ÖZET

Bilgi Güvenliği Yönetim Sistemi ve Kişisel Veri Yönetim Sistemi politikalarının amacı Tuzla Belediyesi personelinin, sistemlerinin, kişisel verilerin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik bakımından yapılması, uyulması gereken iş kurallarını hedeflemek ve bu hedefler kapsamında iş sürekliliğini sağlamaktır.

Kurumun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum bilerek veya bilmeyerek yapılan yasadışı veya zararlı eylemlerine karşı çalışanların ve kurumun haklarını korumaya adamıştır. Bilişim ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik bütün çalışanların içerisine dâhil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

Bilgi güvenliği ve gizliliği politikalarının, gözden geçirilmesi ve güncellenmesinden BGYS Yönetim Temsilcisi ve BGYS Ekibi sorumludur. Tuzla Belediyesi yönetimi Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar. Bu politikalara uyulmasından iç ve dış tüm ilgililer sorumludur.

Yaptırım

Bu politikalara uygun olarak hareket etmeyen tüm personel hakkında İnsan Kaynakları Müdürlüğü'nün disiplin süreçlerine göre işlem yapılır.

POLİTİKA LİSTESİ

- ✓ P.01 BİLGİ GÜVENLİĞİ GENEL POLİTİKASI
- ✓ P.02 İNTERNET ERİŞİM POLİTİKASI
- ✓ P.03 E-POSTA POLİTİKASI
- ✓ P.04 ANTİ-VİRÜS POLİTİKASI
- ✓ P.05 ŞİFRE POLİTİKASI
- ✓ P.06 FİZİKSEL GÜVENLİK POLİTİKASI
- ✓ P.07 SUNUCU GÜVENLİK POLİTİKASI
- ✓ P.08 AĞ YÖNETİMİ POLİTİKASI
- ✓ P.09 TEHDİT İSTİHBARATI POLİTİKASI
- ✓ P.10 UZAK BAĞLANTI VPN POLİTİKASI
- ✓ P.11 BULUT YÖNETİM POLİTİKASI
- ✓ P.12 TEDARİKÇİ VE ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI
- ✓ P.13 KABUL EDİLEBİLİR KULLANIM POLİTİKASI
- ✓ P.14 TEMİZ MASA TEMİZ EKRAN POLİTİKASI
- ✓ P.15 MOBİL VE TAŞINABİLİR CİHAZ POLİTİKASI
- ✓ P.16 VERİTABANI GÜVENLİK POLİTİKASI
- ✓ P.17 DEĞİŞİM YÖNETİMİ POLİTİKASI
- ✓ P.18 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI
- ✓ P.19 KONFİGÜRASYON YÖNETİMİ POLİTAKASI
- ✓ P.20 KRİPTOGRAFİK KONTROLLER POLİTİKASI
- ✓ P.21 ZİYARETÇİ KABUL POLİTİKASI
- ✓ P.22 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI
- ✓ P.23 VERİ SIZINTISI ÖNLEME POLİTİKASI
- ✓ P.24 GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI
- ✓ P.25 ERİŞİM KONTROL POLİTİKASI

- ✓ P.26 KİŞİSEL VERİ GÜVENLİK POLİTİKASI
- ✓ P.27 İMHA POLİTİKASI
- ✓ P.28 LOG YÖNETİM POLİTİKASI

P.01 BİLGİ GÜVENLİĞİ GENEL POLİTİKASI

Tuzla Belediyesi, ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve ISO 27701:2019 Kişisel Veri Yönetim Sistemi Standardı doğrultusunda;

a) Kendisi ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişim sağlamayı,

b) Veri Sorumlusu ve Veri İşleyen sıfatıyla kişisel bilgi ve kurumsal bilgilerin gizliliği, bütünlüğü ve erişilebilirliğini korumayı,

c) Kendisinin ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi,

d) Kurumun güvenilirliğini ve marka imajını korumayı,

e) Bilgi güvenliği ve gizliliği ile ilgili ihlal yaşanması durumunda gerek görülen yaptırımları uygulamayı,

f) Tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, ilgili mevzuat ve standart gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği ve gizliliği gereksinimleri sağlamayı,

g) İş/Hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmayı ve işin sürekliliği ve sürdürülebilirliğini sağlamayı,

h) Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi,

i) Bilgi güvenliği ve gizliliği kapsamında farkındalığı arttırmak amacıyla yetkinlikleri geliştirecek eğitimleri sağlamayı

Taahhüt eder.

P.02 İNTERNET ERİŞİM POLİTİKASI

Amaç

Bu politika; kurum içinde güvenli internet erişimi için sahip olması gereken standartları belirlemeyi amaçlamaktadır. İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.

Kapsam

Bu politika kurum internetini kullanan tüm çalışanları kapsamaktadır.

Sorumluluk

Bu dokümanın hazırlanmasından, güncellenmesinden BGYS Yönetim Temsilcisi, gözden geçirilmesi ve onaylanmasından Destek Hizmetleri Müdürü sorumludur. Dokümanda belirtilen hususları bilmek, uygulamak ve korunmasını sağlamaktan bölüm yöneticileri ve tüm çalışanlar sorumludur.

Politika

a) Kurum bilgisayarları içerik denetimi yapan bir uygulama üzerinden internete çıkacaktır. Kurum kültürüne ve yasalara uygun olmayan siteler yasaklıdır. Ancak üst yönetimin yazılı izni ile yetkilendirilmiş kurum personeline internete çıkarken gerekli servisleri kullanma hakkı tanımlanmıştır. (FTP, sosyal medya)

b) 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az iki yıl arşivlenmektedir.

c) Güvenlik duvarı (Firewall) üzerinde web filtreleme özelliği uygulanmaktadır, bu nedenle tüm çalışanlar iş yerlerinde yalnızca izin verilen ve güvenli internet sitelerine erişim sağlamalıdır. Bilgisayarlar üzerinden yasalara aykırı internet sitelerine girmek ve dosya (film, müzik, program vb.) indirmek yasaktır.

d) Tunnel platformları, proxy ve DNS değişiklikleri yapılarak internete bağlanılması yasaktır.

e) Başkalarının fikri haklarını ihlal edici (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.

f) Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa İnsan Kaynakları Müdürlüğü ‘nün disiplin süreçlerini uygulayabilir veya yasa uygulayıcısı ile işbirliği yapabilir.

g) İnternet üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ile kuruma ve kurumun çalışanlarına, bunların aile fertlerine veya Türkiye Cumhuriyeti devletine, ulusuna, yasama, yürütme ve yargı organlarına, askeri ve emniyet teşkilatına, vatandaşlarına yönelik iftira, karalama mahiyetinde mesajlar yayınlamak ve paylaşmak yasaktır.

h) Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek veya zarar verebilecek online olarak yayın yapan televizyon, radyo, film, oyun vb. içerikli yayınların kullanılması yasaktır.

i) Kurum e-posta adresini ile internet üzerinde forum, alışveriş vb. sitelere üye olunması yasaktır.

j) Kurum hesaplarına ait kullanıcı adı ve şifrenizin internet üzerinden paylaşılması yasaktır.

k) Kurum içerisinde kullanılan kullanıcı adı ve şifreleri ile sosyal hayatta kullanılan kullanıcı adı ve şifrelerinin aynı olmamalıdır.

l) İnternet üzerinden yaptığınız kişisel işlemlerinizde (banka, alışveriş, mail vb.) oluşacak olumsuzluklardan kurumumuz sorumlu değildir. Ayrıca, kurum veya kişisel hesabınızı ele geçiren kişi veya kişiler sizin adınıza suç işleyebilir, bu işlemden mesul olabilirsiniz.

m) İnternette gezinirken reklam veya bilgi çalmak amaçlı (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.

n) Üçüncü şahısların kurum internetini Tuzla Bld-Misafir ağından gerçekleşmektedir.

o) Kurum personeli internete girmek için kendisine verilen kurum kimliği ve şifresini başkalarıyla paylaşması yasaktır.

p) Kurum network ağına kurum dışı cihazların takılması yasaktır.

P.03 E-POSTA POLİTİKASI

Amaç

Bu politika; Tuzla Belediyesi e-posta altyapısına yönelik kuralları ortaya koymaktır. Kurumda oluşturulan e-postalar resmi bir kimlik taşımaktadırlar. E-posta Tuzla Belediyesi 'nin en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır. Bunun yanı sıra e-posta basitliği ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır.

Kapsam

Bu politika; kurum e-postasını kullanan tüm çalışanları kapsamaktadır.

