BODRUM BELEDİYE BAŞKANLIĞI

BİLGİ VE SİSTEM GÜVENLİĞİ POLİTİKALARI YÖNERGESİ

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç

Madde 1 - (1) Bu Yönergenin amacı; Bodrum Belediye Başkanlığı'nın görevi ve konumu nedeniyle sahip olduğu elektronik ortam ve bilgilerinin paylaşımı ve güvenliği konularında bilgi çağı gereklerine uygun olarak tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmektir.

Kapsam

Madde 2 - (1) Bu Yönerge, Bodrum 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.

Hukuki Dayanak

Madde 3 - (1) Bu Yönerge, 06/06/2014 tarih ve 2014/113 sayılı Bodrum Belediye Meclis Kararı ile kabul edilen Müdürlüklerin Kuruluş, Görev ve Çalışma Yönetmeliği, 04/05/2007 tarih ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 6 ncı maddesine dayanılarak hazırlanmıştır.

Tanımlar

Madde 4 - (1) Bu Yönergede geçen;

Ağ Güvenlik Duvarı	:Bodrum Belediye Başkanlığı ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında Başkanlığın karşılaşabileceği sorunları önlemek üzere tasarlanan cihazları,
Ağ Güvenlik Yöneticisi	:Ağ Sistemlerinden Sorumlu Yöneticiyi,
Başkan	:Bodrum Belediye Başkanını,
Başkanlık	:Bodrum Belediye Başkanlığını,
Müdürlük	:Bilgi İşlem Müdürlüğünü,
Güvenlik Yöneticisi	:Bilgi Güvenliği Yöneticisini,
DMZ	:Başkanlık içi ağı ile Başkanlık dışı ağı birbirinden ayıran bölgeyi,
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 Başkanlığı 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	:Bodrum Belediye Başkanlığı 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,
Zincir e-posta	:Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesini,
X.509/LDAP	:Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir internet protokolünü,

İfade eder.

İKİNCİ BÖLÜM

Bilgi Güvenliği Politikaları

E-Posta Politikası

Madde 5 - (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 Belediye Başkanlığında 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 birime 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 birime 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, Belediye 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 Siber Olaylara Müdahale Ekibine (some@bodrum.bel.tr adresine) haber verilmelidir.

f) 6 ay süreyle 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) Müdürlük, e-postaların Başkanlık 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

Madde 6 - (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) Başkanlık 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 8 haneli olmalıdır.

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

ç) Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, ababab...) e)Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)

d) 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 Başkanlığa 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

Madde 7 - İşletim Sistemleri Güvenliği Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

a) Başkanlık son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar verir ve bu işletim sistemine uygun yazılım donanım sistemlerinin kurulumunu temin eder.
b) Başkanlık, işletim sistemlerinin güncel ve güvenli olması için yama yönetimi yapmalıdır.
c) Başkanlık, bilgisayar başındaki kullanıcının doğru kullanıcı olup olmadığını tespit etmek için etki alanı kimlik doğrulamasını sağlamalıdır.

ç) Kullanıcılar Başkanlık mevcut envanteri haricindeki donanımları Başkanlık 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

Madde 8 - 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) Başkanlık, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulamalıdır.

j) Başkanlık, 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.

Antivirus Politikası

Madde 9 - Antivirus Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Başkanlığın 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) Başkanlığın ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.

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

İnternet Erişim ve Kullanım Politikası

Madde 10 - İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Başkanlığın bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır.

b) Başkanlığın politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (terör, pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.

c) Başkanlığın ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.

ç) Başkanlığın ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır. İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.

d) Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.
e) Ancak yetkilendirilmiş kişiler internete çıkarken, Başkanlığın normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla, bütün servisleri kullanma hakkına sahiptir.
f) Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.
g) İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmemelidir. Bu konuda sorumluluk kullanıcıya aittir.
ğ) Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilmelidir.

Sunucu Güvenlik Politikaları

Madde 11 – (1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

a) Başkanlıkta 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 Başkanlık Sistem Yönetimi Birimi 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 Politikasıçerçevesinde, 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 sunucuda da 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.
j) Sunucuların bilgileri yetkilendirilmiş kişi tarafından Tablo (Ek-1)"deki bilgileri kapsayacak şekilde tutulmalı ve güncellenmelidir.

(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.

Ağ Cihazları Güvenlik Politikası

Madde 12 - Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.
b) Acil durumlar haricinde yerel kullanıcı hesapları kullanılmamalıdır. Ağ cihazları kimlik tanımlama için LDAP, RADIUS veya TACACS+ gibi güvenli protokollerden birini kullanmalıdır.
c) Yönlendirici ve anahtarlardaki tam yetkili şifre olan „enable şifresi" kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması Başkanlığın içerisinden yapılmalıdır.
ç) Başkanlığın standart olan SNMPv3 community string"leri kullanılmalıdır. Bu bilgi sadece yetkilendirilmiş kişiler tarafından bilinmelidir.
d) Ağ cihazlarına erişim yetkileri olan yöneticilerin listesi oluşturulmalıdır.
e) Yönlendirici ve anahtarlar Başkanlığın yönetim sisteminde olmalıdır.
f) Yazılım ve firmware güncellemeleri önce test edilmeli, sonra çalışma günlerinin dışında üretim ortamına taşınmalıdır.
g) Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.
ğ) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlenmelidir.
h) Her bir yönlendirici ve anahtar "BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, bu politikaya uyulmamasının disiplin hukuku ve ceza hukuku açısından yaptırımı olabilir ." uyarı yazısına sahip olmalıdır. Yönlendiriciye erişen tüm kullanıcıları uyarmalıdır. ı)Cihazlara erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

Ağ Yönetim Politikası

Madde 13 - 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. Başkanlık 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, Başkanlığın güvenlik politika ve standartlarıyla uyumlu olmalıdır.
ı) Sistem tasarımı ve geliştirilmesi yapılırken Başkanlık 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.

Uzaktan Erişim Politikası

Madde 14 - Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Internet üzerinden Başkanlığın 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) Başkanlık çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
ç) Başkanlığın 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) Başkanlık ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeleri yapılmış olmalıdır.
f) Başkanlıktan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

Kablosuz İletişim Politikası

Madde 15 – (1) Başkanlığın bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.

(2) Bütün kablosuz erişim cihazları Bilgi İşlem Dairesi Başkanlığı 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 Başkanlıkla 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, Başkanlık kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Başkanlık 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 Başkanlığın 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.

Bilgi Sistemleri Genel Kullanım Politikası

Madde 16 - (1) Bilgi sistemlerine sahip olma ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir.

a) Başkanlığın güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Başkanlığın bünyesinde oluşturulan tüm veriler Başkanlığın mülkiyetindedir.
b) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmamalıdır. Bu konuda ilgili politikalar dikkate alınmalıdır.
c) Başkanlık, ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
ç) Başkanlık bilgisayarları etki alanına dahil edilmelidir.
d) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.
e) Başkanlıkta Bilgi İşlem Dairesinin bilgisi ve onayı olmadan Başkanlık Ağ sisteminde (web hosting, e- posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.
f) Birimlerde 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 Başkanlık"a da haber verilmelidir.
b) Bütün cep telefonu, PDA (Personal Digital Assistant) vb cihazlar Başkanlığın 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. Türkiye Cumhuriyeti Bodrum Belediye Başkanlığı 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.

Donanım ve Yazılım Envanteri Oluşturma Politikası

Madde 17 - (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.Başkanlık, ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
c) Envanter bilgileri sık sık kontrol edilmelidir. Bu şekilde bilgi eksikliğinin yol açacağı kayıp ve maliyetlere engel olunmalıdır.

Kriz / Acil Durum Politikası

Madde 18 - Acil Durum politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve yazılı hale getirilmelidir.
b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Problem durumlarında sistem kesintisiz veya makul kesinti süresi içerisinde felaket ve/veya iş sürekliği merkezi üzerinden çalıştırılabilmelidir.
c) 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.
ç) Acil durumlarda Başkanlık içi işbirliği gereksinimleri tanımlanmalıdır.
d) Acil durumlarda sistem kayıtları incelenmek üzere saklanmalıdır.
e) Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır. Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
f) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
g) Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
ğ) Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

Fiziksel Güvenlik Politikası

Madde 19 - Fiziksel Güvenlik ile ilgili kurallar aşağıda belirtilmiştir.

a) Başkanlığın binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.
b) Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
c) Başkanlık dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili personel gözetiminde gerçekleştirilmelidir.
ç) Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılmalı ve izlenmelidir.
d) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
e) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.

