

AĞRI İL ÖZEL İDARESİ BİLGİ VE SİSTEM GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönergenin amacı, Ağrı İl Özel İdaresi bünyesinde bulunan bilişim kaynaklarının kullanımına yönelik usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönerge, Ağrı İl Özel İdaresi teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle idarenin bilişim kaynaklarını kullanma yetkisi verilen 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 hükümlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönergede geçen;

a) İdare: Ağrı İl Özel İdaresi ni,

b) Şube Müdürlüğü: Ağrı İl Özel İdaresi Bilgi İşlem Şube Müdürlüğü nü,

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

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

- g) Personel: Ağrı İl Özel İdaresi,Özel İdare İlçe Müdürlükleri ve bunlara bağlı tüm çalışanları,
- h) Sistem yöneticisi: Uygulama ve/veya donanımdan sorumlu personeli,
- i) 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,) Şube Müdürlüğünce 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 Şube Müdürlüğünce saklanır.

(2) İdare 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 İdarebilşim sistemlerinden yararlanan tüm İdarepersoneli birinci derecede görevli ve sorumludur. Bu Yönerge kapsamında olup teknolojik değişikliklere ya da İdare 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 İdare personeli yayımlanan “Bilgi ve Sistem Güvenliği Politikaları” nı takip etmekle yükümlüdür.

Genel Kurallar

MADDE 6-

(1)Kurum internet kaynakları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi,kurum adına araştırma ve planlama için kullanılır.

(2) Kurum çıkarlarıyla çakışmadığı sürece internet kaynaklarının kişisel kullanımına idarenin onayı ile izin verilmektedir.

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

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

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

(6) Resmi kurum işlerinin yürütülmesi dışında sohbet guruplarına, forumlara, elektronik haber guruplarına katılmak ,facebook,twitter,instagram ve diğer sosyal paylaşım sitelerine giriş yapmak yasaktır.

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

(8) Kurumun internet kaynakları onaylanmamış veya ticari hiçbir yazılımın dağıtılması, indirilmesi veya yüklenmesi için kullanılmadığı gibi Lisansı alınmamış hiçbir üründe kullanılamaz veya yüklenemez.

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

(10) Kurum, internet sistemlerini kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.

(11) 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 idareye talepte bulunulmayacaktır.

(12) Kurumsal ağa dâhil edilecek bilgisayar ve diğer cihazlar kurumun belirlediği standartlara göre kullanılacak ve tüm personel bu standartlara uyacaktır.

(13) 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.

(14) 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.

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

(16) 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.

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

(18) 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 kullanımını 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.

(19) 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 bulundurmaz ve dağıtımını yapamazlar.

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

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

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

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

(24) Kullanıcılar, kişisel bilişim kaynaklarını kurum ağına idareden izin almadan kullanamaz.

(25) 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.

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

(27) 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.

(28) 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.

(29) 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.

(30) 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.

ÜÇÜNCÜ BÖLÜM

Çeşitli Hükümler

Yaptırım ve uygulama

MADDE 7- 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 8-Bu Yönergede hüküm bulunmayan hususlarda ilgili diğer mevzuat hükümlerine göre işlem yapılır.

Yürürlük

MADDE 9- Bu Yönerge onaylandığı tarihte yürürlüğe girer.

Yürütme

MADDE 10- Bu Yönerge hükümlerini Ağrı Valisi yürütür.

Musa İŞİN
Ağrı Valisi