Politika

a) Tuzla Belediyesi çalışanların kurum e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar Tuzla Belediyesi bilgi varlığıdır. Bu yüzden yetkili kişiler gerekli durumlarda önceden haber vermeksizin e-posta mesajlarını denetleyebilir, yasal merciler ile paylaşabilir.

b) Personel e-posta adresi ismin baş harfi "." soyisim olacak şeklinde açılmaktadır. Örnek: Ali Çelik isimli personel için; a.celik@tuzla.bel.tr olacak şekilde mail hesabı açılır. Benzer isim olması durumunda e-posta belirleme talimatına göre kurulum işlemi gerçekleştirilir. Mükerrer.

c) Tuzla Belediyesi kurumsal e-posta hesapları kişisel amaçlar için kullanılmamalıdır.

d) Kişisel kullanım için internetteki sitelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

e) Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine veya Bilgi Güvenliği Ekibine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.

f) Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

g) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen Bilgi Güvenliği Ekibine haber verilmeli, posta kutusundan silinmeli ve kesinlikle başkalarına iletilmemeli. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

h) Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal Bilgi Güvenliği Ekibine haber verilmeli, posta kutusundan silinmeli ve kesinlikle başkalarına iletilmemeli.

i) Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

j) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

k) Kurum çalışanları, kurumsal e-postaların herhangi bir kişi tarafından okunmamasını sağlamakla yükümlüdür.

l) Çok gizli ya da kişisel veri barındıran dosyaların e-posta ile gönderilmesi durumunda, ilgili dosyalar şifrelenmelidir. Şifre farklı metodlar (sms, fotoğraf, sözlü beyan vb.) ile e-posta sahibine iletilmelidir.

P.04 ANTİ-VİRÜS POLİTİKASI

Amaç

Bu politika; Tuzla Belediyesi ’ndeki bilgisayar ve sunucuların zararlı yazılımlardan korunmasını amaçlamaktadır.

Kapsam

Bu politika Tuzla Belediyesi ’ndeki bilgisayarları ve sunucuları kapsamaktadır.

Politika

a) Kurumun bütün bilgisayarları ve sunucuları anti-virüs yazılımına sahip olmalıdır.

b) Düzenli aralıklar ile anti-virüs yazılımı otomatik veya manuel olarak güncellenecektir.

c) Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmamalıdır.

d) Hiç bir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramaz veya durduramaz.

e) Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta ve ekleri virüs içerebilir. Kesinlikle açılmamalıdır. Bu tür özelliklere sahip bir mesaj alındığında hemen Bilgi İşlem Şefliğine veya Bilgi Güvenliği Yönetim Temsilcisine haber verilmesi ve yetkili kişiler müdahale edene kadar mesajın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.

f) Bilinmeyen ve şüpheli kaynaklardan indirilen dosyaların içerisinde virüs olabilir. Bu tür kaynaklardan dosya indirilmesi yasaktır.

g) Bilgisayarlarda kullanacağınız CD, USB gibi depolama aygıtlarını virüs taraması yapmadan kullanmayın.

h) Kurum dışı CD, USB vb. materyaller kurum bilgisayarlarına takılmamalıdır. Oluşabilecek her türlü olumsuzluklardan personel sorumludur.

i) Kurum ağına anti-virüsü güncel olmayan bilgisayarlar dâhil edilmemelidir.

j) Haftalık planlanan antivirüs taramaları esnasında bilgisayarlar kapatılmamalıdır.

P.05 ŞİFRE POLİTİKASI

Amaç

Bu politika; güçlü bir şifreleme oluşturulması ve şifrelerin güvenliğinin sağlanmasını amaçlamaktadır.

Kapsam

Tuzla Belediyesi 'ndeki bilgisayarları ve sunucuları kullanan bütün kullanıcı hesaplarını kapsamaktadır.

Politika

a) Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Şifreler kompleks olmalıdır. Kolay tahmin edilen (memleket, çocuk, doğum tarihi, ardışık rakam ve harfler, İstanbul, Ankara, 1qaz2wsx, qwerty vb.) şifreler kullanılmamalıdır.

b) Kurum içerisinde kullanılan genel kullanıcı bilgisayarları şifreleri 60 günde bir değiştirilmesi zorunlu kılınmıştır. Diğer kullanıcı profilleri şifre içerikleri Şifre Belirleme Talimatı 'na göre yapılmalıdır.

c) Oluşturulacak şifre son 5 şifre ile aynı olamaz.

d) Oluşturulacak şifre içerisinde Türkçe karakter bulunmamalıdır.

e) Bilgisayar kullanıcı hesaplarının şifreleri en az 8 karakter olmalıdır. Kompleks şifre içeriğinde; Büyük harf, Küçük harf, Rakam, Karakter seçeneklerinden en az 3 tanesinin olması gerekmektedir.

f) Kullanıcılar bilgisayar başından kalktığı zaman mutlaka oturumlarını kilitlemelidirler(Windows + L) Genel kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 10 dakika içerisinde şifreli ekran korumasına girecektir.

g) Değişen şifrelere tekrar müdahale etmek için en az 1 gün geçmesi gerekmektedir.

h) Hatalı şifrelerin sıklıkla denenmesi sistemin en az 20 dakika kilitlenmesine sebep olmaktadır. Şifre unutulması durumunda Destek Hizmetleri Müdürlüğü Bilgi İşlem Şefliği yetkilisi ile iletişime geçilmelidir.

i) Kurumsal hesaplarınıza ait şifrelerinizin e-posta iletilerine veya herhangi bir elektronik forma yazılması yasaktır. Kurumsal şifreler, kişisel amaçlar için oluşturulan şifrelerden farklı olmalıdır

j) Şifrenizi aile bireyleri dâhil kimseyle paylaşmayın, kâğıtlara ya da elektronik ortamlara yazmayın.

k) Bilgi İşlem Şefliği tarafından size oluşturulan yeni şifreleri hemen değiştirmeniz gerekmektedir.

l) Bir kullanıcı hesabı birden çok kişi tarafından kullanılmamalıdır.

m) Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

n) Kişisel Verilerin Korunması Kanunu 'na istinaden aktif kurum personelinin bizzat kendi talebi olmaksızın şifresi sıfırlanamaz veya değiştirilemez.

P.06 FİZİKSEL GÜVENLİK POLİTİKASI

Amaç

Bu politika; kurum personeli ve kritik kurumsal bilgilerin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve kurum binalarına yetkisiz girişlerin önlenmesini amaçlamaktadır.

Kapsam

Kurum binalarında yer alan bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını kapsamaktadır.

Politika

a) Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.

b) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.

c) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin düzenli aralıklar ile kontrol edilmelidir.

d) Ofis girişleri, sistem odası, arşiv ve koridorlar güvenlik açısından 7/24 kamera ile sürekli izlenmektedir ve kayıt altına alınmalıdır.

e) Güvenlik personelleri bina çevresinde ve içerisinde 7/24 fiziksel izleme yapmaktadır.

f) Kritik sistemler özel sistem odalarında tutulmalıdır.

g) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.

h) Açık ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.

i) Bireysel kargo alınmamaktadır. Kurumsal kargolar X-Ray cihazından geçirilip Yazı İşleri Müdürlüğü‘ne teslim edilir.

j) Hasar / hırsızlık gibi oluşabilecek risklere karşı güvenlik sağlanmalıdır.

k) Ekipmanların kullanımı zimmetlenen kişiye aittir, bu ekipmanların güvenliğini sağlanması kişinin sorumluluğundadır.

l) Kayıt, sözleşme, evrak vb. kişisel veri barındıran dokümanlar KVKK ya da diğer mevzuatlardan kaynaklı oluşabilecek sorunlara karşı güvenli ortam ya da önlemleri alınmış arşivlerde saklanmalıdır. İlgili dokümanların saklanması sırasında KVKK kapsamında beyan edilen saklama süreleri dikkate alınmalıdır.

P.07 SUNUCU GÜVENLİK POLİTİKASI

Amaç

Bu politika; kurumun sahip olduğu sunucuların temel güvenlik kurallarını oluşturmayı amaçlamaktadır.

Kapsam

Bu politika kurumun sahip olduğu bütün sunucuları kapsamaktadır.

Politika

a) Kurum bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.

b) Bütün sunucular (kurumun sahip olduğu) ilgili envanter yönetim sistemine kayıtlı olmalıdır.

c) Sunucu işletim sistemleri üzerindeki kullanılmayan servisler ve uygulamalar kapatılmalıdır. Port açma talepleri yazılı olarak alınmalı ve alınan talepte portun açık kalma süresi beyan edilmeli.

d) Kullanılmayan sunucular güvenlik ve elektrik tasarrufu açısından kapalı tutulmalıdır.

e) Sunucular üzerinde yapılan işlemlerin log kayıtları en az 15 gün saklanacak şekilde ayarlanmalıdır.

f) İşletim sistemleri, uygulamalar, veri tabanları, ağ donanımları yetkili erişim logları tutulmalıdır.

g) Sunucuların yönetimi için her sunucunun kendi hesabı ile bağlantı yapılmalıdır. Sunuculara dışarıdan yapılan bağlantılar uzak bağlantı politikasının belirlediği kurallara göre yapılmalıdır.

h) Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulunmalıdırlar.

i) Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı denetlenmelidir.

j) Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt altına alınmalıdır. Sistem odası sunucu bakımları refakatçi kontrolünde olmalıdır.

k) Elektrik ve data kabloları sunucu odaları dahil kurum içerisinde kanallardan geçmelidir.

l) Sunucu odalarındaki ekipmanların bakımları düzenli olarak yapılmalı ve bakım kayıtları tutulmalıdır.

m) Kişisel verilerin bulunduğu sunucu ve sistemlere erişim log kayıtları yetkisiz değişiklikleri engelleyecek şekilde saklanmalı ve korunmalıdır.

n) Kişisel veri barındıran sunucuların güvenlik tedbirlerinin azami seviyede alınabilmesi için KVKK Teknik Tedbirler dikkate alınmalıdır.