f) Kritik sistemler özel sistem odalarında tutulmalıdır.
g) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalı ve iklimlendirilmesi sağlanmalıdır.
ğ) Fotokopi, yazıcı vs. türü cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.
h) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

Kimlik Doğrulama ve Yetkilendirme Politikası

Madde 20 - Kimlik Doğrulama ve Yetkilendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Başkanlık sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecek ve yazılı hale getirilecektir.
b) Başkanlık sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve yazılı hale getirilecektir.
c) Başkanlık bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, yazılı hale getirilmeli ve denetim altında tutulmalıdır.
ç) 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.
d) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
e) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız erişim istekleri/girişimleri incelenmelidir.
f) Kullanıcılara erişim hakları yazılı olarak beyan edilmelidir.
g) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
ğ) 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.

Veritabanı Güvenlik Politikası

Madde 21 - 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 Başkanlık 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 rlogin vb. şekilde erişememelidir.
o) Veritabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak Başkanlığın kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfın açılması durumunda firma yetkilileri de bilgilendirilmelidir.
ö) Arayüzden gelen kullanıcılar bir tabloda saklanmalı, bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.
p) Veritabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılmalıdır. Root veya admin şifresi tanımlı kişi/kişilerde olmalıdır.
r) Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.
s) Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.
ş) Veritabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.
t) Veritabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
u) Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmelidir.
ü) Veritabanı sunucularına ancak yetkili kullanıcılar erişmelidir.
v) Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler arayüzden sağlanmalıdır.(örnek; Kullanıcılar tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmamalıdır)
y) Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için)
z) Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için Şifreleme Politikasına bakılmalıdır.
aa)Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

Değişim Yönetim Politikası

Madde 22 - Değişim Yönetim Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri yazılı hale getirilmelidir.
b) Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.
c) İş kritik bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek sistem ve uygulamalar ilgili birim(ler) tarafından belirlenmeli ve yazılı hale getirilmelidir.
ç) İş kritik değişiklikler gerçekleştirilmeden önce ilgili birim yöneticisi ve ilgili diğer yöneticilerin onayı alınmalıdır.
d) Yapılacak değişiklikler öncelikle mümkünse bir test ortamında denenmelidir.
e) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.
f) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı, geri dönüş planları test edilmeli ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
g) Başkanlık adına lisanslanmış programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.
ğ) Teknoloji değişikliklerinin Başkanlığın sistemlerine etkileri belirli aralıklarla gözden geçirilmeli ve yazılı hale getirilmelidir.

Bilgi Sistemleri Yedekleme Politikası

Madde 23 - 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.
ç) Taşınabilir ortamlar (manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır.
d) 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.
e) Kurumsal kritik verilerin saklandığı veya sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak yazılı hale getirilmelidir.
f) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
g) Yedeklenecek bilgiler değişiklik gösterebileceğinden ilgili birimlerde yedeklenecek veriler periyodik olarak gözden geçirilmeli ve güncellenmelidir.
ğ) Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.
h) Yedekleme ortamlarının ve yedeklenmiş verinin düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
ı) Geri yükleme işlemlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dâhilinde tamamlanması gerekmektedir.
i) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
j) Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek bir ortamda bulundurulmalıdır.
k) Son kullanıcılar kendi bilgisayarlarındaki verilerin yedeklenmesinden sorumludurlar.

Personel Güvenliği Politikası

Madde 24 - 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) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
e) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
f) İş tanımı değişen veya Başkanlıktan ayrılan kullanıcıların erişim hakları kaldırılmalıdır.
g) Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
ğ) Başkanlık 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.
h) 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.

ı) 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.

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

j) 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.

Bakım Politikası

Madde 25 - Bakım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

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

b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.

c) Firma teknik destek elemanlarının bakım yaparken “Bodrum Belediye Başkanlığı Bilgi Güvenliği Politikaları‟na uygun davranmaları sağlanmalı ve kontrol edilmelidir.

ç) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak “Değişim Yönetimi Politikası” ve ilişkili standartlar uygulanmalıdır.

d) Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.

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

f) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda “Bodrum Belediye Başkanlığı Bilgi Güvenlik Politikaları” uyarınca hareket edilmelidir. Güvenlik açıkları Başkanlık Siber Olaylara Müdahale Ekibine (some@aile.gov.tr adresine) bildirilmelidir.

g) Başkanlık içinde firmalar tarafından bakımı ve onarımı yapılan sistemlerindeki bakım işlemi yetkili bir çalışanın gözetiminde yapılmalı ve sistemden bilgi alınmasına engel olunmalıdır.

