SAMSUN BÜYÜKŞEHİR BELEDİYESİ
BİLGİ VE SİSTEM GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

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

Kapsam

MADDE 2-(1) Bu Yönerge, Belediyemiz merkez ve taşra teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle Belediyemiz 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 dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4-(1) Bu Yönergede geçen;

a) **Belediye:** Samsun Büyükşehir Belediyesini,

b) **Başkanlık:** Bilgi İşlem Dairesi Başkanlığını,

c) **Bilişim kaynakları:** Elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gerecini,

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

e) **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,

f) **Konuk:** Belediye bünyesinde kullanmış olduğu bilgisayar, bilgisayar ağı, İnternet ve benzeri tüm bilişim sistemleri üzerinde yetkilendirilmemiş olan Belediye personeli dışındaki kişiler ile görev yeri dışında çalışan Belediye personelini,

g) **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,

h) **Paydaş:** Ortak çalışma yapılan kurum veya kuruluşları,

i) **Personel:** Belediye merkez teşkilatı ile ilçe müdürlükleri ve bu müdürlüklere bağlı tüm çalışanları

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

k) **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.

(2) Yönergede kullanılan teknik terim ve tanımlar, (Ek-1) tabloda gösterilmiştir.

İKİNCİ BÖLÜM
Sorumluk 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 İnternet 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 İnternet 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 Belediye genel politikasındaki ve hizmetlerindeki değişikliklere göre bu politikada gerekli düzenlemeler Başkanlıkça yapılır ve resmi İnternet sayfasında "Bilgi ve Sistem Güvenliği Politikaları" adı altında yayımlanır. Tüm Belediye 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) 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

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 (Active Directory) 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, birebir hesabı kullanan kullanıcıya aittir.

(6) Merkezdeki her bir son kullanıcı, etki alanı üyesi olmalıdır. Etki alanında olmayan kullanıcıların İnternet erişimleri engellenir.

E-posta işlemleri kuralları

MADDE 8- (1) Kullanıcı, e-posta adresi olarak, kendisine tahsis edilen adresi kullanır. Bunun dışındaki e-posta servisleri resmi 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 içerisine iliştirilen öğeler de dahildir. 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 malzeme, vb.) göndermemelidir.

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

(6)Kullanıcı, kendisine tahsis edilene-posta adresini sohbet yapmak için kullanmaz.

(?)Kullanıcı, hesabını ticari ve kar amaçlı olarak kullanamaz. Çok sayıda kullanıcıya toplu halde reklam, tanıtım, duyuru ve benzeri amaçlı e-posta gönderemez ve zincire-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 birebir 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 yukarıda isimleri belirtilen kişiler arasında özel haberleşme amacını taşımaktadır. Size yanlışlıkla ulaşmışsa lütfen gönderen kişiyi bilgilendiriniz ve mesajı sisteminizden siliniz. Türkiye Cumhuriyeti Samsun Büyükşehir Belediye Başkanlığı bu mesajın içeriği, ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmemektedir."

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.

d) Şifreler en geç altı ayda bir değiştirilir.

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

f) Şifreler herhangi bir kişi ile paylaşılmaz.

Antivirüs Politikası

Madde 10- (1) Antivirus Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Belediyemizi 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 hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldırmamalıdır.

e) Antivirüs güncellemeleri antivirüs sunucusu ile yapılmalıdır. Sunucular intemete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılmalıdır.

f) Etki alanına dahil 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 geçirilmelidir.

Temiz masa - temiz ekran politikası

MADDE 11-(1) Sistemlerde kullanılan şifreler, masa üstü veya ekran üstü gibi herkes tarafından görülebilecek yerlere yazılmamalı.

(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 İnternet kullanımı politikası

MADDE 12- (1) Tüm kullanıcılar intemeti 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,

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,

d) Belediye tarafından sağlanan güvenlik programlarının aktif olarak kullanılmasından ve güncellenmesinden,

e) Bilişim sisteminin kullanım kurallarına, kanun ve yönetmelikler ile Belediyemizin 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,

d) Gerçek dışı, sıkıntı ve rahatsızlık verici, gereksiz endişe yaratacak materyali üretmek ve dağıtmak,

e) Başka bir kullanıcının e-posta adresini, o kullanıcının izni olmadan kullanmak,

f) Yerel, ulusal, uluslararası bilgisayarları veya hizmetleri kasıtlı olarak yetkisiz kullanmak,

g) Başkalarının telif haklarını ihlal edici konumda olan yazı, makale, kitap, film, müzik eserleri gibi materyali edinmek, yayınlamak, dağıtmak,

h) Siyasi ve ideolojik propaganda yapmak için kullanamaz.

(4)Telif hakları ve lisansları ihlal eden, Belediye 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 Belediye 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.

(?)Kullanıcılar, kişisel bilişim kaynaklarını kurum ağında 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.

(9) Ağ **Yönetim Politikası:**

a) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlenmelidir.

b) Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır. Yönlendiriciye erişen tüm kullanıcıları uyarmalıdır.

"BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR. Bu cihaza erişim *ve* ***yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptınm olabilir."***

c) Sınırsız ağ dolaşımı engellenmelidir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.

d) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.

e) Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır. Kurum kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılmalı ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanmalıdır.

f) Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.

g) Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.