P.08 AĞ YÖNETİMİ POLİTİKASI

Amaç

Kurumun bilgisayar ağında yer alan bilgilerin, ağ alt yapısının ve ekipmanların güvenliğini ve sürekliliğini sağlamayı amaçlamaktadır.

Kapsam

Tuzla Belediyesi bünyesindeki ağ altyapısı, ekipman ve kullanıcıları kapsamaktadır.

Politika

a) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedekli ekipman bulundurulmalı veya bakım anlaşmaları yapılmalıdır.

b) Ağ ekipmanları sadece yetkilendirilmiş kişiler tarafından erişilebilir ve yönetilebilir olmalıdır. Yetkisiz erişime karşı korunmalıdır.

c) Kurum ağına sadece kurum bilgisayarları bağlanmalıdır. Kurum dışında bir bilgisayar bağlanacak ise yetkili kişinin izni ve gözetiminde bağlanmalıdır.

d) Kurum internet ağına misafirler alınmamalı, misafir ağı kurum ağından bağımsız tasarlanmalıdır.

e) Kamera, IP Santral, Kablosuz ağ ve kullanıcı ağları birbirinden ayrı olmalıdır.

f) Uzaktan bağlantı için kullanılacak portların güvenliği sağlanmalıdır.

g) Ağ cihazları yılda en 1 defa açıklık tarama testlerinden geçirilerek güvenli hale getirilmelidir.

h) Ağ cihazlarının konfigürasyonları her değişiklikten sonra yedeği alınarak üzerinde saklanmalıdır.

i) Ağ trafiği düzenli olarak izlenmeli ve anormal davranışlar tespit edildiğinde bilgi güvenliği olay ve ihlal prosedürü kuralları işletilmelidir.

P.09 TEHDİT İSTİHBARATI POLİTİKASI

Amaç

Bu politika; olası tehlikeleri belirleyerek bu tehlikelere karşı önlem almak ve güvenliği sağlamayı amaçlamaktadır.

Kapsam

Tuzla Belediyesi iç ve dış tehditlerine karşı alınan önlemleri içerir.

Politika

a) Tehdit istihbarat çalışmalarında aşağıda belirtilen ilgili ya da uygulamalardan destek alınır;

İlgili Taraf/Uygulama	Açıklama	İletişim Yöntemi	İletişim Detayı
BTK/USOM	Tuzla Belediyesine özel zafiyet bildirimleri	Resmi yazı	Özel zafiyet bildirimleri gizli evrak olarak gelmektedir.
Antivirüs Uygulaması	Zararlı yazılımlardan koruma	Mail ve telefon	Güvenlik tedarikçisinden ihtiyaç doğrultusunda destek alınır.
Firewall	Güvenlik duvarı zafiyet bildirimi	Mail ve telefon	Güvenlik tedarikçisinden ihtiyaç doğrultusunda destek alınır.
Mail Güvenliği	Mail tehditlerinin engellenmesi	Mail ve telefon	Güvenlik tedarikçisinden ihtiyaç doğrultusunda destek alınır.

b) Gelen tehdit bildirimleri değerlendirilir. Değerlendirme sonucunda ilgili tehditin Tuzla Belediyesi açısından risk teşkil ettiğinde, sistem ekibi tarafından sıkılaştırma çalışması yapılmaktadır.

c) İstihbarat çalışmalarında Tuzla Belediyesi, tedarikçi ve kamu otoritelerinden gelen bildirimler, duyurular dikkate alınarak süreç yürütülür.

d) Antivirüs uygulamasında EDR özelliğinden yararlanılarak zararlı bildirimler dikkate alınır.

e) Güvenlik duvarından yararlanılarak olası zafiyetler engellenmektedir.

f) Anlaşmalı tedarikçi firmalar periyodik olarak pentest gerçekleştirir. Gelen bildirimler dikkate alınarak ilgili ortamlarda sıkılaştırmalar yapılmaktadır.

g) Zafiyet tarama araçlarındaki filtreleme özelliği kullanılarak şüpheli mailler belirlenir ve silinir.

P.10 UZAK BAĞLANTI VPN POLİTİKASI

Amaç

Bu politika; kuruma dışarıdan yapılacak uzak bağlantının güvenliği sağlamayı amaçlanmaktadır.

Kapsam

Bu politika dışarıdan bağlantı yapacak tüm kurum çalışanlarını ve tedarikçileri kapsamaktadır.

Politika

a) Uzaktan bağlantı sadece SSL VPN ile yapılmaktadır.

b) Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

c) VPN kullanım hakkı verilen kişiler firewall üzerinde listelenmeli ve düzenli olarak kontrol edilmelidir.

d) Uzak bağlantı yapan kurum dışı bilgisayarlar, Antivirüs Politikasına uygun bir şekilde cihazların antivirüs yazılımları kurulu ve güncel olmalıdır.

e) Sadece kurumun onay verdiği kullanıcılar VPN 'i kullanabilir.

f) Kurum personeli dışında üçüncü taraflara verilecek VPN erişimleri için gizlilik anlaşması yapılmış olmalıdır.

g) Personel, uzaktan çalışma gereken durumlarda sistemlere erişim için kendisine tahsis edilen kullanıcı adı ve parola bilgilerini korumakla yükümlüdür. Erişim bilgilerini üçüncü taraf kişi / kurumlar ile paylaşması yasaktır.

P.11 BULUT GÜVENLİĞİ POLİTİKASI

Amaç

Bulut ortamlarında verinin gizliliği, bütünlüğünü ve kullanılabilirliğini sağlayarak bilgi güvenliğini korumayı amaçlamaktadır.

Kapsam

Bu politikanın uygulamasını tüm çalışanlar sorumludur.

Politika

a) Bulut hizmetlerini kullanmadan önce çalışanların, bilgi güvenliği politikasını ve prosedürlerini anlamaları ve uygulamaları gerekmektedir.
b) Tuzla Belediyesi'nin sahibi ve sorumlusu olduğu tüm veriler kişisel bulut ortamlarında bulundurulmamalıdır.
c) Hassas ve gizli bilgileri bulut ortamlarında yüklenmesi gereken durumlarda, şifreleme yapılarak veriler korunmaktadır.
d) Çalışanlar, Tuzla Belediyesi'nin onayladığı bulut platformları harici bir platform kullanılmamalıdır.

P.12 TEDARİKÇİ VE ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

Amaç

Bu politika; Tuzla Belediyesi 'nin bilgi sistemlerine ve bilgi varlıklarına üçüncü taraflar tarafından ulaşılması durumunda güvenliğinin sağlanması amaçlanmaktadır.

Kapsam

Bu politikanın uygulanmasından tüm departmanlar sorumludur.

Politika

a) Tedarikçiler, bakım firmaları veya üçüncü taraflar (müşteriler) bilgi sistemlerimize veya bilgi varlıklarımıza bakım vb. amaç ile geldiklerinde Gizlilik Anlaşması yapılması gerekmektedir.
b) Üçüncü taraflar kurum içerisinde bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.
c) Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerinde veya bilgi varlıkları üzerinde yapacakları çalışmaları Bilgi Güvenliği Yönetim Temsilcisine bildirilmelidir.
d) Tedarikçiler, bakım firmaları veya üçüncü taraflar kurumun bilgi sistemlerine kendilerine verilen yetki kapsamında erişim sağlayabilirler.

e) Tedarikçiler, bakım firmaları veya üçüncü taraflara verilen erişim yetkileri, erişim amaçlarına uygun olarak sadece çalışma alanlarında olacak şekilde kısıtlı verilmeli, logları saklı tutulmalı ve çalışma bittikten sonra verilen yetkiler hemen geri alınmalı.

f) Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerine ve bilgi varlıklarına eriştikleri süre boyunca refakatçisiz bırakılmamalıdır.

g) Üçüncü taraflara kurumun ağına erişim izni verilecek bilgisayarlar için Uzak Bağlantı VPN Politikası uygulanacaktır. Tuzla Belediyesi, tedarikçi, bakım firmaları veya üçüncü taraflara herhangi bir uyarıda bulunmadan ağa olan erişimlerini kesebilir.

h) Tuzla Belediyesi ‘nin sorumlu olduğu kurumsal ve kişisel verilerin güvenliğinin sağlanabilmesi için tedarikçiler ile gizlilik ihtiva eden kişisel veri güvenliğine ilişkin taahhütler imzalatılmalıdır. Taahhütnameyi imzalamayan tedarikçiler ile çalışılmamalı, kişisel ve kurumsal veri paylaşımı yapılmamalıdır.

i) Tedarikçilerin Kişisel Veri Güvenlik Politikası kurallarına uygun hareket etmesi istenmelidir.

j) Kişisel veriler 3.taraf kişi/kurumlara aktarılırken teknik ve idari tedbirleri alınmalıdır. 3. Taraflara kişisel veri aktarımında, kişisel veriler şifreli gönderilmelidir.

k) Kişisel verilerin kullanılmasını gerektiren sebeplerin ortadan kalkması hâlinde verilerin aktarıldığı 3.taraf kişi/kurumlar bilgilendirilmelidir.

l) Tuzla Belediyesi, verilerini işleyen üçüncü taraf firmalar ile yapacağı sözleşmelerde; Tuzla Belediyesi verilerini işleyen firma personellerin işten ayrılması durumunda, veri güvenliği alınmadan zimmetli ürünün başka operasyon yürüten personellere teslim edilemeyeceğine ilişkin hükümler eklenmesine dikkat edilmelidir.

