

DİYARBAKIR BÜYÜKŞEHİR BELEDİYESİ
BİLGİ VE SİSTEM GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1-(1) Bu Yönergenin amacı, DİYARBAKIR BÜYÜKŞEHİR BELEDİYESİ bünyesinde bulunan bilişim kaynaklarının kullanımına yönelik usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönerge, Diyarbakır Büyükşehir Belediyesi merkez ve bağlı birimlerinde görev yapan tüm personel ile kendilerine herhangi bir nedenle belediye bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları kapsar.

Hukuki 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 Kanunu, 3/7/2005 tarihli ve 5393 sayılı Belediye Kanunu, 10/7/2004 tarihli ve 5216 sayılı Büyükşehir Belediyesi Kanunu hükümlerine göre hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönergede geçen;

- a) **Belediye:** Diyarbakır Büyükşehir Belediyesini,
- b) **Başkanlık:** Bilgi İşlem Daire Başkanlığını,
- c) **Daire Başkanı:** Görev bölümünde birimin bağlı olduğu daire başkanını,
- d) **Birim amiri:** Diyarbakır Büyükşehir Belediyesi Başkanlığı bünyesindeki müdürleri,
- e) **Bilişim kaynakları:** Elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gerecini,
- g) **E-posta:** İnternet üzerinden bilgisayarlar aracılığıyla bilgi alışverişini sağlamak için kullanılan elektronik haberleşme sistemini,
- f) **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,
- g) **Konuk:** Belediye bünyesinde kullanmış olduğu bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemleri üzerinde yetkilendirilmemiş olan Belediye personeli dışındaki kişiler ile görev yeri dışında çalışan Belediye personelini,
- h) **Kullanıcı:** Belediye bünyesinde yer alan bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemlerinden yararlanan tüm Belediye personeli ile Belediye bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları,
- ğ) **Paydaş:** Ortak çalışma yapılan kurum veya kuruluşları,
- ı) **Personel:** Diyarbakır Büyükşehir Belediyesi merkez ve bağlı birimlerinde görev yapan 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 kuruluşları ifade eder.

A 4

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 ajansız iz toplama yöntemleri kullanılarak toplanır ve en az 6 ay süreyle Başkanlıkça saklanır.

(2) Belediye 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 Belediye bilişim sistemlerinden yararlanan tüm Belediye personeli birinci derecede görevli ve sorumludur. Bu Yönerge kapsamında olup teknolojik değişikliklere ya da Belediyenin genel politikasındaki ve hizmetlerindeki değişikliklere göre bu politikada gerekli düzenlemeler Başkanlıkça yapılır ve resmi internet sayfasında "Bilgi ve Sistem Güvenliği Politikaları" adı altında yayınlanır. Tüm Belediye Personeli yayınlanan "Bilgi ve Sistem Güvenliği Politikaları" nı takip etmekle ve uymakla 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) Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, kurumun bünyesinde oluşturulan tüm veriler kurumun mülkiyetindedir.

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

(5) 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 Belediyenin tüm bilişim varlıklarını iade eder. Kullanıcının bilgi ve bilgi işlem olanaklarına erişim hakları kaldırılır.

(6) 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.

(7) Bilgi güvenliğini etkileyen arızalar mümkün olan en kısa sürede uygun yönetim kanalları kullanılarak Başkanlığa rapor edilir.

(8) 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.

AK B

ÜÇÜNCÜ BÖLÜM

Bilgi ve Sistem Güvenliği Kuralları ve Politikaları

Aktif dizin hizmetleri kuralları

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

(2) Kullanıcı, kendisine verilen her türlü "kullanıcı adı"nı ve "şifresi"ni bir başkası ile paylaşmaz ve bir başkasına kullanırmaz. 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, Bilgi İşlem Daire Başkanlığınca 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 kullanılamaz.

(3) Belediyemizle ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisinde iştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

(4) Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzemeler vb.) göndermemelidir.

(5) Kullanıcı, kurumsal mesajlarını, kurum iş akışının aksamaması için cevaplandırmalıdır

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

(7) 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.

(8) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmaz ve derhal silinir.

(9) 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.

(10) Kullanıcılar tarafından gönderilen e-postalarda gereğine göre aşağıdaki şekilde bir açıklama yer almalıdır.

" Bu e-posta iş için gönderilenler hariç sadece yukarıdaki isimleri belirtilen kişiler arasında özel haberleşme amacını taşımaktadır. Size yanlışlıkla ulaşmışsa lütfen gönderen kişiyi bilgilendiriniz ve mesajı sisteminizden siliniz. Diyarbakır Büyükşehir Belediye Başkanlığı bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmemektedir.

A 5

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.

Antivirüs Politikası

MADDE 10- (1) Antivirüs politikası ile ilgili kurallar aşağıda belirtilmiştir.

- a) Belediyemizin tüm istemcileri ve sunucuları antivirüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak antivirüs yazılımı yüklenmeyebilir.
- b) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.
- c) Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
- d) Kullanıcı hiçbir sebepten dolayı antivirüs yazılımını bilgisayarından kaldırmamalıdır.
- e) Antivirüs güncellemeleri antivirüs sunucu ile yapılmalıdır. Sunucular internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılmalıdır.
- f) Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilmelidir.
- g) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
- h) Optik Media ve harici veri depolama cihazları antivirüs kontrolünden geçirilmez.

Temiz masa - temiz ekran politikası

MADDE 11- (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 12- (1) Tüm kullanıcılar interneti bilinçli bir şekilde kullanmak, başkalarının hakkını ihlal edici ve bilişim sisteminin işleyişini engelleyici, bozucu faaliyetlerde bulunmamakla yükümlüdür.

(2) Kullanıcılar;

a) Belediye sunucuları üzerinde kendisine tahsis edilen kullanıcı adı, şifre ve IP adresi kullanılarak gerçekleştirilen her türlü etkinlikten,

A S

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) Belediye tarafından sağlanan güvenlik programlarının aktif olarak kullanılmasından ve güncellenmesinin sağlanmasından,

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

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

a) Belediye 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, Belediye ağına 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 Başkanlık tarafından filtrelenir.

(5) Bilgisayarlara tahsis edilen IP numarası ve ortam erişim kontrolü adresi (MAC adresi) ile BIOS ayarları Başkanlık 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 13- (1) Belediyemiz Kurumları ile Belediyemiz sorumluluğunda yürütülen projelere ait internet sitelerinin barındırma hizmeti Belediyemiz 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) Belediye tarafından belirlenen internet sitesi standartlarına göre hazırlanır.

b) Her türlü içerikten daire başkanı ve birim amiri sorumludur.

c) Uygulamalara yetkisiz kişilerin erişimini engelleyen tedbirler alınır.

ç) Tüm şifrelerinin sorumluluğu daire başkanına aittir.

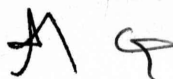
d) İçerikler daire başkanı tarafından görevlendirilen yetkili ya da yetkililerce yedeklenir.

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



DÖRDÜNCÜ BÖLÜM
Çeşitli Hükümler

Hüküm bulunmayan hususlar

MADDE 14- (1) Bu Yönergede hüküm bulunmayan hususlarda ilgili diğer mevzuat hükümlerine göre işlem yapılır.

Yürürlük

MADDE 15- (1) Bu Yönerge Diyarbakır Büyükşehir Belediye Başkanının onayı ile yürürlüğe girer.

Yürütme

MADDE 16- (1) 16 maddeden oluşan işbu yönerge hükümlerini Diyarbakır Büyükşehir Belediye Başkanı yürütür.

A S