MURATPAŞA BELEDİYESİ
BİLGİ GÜVENLİĞİ POLİTİKALARI
YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Belediyemiz Bilişim Sistemlerinde Tüzel ve Kurumsal birçok önemli fonksiyonlar icra edilmekte olup, bu bilgilerin güvenliği, gizliliği ve kişisel mahremiyetin korunması (KVKK) büyük önem arz etmektedir. Bilgisayar ağına bağlı olan her hangi bir bilgisayardaki güvenlik açığı, kurumumuzun bütün Bilişim sistemlerinin güvenliğini riske atmasına sebep olabilir.

Bu nedenle; Kurumsal Bilişim sistemlerinin güvenliğinde her hangi bir aksamaya mahal verilmemesi için, genel sistem seviyesinde alınmış olan güvenlik tedbirlerinin yanında, çalışanlarımızın da bu hususta titizlikle uyması gereken bir takım kurallar vardır bu kurallara bütün Kurum çalışanları uymak zorundadır. Uyulması gereken kurallar aşağıda belirtilmiştir.

AMAÇ

MADDE 1- Bu Yönergenin amacı; Muratpaşa Belediyesinin sahip olduğu elektronik ortam ve bilgilerinin paylaşımı ve güvenliği konularında tedbir almak, bilginin Gizlilik, Bütünlük ve Erişebilirlik kapsamında değerlendirilerek içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak, yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirmek ve sistem devamlılığını sağlamaktır.

KAPSAM

MADDE 2- Bu Yönerge, Muratpaşa Belediye Başkanlığına bağlı Merkez Bina ve Ek Hizmet Binaları/Noktalarında bulunan bütün birimlerdeki personelin, bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

HUKUKİ DAYANAK

MADDE 3- Bilgi işlem Müdürlüğü, Belediye Başkanınca verilen ve bu yönetmelikte tarif edilen görevler ile ilgili yasalarda belirtilen görevleri gereken özen ve çabuklukla yapmak ve yürütmekle sorumludur.

TANIMLAR

MADDE 4- Bu Yönetmelikte geçen;

1) **Kurum:** Muratpaşa 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) Dışarıdan erişim: Ağ kaynaklarına, erişilmek istenen bilgiye fiziksel olarak farklı bir ağda bulunan bilgisayar aracılığı ile erişme sürecini,
8) **Güvenlik duvarı (UTM Birleşik Tehdit Yönetim Sistemi Firewall):** Yetkisiz erişimi engellemek amacıyla güvenilir bir ağ ile herkese açık bir ağ arasına yerleştirilen bir yazılım-donanım çözümünü,
9) **Modem:** Veriyi telefon hatları, kablolar veya mikrodalga gibi transmisyon ortamları üzerinden iletilebilecek duruma getirmek üzere kodlayan aygıtı,
10) **Güvenlik ihlali:** Bilgi Güvenlik Kuralları ve talimatlarını ihlal eden veya bununla ters düşen herhangi bir olayı,
11) **Yazılım:** Bir bilgisayar sisteminde çalışmak üzere tasarlanmış bir uygulamayla ilişkili kod, prosedür ve ilişkili dokümandan oluşan yapıyı,
12) **Hassas bilgi:** Kurumun isteği dışında açığa çıkması ile kurum ve ilişkisi olduğu kişi ve kuruluşlara ciddi stratejik ve finansal zararlar verebilecek verileri,
13) **Şifreleme:** Bilgiyi gizli bir şifre veya anahtar olmadan okunamayacak (deşifre edilemeyecek) bir kod haline getirme işlemini,
14) **Virüs:** Virüs, herhangi bir bilgisayara değişik yollarla girebilen ve bu bilgisayarlarda istenmeyen sonuç ve zararlara yol açan programları,
15) **Dosya:** Herhangi bir kayıt ortamında saklanan kayıtlar topluluğunu,
16) **Router:** Ağlar arasındaki bağlantıları gerçekleştiren cihazları, ifade eder.
17) **Crack:** Ücretli yazılımların ücretsiz bir şekilde kullanılır hale getirilmesi.
18) **Everyone:** Tüm kullanıcılar
19) **VPN:** Sanal özel ağ
20) **DMZ:** Arındırılmış bölge
21) **SSH:** Güvenli uzaktan yönetim protokolü
22) **KVKK:** Kişisel Verilerin Korunması Kanunu
23) **Gizlilik:** Bilginin yetkisiz kişilerce erişilememesidir. Bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.
24) **Bütünlük:** Bilginin doğruluğunun ve tamlığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır. Kazara veya kasıtlı olarak bilginin bozulmamasıdır.
25) **Erişebilirlik:** Bilginin her ihtiyaç duyulduğunda sadece erişim yetkisi olanlar tarafından kullanıma hazır durumda olması demektir.

SORUMLULUKLAR

MADDE 5- Kurum bilgi sistemlerinde güvenliğin sağlanmasına yönelik güvenlik kurallarının hazırlanması, hazırlanan kuralların uygulanmasının sağlanması, düzenli olarak gözden geçirilerek güncellenmesi, uygulandığının denetlenmesi veya denetlenmesinin sağlanması, Kurum bilgi sistemlerine ilişkin bir güvenlik ihlalinin tespit edilmesi durumunda ise sistem üzerindeki delillerin toplanarak Kurumun ilgili birimine sunulması Bilgi İşlem Müdürlüğünün sorumluluğundadır.

Kurum kullanıcıları, Kurum bilgi sistemlerinde güvenliğin sağlanmasına yönelik olarak hazırlanan kurallara ve aşağıda belirtilen temel kurallara uygun davranmaktan sorumludur:

İSTİSNALAR

MADDE 6- İnternet üzerindeki erişim hakları veya program kullanımları, Bilgi İşlem Müdürlüğü tarafından Kurum bilgi sistemlerinde güvenliğin sağlanmasına yönelik olarak hazırlanan yönetmelikler doğrultusunda düzenlenmekte olup, internet kullanımı kısıtlanan kullanıcıların, işleri için gerekli ancak güvenlik açısından

engellenmiş internet sayfa, servis ve programları kullanabilmeleri, görev yaptıkları birim tarafından talep nedeni ve kullanım süresi de açıkça belirtilerek Bilgi İşlem Müdürlüğüne yazılı olarak başvurulması ve bu talebin Bilgi İşlem Müdürlüğünce yapılacak ihtiyaç/güvenlik değerlendirmesi sonucunda uygun görülmesi şartlarına bağlıdır.

İKİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ KURALLARI

MADDE 7- Kurum Bilgi Güvenliği Kuralları aşağıdaki gibidir;

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) Kurum bu kurallar çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
4) Kurum bilgisayarları etki alanına dahil edilmelidir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkartılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi olmamalıdır.
5) 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.
6) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.
7) Bilgi İşlem Müdürlüğü bilgisi ve onayı olmadan kurum ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.
8) Bilgi İşlem Müdürlüğü personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilememelidir.
9) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
10) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar vermemeli, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunmamalı, içeriğini izinsiz olarak değiştirmemelidir.
11) Kuruma ait cihazların çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Müdürlüğü'ne haber verilmelidir.
12) Bütün cep telefonu, tablet bilgisayarlar ve PDA (Personel Digital Assistant) cihazlarının kurumun ağı ile senkronize olsun ya da olmasın şifreleri aktif halde olmalıdır. Kablosuz erişim (kızılötesi, bluetooth, hotspot vb.) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.
13) "Bu elektronik posta ve onunla iletilen bütün dosyalar; göndericisi tarafından alması amaçlanan; yetkili gerçek ya da tüzel kişinin kullanımı içindir. Eğer söz konusu yetkili alıcı değilseniz bu elektronik postanın içiriğini açıklamanız, kopyalamanız, yönlendirmeniz ve kullanmanız kesinlikle yasaktır ve bu elektronik postayı derhal silmeniz gerekmektedir. Muratpaşa Belediyesi bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmemektedir." Bu iletinin bildirim(disclaimer) olarak kullanılması zorunludur.

14) Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı, ek dosyalar eklenecekse en fazla 10Mb boyutunda ek dosyalar eklenmeli ve mümkünse dosyalar sıkıştırılmalıdır.
15) Masaüstü bilgisayar, dizüstü bilgisayar, yazıcı, tarayıcı vb. cihazların Bilgi İşlem Müdürlüğü'nün haberi olmadan yeri değiştirilmemeli ve zimmetsiz olarak başka birime verilmemelidir. Kuruma ait diz üstü bilgisayarlar kurum dışına çıkartılmamalı zorunlu olarak kurum dışına çıkartılanlar ise güvenlik açıklarına karşı daha dikkatle korunmalıdır.
16) Güç kaynağı prizlerine bilgisayar ve monitör dışında herhangi bir cihaz bağlanmamalıdır (ısıtıcı, elektrikli süpürge vb.)
17) Tablet bilgisayarların ve notebooklar güç tuşundan değil, tüm çalışan programlar kapatıldıktan sonra "bilgisayarı kapat" menüsünden kapatılması gerekmektedir.
18) Hukuki ve cezai sorumluluk doğurması nedeniyle, lisanslı olmayan programlar bilgisayarlara yüklenmemelidir.
19) 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.
20) Kurumun Bilgisayarlarını ve internetini kullanarak taciz veya yasa dışı olaylara karışılmamalıdır.
21) Kullanıcılar Ağ güvenliğini (Bir kişinin yetkisi olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket sniffing ,paket spoofing,denial of service vs.)ortadan kaldıracak hiçbir eylemde bulunmamalıdır.
22) Bilgi İşlem Müdürlüğünün haberi olmadan network çözümlerine yönelik programlar kullanıcılar tarafından illegal yollardan bilgisayarlara yüklenip bu programlar aracılığı ile port yada ağ taraması yapılması kesinlikle yasaktır.
23) Kuruma ait Network,Ağ ve Donanım bilgileri kurum dışından herhangi tüzel kişi yada kuruluşa kesinlikle bilgi amaçlı olarak verilemez.
24) Kullanıcılar kurum içerisinde kullanmakta oldukları bilgisayarlarına Bilgi işlem Müdürlüğünün haberi olmadan ve onayı alınmaksızın her hangi bir çevre birimi bağlantısı yapamazlar.
25) Kuruma ait cihaz,yazılım ve veriler izinsiz olarak kurum dışına çıkarılmamalıdır,çıkarılması durumunda tüm sorumluluk kullanıcıya aittir.
26) Kurum kullanıcıları kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masa üstü ve diz üstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak farklı ortamlara (cd, dvd, usb external harddisk vb.) yedeklenmesinden ve yedeklerin başka kişilerin eline geçmemesinden sorumludur.
27) Bilgi İşlem Müdürlüğünce yetkili personel kullanıcıya haber vermeden yerinde veya uzakta 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.
28) Kurumda sorumlu bilgi işlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar, ağ yazıcıları üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeler hiçbir şekilde oynanmamalı ve değiştirilmemelidir.
29) 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.

30) Bilgi işlem sistemlerinin yönetiminde herhangi bir bilgiye sahip personelin görevden ayrılması veya görev yerinin değiştirilmesi durumunda ilgilinin vakıf olduğu tüm sistem kullancıları kapatılıp, parolaları derhal değiştirilmelidir.
31) Müdürlüğün kullanımında olan bir bilgisayar kurum bilgisayar ağına bağlanmadan belediyenin iş ve işlemleri için kullanılacaksa, ilgili müdürlükten resmi yazı istenir. Bu yazıya müteakip bilgisayar domainden çıkartılır. Kullanıcıya teslim edilir. Bu işlemden sonra bilgisayar ile ilgili tüm lisans ve güvenlik yazılımlarından kullanıcı sorumlu olup bilgisayar kesinlikle kurum ağına dahil edilmemelidir.
32) Kurum ağından çıkartılan bir bilgisayar tekrar kurum ağına dahil edilecekse ilgili müdürlük tarafından yazılı talepte bulunulur. Bahsedilen cihaz yedek alınmaksızın formatlanır ve gerekli yazılımlar yüklenerek kurum ağına bağlanacak duruma getirilir.
33) Belge tarama işlemi yapan kullanıcılar Bilgi İşlem Müdürlüğünün hazırlamış olduğu ve bilgilendirdiği şekilde tarama yapması gerekmektedir. Bu kurala uyulmayarak yapılan yüksek boyutlu taramalar bilgi sistemleri üzerinde çok büyük yük oluşturduğundan ve daha sonra görülmek istendiğinde ilgili dokümana ulaşmak zorlaştığından dolayı ilgili talimata uyulması gerekmektedir.