P.13 KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Amaç

Bu politika; personelin sistem, bilgi ve varlıkların gizlilik, bütünlük ve erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarını bildirmeyi amaçlamaktadır.

Kapsam

Bu politika Tuzla Belediyesi bünyesindeki tüm çalışanları kapsamaktadır.

Politika

a) Tuzla Belediyesi 'nin gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Kurumun iş gereksinimi dışında bu bilgilerin kopyalanması ve iletilmesi yasaktır.

b) Tuzla Belediyesi personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş cihazların güvenliğini sağlamakla sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.

c) Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz.

d) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

e) Bilgisayarlara hiçbir surette lisanssız program yüklenmemelidir.

f) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmeli veya yetkili kişiler dışında erişilemeyecek alanlarda saklanmalıdır.

g) Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde (müzik, film vb.) dosya alışverişinde bulunulmamalıdır.

h) Bilgisayarlarda oyun, eğlence vb. uygulamaların çalıştırılması ve kopyalanması yasaktır.

i) Kritik raporların dökümünü alan kullanıcı, rapor içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.

j) Herhangi bir kişi kendine ait olmayan kritik bir rapor bulur ise bu durumu Bilgi Güvenliği Yönetim Temsilcisine bildirmelidir.

k) "Gizli" kâğıt belgeleri kilitli dolaplarda muhafaza edilecektir.

l) Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez, saatler sistem tarafından otomatik olarak yönetilmektedir.

m) Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda hemen Destek Hizmetleri Müdürlüğü Bilgi İşlem Şefliği ile iletişime geçilmeli.

n) Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer kurum bilgileri, yazılım lisansları vb. hakları kesinlikle ihlal edilmemeli.

o) Kurum bilgileri kurum dışından üçüncü şahıslara iletilmemelidir.

p) Tüm personel, kendi alanlarına ait Güvenlik Politikalarına uymak zorundadır.

q) Kurum politika ve prosedürleri, İnsan Kaynakları ve ilgili yöneticiler tarafından Tuzla Belediyesi çalışanlarına, yeni işe başlayanlara ve paydaşlara duyurulacaktır. İlgili Güvenlik Politikalarına uyulacağı personel iş sözleşmesinde yer almalı ve personele imzalatılmalıdır.

r) Kurum bilgisayarlarında kişisel verilerin barındırılması yasaktır. Tuzla Belediyesi kurum ortamında tutulan ve iletilen tüm bilgiler kurumun malıdır ve Tuzla Belediyesi bu bilgileri izleme ve denetleme hakkına sahiptir.

s) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

t) Hiç bir personel izin almadan kendi PC' sinden veya başka bir kaynak kullanarak, Tuzla Belediyesi'nin bilişim ağını tarayamaz, izleyemez veya dinleyemez.

u) Hiç bir personel, kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

v) Sosyal medya erişimi verilen kullanıcılar görevlerinin dışında bu haklarını kullanmaları yasaktır.

w) Sosyal medya üzerinden kurumu rencide edici, karalayıcı paylaşımlar yapılmamalıdır. Kurumun hassas bilgileri sosyal medya üzerinden paylaşılamaz.

x) Kuruma ait yazıcı, fax, fotokopi, tarayıcı vb. donanımları şahsi işlemler için kullanılmamalıdır.

y) Ortak kullanılan cihazların (yazıcı, fax, fotokobi vb.) üzerinde kişisel veri barındıran belgeler bırakılmamalıdır.

z) Kişisel veri barındıran donanımlar kesinlikle parola güvenliği ile korunmalıdır.

aa) 3. Taraf olan alakasız kişiler ile personel, vatandaş, tedarikçi, yönetici kişisel bilgileri paylaşılmamalıdır.

bb) Kurumsal ve kişisel veri barındıran, hatalı çıktı alınan çıktılar müsvedde kağıt olarak kullanılmamalıdır.

P.14 TEMİZ MASA TEMİZ EKRAN POLİTİKASI

Amaç

Bu politika; Çalışanların mesai saatleri içi veya dışında kendilerine görevleri gereği paylaşılmış olan bilgilerin yetkisiz erişimler veya uygunsuz kullanımı sonucunda başına gelebilecek riskleri en aza indirmeyi amaçlar.

Kapsam

Çalışma masaları, ekranlar, basılı dokümanlar, belgeler ve kayıtlar.

Politika

a) Çalışma sonunda kâğıt ortamında ya da elektronik cihazlar üzerinde tutulan "gizli ya da çok gizli" bilgiler güvenlikli ortamlarda (çelik kasa, kilitli dolap ve çekmeceler vb.) saklanacaktır.

b) Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) yetkisiz erişimlere bırakılmayacaktır. Cihazlar üzerinde belge, doküman bırakılmayacaktır.

c) Her türlü ekrandan ulaşılabilen bilgiler, şifreler, anahtarlar ve kodlar, bilginin sunulduğu sistemler, ana makineler (sunucu), PC'ler vb. cihazlar şifresiz kullanılmayacaktır.

d) Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası vb. hassas bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.

e) Her türlü bilgi, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), bilgisayarlar vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

f) Faks ve fotokopi makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır.

g) Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale gelmesinin önüne geçilmelidir.

h) Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.

i) Bilgisayarların masaüstlerindeki klasör ve dosyalar düzenli tutulmalıdır.

j) Gizli olarak tanımlanan (sözleşme, fatura, kişisel veri içeren, şartnameler, veri dokümanları vb.) dokümanlar ve kopyaları, müsvedde olarak kullanılmamalı ve kâğıt öğütücü ile imha edilmelidir. Kâğıt öğütücü olmayan ortamlarsa çıktılar ince ince kıyılmalıdır.

k) Kişisel verilerin çıktıları alınırken ihtiyaç duyulan (ölçülü) kadar çıktı alınmalıdır. Çıktısı alınan veriler Bilgi Sınıfları Planı kapsamında belirtilen saklama, etiketleme vb. hususlar dikkate alınarak işlenmeli ve depolanmalıdır. Bilgi Sınıfları Planına Göre;

- Çok Gizli ve Özel Nitelikli Kişisel Veriler: Kilitli ortamlarda saklanmalı ve ilgili ortam kare sembolü ile etiketlenmelidir.
- Gizli ve Kişisel Veriler: Kilitli ortamlarda saklanmalı ve ilgili ortam üçgen sembolü ile etiketlenmelidir.

- Kurum Özel Veriler: Birime özel dolaplarda saklanmalı ve ilgili ortam daire sembolü ile etiketlenmelidir.
- Halka Açık Veriler: Korumayı gerektirmeyen veriler olup Belediye 'nin görünür alanlarında tutulabilir ve ilgili ortamda sembol kullanılmaz.

P.15 MOBİL VE TAŞINABİLİR CİHAZ POLİTİKASI

Amaç

Bu politika; Tuzla Belediyesi 'ne ait bilgi içeren mobil ve taşınabilir cihazların kullanımı ile ilgili kuralları belirlemeyi amaçlar.

Kapsam

Bu politikanın uygulanmasından mobil ve taşınabilir cihaz kullanan tüm çalışanlar sorumludur.