(10) **Uzaktan Erişim Politikası:**

a) Intemet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamaktadır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.

b) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

c) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

d) **Kurum** ağına uzaktan erişecek bilgisayarların işletim sistemi ve antiviıüs yazılımı güncellemeleri yapılmış olmalıdır.

(11) **Kablosuz İletişim Politikası:**

(a) Bütün kablosuz erişim cihazları Sistem yönetici (leri) tarafından onaylanmış olmalı ve Bilgi İşlemin belirlediği güvenlik ayarlarını kullanmalıdır.

(b)Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 **(WP**A2-kurumsal) şifreleme kullanılmalıdır. IEEE 802. lx erişim kontrol protokolü ve TACACS+ ve **RADIUS** gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.

(c)Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

(d)Varsayılan SSID isimleri kullanılmamalıdır. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vb.

(e)Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.

Sunucu (Server) Güvenlik Politikaları

MADDE 13- (1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

a) Belediyemiz de bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel (ler) sorumludur.

b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.

c) Sunuculara ait bilgilerin yer aldığı tablo oluşturulmalıdır. Bu tabloda, sunucuların isimleri, ip adresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personel(ler)in isimleri ve telefon numaraları bilgileri yer almalıdır.

d) Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri, Başkanlık bildirimlerine göre yapılmalıdır.

e) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

f) Ayrıcalıklı (Bakım ve Teknik Problemler, Güncellemeler, Özel Bağlantılar v.s) bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

g) Sunucu üzerinde zararlı yazılım (malvvare, spyware, hack programları, vvarez programları, vb.) çalıştırılmamalıdır.

h) Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.

i) Denetimler, Başkanlık tarafından yetkilendirilmiş kişilerce yönetilmeli ve periyodik aralıklarda yapılmalıdır.

j) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.

k) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

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

Bilgi Sistemleri Yedekleme Politikası

MADDE 14- (1) Bilgi Sistemleri Yedekleme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerini ve kurumsal veriler düzenli olarak yedeklenmelidir.

b) Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır.

c) Taşınabilir ortamlar (manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır.

d) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.

e) Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilmemelidir.

f) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.

g) Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenmelidir.

h) Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

i) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.

j) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dahilinde tamamlanması gerekmektedir.

k) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.

1) Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek bir ortamda bulundurulmalıdır.

m) Veri Yedekleme Standardı, yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği belirlenmelidir. Yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

Bakım Politikası

MADDE 15- (1) Bakım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır.

b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.

c) Firma teknik destek elemanlarının bakım yaparken "Samsun Büyükşehir Belediye Başkanlığı Bilgi ve Sistem Güvenlik Politikaları"na uygun davranmaları sağlanmalı ve kontrol edilmelidir.

d) Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.

DÖRDÜNCÜ BÖLÜM
Çeşitli Hükümler

Hüküm bulunmayan hususlar
MADDE 16-(l)Bu Yönergede hüküm bulunmayan hususlarda ilgili diğer mevzuat hükümlerine göre işlem yapılır.

Yürürlük
MADDE 17-(1) Bu Yönerge onaylandığı tarihte yürürlüğe girer.

Yürütme
MADDE 18-(1) Bu Yönerge hükümlerini Büyükşehir Belediye Başkanı yürütür.

Tablo (Ek-1) Kısaltmalar Tablosu

Kısaltma	**Tanım**
Zincir e-posta	Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesi
Spam	Yetkisiz ve/veya istenmeyen reklam içerikli e-postalar
Sahte e-posta	Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasadışı yoldan) erişmek
RADIUS (Remote Authentication Dial- in User Service)	Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan İnternet protokolü
X.509/LDAP(Light weight Directory Access Protocol	Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir internet protokolü
Portal	Birden çok içeriği bir arada bulunduran alan
SSL (Secure Socket Layer)	Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolü
VPN	Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknoloji
IPSec (lnternet Protocol Security) **VPN**	Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlama
IP	Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adres
MAC adresi	Bir ağ cihazının tanınmasını sağlayan kendisine özel adres
SNMP	Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokol
Firmware	Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımlar

DMZ	Kurum içi ağı ile kurum dışı ağı birbirinden ayıran bölge
Kısaltma	**Tanım**
Uzaktan Erişim	İnternet, telefon hatları veya kiralık hatlar vasıtası ile Kurumun ağma erişilmesi
Risk	Kurumun bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörler
Güvenli Kanal	Güçlü bir şifrelemeden oluşan iletişim kanalı
Uygulama Sunucusu	Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımıdır. Üç katmanlı uygulamaların bir parçasıdır. Bu üç katman: Kullanıcı arayüzü (GUI), uygulama sunucusu ve veritabanı sunucusu
Yetkilendirme	Sisteme giriş izni verilmesi, çok kullanıcılı sistemlerde sistem yöneticisi tarafından, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesi
Yedekleme	Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veri tabanının başka bir yere kopyalanması işlemi.
Veritabanı.	Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğu
Şifreleme	Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritma
VLAN (Virtual LAN)	Sanal yerel ağ. Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubu