URLA BELEDİYESİ

BİLGİ GÜVENLİĞİ POLİTİKALARI

YÖNERGESİ

BİRİNCİ BÖLÜM

AMAÇ,KAPSAM,DAYANAK,TANIMLAR

Amaç

MADDE 1- (1) Bu yönergenin amacı; Urla Belediyesi tarafından kullanılan bilişim sistemlerinin etkin, yerinde ve verimli kullanımını sağlamak, tüm bilgisayarların,yardımcı donanımların ve diğer bilgi sistemlerinin güvenli bir şekilde çalışmasını temin etmek, ağ kaynaklarından en yüksek seviyede yararlanmak, ağ kaynaklarının güvenliğine yönelik genel kuralları belirlemek, bilgi paylaşımı ve güvenliği konularında tedbir almak, kişisel verilerin ve kurum bilgilerinin gizlilik, bütünlük ve erişilebilirliğine karşı kasıtlı ya da kazayla oluşabilecek tehditler için tedbir almaktır.

Kapsam

MADDE 2- (1) Bu yönerge, Urla Belediyesine ait bilişim sistemlerini kullanan çalışanlar ile kendilerine herhangi bir nedenle bilişim sistemlerini kullanma yetkisi verilen misafirlerin bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği, ilke, standart ve kurallarını kapsamaktadır.

Dayanak

MADDE 3- (1) Bu yönerge,5237 sayılı Türk Ceza Kanunu'nun, Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar ile ilgili maddeleri; Bilişim Alanında Suçlar ile ilgili maddeleri, 6698 Kişisel Verilerin Korunması Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 20.07.2008 tarih ve 26942 sayılı Resmi Gazetede yayımlanan Elektronik Haberleşme Güvenliği Yönetmelik, 01.11.2007 tarih ve 26687 sayılı Resmi Gazetede yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik hükümlerine dayanılarak hazırlanmıştır.

TANIMLAR

MADDE 4- Bu Yönetmelikte geçen;

1) Kurum: Urla Belediye Başkanlığını,

2) Kullanıcı: İnternet erişimi, Belediye otomasyon Programları vb. kurum ağ kaynaklarına erişim yetkisi bulunan bilgisayar kullanıcısını,

3) İnternet: Birçok bilgisayar sistemini birbirine bağlayan dünya çapında yaygın olan ve sürekli büyüyen iletişim ağını,

4) Web tarayıcı (Browser): İnternet sayfalarını görüntülemek için kullanılan programı,

5) Protokol: Bilgisayarların internet üzerinden nasıl iletişim kuracağını belirleyen kurallar setini,

6) İndirme (Download): İnternetten veya herhangi bir uygulamadan yapılan bilgi transferini,

7) Sunucu: İstemci bilgisayarlardan gelen taleplere hizmet veren ana bilgisayarı,

8) İstemci: Sunucuların verdiği hizmeti alan personel bilgisayarlarını,

9) Bilişim Cihazları: Bilgisayar (taşınabilir, masaüstü, tablet, PDA), yazıcı, tarayıcı, fotokopi, faks, telefon, santral, vb.

10) Şifreleme/Parola: Bilgiyi gizli bir şifre veya anahtar olmadan okunamayacak (deşifre edilemeyecek) bir kod haline getirme işlemini,

11) Virüs: Virüs, herhangi bir bilgisayara değişik yollarla girebilen ve bu bilgisayarlarda istenmeyen sonuç ve zararlara yol açan programları,

12) Dosya: Herhangi bir kayıt ortamında saklanan kayıtlar topluluğunu,

13) Gizlilik: Bilginin yetkisiz kişilerce erişilememesidir. Bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

14) Bütünlük: Bilginin doğruluğunun ve tamlığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır. Kazara veya kasıtlı olarak bilginin bozulmamasıdır.

15) Erişebilirlik: Bilginin her ihtiyaç duyulduğunda sadece erişim yetkisi olanlar tarafından kullanıma hazır durumda olması demektir.

İKİNCİ BÖLÜM
Elektronik Haberleşme, Bilgi Güvenliği ve Bilgi Sistemlerinin Genel Kullanım Politikaları

MADDE 5- BİLGİ SİSTEMLERİ GENEL KULLANIM KURALLARI

1) Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, kurum bünyesinde oluşturulan tüm veriler, tüm bilgisayarlar ve bilişim sistemleri kurumun mülkiyetindedir.

2) Kullanıcılar bilgi sistemlerini kişisel amaçlar için kullanmamalıdır. Bu konuda ilgili kurallar dikkate alınmalıdır.

3) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır. Kullanıcıların tamamı kullanımlarına tahsis edilen cihazların ve sistemlerin güvenliğinden sorumludurlar. Kurum bilgisayarlarında portable işletim sistemi, program, oyun vb.. yazılımlar ve lisansız crack yazılımlar barındırılmamalıdır ve kullanılmamalıdır. Aksi durumda oluşacak tüm sorumluluklar bu tür işlemleri gerçekleştiren personellere aittir.

4) Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilmemelidir.

5) Bilgisayarlara lisanssız program yüklenmemelidir.

6) Kullanıcı bilgisayarlarında resmi belgeler veya çalışmalar haricinde dosya bulundurulmamalıdır.

7) Sistem ve Güvenlik Yöneticilerinin bilgisi ve onayı olmayan hiçbir cihaz ağ sistemine alınmamalıdır.

8) Tüm kullanıcılar kendilerine tahsis edilen bilgisayarların güvenliğinden sorumludurlar. Kullanıcı hatası veya ihmali neticesinde ortaya çıkabilecek kuruma veya kişiye yönelik saldırılardan kullanıcılar sorumludurlar.

9) Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Antivirüs yazılımı bulunmayan yada üzerinde bulunan antivirüs programı uzun süredir güncellenmeyen kullanıcılar bu durumu ivedi olarak Bilgi İşlem Müdürlüğüne bildirmek durumundadır. Bu bilgisayarlar üzerinden kaynaklanabilecek kuruma yada kişiye yönelik saldırılardan sistemin sahibi sorumludur.

10) Personel bilgisayar yer değişimleri Bilgi İşlem Müdürlüğünden gelen izin sonrası gerçekleşecektir, izinsiz yer değişimleri kesinlikle gerçekleşmeyecektir. İzinsiz yer değişimleri tutanak altına alınıp, cezai işlem başlatılacaktır.

11) Birimlerden format atılması sebebiyle alınan veya gönderilen bilgisayarlar içerisinde bulunan ve söz konusu bilgisayarın kullanıcısı tarafından konumları belirtilen veriler Müdürlük personeli tarafından yedeklenecektir. Kullanıcı tarafından doğru konumu belirtilmeyen ve yedeklenemeyen verilerin kaybolması durumunda sorumluluk söz konusu bilgisayarın kullanıcısına aittir.

13) Kurum ağ sisteminde yer alan tüm bilişim cihazlarına teknik destek verilmekte olup Müdürlüğün bilgisi dışında yetkisiz kişiler tarafından bilişim cihazlarına teknik destek verilmemeli veya bakım-onarım-değişiklik yapılmamalıdır.

MADDE 6- Elektronik imza politikası

1) Kullanıcılar sahip oldukları elektronik imzanın ve pin şifresinin başkaları tarafından kullanılmasına izin verdikleri/paylaştıkları durumlarda haklarında oluşacak hukuki ve idari sonuçları kabul etmiş sayılırlar.

2) Kullanıcılar elektronik imzaları veya cihazları kaybolduğunda/çalındığında konuyu Müdürlüğe bildirmekle ve en kısa sürede yenisini temin etmekle yükümlüdürler.

3) Yeni kullanıcılar (adlarına elektronik imza gelmemiş olanlar), elektronik imzaları kaybolmuş, çalınmış veya cihazları arızalanmış olanlar hariç tüm kullanıcılar elektronik imzalarını sistemde kullanmak zorundadırlar.