Politika

a) Kuruluşa ait bilgi içeren taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilmelidir.

b) Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.

c) Etki alanı dâhilindeki bilgisayarlar admin yetkisi sınırlandırılarak yalnızca User yetkilendirmesi ile ilgili kişiye teslim edilmelidir. Etki alanından bağımsız olan bilgisayarların sorumluluğu personele aittir.

d) Mobil telefonlar ve taşınabilir cihazlara yetkisiz erişime karşı şifre tanımlanmalıdır.

e) Kuruluş telefon hatları ve bilgisayarlar üzerinden üçüncü taraf kişilerle borç alacak ilişkisi, tehdit, küfür, kuruluş itibarını zedeleyecek mesajlar ve yasa dışı olan iletişim kurulamaz.

f) Etki alanı dâhilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar departmanlara ait ilgili ortak alana kaydedilmelidir.

g) Mobil telefonlar ve taşınabilir cihazlar aile bireyleri dâhil yetki dışı hiç kimse tarafından kullandırılmamalıdır.

h) Mobil, taşınabilir cihazları, görüntüleme aygıtları (fotoğraf makinası, video kamera) vb. cihazlarda hassas ve gizli bilgileri mümkün olduğunca mobil cihazınızda bulundurulmamalıdır.

i) Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

j) Personele tahsis edilen GSM telefon numaraları ilgili GSM operatörlerine ait kurumsal portala işlenecektir.

k) Çok Gizli ve Özel nitelikli kişisel verilerin kurum dışına taşınması gereken durumlarda ilgili medya kriptolanmalı ya da verinin olduğu dosya şifreli olacak şekilde sıkıştırılarak kurum dışına çıkarılmalıdır. Oluşturulan şifreler kompleks yapıda olmalıdır.

l) Usb aygıtlarında kişisel veri bulunuyorsa, ilgili medyalardaki kişisel verilerin şifrelenmeli ya da disk kriptolanmalı. Kriptolama ya da şifreleme yapılamadığı durumlarda ilgili medya

aygıtları kurum dışına çıkarılmamalıdır. Medya aygıtının kurum dışına çıkarılması gereken durumlarda yönetici onayını almalıdır. Tüm sorumluluk personelin yükümlülüğündedir.

m) İçeriğinde kişisel veri barındıran medya ve bilgisayarları, verileri işleyen Belediye personeli kullanmalı ve taşımalıdır.

P.16 VERİTABANI GÜVENLİK POLİTİKASI

Amaç

Bu Politika; kurumun veri tabanı sistemlerinin, kesintisiz ve güvenli şekilde işletilmesine yönelik standartları belirtmeyi amaçlamaktadır.

Kapsam

Tüm veri tabanı sistemleri, bu politikaların kapsamı altında yer alır.

Politika

a) Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir. Log kayıtlarına, yetkilinin izni olmadan kesinlikle hiçbir şekilde erişim yapılamaz.

b) Veri tabanı sunucusuna, sadece admin hakkına sahip olanlar bağlanır.

c) Veri tabanı bulunan sistemlere erişim yetkileri kayıt altına alınmalı ve bu yetkiler kontrol edilmelidir.

d) Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılır ve uygun yedekleme politikaları oluşturulur. Yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli alınması sağlanır.

e) Bilgilerin saklandığı sistemler, fiziksel güvenliği sağlanmış sistem odalarında tutulur.

f) Veri tabanı sistemlerinde yapılacak bakım onarım, yama ve güncelleme çalışmalarından önce, ilgili birimlere duyuru yapılmalıdır.

g) Veri tabanına acil erişim gerekmesi durumunda aksiyon öncesinde ve sonrasında ilgili birimlere veya personellere bilgilendirme yapılır.

h) Veri tabanı aksiyonlarında destek firmasına talepler yazılı olarak bildirilmelidir.

i) Veri tabanları yedekleme listesine göre düzenli olarak yedeklenmelidir.

j) Veri tabanı bulunan medyalar kurum dışına çıkarılmamalıdır.

k) Veri tabanlarına kurum dışından SSL VPN ile bağlantı yapılmalıdır.

l) Veri tabanlarının bulunduğu medyaların doluluk oranları düzenli olarak kontrol edilmelidir.

m) Veri tabanının yönetildiği uygulamada, ilgili personele ihtiyacı kadar veriyi görecek şekilde yetki verilmelidir. En az yetki prensibi uygulanmalıdır.

P.17 DEĞİŞİM YÖNETİMİ POLİTİKASI

Amaç

Bu Politika; kurumun bilgi sistemlerinde yapılması gereken yazılımsal ve donanımsal değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesini sağlamayı amaçlamaktadır.

Kapsam

Tüm bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

Politika

a) Yazılımsal ve donanımsal değişikliklerin talepleri kayıt altında tutulmalıdır.

b) Bilgi sistemlerinde değişiklik yetkilendirilmiş kişiler tarafından yapılır.

c) Herhangi bir sistemde uzun süreli veya önemli değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve ilgili kişilere bilgi verilmeli.

d) Değişiklikler gerçekleştirilmeden önce kurumun ilgili birimine bilgi verilmelidir.

e) Yapılacak değişiklikten önce değişikliğin yapılacağı sistemlerin yedekleri alınmalıdır.

f) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticilere bilgi verilmelidir.

g) Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.

h) Yapılacak değişiklikler mümkün olduğunca test sunucuları üzerinde gerçekleştirilmelidir, yapılan testlerin başarılı geçmesi halinde canlı sistemde değişiklik gerçekleştirilmelidir.

i) Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler, işlemi yapacak bilgi işlem personeli tarafından yönetime bildirmelidir.

P.18 KONFİGÜRASYON YÖNETİMİ POLİTAKASI

Amaç

Bu politika; bilgisayar sistemlerinin ve yazılım uygulamalarının düzenli, güvenilir ve güncel bir şekilde çalışmasını sağlaması için uygulanmaktadır.

Kapsam

Konfigürasyon yönetiminin kapsamı; bilgisayar sistemlerinin, yazılım uygulamalarının, ağ altyapısının ve diğer teknolojik varlıkların yapılandırılmalarının oluşturulması, belgelenmesi, uygulanması, izlenmesi ve gözden geçirmesini kapsamaktadır.

Politika

a) Konfigürasyon değişiklileri yapılan donanım ya da yazılımın kritikliği dikkate alınmalıdır.

b) Değişikliği yapılan donanım ya da yazılımın, konfigürasyon değişikliği öncesinde ilgili ortamın ya da kuralın yedeği alınmalıdır.

c) Konfigürasyon değişiklikleri öncesinde aşağıdaki konular dikkate alınmalıdır.

Kontrol Noktası	**Kontrol Açıklaması**
Donanım Uyumluluğu	Yedeği alınan konfigürasyon bilgilerinin, ihtiyaç durumunda aynı ürün ve versiyonda başka cihazlara aktarıldığından emin olunulmalıdır.
Etkilenen dokümantasyonun belirlenmesi	Konfigürasyonların değişikliği sonrasında, ilgili mevcut dokümanlar gözden geçirilmeli ve gerekli güncellemeler yapılmalıdır.
Gizlilik taahhütleri	Konfigürasyon değişikliği yapacak olan üçüncü taraflar ile gizlilik taahhütleri oluşturulmalıdır.
Hizmet Sözleşmesi	Konfigürasyon değişikliği yapacak olan üçüncü taraflar ile hizmet sözleşmeleri oluşturulmalıdır.
Hizmet sözleşmesinde SLA şartları	Konfigürasyon değişikliği yapacak olan üçüncü taraf sözleşmelerinde gerek duyulması durumunda SLA süreleri belirlenerek hizmet devamlılığı sağlanmalıdır.
Personel sayısının yeterliliği	Konfigürasyon değişikliğini gerçekleştirecek olan üçüncü taraf kuruluşun norm kadro yeterliliği denetlenmelidir.
Personel yetkinliği	Konfigürasyon değişikliklerini yapacak olan çalışanların konusunda uzman kişilerden oluşmasına dikkat edilmelidir. Yetkinlik sorunu olanlar için eğitim şartı sunulmalıdır.
Yedek Güvenliği	Konfigürasyon yedeklerinin alındığı ortamlara erişimler sınırlandırılmalıdır. Konfigürasyon isimlendirmeleri anlaşılır şekilde olmalıdır.
Yedekleme	Kritik konfigürasyon değişikliği olmasında ya da belirli periyodlarda bir önceki konfigürasyon bilgisinin yedek, backup veya imajı alınmalıdır.
Yetkilerin düzenlenmesi	İlgili donanım ve uygulamaların konfigürasyonlarının yönetildiği arayüzlere erişimler kısıtlanmalıdır.

Zamanlama	Konfigürasyon değişikliklerinin kritik olması durumunda mesai dışı, iş yoğunluğunun az olduğu zaman dilimleri dikkate alınarak değişiklikler yönetilmelidir.
Planlı kesinti	Altyapısal ve sistemsel konfigürasyon değişiklikler esnasında doğabilecek kesintilere karşı ilgili kullanıcılar bilgilendirilmelidir.
Performans	Birbiri ile eşleşen kurallar hem yönetim açısından karmaşıklık hem cihazın işlemci gücünü gereksiz yere kullanacağından dolayı tespit edilip silinmelidir.
Konfigürasyon kurallarının kontrolü	Hit almayan kurallar hem yönetim açısından karmaşıklık hem cihazın işlemci gücünü gereksiz yere kullanacağından dolayı tespit edilip silinmelidir.

P.19 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

Amaç

Bu politika; kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktır.

Kapsam

Tuzla Belediyesi bilgi sistemlerine erişen kurum personeli ile kurum dışı kullanıcılar bu politika kapsamı altındadır.

