NARLIDERE

BELEDİYESİ

# BİLGİ GÜVENLİĞİ POLİTİKASI

## 1-) GENEL BİLGİLER

Hizmet verilen Kurum ve Kuruluşların, vatandaşların güvenini temin etmek amacıyla ve verdiğimiz hizmetler için kullandığımız bilgi varlıklarımızın güvenliğini sağlamak öncelikli amacımızdır. Bu bağlamda; iş birliğinde bulunduğumuz, hizmet verdiğimiz vatandaşlar, resmi kurum kuruluşlar ve paydaşlarımız ile ilişkilerimiz çok değerlidir. Sunmakta olduğumuz Hizmetlerin sürekliliği, elimizde tuttuğumuz bilgilerin gizliliği, hizmet verdiğimiz tarafların veya kendi içimizdeki bilgi varlıklarının bütünlüğü yüksek öneme sahiptir.

Günümüzde Kurumlar, bilgilerinin büyük bir kısmını Elektronik ortamda bulundurmakta ve bu bilgileri Bilişim Sistemleri altyapısı kullanarak işlemektedir. İş ve işlemlerin elektronik ortama taşınması, kamu hizmetlerinin etkinleştirilmesi, yasa dışı faaliyetlerin tespit edilebilmesi ve önlenmesine yönelik olarak kişisel bilgilerin de elektronik ortamda bulunması ve işlenmesi yoğun bir şekilde artmıştır. Ancak bu durum kişisel bilgilerin sahiplerinin isteği dışında ilgisiz ve yetkisiz tarafların eline geçmesi, kişisel bilgi sahibini rahatsız edecek veya onlara zarar verecek şekilde yasa dışı olarak kullanılması ve kişi mahremiyetinin ihlali ilkesi doğurmaktadır. Dolayısı ile gelişen Bilişim Teknolojileri bilgi güvenliği olgusunu da beraberinde önce ihtiyaç sonra zorunluluk haline getirmiştir.

Bilgi Güvenliği Politikaları, bir Kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür.

### 1.1-) Bilgi Güvenliği Politikaları Tanımı

Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken varlıktır. Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar. Bilgi güvenliği politikaları, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür.

Bilgi güvenliğinde temelde aşağıdaki üç unsuru hedeflenmektedir.

**1.** Gizlilik (Confidentiality)

**2.** Bütünlük (Integrity)

**3.** Kullanılabilirlik (Availability)

**Gizlilik**

Bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

**Bütünlük**

Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca sehven veya kasıtlı olarak bilginin bozulmaması diyebiliriz.

**Kullanılabilirlik**

Bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir

### 1.2-) Bilgi Güvenliği Politikaları Kapsamı

Bu politika, kurum Bilgi İşlem altyapısını kullanmakta olan tüm Müdürlükleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

### 1.3 -) Bilgi Güvenliği Politikaları Amacı

Kurum Yönetimi; Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

### 1.4 -) Bilgi Güvenliği Politika İhlali ve Yaptırımlar

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, ilgililer hakkında adli ve idari yasal işlemler yapılabilecektir. Belediyemize ait Bilgi Güvenliği Politikası oluşturulmuş olup bu politika kapsamında hazırlanmış olan talimatlar aşağıda gösterilmiştir. Kurumsal Bilişim sistemlerinin güvenliğinde herhangi bir aksamaya mahal verilmemesi için genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında çalışanlarımızın da bu hususta titizlikle uyması gereken bu kurallara bütün kurum çalışanları uymak zorundadır.

## 2-) TEMEL İLKELER

- Tüm Müdürlükler kendi sorumluluk alanlarındaki veri işleme ve güncelleme işlemleri ile ilgili alanlara veri işleyecek kişilerden ve yetkilendirmelerinden sorumludurlar.
- Her kullanıcı tamim ve taahhütname ile gönderilen çalışma alanları ile ilgili hususlara uymak ile yükümlüdür.
- Kullanıcı, güvenlik tehditlerini bilmek, önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmekten sorumludur.
- Kullanıcılar, bilgi sistem ve ekipmanlarının kullanımında birbirlerinin haklarına saygı göstermekle yükümlüdürler.
- Kullanıcı, idarece yapılmış olan risk değerlendirmelerinde kendileriyle ya da çalışma alanlarıyla ilgili öngörülen tedbirlere uymak zorundadır.
- Kullanıcı, güvenliği, bilgi sistem ve ağlarının önemli bir unsuru olarak değerlendirilmelidir.
- Kurumlar hedeflenmek sureti ile içerden ya da dışarıdan yapılacak siber saldırılara karşı kurumsal sorumluluk ve yetkiler çerçevesinde gerekli tedbirler alınmalıdır.
- İdare bilgi güvenliği yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.
- İdare, bilgi sistem ve ağlarını güvenliklerini incelemeli ve yeniden değerlendirmelidir. İnceleme ve yeniden değerlendirme neticesinde, güvenlik ile ilgili politika, uygulama, önlem ve prosedürlerde gerekli değişiklikleri zamanında yapmakla yükümlüdür.

### 2.1-) Bilgi Güvenliği Politikaları

Belediyemiz, T.C. Anayasası ve kanunlar çerçevesinde yürütmekte olduğu iş ve işlemlerin işleyen süreçlerinde ilçemiz sınırları içerisinde belediye hizmetleri ile ilgili tüm süreçlerde çalışmakla yükümlendirilmiş bir kurum olma hüviyeti ile Belediyemizde hizmet alan her bir vatandaşa karşı sorumlulukları olan kuruluşlardan birisidir. Her bir vatandaşın Belediyemize müracaat ettiğinde en gizli ve mahrem sayılabilecek bilgilerine dair erişebilen kaydedebilen bir kuruluştur. Bu nedenle kurumumuz kayıt altına alınan bireyin her türlü veri ve bilginin kendisine emanet edilmiş bir değer olduğu düşüncesiyle kendisini bu sorumluluğun yerine getirilmesinde mükellef olarak görmektedir. Ayrıca kurumumuz kişi verilerinin ve bilgilerinin korunması ve güvenliği ile alakalı her türlü "teknik idari ve hukuki yöntemi" kullanmak sureti ile emanetinde bulunan tüm bilgi sistemleri kaynaklarını "bilgi güvenliği ana politikası çerçevesinde" korumakla ve bu hususta tüm tedbirleri almakla yükümlü olduğunun bilincindedir.

Tüm belediyemizde üretilen bilginin de en üst seviyelerde güvenlik anlayışı içerisinde korunması gerektiği bilinci ile hareket eden Belediyemiz misyon ve vizyonuna bağlı kalarak Bilgi Güvenliği konseptinin esasını oluşturan basılı ve elektronik ortamdaki bilgilerin yasal mevzuat ışığında ve risk metotları kullanılarak "gizlilik, bütünlük ve kullanılabilirlik" ilkelerine göre yönetilmesi amacıyla;

- Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmek,
- Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,
- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
- Bilgi Güvenliği Yönetim Sistemini sürekli gözden geçirmek ve iyileştirmek,
- Bilgi Güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmek, ana politikalar olarak öngörülmektedir.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuyu da kapsar.

Bilgi güvenliği bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir. Kurum çalışanları, yüklenici firma personeli, stajyerler, diğer kurum çalışanları, ziyaretçiler, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir. Kullanıcılar, bilgi güvenliği bilinçlendirme sürecindeki en büyük ve önemli hedef kitledir. Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir. Yöneticiler, bilgi güvenliği bilinçlendirme ve eğitimi sürecinin gereklerine personelinin uymasını sağlamakla sorumludurlar.

Başarılı ve etkin işleyen bir bilgi güvenliği bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekmektedir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür.

Sonuç olarak Bilgi Güvenliği Politikasının amacı bilgi varlıklarını korumak, bilginin ve verinin gizliliğini sağlamak, bütünlüğünü bozmaya çalışacak yetkisiz kişilerin erişimine karşı korumak ve böylece Belediyemiz güvenini ve itibarını sarsacak durumları bertaraf etmektir.

## 2.2-) Bilgi Güvenliği Organizasyonu

Bilgi Güvenliği ana sorumlusu olarak kurumumuz içerisinde Bilgi İşlem Müdürlüğü, görevlendirilmiştir.

**Bilgi İşlem Müdürlüğü görevleri**;

- Bilgi güvenliği politika ve stratejilerini belirler,
- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlanması amacı ile İnsan kaynakları ve Eğitim Müdürlüğü ile iletişime geçer,
- Bilgi güvenliği faaliyetleri ve kontrollerinin tüm kurum içerisinde koordine edilmesini sağlar.

## 2.3-) Bilgi Güvenliği İhlal Yönetimi

Bilgi güvenliği olaylarının rapor edilmesi;

Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan idari uygulama planı oluşturulur. Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği ihlal raporu hazırlanır. Güvenlik ihlaline neden olanlar hakkında, hukuki süreç başlatılır. Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan Bilgi İşlem Müdürlüğüne mümkün olan en kısa sürede rapor ederler.

## 2.4-) Bilgi Güvenliği Denetimleri

- Bilgi İşlem Müdürlüğü bilgi güvenliği denetimlerini yapar.
  - Bilgi güvenliği denetimlerini yapacak personel Bilgi İşlem Müdürlüğü tarafından belirlenir.
  - Senaryoları idarece önceden onaylanmak kaydıyla "bilişim güvenliği testleri" yapılabilir.
  - Bilgi Güvenliği ile ilgili çalışmaların doğruluk ve güvenirliğini test etmek amacı ile danışmanlık hizmetleri ile penetrasyon testleri yaptırılır.

## 3-) BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ

Bu Yönergede geçen;

**Ağ Güvenlik Duvarı :** Belediyemiz ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında Belediyemizin karşılaşabileceği sorunları önlemek üzere tasarlanan cihazları,

**Ağ Güvenlik Yöneticisi :** Ağ Sistemlerinden Sorumlu Yöneticiyi,

**Bilgi Güvenliği Yöneticisi :** Bilgi Güvenliği Yöneticisini,

**Firmware :** Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımları,

**Güvenli Kanal :** Güçlü bir şifrelemeden oluşan iletişim kanalını,

**HTTP :** Bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiper ortam bilgi sistemleri için uygulama seviyesindeki iletişim kuralını

**IP :** Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adresi,

**IPSec :** Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlamayı,

**İstemci :** Sunucuların verdiği hizmeti alan bilgisayar sistemini,

**Kullanıcı :**Belediye Bilgi Sistemlerini Kullanan tüm kişileri,

**MAC adresi :**Bir ağ cihazının tanınmasını sağlayan kendisine özel adresi,

**Portal :** Birden çok içeriği bir arada bulunduran alanı,

**POP3 :** Gelen e-posta iletilerini, iletilerin bilgisayara aktarıldığı e-posta denetleme işlemi yapılıncaya kadar tutan kişisel e-posta hesap türünü,

**RADIUS :**Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolünü,

**Risk :**Belediyenin bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörleri,

**Sahte e-posta :** Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasadışı yoldan) erişmeyi,

**Sistem Yöneticisi :**Bilgi Sistemleri Yöneticisini,

**SMTP :**Bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokolü,

**SNMP :** Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokolü,

**SOME :** Bilgi İşlem Müdürlüğü Siber Olaylara Müdahale Ekibini,

**Spam :** Yetkisiz ve/veya istenmeyen reklam içerikli e-postaları,

**SSL :** Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolünü,

**Sunucu :** İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini,

**Şifreleme :**Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritmayı,

**Uygulama Sunucusu :** Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımını,

**Uzaktan Erişim :**İnternet, telefon hatları veya kiralık hatlar vasıtası ile Belediyenin ağına erişilmesini,

**Veritabanı :**Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğunu,

**Veritabanı Yöneticisi :**Veritabanı Sistemlerinden Sorumlu Yöneticiyi,

**VLAN :** Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubunu,

**VPN :**Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknolojiyi,

**Yedekleme :** Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritabanının başka bir yere kopyalanması işlemini,

**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 verilmesini, İfade eder.

## E-Posta Politikası

(1) E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.

a)Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.

b)Belediyeye 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.

c)Kullanıcılar, Belediyenin e-posta sistemini taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Belediyedeki ilgili birime haber verilmelidir.

ç)Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçlar ile e-posta gönderilmemelidir.

d)Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında açılmayıp, başkalarına iletilmeyip, ilgili Müdürlüğü haber verilmelidir.

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

f)Kullanıcılar, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

g)Kullanıcılar, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların gönderilmesinden sorumludur.

(2) E-Posta ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.

a)Kurumsal e-posta kişisel amaçlar için kullanılmamalıdır.

b)Kullanıcı, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

c)Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu epostalara herhangi bir işlem yapmaksızın ilgili Müdürlüğe haber vermelidir.

ç)Kullanıcı, kurumsal mesajlarını, Belediye iş akışının aksamaması için cevaplandırmalı ve kurumsal mesajlarda kişisel e-posta adresleri değil kurumsal e-posta adresi kullanılmalıdır.

d)Kullanıcı, kurumsal e-postalarının, Bakanlık dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.

e)Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Belediye Bilgi İşlem Müdürlüğüne haber verilmelidir.

f)Belirli bir süre kullanılmamış e-posta adresleri kullanıcıya haber vermeden sunucu güvenliği ve veri depolama alanının boşaltılması için kapatılmalıdır.

g)Kullanıcı, kendilerine ait e-posta parolasının güvenliğinden ve gönderilen epostalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren ilgili birime haber vermelidir.

ğ)Her bir kullanıcının yalnızca 1 adet e-posta hesabı olmalıdır.

(3) Kurumsal e-postalar yetkili kişilerce hukuksal açıdan gerekli görülen yerlerde önceden haber vermeksizin denetlenebilir.

(4) Kullanıcı, e-postalarına erişirken, POP3, SMTP, HTTP vb kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanmamalıdır.

(5) Belediye, e-postaların Belediye bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.

(6) Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan e-postalar antivirüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenmelidir. Ağa dâhil edilmiş bilgisayarlarda ve sunucularda ağ güvenlik yöneticileri bu yazılımdan sorumludur.

## Parola Politikası

(1) Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

a)Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) ve kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 90 (doksan) günde bir değiştirilmelidir.

b)Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.

c)Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir ve otomatik parola anımsama seçenekleri işaretlenmemelidir.

ç)Kullanıcı, parolasını başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazması durumunda güvenliğini sağlamalıdır.

d)Belediye uygulamalarında bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

(2) Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

a)En az 6 haneli olmalıdır.

b)İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)

c)İçerisinde en az 1 tane rakam bulunmalıdır. (1, 2, 3...) ç)İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,$,#,&,/,{,*,-,],=,...)

d)Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, abababab...) e)Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...) f)Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

(3) Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

a)Bütün parolalar Belediyeye ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.

b)Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılmamalıdır.

c)Parola kırma ve tahmin etme operasyonları belli aralıklar ile bilgi güvenliği yetkililerince yapılabilir.

ç)Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

(4) Uygulama Geliştirme Standartları

a)Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.

b)Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.

c)Parolalar, şifrelenmiş olarak saklanmalıdır.

ç)Uygulama geliştirme standartları en az RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

## İşletim Sistemleri Güvenliği Politikası

İşletim Sistemleri Güvenliği Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

a) Belediye son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar verir ve bu işletim sistemine uygun yazılım donanım sistemlerinin kurulumunu temin eder.

b) Belediye, işletim sistemlerinin güncel ve güvenli olması için yama yönetimi yapmalıdır.

c) Belediye, bilgisayar başındaki kullanıcının doğru kullanıcı olup olmadığını tespit etmek için etki alanı kimlik doğrulamasını sağlamalıdır.

ç)Kullanıcılar Belediye mevcut envanteri haricindeki donanımları Belediye bilgisayarlarında kullanmamalıdır.

d)İşletim sistemlerinde kurulumda gelen yönetici hesaplarının (Administrator, root) kaba kuvvet saldırılarına karşı, Microsoft ürünlerinde pasif hale getirilmesi, Linux tabanlı ürünlerde root hesabına ssh erişiminin en aza indirgenmesi gerekir.

## Son Kullanıcı Güvenliği Politikası

Son Kullanıcı Güvenliği Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

a)Son kullanıcılar sistemlere, etki alanları dâhilinde kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanmalıdır.

b)Her bir son kullanıcının yalnızca bir adet kullanıcı hesabı olmalıdır.

c)Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir.

ç)Son kullanıcıların yetkileri, içinde bulundukları grup politikasına göre belirlenmelidir.

d)Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı 5651 sayılı kanuna uygun olarak kayıt altına alınmalıdır.

e)Güvenlik zafiyetlerine karşı, son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır.

f)Son kullanıcılar bilgisayarlarındaki ve sorumlusu oldukları cihazlardaki bilgilerin düzenli olarak yedeklerini almalıdır.

g)Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.

ğ)Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde harici veri depolama cihazları (bellek ve/veya harici hard disk gibi taşınabilir medya araçları ) bırakmamalıdır.

h)Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır.

ı)Kullanıcı bilgisayarlarında, güncel anti virüs bulunmalıdır.

i)Belediye, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulamalıdır.

j)Belediye, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişikleri merkezi grup politikalarıyla engellemelidir.

k)Kullanıcılarına yeni parolaları bildirilirken sms gibi daha güvenli yöntemler kullanılmalıdır.

l)Temiz masa, temiz ekran ilkesi benimsenmeli ve hayata geçirilmelidir.

## Antivirüs Politikası

Antivirus Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a)Belediyenin tüm istemcileri ve sunucuları güncel 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.

ç)Kullanıcı hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldırmamalıdır.

d)Antivirüs güncellemeleri antivirüs sunucusu 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.

e)Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilmelidir.

f)Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir. g)Bakanlığın ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.

ğ)Optik Media ve harici veri depolama cihazları her kullanımda antivirüs kontrolünden geçirilmelidir.

## Uzaktan Erişim Politikası

Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a)Internet üzerinden Belediyenin 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)Uzaktan erişim güvenliği denetlenmelidir.

c) Belediye çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

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

d)Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.

e)Belediyeden ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

f)Mesai saatleri içerisinde uzaktan erişim mümkün olup, mesai saatleri dışında kullanımı sistem üzerinde yasaklanmıştır. İlgili iş ve işlemler bu doğrultuda yürütülmektedir.

**Sunucu Güvenlik Politikaları**

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

a)Belediyede bulunan sunucuların yönetiminden, ilgili sunucu üzerinde 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.

ç)Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.

(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.

a)Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri Belediye Bilgi İşlem Müdürlüğü Sistem Yönetimi talimatlarına göre yapılmalıdır.

b)Sunucuyu kullanan birim tarafından, kullanılmayan servisler ve uygulamalar kapatılmalıdır.

c)Servislere erişimler, kaydedilmeli ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.

ç)Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs vb. koruma amaçlı yazılımlar güncel tutulmalıdır. Antivirüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce Değişiklik Yönetimi Politikası çerçevesinde, bir onay ve test mekanizmasından geçirilmeli, sonra uygulanmalıdır.

d)Sistem yöneticileri „Administrator" ve „root" gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.

e)Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

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

g)Sunucular üzerine lisanslı yazılımlar kurulmalıdır.

ğ)Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

(3) Sunucu gözlemleme kuralları aşağıda belirtilmiştir.

a)Kritik sistemlerde, uygulamalar kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.

b)Kayıtlara çevrimiçi olarak minimum 90 gün süreyle erişebilmelidir.

c)Günlük tape backuplar en az 1 ay saklanmalıdır.

ç)Haftalık tape backuplar en az 1 ay saklanmalıdır.

d)Aylık full backuplar en az 6 (altı) ay saklanmalıdır.

e)Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sistemde saklanmalıdır.

f)Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.

g)Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.

ğ)Port tarama işlemleri düzenli olarak bilgi güvenliği yetkililerince yapılmalı ya da yaptırılmalıdır.

h)Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.

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

i)Denetimler, Bilgi İşlem grubu tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.

(4) Sunucu işletim kuralları aşağıda belirtilmiştir.

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

b)Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

c)Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.