ğ) Depolama ortamının (örn. sabit disk) bakım, onarım gibi amaçlarla Başkanlık dışına çıkarıldığı durumlar kayıt altına alınmalı ve firma yetkilisi tarafından imzalanmalıdır. Gerekli durumlarda firma ile gizlilik sözleşmesi imzalanmalıdır.

Yazılım Geliştirme Politikası

Madde 26 - Yazılım Geliştirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Başkanlıkta kullanılacak bütün yazılımlar güvenli yazılım geliştirme konusunda dünyada kabul görmüş standartlara ve kurallara uygun olarak, güncel tehditlere karşı gerekli tedbirlerin alındığı şekilde geliştirilmelidir.

b) Yazılım planlama aşamasında güvenlik ihtiyaçları planlanmalıdır.

c) Yazılım Başkanlık Bilgi Güvenliği Politikalarına uygun olarak geliştirilmeli, yetkisiz kişilerin müdahale etmesi şifreleme işlemleri ile engellenmelidir.

ç) Yazılım geliştirme aşamasında gerekli siber güvenlik önlemleri göz önünde bulundurulmalıdır.

d) Yazılım test ve kabul aşamasında xss, injection, broken autentication and session management, csrf… gibi kritik güvenlik saldırılarına karşı testler gerçekleştirilmelidir.

e) Yazılım kodları, sadece geliştirme ekibinin kişisel bilgisayarlarında depolanmamalı, dışarıdan erişime kapalı olan bir sunucuda da saklanmalıdır.

f) Yazılım geliştirme, test ve uygulama ortamları ayrılmalı, her biri için özel olarak tahsis edilmiş ayrı sistemler kullanılmalıdır.

g) Yazılım geliştirme çalışmalarında tasarımcı ve yazılımcı olarak görev alan çalışan ve üçüncü taraf

personeli, yazılımların çalışabilir sürümlerini canlı ortama yükleyememelidir. Yazılım geliştirme ve canlı sistemlerin yönetimi için görev ayrımı ilkesi uygulanmalıdır.

ğ) Yazılım geliştirme süreçleri uluslararası kabul görmüş proje yönetim mantığına uygun şekilde yazılı hale getirilmelidir. (Yazılımın veri akışı ve işleme özelliklerini içeren tasarım belgesi, vb.)

Belgelendirme Politikası

Madde 27 - Belgelendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.
b) İş akışları uygun şekilde belgelenmelidir.
c) Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.
ç) Girdi türleri ve girdi form örnekleri belgelenmelidir.
d) Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.
e) Çıktı form örnekleri ve çıktıların kimlere dağıtılacağı belgelenmelidir.
f) Programların nasıl test edildiği ve test sonuçları belgelenmelidir.
g) Bütün program değişikliklerinin detayları belgelenmelidir.

ÜÇÜNCÜ BÖLÜM

Çeşitli Hükümler

Sorumluluk

Madde 27 - Belgelendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

Yürürlük

Madde 29 - Bu Yönerge Bodrum Belediye Başkanının onayı ile yürürlüğe girer.

Yürütme

Madde 30 - Bu Yönerge hükümlerini Bodrum Belediye Başkanı yürütür.

OLUR

…. /…. /2017

Mehmet KOCADON
Belediye Başkanı

Tablo (EK-1)

Sunucu Adı	……. bodrum.bel.tr
IP Adresi	
Mac Adresi (Ethernet 1) Mac Adresi (Ethernet 1)	
Projenin Amacı	
Sunucunun Bulunduğu Birim Adı (Fiziksel Konumu)	
Sorumlular (Yönetici Kullanıcıların Ad ve Soyadları)	
Ulaşılabilecek Telefon ve E-Posta Adresi	
Genel Donanım Özellikleri (Marka, Model, CPU, Ram, Hdd)	
İşletim Sistemi	
Kullanıcı Kitlesinin Kimlerden Oluştuğu	
Yerel Kullanıcı Sayısı	
Tahmini Kurum Dışı Kullanıcı Sayısı	
Sunucu Üzerinde Bulunan Güvenlik Yazılımları	
Bünyesinde Güvenlik Uygulamalarından Yararlanılmak İsteniliyorsa Erişime Açık Tutulması İstenen Servis Adları ve Port Numaraları	
Ek Açıklamalar	