4)Kullanıcılar Elektronik İmza kullanım sürelerini kendileri takip etmek ve bitim süresine 3 ay kala yenilenmesi için Bilgi İşlem Müdürlüğü'ne başvuru yapmaları kendi sorumluluklarındadır.

MADDE 7- E-POSTA KULLANIM KURALLARI

1) Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.

2) Urla Belediyesine ait "gizlilik" içeren bilgiler e-posta ve eklerinde bulunmamalı, mail gönderilen kişilere ait iletişim bilgileri yeterince kontrol edilmeden Belediyeye ait iş ve işlemleri kapsayan e-postalar gönderilmemesine özen gösterilmelidir

3) Kullanıcı tarafından kurumun e-posta sistemini taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajlar gönderilmemelidir. Bu tür özelliklere sahip bir mesaj alındığında Bilgi İşlem Müdürlüğüne haber verilmelidir.

4) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

5) Kullanıcı, e-posta ile uyumlu olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme vb.) göndermemelidir.

6) Kullanıcı e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek tehditkâr, yasadışı, hakaret edici, küfür ve iftira içeren, ahlaka aykırı mesajları yollamaktan sorumludur.

7) Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren Bilgi İşlem Müdürlüğü'ne haber vermelidir

8) Kullanıcı, kurumsal e-postalarının, kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesini ve okunmasını engellemelidir.

9) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Bilgi İşlem Müdürlüğü'ne haber verilmelidir

10) Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.

11) Elektronik postaların sık sık gözden geçirilmesi, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmaması ve bilgisayardaki kişisel klasörler oluşturulup bu klasörlere aktarılması gerekmektedir.

12) Kurumdan ayrılan yada emekli olan personel kurumsal e-posta sistemini kullanamaz. Bu gibi durumlarda ilgili birim ayrılan personelin ismini Bilgi işlem Müdürlüğüne ivedi olarak bildirip bu personele ait tüm yetkilerin ve erişimin kapatılmasını istemek zorundadır. Aksi durumunda doğacak tüm mesuliyetlerden ilgili birim müdürleri sorumlu olacaklardır.

MADDE 8- PAROLA GÜVENLİĞİ KURALLARI

1)Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) ve kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 3 (üç) ayda bir değiştirilmelidir

2) Parolalar e-posta iletilerine , web tarayıcısı veya herhangi bir elektronik forma eklenmemelidir ve otomatik parola anımsama seçenekleri işaretlenmemelidir.

3) Kullanıcı, parolasını başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmelidir.

4) Her hangi bir kişiye telefonda parola verilmemeli ve paylaşılmamalıdır

5) Şifreler işten uzak olunduğu zamanlarda iş arkadaşlarına verilmemelidir.

6) Bütün kullanıcılar, mutlaka kendilerine ait "Kullanıcı Adı" ve "Şifre"sini kullanmalıdır. Kurum çalışanının kullanıcı adı ile yapılan işlerdeki tüm sorumluluk kullanıcı adı kullanılan kurum çalışanına ait olacağından hiçbir kullanıcı kendi kullanıcı adı ve şifresini başkaları ile paylaşamaz. Kendisi tarafından kullanılmakta iken, çalışmaya geçici olarak ara verdiği durumlarda da başkası tarafından kullanılmaması için gereken önlemleri alacaktır

7) İzne ayrılan, işten ayrılan veya görev yeri değişen personeller mutlaka bilgi işlem müdürlüğüne bildirilecektir. Bildirilmemesi durumunda yaşanacak tüm sorumluluklar personelin müdürlüğüne aittir.

MADDE 9- ANTİVİRÜS KURALLARI

1) Kurumun tüm istemcileri ve sunucuları antivirüs yazılımına sahip olmalıdır.

2) Kullanıcı hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldırmamalı veya servislerini durdurmamalıdır.

3) İllegal yollar ile kurum anti virüs sistemini ve UTM sistemini atlatacak yöntemler kesinlikle yasaktır.Tespit edilmesi durumunda gerekli hukuki süreç başlatılacaktır.

4) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.

5) Optik Medya ve harici veri depolama cihazları Anti-virüs kontrolünden geçirilmelidir.