## Donanım ve Yazılım Envanteri Oluşturma Politikası

(1) Donanım ve yazılım envanteri oluşturma ile ilgili kurallar aşağıda belirtilmiştir.

a)Oluşturulan envanter tablosunda şu bilgiler olmalıdır: sıra no, donanım/yazılım adı, bölüm, marka, model, seri no, özellikler, ek aksamlar, işletim sistemi, garanti süresi vs.

b)Bu tablolar merkezi bir web sunucuda tutulmalı ve belirli aralıklarla güncellenmelidir. İlgili siteye girişler güvenlik politikaları çerçevesinde yapılmalıdır.

c)Envanter bilgileri sık sık kontrol edilmelidir. Bu şekilde bilgi eksikliğinin yol açacağı kayıp ve maliyetlere engel olunmalıdır.

## Ağ Yönetim Politikası

Ağ yönetim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a)Ağ cihazları yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrılmalıdır.

b)Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.

c)Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimle ilgili tedbirler alınmalıdır. ç)Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.

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

e)Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.

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

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

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

h)Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Belediyenin güvenlik politika ve standartlarıyla uyumlu olmalıdır.

ı)Sistem tasarımı ve geliştirilmesi yapılırken Belediye tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.

i)İnternet trafiği, İnternet Erişim ve Kullanım Politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.

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

k)Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.

l)Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

## Kablosuz İletişim Politikası

(1)Belediyenin bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.

(2)Bütün kablosuz erişim cihazları Bilgi İşlem Müdürlüğü tarafından belirlenen güvenlik ayarlarını kullanmalıdır.

(3)Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.

a)Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.

b)Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.

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

ç)Varsayılan SSID isimleri kullanılmamalıdır. SSID ayarı bilgisi içerisinde Belediye ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vb.

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

e)Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Belediye kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Belediye kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.

f)Erişim Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.

g)Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Belediyenin tüm internet bant genişliğinin tüketilmesi engellenmelidir.

ğ)Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.

h)Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmalıdır.

ı)Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

## Veritabanı Güvenlik Politikası

Veritabanı güvenlik kuralları aşağıda belirtilmiştir.

a)Veritabanı sistemleri envanteri tutulmalı ve bu envanterden sorumlu personel tanımlanmalıdır.

b)Veritabanı işletim kuralları belirlenmeli ve yazılı hale getirilmelidir.

c)Veritabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.

ç)Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.

d)Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.

e)Yedekleme planları yazılı hale getirilmelidir.

f)Manyetik kartuş, DVD veya CD… vb. ortamlarında tutulan log kayıtları en az 6(altı) ay en fazla 2(iki) yıl süre ile güvenli ortamlarda saklanmalıdır.

g)Veritabanı erişim politikaları “Kimlik Doğrulama ve Yetkilendirme” politikaları çerçevesinde oluşturulmalıdır.

ğ)Hatadan arındırma, bilgileri yedekten dönme kuralları “Acil Durum Yönetimi” politikalarına uygun olarak oluşturulmalı ve yazılı hale getirilmelidir. h)Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

ı)Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.

i)Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

j)Bilgi saklama medyaları Belediye dışına çıkartılmamalıdır.

k)Sistem dokümantasyonu güvenli şekilde saklanmalıdır.

l)İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.

m)Veritabanı sunucusu sadece ssh, rdp, ssl ve veritabanının orijinal yönetim yazılımına açık olmalı; bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır. Ancak ftp, telnet vb. açık metin şifreli bağlantılar veri tabanı sunucudan dışarıya yapılabilir.

n)Uygulama sunucularından veritabanına login vb. şekilde erişememelidir.

o)Arayüzden gelen kullanıcılar bir tabloda saklanmalı, bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.

ö)Veritabanı sunucusuna ancak zorunlu hallerde “root” veya “admin” olarak bağlanılmalıdır. Root veya admin şifresi tanımlı kişi/kişilerde olmalıdır.

p)Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.

r)Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.

s)Veritabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.

ş)Veritabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.

t)Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmelidir.

u)Veritabanı sunucularına ancak yetkili kullanıcılar erişmelidir.

