b) Her türlü içerikten kurum amiri sorumludur.

c) Uygulamalara yetkisiz kişilerin erişimini engelleyen tedbirler alınır.

ç) Tüm şifrelerinin sorumluluğu kurum amirine aittir.

d) İçerikler kurum tarafından görevlendirilen yetkili ya da yetkililerce yedeklenir.

e) Herhangi bir saldırı hâlinde site üzerinde herhangi bir değişiklik yapılmaz ve Başkanlığa haber verilir.

f) Üzerinde virüs, truva atı ve yetkisiz erişime sebep olabilecek uygulamalar bulundurulmaz.

g) Yayınlanacak her türlü içerik telif hakları, fikrî haklar, şeref ve haysiyetin korunması ve gizlilikle uyumlu olur.

ğ) Bakanlığın herhangi bir politikasını, kuralını ya da düzenlemesini ihlal edemez.

### **DÖRDÜNCÜ BÖLÜM**

#### **Çeşitli Hükümler**

#### **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 Millî Eğitim Bakanı yürütür.