6) Ağa bağlı olan kurum içerisindeki bütün bilgisayarlarda Kurumun lisanslı anti-virüs yazılımı yüklü olmalıdır ve merkezi olarak güncellenmelidir. Üzerinde her hangi bir anti-virüs yazılımı bulunmayan bilgisayarlar Bilgisayar ağına kesinlikle bağlanmamalıdır.

MADDE 10- İNTERNET ERİŞİM VE KULLANIM KURALLARI

1)Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır.Kurumun kuralları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. Kurum iş ve işlemleri dışındaki istenmeyen siteler ve kategoriler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.

2) Kurum ağları kullanılarak iş ile ilgili olmayan sitelerde gezinilmemelidir. İnternet üzerinden TV, radyo ve video izlenmemeli/dinlenmemelidir. Bu konudaki tüm sorumluluk kullanıcıya aittir. İş ile ilgili olmayan (müzik, video dosyaları vs.) dosyalar gönderilmemeli ve indirilmemelidir. Bu konudaki tüm sorumluluk kullanıcıya aittir.

3)Kurumda e-posta,internet vb. varlıkları kullanılarak hiçbir platforma yorum yazılamaz,görüş bildiremez.İş ile ilgili olmayan (müzik,video dosyaları) yüksek hacimli dosyalar göndermek(upload) ve indirmek(download) yasaktır.

4) İnternet üzerinden radyo dinlenilmesi, tv seyredilmesi, film, görüntülü iletişim kurulması veya on-line kamera çalışan web sitelerine girilmesi mevcut bant genişliğini dolduracağından yasaktır.

5) Korsan Yazılımlar ile güvenlik duvarını aşmaya çalışmak suçtur ve kullanılamaz. Bütün sorumluluk kullanıcıya aittir. IP değiştirmeye, Proxy kullanmaya yönelik programların kurulması veya kullanılması yasaklanmıştır. Kurumsal ağ üzerindeki paketleri yakalama, izleme, değiştirme, ip (internet protokol numarası) değiştirme, msn dinleme vb. işlemleri gerçekleştirmeye yönelik programlar kullanılamaz, işlem yapılamaz.

6) Kurum web uygulamalarının internet erişimlerinin hızlı olması amacıyla resmi siteler haricindeki (gov.tr, edu.tr vb. resmi uzantılı) sitelere Müdürlüğümüzce gerekli görüldüğünde kısıtlama getirilecektir.

7) İçerik filtreleme sistemince engellenmiş, kelime bazlı engellenen (resmi internet siteleri hariç) sitelere erişimin açılması için sözlü talepte bulunulamaz.

8) İnternet trafiği, 5651 sayılı Kanuna uygun şekilde izlenebilmelidir

MADDE 11- SUNUCU GÜVENLİK KURALLARI

1) Kurumda bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel(ler) sorumludur.Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.

2) Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve anti-virüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir. Anti-virüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve test mekanizmasından geçirilmeli, sonra uygulanmalıdır. Bu çalışmalar için yetkilendirilmiş personel olmalıdır.

3) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

4) Sunucular elektrik, ağ yapısı, sıcaklık ve nem değerleri düzenlenmiş tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulmalıdır.

5) sunucu back up ları periyodik olarak alınmalı ve saklanmalıdır.

6) Sunucu odası 7/24 güvenlik kamerası ile kayıt altına alınmalıdır ve yetkisi olmayan kişilerin odaya girmesi yasaktır.

7) Sistem odasında güç kaynağı bulundurulmalı ve elektrik kesintisine karşı önlem alınmalıdır.

ÇEŞİTLİ HÜKÜMLER – HÜKÜM BULUNMAYAN HUSUSLAR

MADDE 12- Bu Yönergede hüküm bulunmayan hususlarda ilgili diğer mevzuat hükümlerine göre işlem yapılır.

Yürürlük

MADDE 13-Bu Yönerge onaylandığı tarihte yürürlüğe girer.

Yürütme

MADDE 14- Bu Yönerge hükümlerini Urla Belediye Başkanı yürütür