BELGELENDİRME KURALLARI

1) Bilişim sisteminin yapısı ile ilgili bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir olmalıdır.
2) İş akışları uygun şekilde belgelenmelidir.
3) Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.
4) Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelendirilmelidir.
5) Çıktı form örnekleri ve çıktıların kime dağıtılacağı belgelenmelidir.
6) Programların nasıl test edildiği ve test sonuçları belgelendirilmelidir.
7) Bütün program değişikliklerinin detayları belgelenmelidir.

E-POSTA KULLANIM KURALLARI

1) E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.
    a) Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.
    b) Muratpaşa 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
    c) 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.
    d) Kullanıcı hesapları, ticari ve kar amaçlı olarak kullanılmamalı ve e-posta gönderilmemelidir.
    e) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında çalıştırılmayıp, başkalarına iletmeyecek ve Bilgi İşlem Müdürlüğüne haber verilmelidir.
    f) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
    g) Kullanıcı, e-posta ile uyumlu olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme vb.) göndermemelidir.
    h) 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.
2) E-Posta ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.
    a) E-posta kişisel amaçlar için kullanılmamalıdır.

b) Kullanıcı, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden parola kullanılmalı ve kullanılan parola en geç 30 günde bir değiştirilmelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişime karşı korunmalıdır.
c) Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu postalara herhangi bir işlem yapmaksızın Bilgi İşlem Müdürlüğü'ne haber vermelidir.
d) Kullanıcı, kurumsal e-postalarının, kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesini ve okunmasını engellemelidir.
e) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Bilgi İşlem Müdürlüğü'ne haber verilmelidir.
f) 6 ay süreyle kullanılmamış e-posta adresleri kullanıcıya haber verilmeden sunucu güvenliği ve veri depolama alanlarının boşaltılması için kapatılmalıdır.
g) Kullanıcı parolaları en az 8 karakterden oluşmalı ve parolaların içinde en az 1 tane harf, en az 2 tane rakam ve en az 1 tane özel karakter (@,!,?,^,+,$,#,&,/,{,*,-,],=,...) içermelidir.
h) 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.

3) "Bu elektronik posta ve onunla iletilen bütün dosyalar; göndericisi tarafından alması amaçlanan; yetkili gerçek ya da tüzel kişinin kullanımı içindir. Eğer söz konusu yetkili alıcı değilseniz bu elektronik postanın içiriğini açıklamanız, kopyalamanız, yönlendirmeniz ve kullanmanız kesinlikle yasaktır ve bu elektronik postayı derhal silmeniz gerekmektedir. Muratpaşa Belediyesi bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmemektedir." Bu iletinin bildirim(disclaimer) olarak kullanılması zorunludur.
4) Kurumsal e-postalar yetkili kişilerce hukuksal açıdan gerekli görülen yerlerde önceden haber verilmeksizin denetlenebileceklerdir.
5) Kullanıcı, kurumsal mesajlarını, belediye iş akışının aksamaması için cevaplandırmalı ve kurumsal mesajlarda kişisel e-posta adresleri değil kurumsal e-posta adresi kullanılmalıdır.
6) Kullanıcı,e-postalarına erişirken kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokollerini kullanmamalıdır.
7) Kurum, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve altyapıyı sağlamakla sorumludur.
8) Virüs, solucan, Truva atı veya diğer zararlı kodlar bulaşmış olan herhangi bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar antivirüs, antispam özellikleri ve yazılımları tarafından analiz edilip, içeriği korunarak virüsten temizlenmelidir.
9) Kurumun haberi ve izni olmadan Kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
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.

13) Kurumdan ayrılan yada emekli olan personel herhangi bir sebeple halen kurumsal email sistemine erişebiliyorsa,ivedilikle Bilg İşlem Müdürlüğü'ne haber vermek zorundadır.Aksi durumda oluşan tüm sorumluluklar ilgili kişi/kişilere aittir.

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 6 (altı) ayda bir değiştirilmelidir.
2) Kullanıcı hesaplarına ait parolalar (e-posta, web, masaüstü bilgisayar vs.) en geç 30(otuz) günde bir değiştirilmelidir.
3) Sistem yöneticisi, sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.
4) Parolalar e-posta iletilerine,web tarayıcısı veya herhangi bir elektronik forma eklenmemelidir ve otomatik parola anımsama seçenekleri işaretlenmemelidir.
5) Kullanıcı, parolasını başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmelidir.
6) Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılamayacak güçlü parolaya sahip olmalıdır.
7) Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.
8) Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır:
    a. En az 8 haneli olmalıdır.
    b. İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)
    c. İçerisinde en az 2 tane rakam bulunmalıdır. (1, 2, 3...)
    d. İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,$,#,&,/,{,*,-,],=,...)
    e. Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, ababab...)
    f. Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)
    g. Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)
9) Parolalarda aile bireylerinin isimleri kullanılmamalıdır.
10) Bütün parolalar Kuruma ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.
11) Her hangi bir kişiye telefonda parola verilmemeli ve paylaşılmamalıdır.
12) Parolalar aile bireyleri ile paylaşılmamalıdır.
13) E-posta, SMS vb. alanlarda parola paylaşılmamalıdır.
14) Şifreler işten uzak olunduğu zamanlarda iş arkadaşlarına verilmemelidir.
15) Kurum kullanıcıları ile Kurum kullanıcısı olmadığı halde Bilgi İşlem Müdürlüğü tarafından kendilerine kullanıcı adı ve şifresi tahsis edilmiş olanlar (Danışmanlar, hizmet alınan firmaların teknisyenleri, vb.) dışındakilerin, Kurumun herhangi bir biriminde mevcut bilgisayar veya ağ bağlantı ucunu kullanması yasaktır. Bu tür bir girişime Kurum çalışanlarınca müsaade edilmemesi gerektiği gibi fark edildiği durumlarda da engellenmesi zorunludur.
16) Kurum personeli olmayan kişiler (Danışmanlar, hizmet alınan firmaların teknisyenleri, vb.) için hizmet verdikleri birimin yöneticileri tarafından Bilgi İşlem Müdürlüğü kullanıcı adı ve şifresi tahsis edilmesi için yazılı talepte bulunulmalı ve bu talebe istinaden Bilgi İşlem Müdürlüğü tarafından verilen kullanıcı adı ve şifresinin kullanılması sağlanmalıdır
17) 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.

18) Kullanıcıların şifrelerinin öğrenildiği ya da kullanıldığını düşündüğü hallerde şifrelerini yenilemeleri gerekmektedir.

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

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

21) Bireylerin ve grupların kimlik doğrulaması işlemlerini desteklemelidir.

22) Parolalar, metin olarak veya kolay anlaşılabilir formatta saklanmamalıdır.

23) Parolalar şifrelenmiş olarak saklanmalıdır.

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

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

6) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalı, virüs temizliğinden sonra tekrar etki alanına alınmalıdır.

7) Sistem yöneticileri antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.

8) Antivirüs güncellemeleri antivirüs sunucusu/sunucuları tarafından yapılmalıdır. Antivirüs sunucuları internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcileri, otomatik olarak antivirüs sunucuları tarafından güncellemeleri yapılmalıdır.

9) Haklı bir gerekçe ile etki alanı dışında tutulması gereken kullanıcı talebi olması durumunda; her türlü maddi/manevi oluşabilecek zararların kişi ve amiri tarafından kabul edildiğini beyan eden form doldurularak Bilgi İşlem Müdürlüğüne teslim edilmelidir. Bu tip kullanıcıların her türlü güncelleme sorumluluğu kendilerine aittir.

10) Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda ilgili müdürlük Bilgi İşlem Müdürlüğünü yazı ile bilgilendirmek zorundadır.

11) Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

12) Ağa bağlı olan kurum içerisindeki bütün bilgisayarlarda Kurumun lisanslı anti-virüs yazılımı yüklü olmalıdır ve merkezi olarak güncellenmelidir.

13) Üzerinde her hangi bir anti-virüs yazılımı bulunmayan bilgisayarlar Bilgisayar ağına kesinlikle bağlanmamalıdır.

14) Zararlı programları(örnek;virüsler,solucanlar,truva atı,e-mail bombaları vs)Kurum bünyesinde oluşturmak ve bunları dağıtmak kesinlikle yasaktır.

15) Kurum içerisinde ağa bağlı hiçbir kullanıcı her hangi bir sebepten dolayı antivirüs programını sisteminden kaldıramaz,buna teşebbüs edemez.
16) Kişisel kullanımda bulunan USB ,harici diskler bilgisayarlara bağlanmamalı, bağlanılması gereken durumlarda mutlaka Antivirus programı ile tarama yapılmalıdır.

İNTERNET ERİŞİM VE KULLANIM KURALLARI

1) Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır.
2) Kurumun kuralları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. Kurum iş ve işlemleri dışındaki istenmeyen siteler ve kategoriler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.
3) Kurumun ihtiyaçları doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.
4) Kurumun ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır. İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.
5) Kullanıcıları internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.
6) Kurum ağları kullanılarak iş ile ilgili olmayan sitelerde gezinilmemelidir. İnternet üzerinden TV, radyo ve video izlenmemeli/dinlenmemelidir. Bu konudaki tüm sorumluluk kullanıcıya aittir.
7) İş ile ilgili olmayan (müzik, video dosyaları vs.) dosyalar gönderilmemeli ve indirilmemelidir. Bu konudaki tüm sorumluluk kullanıcıya aittir.
8) Hiçbir Kullanıcı Peer to peer(p2p-noktadan noktaya) dosya paylaşım programları,telif hakları ve lisansları ihlal etmenin yanısıra,yüksek band genişliği tüketerek birinci amaçlar için ağ kullanımına kaynak bırakmamaktadır. Bu nedenle,aşağıda sıralanan fakat bunlarla sınırlı olmayan tüm"Peer to peer" dosya paylaşım araçlarının kullanılması ve ağ güvenliğini tehdit edici faaaliyetlerde bulunmak(Dos saldırısı,port-network taraması vb),gereksiz dosya indirimleri yasaktır. (Kazaa, imesh, eDonkey2000, Gnutella, Napster, Aimster, Madster, Fasttrack, Audigalaxy, MFTP, eMule, Overnet, NeoMudus, Direct Connect, Acguisition, BearShare, Gnucleus, GTK-Gnutella, LimeWire, Mactella, Mopheus, Phex, Qtella, Shereaza, XoloX, Opennap, WinMX, DC++, BitTorrent, Dc++, ultrasurf, psiphon vs)
9) Potansiyel olarak virüs, solucan veya bunlara benzer güvenlik açısından tehlikeli programların bulaşması/bulaştırılması tehlikesi taşıyan bazı internet sitelerine (Örn: yetişkin (adult), kumar, oyun, şifre çözme (crack), hack (saldırı), illegal arama (underground search), sohbet odaları ve yasadışı siteler vb.) girilmemeli, HTTP, SMTP, POP3 dışında kalan servisler (örn: FTP, ICQ, IRC, telnet, messenger vb.) ve bazı uzaktan erişim programları (Dame-Ware, PcAnywhere vb.) kullanılmamalıdır. Hiçbir kullanıcı internet üzerinden multimedia streaming(İnternet üzerinden video,film,tv izleme vb) gibi faaliyetlerde bulunmayacaktır.
10) Kurumda e-posta,internet vb. varlıkları kullanılarak hiçbir platforma yorum yazılamaz,görüş bildiremez.
11) İş ile ilgili olmayan (müzik,video dosyaları) yüksek hacimli dosyalar göndermek(upload) ve indirmek(download) yasaktır.
12) İnternet üzerinden Kurum tarafından onaylanmamış yazılımlar indirilemez ve Kurum sistemleri üzerine bu yazılımlar kurulamaz.
13) Bilgisayarlar üzerinden Genel ahlak anlayışına aykırı internet sitelerine girilmesi ve dosya indirimi yapılması kesinlikle yasaktır.
14) Bilgisayar işletim sistemlerini büyük ölçüde tehdit ettiği için internet üzerinden yada flash belleklerden vb. cihazlar aracılığı ile ekran koruyucu, masaüstü resimleri yada kişisel aile resimleri indirilmesi ve

kopyalanması kesinlikle yasaktır. Bilgi İşlem Müdürlüğü tarafından onaylanmayan herhangi bir içerik ekran koruyucu, ekran kilidi, masaüstü arka plan görseli olarak ayarlanması yasaktır.
15) Üçüncü şahısların kurum içerisinden internet kullanmaları Bilgi İşlem Müdürlüğü izni ve bu konudaki kurallar dahilinde gerçekleştirilecektir. Birimlere ulaşan bu konudaki istekler her hangi bir ağa bağlanılmayı denemeden Bilgi işlem Müdürlüğüne ivedi olarak bildirilecektir. Bilgi İşlem müdürlüğünün belirlemiş olduğu tutanak doldurulduktan sonra gerekli erişimler sağlanacaktır.
16) Bilgi İşlem Müdürlüğü, Kurum bilgi sistemleri güvenliğini sağlamak amacıyla kullanıcılara tahsis edilen/edilecek cihazlardaki web tarayıcı (browser), güvenlik duvarı (firewall) ve virüs tarama (antivirüs) , vs. programlarında özel ayarlar yapacak ve sınırlı bir kullanıcı hesabı (user account) tanımlayacaktır. Bu nedenle söz konusu programların ayarları ve kullanıcı hesabı türü kullanıcılar tarafından kesinlikle değiştirilmemelidir.
17) Kişisel internet erişimi için Kurum ağı kullanılmalıdır. Mobil İnternet cihazları, Modem kullanarak telefon hatları vasıtası ile internet bağlantısı kurulması yasaktır. Kişisel diz üstü bilgisayarların kuruma getirilerek yeni nesil 3G/4,5G protokolu ve diğer internet hizmetleri üzerinden Kurum dışındaki başka bir internet sağlayıcısına bağlanılması kesinlikle yasaktır.
18) Yetkisi olmayan Kurum çalışanları, yönetilen bilgi sistemleri üzerinde hiçbir şekilde güvenlik araştırması yapmaya kalkışmamalı ve güvenlik mekanizmalarını test etme girişiminde bulunmamalıdır. Güvenlik mekanizmalarının bozulmasına neden olabilecek her türlü eylem ve işlem yasaktır
19) Kullanıcılar, Kuruma ait hassas bilgileri, iletişim araçları, İnternet vasıtası veya her hangi bir şekilde yayınlayamaz ve açıklayamazlar
20) Yerel, ulusal, uluslararası bilgisayarları veya hizmetleri kasıtlı olarak yetkisiz kullanmak yasaktır.
21) Başkalarının telif haklarını ihlal edici konumda olan yazı, makale, kitap, film, müzik eserleri gibi materyali edinmek, indirmek yayınlamak, dağıtmak yasaktır.
22) Tüm kullanıcılar kendilerine verilen internet kullanıcı adı ve şifresini korumakla yükümlüdür. Bu bilgilerin kasıtlı yada kasıtsız olarak kurum içi veya dışı herhangi bir kişiye verilmemelidir. Bu kullanıcı adı ve şifrenin başka kullanıcılar tarafından öğrenilmesi veya sistem tarafından uyarı gelmesi durumunda derhal Bilgi İşlem Müdürlüğüne haber verilmelidir.
23) İnternet üzerinden radyo dinlenilmesi, tv seyredilmesi, film, görüntülü iletişim kurulması veya on-line kamera çalışan web sitelerine girilmesi mevcut bant genişliğini dolduracağından yasaktır.
24) Bu Protokol, Kurum içerisinde aynı ağ üzerinden internete çıkışı olan bulunduğu konum ve yükümlü olduğu iş nedeni ile kısıtlı olmayan kullanıcıları da kapsamaktadır.

SUNUCU GÜVENLİK KURALLARI

1) Kurumda bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel(ler) sorumludur.
2) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.
3) 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.
4) Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.
5) Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri test edilmeli ve üretim ortamına hazırlanmalıdır.
6) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
7) Servislere erişimler, kaydedilmeli ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.

8) 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.
9) Sistem yöneticileri "Administrator" ve"root" gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.
10) Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
11) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'ların tanımlı olduğu portlardan bağlantı sağlanmalıdır.
12) İhtiyaç halinde sunucular üzerinde lisanslı veya güvenliği test edilmiş açık kaynak kodlu yazılımlar kurulabilir.
13) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.
14) Kritik sistemlerde, uygulamalar kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.
15) Aylık backuplar günlük,haftalık ve aylık olarak saklanmalıdır.
16) Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanmalıdır.
17) Sunucular üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları vb.) çalıştırılmamalıdır.
18) Kayıtlar sorumlu kişi(ler) tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.
19) Port tarama atakları düzenli olarak yapılmalıdır.
20) Yetkisiz kişilerin ayrıcalıklı hesaplara yönelik girişimlerinin kontrolü periyodik olarak yapılmalıdır.
21) Sunucularda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.
22) Denetimler, Bilgi İşlem Müdürlüğü tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.
23) Sunucuların bilgileri yetkilendirilmiş kişi(ler) tarafından tutulmalıdır.
24) Sunucular elektrik, ağ yapısı, sıcaklık ve nem değerleri düzenlenmiş tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulmalıdır.
25) Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.
26) Sistem odalarına giriş ve çıkışlar erişim kontrolü olmalı ve bilgisayar sistemine kayıt edilmelidir.
27) Sunucularda (Coğrafi Bilgi Sistemleri, Yönetim Bilgi Sistemi, Etki alanı, internet vb.) bulunan kullanıcı adları ilgili bilgi işlem müdürlüğü personelleri tarafından periyodik aralıklarla kontrol edilmelidir.

AĞ CİHAZLARI GÜVENLİK KURALLARI

1) Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.
2) Yerel kullanıcı hesapları açılmalıdır. Ağ cihazları kimlik tanımlama için LDAP, RADIUS veya TACAS+ protokollerinden birini kullanmalıdır.
3) Yönlendirici ve anahtarlama cihazlarındaki tam yetkili şifre olan "enable şifresi" kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması kurumun içerisinden yapılmalıdır.
4) Kurumun standart olan SNMP community string'leri kullanılmalıdır. Bu bılgı sadece yetkilendirilmiş kişiler tarafından bilinmelidir.
5) İhtiyaç duyduğu zaman erişim listeleri eklenmelidir.

6) Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin/mesai saatleri dışında üretim ortamına taşınmalıdır.
7) Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.
8) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, pasif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlendirilmelidir.
9) Yönlendiriciye erişen tüm kullanıcılar uyarılmalıdır.
10) Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır. "BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, bu kurala uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir."

AĞ YÖNETİM KURALLARI

1) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.
2) Erişimine izin verilen ağlar için ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimlerle ilgili tedbirler alınmalıdır.
3) Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.
4) Sınırsız ağ dolaşımı engellenmelidir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.
5) Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.
6) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.
7) Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır. Kurum kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirinden ayrılmalı ve ağlar arası geçiş güvenlik sunucuları (firewall) üzerinden sağlanmalıdır.
8) Uzak teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.
9) Bilgisayar ağına bağlı bütün makinelerde (Bilgisayar, Tablet vb.) kurulum ve yapılandırma parametreleri, kurumun güvenlik kuralları ve standartlarıyla uyumlu olmalıdır.
10) İnternet trafiği, İnternet Erişim ve Kullanım Kuralları ve ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.
11) Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. Şahıs ve sistemlerin ulaşamayacağı şekilde tasarlanmalıdır.
12) Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.
13) Ağ cihazları konfigürasyonu Bilgisayar Ağları ve Altyapı Hizmetleri Servisi tarafından yapılmalıdır.
14) İlgili dokümanlar hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

UZAKTAN ERİŞİM KURALLARI

1) Internet 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.

2) Bilgi İşlem Müdürlüğü tarafından hazırlanan Uzaktan Erişim Formu doldurulmalıdır. Doldurulmayan bağlantılar sonlandırılacaktır.
3) Uzaktan erişim denetlenmelidir.
4) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
5) Kurumun ağına uzaktan erişim yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka ağa bağlı olmamalıdırlar.
6) Telefon hatları üzerinden uzaktan erişim mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.
7) Kurum ağına uzaktan erişecek olan bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeleri yapılmış olmalıdır.
8) Kurum ağına uzaktan erişim yapacak kullanıcıların İnternet IP adresleri sabit ip olmalıdır.
9) Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

KABLOSUZ ERİŞİM KURALLARI

1) Kurum ağı içerisinde bulunan cihazların kablosuz erişim özellikleri kapalı tutulmalı ve kullanılmamalıdır.
2) İş sürekliliğini sağlamak amacıyla kurum ağı dışında kullanılması gereken bilgisayarlar ilgili müdürlüğün yazılı talebi sonrası Bilgi İşlem Müdürlüğü tarafından bilgisayarlar etki alanından çıkarılarak ilgili müdürlüğe teslim edilir. İlgili bilgisayar kurum ağına yeniden girmesi gerektiği durumda Bilgi İşlem Müdürlüğü tarafından işletim sistemi ve profiller sıfırlanarak ilgili müdürlüğe teslim edilir.

DONANIM VE YAZILIM ENVANTERİ OLUŞTURMA KURALLARI

1) Oluşturulan envanter tablosunda şu bilgiler olmalıdır; sıra no, bilgisayar adı, bölüm, marka, model, seri no, özellikler, ek aksamlar, işletim sistemi, vs.
2) Bu tablolar merkezi bir web sunucuda tutulmalı ve belirli aralıklarla güncellenmelidir. İlgili siteye girişler güvenlik kuralları çerçevesinde yapılmalıdır.
3) Envanter bilgileri sık sık kontrol edilmelidir.

KRİZ / ACİL DURUM YÖNETİM KURALLARI

1) Acil durum sorumluları atanmalı, yetki ve sorumlulukları belirlenerek dokümante edilmelidir.
2) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Problem durumlarında sistem kesintisiz veya makul kesinti süresi içerisinde felaket ve/veya iş sürekliliği merkezi üzerinden çalıştırılabilmelidir.
3) Bilişim sistemlerinin kesintisiz çalışmasının sağlanması için aynı ortamda kümeleme veya uzaktan kopyalama veya yerel kopyalama veya pasif sistem çözümleri hayata geçirilmelidir. Sistemler tasarlanırken minimum sürede iş kaybı hedeflenmelidir.
4) Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.
5) Acil durumlarda sistem kayıtları teknik olabilirlik çerçevesinde (ortam izleme, kamera vs.) incelenmek üzere saklanmalıdır.
6) Yaşanan acil durumlar sonrası kurallar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
7) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.

8) Bilgi sistemlerini etkileyecek acil durumlarda Bilgi İşlem Müdürüne erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
9) Bilgi İşlem Müdürlüğü tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

FİZİKSEL GÜVENLİK KURALLARI

1) Kurum binalarının fiziksel olarak korunması ilgili müdürlükler tarafından farklı koruma mekanizmaları ile donatılması temin edilmelidir.
2) Kurumsal bilgi varlığının dağıtımı ve bulundurulan bilgilerin kritik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
3) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilmelidir.
4) Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılmalı ve izlenmelidir.
5) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
6) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.
7) Kritik sistemler özel sistem odalarında tutulmalıdır.
8) Sistem odaları elektrik kesintilerine ve voltaj değişikliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınması ve iklimlendirilmesi sağlanmalıdır.
9) Fotokopi, yazıcı vs. türü cihazlar mesai dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.
10) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.
11) Bilgi Sistemlerini etkileyecek acil durumlarda (Yangın, Su baskını, Deprem vs.) güvenlik personellerinin ilgili birimlerle acil olarak iletişime geçmek zorundadır.

KİMLİK DOĞRULAMA VE YETKİLENDİRME KURALLARI

1) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenmelidir.
2) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanmalıdır.
3) Kurum bünyesinde kullanılan ve merkezi olarak erişen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri ve açılış ekranları olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri ilgili müdürlükten gelen yazı ile belirlenmeli ve denetim altında tutulmalıdır.
4) Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
5) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
6) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız istekleri/girişimleri incelenmelidir.
7) Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar ve rollerin sistem kaynakları üzerindeki yetkileri uygun araçlar kullanılarak belirli aralıklarla listelenmelidir. Bu listeler yetki seviyeleri ile karşılaştırılmalıdır. Eğer uyumsuzluk varsa dokümanlar ve yetkiler düzeltilerek uyumlu hale getirilmelidir.

8) Kullanıcı, kendisine verilen "kullanıcı adı"nı ve "şifresi"ni bir başkası ile paylaşmaz ve bir başkasına kullandırmaz.
9) Kullanıcının Bilgi İşlem Müdürlüğünce belirlenecek periyotlarla "kullanıcı şifresini" değiştirmesi gerekmektedir.
10) 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 Bilgi İşlem Müdürlüğü yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.
11) İlgili hesabın amacı dışında kullanılması ve bu hesaptan doğabilecek zararların sorumluluğu, hesabı kullanan kullanıcıya aittir.
12) Merkezdeki her bir son kullanıcı, etki alanı üyesi olmalıdır. Etki alanında olmayan kullanıcıların internet erişimleri engellenir.
13) Kullanıcıların kullanmış olduğu bilgisayarlardaki iş ile ilgili dosyalara kullanıcının kurum dışında olması durumunda ilgili müdürlüğün yazılı talebi sonrası yazıda belirtlen personele Bilgi İşlem Müdürlüğü tarafından ilgili kullanıcının profiline erişim izni verilecektir.
14) İzinli kullanıcıların ilgili birimlere bildirilmesi gerekmektedir.

VERİTABANI GÜVENLİK KURALLARI

1) Veritabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.
2) Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.
3) Veritabanı sistem kayıtları tutulmalı ve gereğinde idare tarafından izlenmelidir.
4) Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.
5) Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme kuralları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.
6) Belirli periyodlarla yedekten dönme / yedek kontrolü yapılmalıdır.
7) Yedekleme ünitesinde tutulan log kayıtları yasalarda belirtilen sürelerde ilgili güvenli ortamlarda saklanmalıdır.
8) Veritabanı erişim kuralları “”Kimlik Doğrulama ve Yetkilendirme” kuralları çerçevesinde oluşturulmalıdır.
9) Hatadan arındırma, bilgileri yedekten dönme kuralları “Kriz/Acil Durum Yönetimi” kurallarına uygun olarak oluşturulmalı ve dokümante edilmelidir.
10) Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış olup sistem odalarında tutulmalıdır.
11) Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarından yetkili bir personel bilgilendirilmelidir.
12) Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.
13) Bilgi saklama medyaları kurum dışına çıkarılmamalıdır.
14) İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.
15) Veritabanı sunucuları sadece SSH, RDP, SSL ve veritabanının orijinal yönetim yazılımına açık olmalı; bunun dışında FTP, TELNET vb. gibi açık metin şifreli bağlantılar veritabanı sunucusundan dışarıya yapılmalıdır.
16) Veritabanı sunucularına belirlenen IPler ve yetkililer dışında erişimler kapatılmalıdır.

17) Veritabanı sunucusuna ancak zorunlu hallerde “root” veya “admin” vb. yetkili kullanıcılarla bağlanılmalıdır. Root veya admin şifresi, tanımlı kişi/kişilerde olmalıdır.
18) Bağlanacak kişilere kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.
19) Bütün kullanıcıların veritabanı üzerinde yaptıkları işlemler kaydedilmelidir.
20) Veritabanı yöneticiliği en az 2 (iki) kullanıcıda olmalıdır.
21) Veritabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişimi engellenmelidir.
22) Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler arayüzden sağlanmalıdır.
23) Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir.
24) Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için “Şifreleme Kurallarına” bakılmalıdır.
25) Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları içinde geçerlidir.

DEĞİŞİM YÖNETİM KURALLARI

1) Bilgi sistemlerinde değişiklik yapmaya yetkili personeller ve yetki seviyeleri dokümante edilmelidir.
2) Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.
3) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve kayıt altına alınmalıdır.
4) Değişiklikler gerçekleştirilmeden önce ilgili yöneticilerin onayı alınmalıdır.
5) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve Bilgi İşlem Müdürlüğünden onay alınmalıdır.
6) Teknoloji değişikliklerinin kurum sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir.

BİLGİ SİSTEMLERİ YEDEKLEME KURALLARI

1) 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.
2) Kurumsal kritik verilerin saklandığı veya sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.
3) Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamanın çalıştığı ve yedeği alınacak dizin, dosya bilgi sistemlerinde değişiklik yapmaya yetkili personel(ler) ve yetki seviyeleri dokümante edilmelidir.
4) Yedekleme konusu bilgi güvenliği bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
5) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
6) Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilmemelidir.
7) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
8) Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenmelidir.
9) Yedekleme işlem için yeterli sayı ve kapasite yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

10) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
11) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dahilinde tamamlanması sağlanmalıdır.
12) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
13) Yedekleme standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek farklı bir fiziksel ortamda bulundurulmalıdır.
14) 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.
15) Son kullanıcılar kendi bilgisayarlarındaki verilerin yedeklenmesinden sorumludurlar.

PERSONEL GÜVENLİĞİ KURALLARI

1) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
2) Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden veya dışından referans sorulması sağlanmalıdır.
3) Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
4) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
5) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
6) İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları kaldırılmalıdır.
7) Kurum bilgi sistemlerinin işletilmesinden sorumlu personelin konuları ile ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılmalı, bütçe ayırılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.
8) Yetkiler "görev ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılmasıyla 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.
9) Çalışanlar, 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.
10) Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında ilgili müdürlüklere bildirilmelidir. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.
11) Son kullanıcılar sistemlere, etki alanları dâhilinde kendilerine verilmiş kendi kullanıcı adı ve şifreleri ile bağlanmalıdır.
12) Her bir son kullanıcının yalnızca bir adet kullanıcı hesabı olmalıdır.
13) Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir.
14) Son kullanıcıların yetkileri, içinde bulundukları grup politikalarına göre belirlenmelidir.
15) Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı 5651 sayılı kanuna uygun olarak kayıt altına alınmalıdır.

16) 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. İhlal durumunda yasal süreç başlatılmalıdır.
17) Son kullanıcılar bilgisayarlarındaki ve sorumlusu oldukları cihazlardaki bilgilerin düzenli olarak yedeklerini almalıdır.
18) Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.
19) Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde harici veri depolama cihazları (bellek ve/veya harici hard disk gibi taşınabilir medya araçları)bırakmamalıdır.
20) Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır.
21) Kullanıcı bilgisayarlarında, güncel antivirüs bulunmalıdır.
22) Bilgi İşlem Müdürlüğü, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulamalıdır.
23) Bilgi İşlem Müdürlüğü, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişikleri merkezi grup politikalarıyla engellemelidir.
24) Kullanıcılarına yeni parolaları bildirilirken sms gibi daha güvenli yöntemler kullanılmalıdır.
25) Temiz masa, temiz ekran ilkesi benimsenmeli ve hayata geçirilmelidir.

BAKIM KURALLARI

1) Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Gerektiğinde anlaşmalar için yıllık bütçe ayrılmalıdır.
2) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
3) Firma teknik destek elemanlarının bakım yaparken “Muratpaşa Belediyesi Bilgi Güvenlik Kuralları ” na uygun davranmaları sağlanmalı ve kontrol edilmelidir.
4) Bilgi sistemleri üzerinde yapılacak değişiklikler ile ilgili olarak “Değişim Yönetimi Kuralı” ve ilişkili standartlar uygulanmalıdır.
5) Bakım yapıldıktan sonra gerekiyorsa tüm sistem dokümantasyonu güncellenmelidir.
6) Sistem bakımlarının ilgili kurallar standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.
7) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda “Muratpaşa Belediyesi Bilgi Güvenlik Kuralları” uyarınca hareket edilmelidir. Güvenlik açıkları Bilgi İşlem Müdürlüğü Siber Olaylara Müdahale Ekibine (some@muratpasa-bld.gov.tr adresine) bildirilmelidir.

YAZILIM GELİŞTİRME KURALLARI

1) Yazılımlarda mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına olan güncellemeler ile etkisiz hale getirmemelidir.
2) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.
3) İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.
4) Yazılım geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
5) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
6) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.