Politika

d) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.

e) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak.

f) Kurum bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli ve denetim altında tutulmalıdır.

g) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.

h) Kullanıcılar da kurum tarafından kullanımlarına tahsis edilen sistemlerin güvenliğinden sorumludur.

i) Sistemler başarılı ve başarısız erişim logları düzenli olarak tutulmalıdır.

j) Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

k) Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve kayıt alınmalıdır.

l) Kullanıcı hatalarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

m) İşten ayrılan personellerin hesapları kapatılır. Yeni işe başlayan personele, eski personellere ait kullanıcı hesabıyla erişim sağlaması engellenir. Yeni işe başlayan her personel için ayrı hesap oluşturulur.

n) Personellere en az yetki prensibine uygun olarak yetkiler tanımlanır. Personel sadece ihtiyacı kadar kurumsal ve kişisel veriye erişebilir. Personel yetki aşımına teşebbüste bulunamaz.

P.20 KRİPTOGRAFİK KONTROLLER POLİTİKASI

Amaç

Bu Politika; bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunmasıdır.

Kapsam

Bu politika bilgi varlıklarının saklandığı sistemler ve o sistemlere erişimin yapıldığı ağların şifre politikasını kapsamaktadır.

Politika

a) Kurum içerisinde tanımlanan gizli bilgi varlıklar kriptografik şifreleme yöntemleri ile saklanmalıdır. Her personel kendi barındırdığı bilgi varlıklarından güvenliğinden sorumludur.

b) Risk değerlendirmelerine göre yüksek düzeyde koruma gerektiren bilgi varlıklarının korunmasında güçlü şifreleme algoritması kullanılmalıdır.

c) Mobil cihazlardaki verilerin korunmasında güçlü şifre kullanılmalıdır.

d) Mail hesabı kurulu akıllı telefonlarda telefon kilidi kullanılması zorunludur.

e) Tanımlanan şifreler belirli aralıklarla değiştirilmelidir.

f) Active Directory hesap şifreleri kolay tahmin edilmeyen karmaşık şifreler olmalıdır.

g) Tuzla Belediyesi Kablosuz ağ erişimi misafirler için, NVİ üzerinden TC Kimlik doğrulaması ile gelen SMS şifresi ile kullanılmaktadır. Bütün Tuzla Belediyesi personeli kendi Domain hesaplarıyla erişmektedirler.

h) Misafirler için oluşturulan kablosuz erişimleri 12 saat ile kısıtlandırılmıştır. Personel için bu süre 3 gün olarak belirtilmiştir.

i) Özel nitelikli kişisel verilerin kurum dışına taşınması gereken durumlarda ilgili medya kriptolanmalı ya da verinin olduğu dosya şifreli olacak şekilde sıkıştırılarak kurum dışına çıkarılmalıdır. Oluşturulan şifreler kompleks yapıda olmalıdır. Medya aygıtının kurum dışına çıkarılması gereken durumlarda yönetici onayını almalıdır. Tüm sorumluluk personelin yükümlülüğündedir.

j) Özel nitelikli kişisel veriler, kurum içinde sadece sorumlu verilen personel tarafından ulaşılabilir olmalı ve işlenmelidir. Verilerin kurum içinde farklı bir ortamda yer alması durumunda kriptolu ya da şifreli olmalıdır.

k) Veri sahipleri ya da vatandaş tarafından işlem yapılan Tuzla Belediyesi 'ne ait web ara yüzlerinde ve web servislerinde SSL sertifikalı internet siteleri kullanılmalıdır.

l) Tuzla Belediyesi 'ne ait sitelerin SSL sertifika süreleri belirli periyodlarda kontrol edilmelidir.

P.21 VERİ SIZINTISI ÖNLEME POLİTİKASI

Amaç

Kurum içerisindeki hassas bilgilerin yetkisiz erişim, ifşa veya kaybını önleyerek bilgi güvenliğini sağlamak.

Kapsam

Tüm kullanıcılar bu kapsam dahilindedir.

Politika

a) Hassas verilerin işlendiği, depolandığı veya iletilen sistemler, ağlar ve diğer cihazlar veri sızıntısı önleme tedbirlerine tabirdir.

b) Kritik ve hassas veriler, daha yüksek koruma önlemleri alınarak ayrıştırılmalıdır.

c) Hassas verilerin depolandığı ve taşındığı yerlerde şifreleme kullanılmalı, yetkisiz kişilerin şifresiz verilere erişmesi engellenmelidir.

d) Veri sızıntısını önlemek için uygun teknik ve organizasyonel önlemler alınmalıdır.

e) Çalışanlar, veri sızıntısı önleme politika ve prosedürleri konusunda eğitilmeli ve bilinçlendirilmelidir.

f) Veri paylaşımı gerçekleştirildiğinde kişisel bulut platformları kullanılmamalıdır.

P.22 ZİYARETÇİ KABUL POLİTİKASI

Amaç

Bu politika; dışarıdan gelen misafirlerin kabulü, kuruluş içinde dolaşmaları ve kuruluştan uğurlanmaları ile ilgili kuralları belirlemektir.

Kapsam

Bu politikanın uygulanmasından Tuzla Belediyesi 'ndeki tüm yönetici ve çalışanlar sorumludur.

Politika

g) Dışarıdan ziyaret amaçlı gelen kişiler kuruluş girişinde güvenlik tarafından karşılanır ve X-Ray cihazı ile kontrolü sağlanıp kurum içine girişine izin verilir.

h) Çalışma alanlarına erişim bakım onarım ve denetleme firmaları dışında kesinlikte ziyaretçi erişimine kapalıdır.

i) Kurum adı haricinde gelen kargolar kabul edilmez. Kurum adına gelen kargolar X-Ray cihazından geçirilerek Yazı İşleri Müdürlüğü 'ne teslim edilir.

j) Kurum içine gelen ziyaretçiler kamera sistemi ile takip edilmektedir. Ziyaretçilerin yetkisiz girişleri kısıtlanmalıdır.

k) Kritik birimlere yetkisiz ziyaret girişlerini kısıtlamak için fizik güvenlik önlemleri alınmıştır.

l) Kritik verilerin bulunduğu birimlerde çalışan personellerin ziyaretçileri ile görüşmeleri bekleme salonunda yapılmalıdır.

m) Ziyaretçiler internet kullanmak istediklerinde sadece Tuzla Bld - Misafir kablosuz internet ağını kullanabilirler.

n) Bu politikaya uygun olarak çalışmayan tüm personel hakkında İnsan Kaynakları Müdürlüğü 'nün disiplin süreçlerine göre işlem yapılır.

P.23 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI

Amaç

Bu politika; Tuzla Belediyesi 'in bilgi güvenliği olay ihlal süreçlerini belirlenmesidir.

Kapsam

Bu politikanın uygulanmasından tüm personel sorumludur.

Politika

a) Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır. İhlal bildirimleri otomasyon uygulaması üzerinden yapılmalıdır.

b) Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

c) Bilgi güvenliği ihlâli oluşması durumunda, kişilerin tüm gerekli faaliyetleri değerlendirmesi Bilgi Güvenliği Ekibi ile birlikte yapılmalıdır.

d) İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

e) Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği ihlallerini önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine ve Bilgi Güvenliği Ekibine mümkün olan en kısa sürede rapor verilmelidir.

f) Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.

g) İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.

h) Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.

i) Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe, yeni kontrollerin oluşturulması, olayların kök nedenine inilmesi ve yazılı hale getirilmesi gerekmektedir.

j) Kanıt toplama faaliyetinde aşağıdaki süreçler takip edilmelidir;

- Kanıtın niteliği ve tamlığını gösteren içerik.
- İhlale neden olan olayların kanıtları için kamera kayıtları, giriş çıkış kayıtları, sunucu/program ve bilgisayar logları, firewall logları ve internet loglarından faydalanır.
- Olay kanıtlarının korunması yetkili kişilerin dışında erişimi kapatarak veya yedekleme yaparak sağlanır.

k) Bu politikaya uygun olarak çalışmayan tüm personel hakkında cezalar İnsan Kaynakları ve Eğitim Müdürlüğü ‘nün disiplin süreçlerine göre hareket edilir.

l) Kişisel veriler ile ilgili bir ihlal gerçekleşmesi durumunda aynı gün Veri Sorumlusu İrtibat Kişisi ya da Yönetim Temsilcisi bilgilendirilmelidir. İhlal Veri Sorumlusu İrtibat Kişisi tarafından 3 gün içerisinde KVKK ‘ya https://ihlalbildirim.kvkk.gov.tr adresinden bildirilir.

m) Kişisel veri ihlalleri yaşanması durumunda KVKK Yönetim Prosedürü ‘nde belirtilen adımlara göre ihlaller yönetilmelidir.

P.24 GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI

Amaç

Bu politika; Tuzla Belediyesi ’in bilgi güvenliği güvenli yazılım geliştirme süreçlerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesini amaçlamaktadır.

Kapsam

Bu politikanın uygulanmasından tüm personel sorumludur.

Politika

a) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

b) Uygulama yazılımlarının kurum içerisinde mi hazırlanacağı yoksa satın mı alınacağının belirlenmesi, uygun bir şekilde tanımlanmalıdır.

c) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

d) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler, ihtiyaçları karşılamalıdır.

e) Yazılım geliştirme politikalarına uygun olmayan, ulusal ve uluslararası yazılım geliştirme standartları çerçevesinde geliştirilmemiş ve kurum talebi olmaksızın üretilmiş olan yazılımların kurumsal sistemler üzerine entegre edilmesine izin verilmemelidir.

f) Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları ilgili personele e-posta ile bilgilendirmesi yapılır.

g) Yeni alınmış veya revize edilmiş bütün yazılımlar test ortamında kontrol edilmelidir. Herhangi bir sorun görülmesi durumunda üretici firma ile iletişime geçilip çözüm arayışına girilir.

h) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

i) Yazılımlar sınıflandırılmalı/etiketlenmeli ve envanterleri çıkarılarak varlık envanterinde güncellenmelidir.

j) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması engellenmelidir.

k) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

l) Test verilerinde kişisel veri kullanılmamalıdır. Anonimleştirme yöntemleri kullanılarak kişisel veriler kullanılmalıdır.

m) Halka açık ağ ya da hizmetlerin (web sayfaları) https, katmanlı doğrulama, veritabanı güvenliği, DMZ vb. güvenlik önlemlerinin olmaması durumunda kişisel veri girişleri engellenmelidir. Yazılım geliştirmeleri yapılarak gerekli önlemler alındıktan sonra kişisel veri girişleri sağlanmalıdır.

n) Paydaşlar ile yapılan sözleşme ve yasal mevzuat kaynaklı yükümlülükler dikkate alınarak yazılım geliştirme yapılmalıdır.

o) Yazılım geliştirme faaliyetleri için dışarıdan destek alınması durumunda, ilgili taraflar ile yapılan sözleşmeler ve yasal mevzuatlardan kaynaklı sorumluluklar dikkate alınarak destek firması ile yapılan sözleşmelerine ilgili hususlar eklenmelidir. Kişisel ve gizli bilgi güvenliğine ilişkin sözleşme yapılmadan tedarikçi ile veri paylaşımı yapılmamalıdır.

p) Yazılım geliştirme faaliyetlerinde kabul görmüş uluslararası standart ve prensipler referans alınarak çalışmalar yürütülmelidir.

P.25 ERİŞİM KONTROL POLİTİKASI:

Amaç

Bu politika; yetkili kullanıcı erişimini sağlamak ve yetkisiz erişimi önlemek amacıyla oluşturulmuştur.

Kapsam

Tuzla Belediyesi 'nin paydaşlara, çalışanlarına ve tedarikçilerine sunduğu yazılım ve donanım sistemlerinde, yetkili ve yetkisiz kullanıcı erişimleri, yeni kullanıcıların kayıt başlangıçlarından, bilgi sistemlerine ve hizmetlerine erişim gereksinimi artık kalmamış kullanıcıların son kayıttan çıkışlarına kadar olan basamakları içermelidir.

Politika

a) Kurum içerisinde giriş çıkışlar kamera sistemi ile kayıt altına alınmalıdır.

b) Kullanıcı yetkilendirilmeleri birim bazında yapılmalıdır.

c) Kullanıcılar taşınabilir medyaları (CD, USB, vb.) sadece iş amaçlı kullanmalı ve bu medyalar takıldığı zaman antivirüs yazılımı ile taranmalıdır.

d) Aktif dizine bağlanan kullanıcı parolaları Şifre Politikasına uygun tanımlanmalıdır.

e) Erişim gereksinimi artık kalmamış kullanıcılar için İnsan Kaynakları Prosedürüne göre hareket edilir. Sistemden de bu personelin erişim şifresi silinir.

f) Ağ üzerinde aktif dizin kullanıcıları için sürücüler oluşturulmalıdır.

g) Bu sürücüler üzerindeki birimler ve kullanıcılara göre yetkilendirme yapılmalıdır.

h) Yönetim tarafından yetkilendirilen personel haricinde hiç bir personelin dosya silme yetkisi bulunmamalıdır. Silme işlemi sadece ilgili müdürlük tarafından tanımlanan kişiler tarafından yapılmalıdır.

i) ISO Dokümanlarına erişim Kurum içi paylaşım üzerinden personellere sunulmaktadır.

j) Paylaşımlar sistem yöneticisi tarafından belirlenmektedir.

k) ISO formları dizinine tüm kullanıcılar erişebilmekte ancak sadece okuma yetkisine sahiptirler. Kalite Birimi dışında kullanıcıların dosya ve/veya form oluşturma, ekleme, değiştirme yetkisi bulunmamaktadır. Bu şekildeki istekleri var ise İnsan Kaynakları birimine haber verilmelidir.

l) Kurumda mümkün olduğunca SSL ya da benzeri güvenlik protokollerinin kullanılması benimsenmiştir.

m) Kişisel ve özel nitelikli kişisel verilere erişim talepleri, birim yönetici onayından sonra mail ya da otomasyon yazılımı ile Bilgi İşlem Şefliği ‘ne iletilmelidir. Bilgi İşlem Şefliği ‘nin onayına müteakip yetkiler verilmektedir.

n) Çok gizli ve kişisel veri bulunan sistemlere ayrıcalıklı erişim sağlayan personel ve üçüncü taraf kişi / kurumların log kayıtları ya da ekran hareketlerinin görüntüsü alınmalıdır.

P.26 KİŞİSEL VERİ GÜVENLİK POLİTİKASI:

Amaç

Bu politika; kullanıcıların Tuzla Belediyesi ‘nin sorumlusu olduğu kişisel veriler ile ilgili ihlalleri önlemek amacıyla oluşturulmuştur.

Kapsam

Tuzla Belediyesi’nin paydaşlarına, çalışanlarına ve tedarikçilerine ait olan kişisel veri ve ilgili kişisel verilerin bulunduğu ortamları kapsamaktadır.

Politika

a) Kişisel veriler amacı dışında kullanılmamalıdır. Kişisel veri, veri sahibinden işin gereği kadar talep edilmelidir. Elde edilen kişisel veriler bütünlüğü sağlayacak şekilde korunmalıdır.

b) Kişisel veriler kullanım amacı haricinde üçüncü taraflar ile paylaşılmamalıdır.

c) Kişisel ve özel nitelikli kişisel verilere erişim gerektiren durumlarda üst yönetimin onayı yazılı olarak alınmalı ve verilen onayla sınırlı kalmak şartıyla operasyon yürütülmelidir.

d) Kişisel veriler, kurumun onaylamış olduğu imha yöntemleri ile yok edilmelidir. İmhanın üçüncü taraf kişi / kurumlara yaptırılması gereken durumlarda bilgi güvenliği ve gizliliği kapsamında sözleşmeler yapılmalıdır. Kişisel verilerin saklama süreleri en geç 6 ayda bir kontrol edilmelidir.

e) Tuzla Belediyesi'nin sorumlu olduğu kişisel veriler hiçbir hukuki şart, sözleşme ya da yasal dayanak yoksa kurum dışından üçüncü şahıslara iletilmemelidir. Tuzla Belediyesi'nin sorumlu olduğu kişisel veriler (çalışanlar, paydaşlar, tedarikçiler vs.) ilgili kişinin izni olmadan üçüncü taraf kişiler ile paylaşılmamalıdır. Güvenilir kaynaklardan gelen talepler doğrultusunda işin gereği kadar veri paylaşılmalıdır.

f) Kişisel veriler üçüncü taraf kişi / kurumlara aktarılırken teknik ve idari tedbirleri alınmalıdır. Üçüncü taraflara kişisel veri aktarımında, kişisel veriler şifreli gönderilmelidir.

g) Kişisel verilerin kullanılmasını gerektiren sebeplerin ortadan kalkması hâlinde verilerin aktarıldığı üçüncü taraf kişi / kurumlar bilgilendirilmelidir.

h) Özel nitelikli kişisel veri ya da gizli bilgilerin bulunduğu medya aygıtları ya da kâğıt ortamında fiziksel olarak Tuzla Belediyesi dışına çıkması gereken durumlarda üst yönetim ya da Veri Sorumlusu İrtibat Kişisi bilgilendirilir. Kurum dışına çıkan medya aygıtı ya da kâğıt ortam bilgisi Medya Cihazları ve Bilgi Aktarım Formu kullanılarak kayıt altına alınır.

i) Ortak kullanılan cihazların (yazıcı, faks, fotokopi vb.) üzerinde kişisel veri barındıran belgeler bırakılmamalıdır.

j) Temiz Masa Temiz Ekran Politikası kurallarına uyulmalı, kişisel veri bulunduran basılı doküman ve bilgi depolayan medyalar (usb bellek, harici disk, cd vb.) masaların üzerinde bırakılmamalıdır.

k) Kişisel verilerin bulunduğu ortamlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

l) Aşağıda belirtilen hususların yaşanması durumunda Tuzla Belediyesi İrtibat Kişisi aynı gün bilgilendirilmelidir;

- Kişisel veri ihlâlinin gerçekleşmesi durumunda,
- Kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde,
- Kurum içinde ihlale sebebiyet verebilecek / verebilen açıklıkların oluşması durumunda,
- Saklama süresi dolan verilere aksiyon alınması gereken durumlarda,

m) Kurum içi ve kurum dışı kişisel veri sahiplerinin, işlenen kişisel verileri hakkındaki talepleri Aydınlatma Beyanında (web sayfasında mevcut) belirtilen yöntemlere göre alınmalıdır.

n) Veri sahiplerinden gelen kişisel veri talepleri olumlu ya da olumsuz en geç 30 gün içinde veri sahibine dönüş yapılmalıdır. Veri sahibi talebinin kabul edilmesi durumunda ise cevap dönülmesinden itibaren en geç 30 gün içerisinde aksiyon tamamlanmalıdır.

o) Tuzla Belediyesi'nin KVKK 'ya şikâyet edilmesi durumunda en kısa sürede deliller toplanmalıdır. Talep ve şikâyetlerin yönetimi için idari ve teknik tedbirlere göre uygun hareket edilmelidir.

p) Veri sahiplerine ait kişisel verilerin işlenmesi için açık rıza alınması gereken durumlarda, açık rıza alınmadan kişisel veriler kullanılmamalıdır.

q) Çalışanlar, birimlerinde yeni bir iş süreci oluşması ve / veya kişisel verilerin kullanma amaçlarının değişmesi durumunda, birim yöneticilerini ve Tuzla Belediyesi İrtibat Kişisi'ni bilgilendirmelidir.