ü)Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler arayüzden sağlanmalıdır.(örnek; Kullanıcılar tablolardan “select” sorgu cümleciklerini yazarak sorgulama yapmamalıdır)

v)Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için)

y)Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için Şifreleme Politikasına bakılmalıdır. Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

## Bilgi Sistemleri Yedekleme Politikası

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 bilgileri ve kurumsal veriler düzenli olarak yedeklenmelidir.

b)Veri yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği kritiklik derecesine göre belirlenmesi ve yazılı hale getirilmesi ilgili birimlerin sorumluluğundadır.

c)Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak manyetik kartuş, DVD, disk , CD… vb ortamda yedekleri alınmalıdır.

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

e) Bütün sistemlere ait log kayıtları 5651 sayılı kanun kapsamında en az 6 ay en fazla 2 yıl süre ile saklanmalıdır. Tutulma süresi dolan yedekler güvenli bir şekilde imha edilmelidir.

f) Kurumsal kritik verilerin saklandığı veya sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak yazılı hale getirilmelidir.

g)Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.

h)Yedeklenecek bilgiler değişiklik gösterebileceğinden ilgili birimlerde yedeklenecek veriler periyodik olarak gözden geçirilmeli ve güncellenmelidir.

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

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

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

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

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

m)Son kullanıcılar kendi bilgisayarlarındaki verilerin yedeklenmesinden sorumludurlar.

## Personel Güvenliği Politikası

(1) Personel Güvenliği Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a)Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.

b)Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.

c)Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, yeterlilikleri değerlendirilmelidir.

ç)Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.

d)Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

e)İş tanımı değişen veya Belediyeden ayrılan kullanıcıların erişim hakları kaldırılmalıdır.

f)Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

g)Belediye bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.

ğ)Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılması ile ilgilidir. Bu paylaşım ile kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılmalıdır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamasıdır. Sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmalıdır.

h)Çalışanlar, kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilmelidir.

ı)Çalışanların 5651 sayılı kanun uyarınca sistemlere erişim aktiviteleri izlenmelidir.

i)Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

## Bilgi Sistemleri Genel Kullanım Politikası

(1) Bilgi sistemlerine sahip olma ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir.

a)Belediyenin güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Belediye bünyesinde oluşturulan tüm veriler Belediyenin mülkiyetindedir.

b)Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmamalıdır. Bu konuda ilgili politikalar dikkate alınmalıdır.

c)Belediye, ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

ç)Belediye bilgisayarları etki alanına dahil edilmelidir.

d)Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.

e)Belediye Bilgi İşlem Müdürlüğünün bilgisi ve onayı olmadan Belediye Ağ sisteminde (web hosting, eposta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.

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

g)Bilgisayarlara lisanssız program yüklenmemelidir.

ğ)Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

h) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar vermemeli, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunmamalı, içeriğini izinsiz olarak değiştirmemelidir.

(2) Bilgi sistemleri genel yapılandırması ile ilgili kurallar aşağıda belirtilmiştir.

a)Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda ilgili Müdürlüğe haber verilmelidir.

b)Bütün cep telefonu, PDA (Personal Digital Assistant) vb cihazlar Belediyenin ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızılötesi, bluetooth, vb) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.

c)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. Belediye bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmemektedir.”

ç)Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve mümkünse dosyalar sıkıştırılmalıdır.

d) Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.

e) Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur.

f) Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişmemelidir.

g) Port veya ağ taraması yapılmamalıdır.

h) Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.

I) Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Müdürlüğünün onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

i) Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.

j) Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD' leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.

k) Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliği ile sorumludur.

l) Bilgi İşlem Müdürlüğü tarafından yetkili kişiler kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel kişisel bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.

m) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

n) Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

o) Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Müdürlüğüne haber verilmelidir.

ö) Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Müdürlüğüne haber verilmelidir.

p) Belediye'nin bütün çalışanları "Bilgi Güvenliği Politikalarını" bilmek ve uygulamak ile yükümlüdür. Aksi belirtilmedikçe 3. taraflar da bu politikaya uymakla yükümlüdür.

r) Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.

Kurum yönetimi olarak "Kurum Bilgi Güvenliği Politikası"nın uygulanmasının sağlanmasının ve kontrolünün yapılmasının güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.