7) Hazırlanan yazılımlar mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.
8) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır. Gerektiğinde TSE onaylı Pentest firmalarına bu testler yaptırılmalıdır.
9) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.
10) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak ilgili yönetim tarafından verilmelidir.
11) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.
12) Yazılımlar sınıflandırılmalı/ etiketlendirilmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

İŞLETİM SİSTEMLERİ GÜVENLİĞİ KURALLARI

1) Kullanıcılar Muratpaşa Belediyesi mevcut envanteri haricindeki donanımları kurum bilgisayarlarında kullanmamalıdır.
2) Kurum bilgisayarlarında (etki alanıda olan veya olmayan) bilgisayarların işletim sistemleri ve diğer yazılımları lisanslı olmalıdır.
3) Kurum serverlarında kullanılan işletim sistemleri (Windows,Linux ve türevleri,macos vb.) kesinlikle lisanslı olmalıdır. Crack işletim sistemleri kullanılmamalıdır.

4) Kurum tablet cihazlarında (android,ios vb.) crack işletim sistemleri kullanılmamalıdır.

5) Server,tablet,Switch,Yedekleme cihazları, bilgisayarların işletim sistemlerinin (donanım arayüz uygulamaları dahil) ve güvenlik sistemlerinin güncelliği takip edilmelidir.

6) Güncel işletim sistemlerine uygun olarak donanım sürücüleri de güncel olmalıdır.

7) Server,Yedekleme cihazları ve önemli ağ cihazlarının kritik logları gözlemlenmelidir.

ÜÇÜNCÜ BÖLÜM

DENETİM VE RAPORLAMA

MADDE 8- Kurum, prensip olarak Yönetici, idari birim mensupları ve son kullanıcılarının şahsi elektronik postalarını, bilgisayarlarında kayıtlı bulunan dosyaları denetlemeyip takip etmeyeceğini taahhüt eder.

Ancak, söz konusu bilişim ve iletişim araçlarının, usul ve amacına aykırı kullanımı hakkında yapılmış ciddi şikâyetlerin veya bunlara ilişkin delillerin ortaya çıkması ve Bilgi İşlem Müdürlüğü tarafından yapılan rutin kontroller sonucunda gözlemlenen tehditler oluşması halinde, **Başkanlık Makamının (TEFTIS)** yazılı onayı ile kullanıcılara sağlanan bilişim araçları ve kanalların izlenmesi hakkı saklıdır.

Belirtilen durumlarda takip hakkının kullanılması **Başkanlık makamının (TEFTIS)** yazılı izin ve talimatıyla mümkündür.

İzleme ve kayıt işleminin yapılmasını öngören Başkanlık makamı yazısında, hakkında takip ve kayıt işlemi yapılacak kişinin bilgileri, işlemin başlangıç ve bitiş zamanı, izleme ve kaydetme işleminin ne şekilde yapılacağı belirtilir.

Bilgi işlem Müdürlüğü **teknik birim** yetkililerinin kendilerine verilen yazılı talimat çerçevesinde yukarıda belirtilen hususlarda yapacağı izleme ve kayıt faaliyetleri gizli tutulur ve suç kapsamında değerlendirilemez.

YETKİSİZ DENETİM

MADDE 9- Kurum Bilgi İşlem Müdürlüğü **teknik birim** çalışanları ve idari birim mensuplarının yukarıda belirtilen usul ve amaçlar haricinde, yetkisiz olarak yapacakları denetim ve kayıt faaliyetleri kesinlikle yasak olup buna aykırı davrananlar hakkında gerekli idari, hukuki ve cezai takibat Başkanlık makamınca yetkili kurumlarla işbirliği içinde yürütülecek ve ilgili mevzuat hükümleri çerçevesinde öngörülen müeyyideler bu kişiler hakkında uygulanacaktır.

USULSÜZ KULLANIMLARIN DENETİMİNDE UYGULANACAK PROSEDÜR

MADDE 10- Bilişim araçlarının usulsüz kullanıldığına ilişkin ciddi şikâyet, Bilgi İşlem Müdürlüğü tarafından yapılan rutin kontroller sonucunda gözlemlenen tehditler ve delillerin ortaya çıkması halinde, Başkanlık makamınca söz konusu olay ve iddiaları araştırmak üzere Teftiş Kurulu Müdürlüğü bünyesinde üç kişiden oluşan bir "**Bilişim Suçları İnceleme Komisyonu**" tayin edilir. Komisyonda Kurum Bilgi İşlem Müdürlüğünü temsilen bir üye ve hakkında inceleme başlatılan kişinin mensup olduğu birimi temsilen bir üye ve Teftiş Kurulu Müdürlüğünden bir üye yer almak zorundadır. Komisyon, kendisine verilen görevi **20 (yirmi) gün** içinde tamamlayarak raporunu Başkanlık makamına sunmakla yükümlüdür. Komisyon, hakkında inceleme başlatılan kişinin savunmasını almadan raporunu düzenleyemez. Düzenlenen raporda, kullanıcının beyanlarına ve ulaşılan diğer delillerin değerlendirilmesi ile ilgili bilgilere, soruşturmanın aşamalarına, komisyon üyelerinin görüş ve tekliflerine ayrı ayrı yer verilir.

GİZLİLİK

MADDE 11- Komisyon raporları gizli olup Başkanlık makamının yazılı talimatı olmaksızın hakkında inceleme yapılan kişi hariç kimseye gösterilemez ve bilgi verilemez. Buna aykırı davranan kişiler hakkında gerekli yasal işlemler ayrıca yapılır. Kurum personelleri yetkileri dahilinde eriştiği kişisel ve kurumsal tüm bilgilerin amacı dışında kullanılmasından, ifşa edilmesinden ilgili yasa ve mevzuatlara karşı sorumludur.

KARARLARIN BİLDİRİLMESİ

MADDE 12- Hakkında inceleme yapılan kişilerle ilgili olarak alınan kararlar kendilerine yazılı olarak tebliğ edilir. Yapılan inceleme sonucunda diğer mevzuat hükümlerine göre suç olduğu kanaatine ulaşılan eylemler hakkında yetkili makamlara Başkanlıkça bildirimde bulunulur.

YÜRÜLÜK

MADDE 13- Bu yönerge yayımı tarihinde yürürlüğe girer.

YÜRÜTME

MADDE 14- Bu yönerge hükümlerini Muratpaşa Belediye Başkanı yürütür.