P.27 İMHA POLİTİKASI:

Amaç

Bu politikada; kullanıcıların Tuzla Belediyesi'nin sorumlu olduğu kişisel ve kurumsal bilgilerin imhası sırasında dikkat edilmesi gereken hususların anlatılması amaçlanmaktadır.

Kapsam

Tuzla Belediyesi'nin sorumlu olduğu tüm kişisel ve kurumsal bilgiler ile bilgilerin bulunduğu ortamları kapsamaktadır.

Politika

a) Kişisel verilerin imhası gerçekleştirileceği zaman Kişisel Verilerin Korunması ve İmha Politikası dikkate alınarak imhalar gerçekleştirilmeli ve gerçekleştirilen imhalar kayıt altına alınmalıdır.

b) Kişisel verilerden saklama süreleri dolan veri olup olmadığı en geç 6 ayda bir kontrol edilmelidir.

c) Elektronik cihazların imhasına karar verilmesi durumunda depolama alanları (harddisk) çıkartılarak bilgi işlem personeline teslim edilmelidir. Çıkartılan depolama alanları bilgi işlem personeli kontrolünde saklanmalıdır.

d) Saklanan ya da ihtiyaç duyulmayan donanımların imhası aşamasında İmha Tutanağı Formu kullanılmalıdır.

e) Gerek duyulması halinde atık hale gelen elektronik cihazlar Çevre ve Şehircilik Bakanlığı'ndan atık elektrikli ve elektronik eşya işleme konusunda lisansa sahip firmalar ile sözleşme yapılarak, imha işlemleri yapılabilir. Bu tarz durumlarda teslim edilen imha edilecek ürün bilgisi İmha Tutanağı Formu ile kayıt altına alınmalıdır.

f) İhtiyaç duyulmadığına karar verilen dokümanlar uygun metotlarla (kâğıt öğütücü, yakma vb.) imha edilmelidir. İmha yöntemleri Kişisel Verilerin Korunması ve İmha Politikası 'nda detaylandırılmıştır.

g) Gizli olarak tanımlanan (sözleşme, fatura, kişisel veri içeren, şartnameler, veri dokümanları vb.) dokümanlar ve kopyaları, müsvedde olarak kullanılmamalı ve kâğıt öğütücü ile imha edilmelidir.

h) Kişisel veri barındırılan medyaların yeniden kullanılması gereken durumlarda, eski verilere tekrar erişimin engellenebilmesi için özel wipe (silme) uygulamaları kullanılmalıdır.

i) Kurum içeresindeki tüm kullanıcılar, gereksiz veya artık kullanılmayan bilgileri güvenlik standartlarına uygun olarak silmelidir.

P.28 LOG YÖNETİM POLİTİKASI

Amaç

Tuzla Belediyesi'nin sahibi ve sorumlusu olduğu kullanıcı, sistem ve paydaş log kayıtlarının korunmasına ilişkin kuralların belirlenmesi amaçlanmaktadır.

Kapsam

Tuzla Belediyesi loglarının olduğu sistem ve lokasyonları kapsamaktadır.

Politika

a) Logların yönetimi, log alınacak sistemlerin belirlenmesi ile başlar. Tuzla Belediyesi'nin kullandığı uygulama, sistem ve erişim log kayıtları alınması KVKK açısından önem arz etmektedir. Yasal ve operasyonel gereksinimler öncelikli olarak göz önünde bulundurulmalıdır. Bu amaçla loglama yapılacağı belirlenen altyapı kaynağında ne tür vakalar için hangi logların üretileceğine ve loglar üzerinde ne tür korelasyon kuralları uygulanacağına Sistem Birimi ve varsa anlaşmalı firma ile karar verilir.

b) Yavaşlama veya sistem kesintisine sebep olmayacak ölçüde log üretilmelidir.

c) Karar verilen log bilgilerinin haricinde, yüksek miktarda loglama yapılmamalıdır.

d) Logların yedekleri kayıtları üreten uygulama, donanım ya da sistem haricinde farklı bir ortama alınması tercih edilmelidir.

e) Log kaynağına ait sistem zamanının tutarsız veya anlamsız olmaması için log kaynaklarına ilişkin saat bilgisi temel bir zaman kaynağı ile uyumlu hale getirilmelidir.

f) Log analizine yardımcı olmak amacıyla, değişik log yapılarını tek bir standart ve tutarlı log yapısına dönüştürme yöntemleri kullanılmalıdır.

g) Loglar, 5651 sayılı kanun uyarınca iki yıl saklanmalıdır.

h) Loglar sistem ve ağ güvenliği ile ilgili bilgileri de içerebildiğinden, gizlilik ve bütünlük ihlallerine karşı korunmalıdır.

i) Logların güvenliği, sadece depolandıkları yerlerde değil, iletim esnasında da kasıtlı veya kasıtlı olmayan değişiklik ve tahribata karşı farklı ortamlarda da depolanması tercih edilmelidir.

j) Arşivlenen logların da gizlilik ve bütünlüğünün korunması sağlanmalıdır.

k) Log kaynak sistemlerinde, Sistem Birimi personelleri haricinde, hiçbir personele okuma, yazma veya değişiklik amaçlı erişim izni verilmemelidir.

l) Log kayıtlarının üçüncü taraf kişi / kurumlar tarafından talep edilmesi durumunda, adli mercilerin verdiği karar doğrusunda log kayıtları ilgili kişi ya da adli mercilere teslim edilmelidir.

m) Sistemlerde tespit edilen anormallikler için Olay İhlal Prosedürü 'nde belirtilen yöntemlere göre aksiyon alınmalıdır.

n) Logların alınmaması durumları için otomatik uyarı sistemleri kurulmalıdır. Uyarı sisteminin kurulamadığı durumlarda belirli periyodlarda (en geç 2 haftada bir öngörülmektedir) loglar manuel kontrol edilmelidir.

o) Çok gizli ve özel nitelikli kişisel veri bulunan ortamlarda yapılan erişim, silme, kaydetme durumlarının log kayıtları alınmalıdır.

p) Tuzla Belediyesi adına veri işleyen tedarikçi ya da alt taşeron olması durumunda; kişisel veri talepleri geldiği zaman sadece ilgili talebe ilişkin log kayıtlarını yetkili makamlarla paylaşmalıdır. Ölçülü veri paylaşımı esas alınmalıdır.

q) Log kayıtları üzerinde yetkisiz kişiler tarafından değişiklik yapılmasının önüne geçilmesi ve kanıt niteliğinde olması için log kayıtlarına zaman damgası vurulması tercih edilmelidir.

r) Çok gizli ve kişisel veri bulunan sistemlere ayrıcalıklı erişim sağlayan personel ve üçüncü taraf kişi / kurumların log kayıtları ya da ekran hareketlerinin görüntüsü alınmalıdır.

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKALARI KABUL ONAYI

Tuzla Belediyesi Yönetim Sistemi Politikalarında ifade edilen tüm kurallara uymayı, iş bu güvenlik politikalarının ve revizyonlarının Bilgi Güvenliği Yönetim Sistemi'nde yayınlandığını bildiğinizi ve güncellemeleri takip ederek iş bu değişikliklere uygun davranacağınızı aksi takdirde hakkınızda disiplin ve yasal her türlü işlemin başlatılacağını bildiğinizi kabul ve taahhüt etmektesiniz.

İzlenecek Prosedür

1. Bilgi Güvenliği Politikasını okuyunuz.
2. Aşağıdaki belirtilen bölümlere bilgileri doldurup imzalayınız.
3. Bu sayfayı İnsan Kaynakları Müdürlüğü'ne teslim ediniz.

Anlaşma

Bu forma imza atarak aşağıda yazılanları kabul etmiş oluyorum.
Tuzla Belediyesi Bilgi Güvenliği Politikası kabul onayının bir kopyasını teslim aldım, okudum ve anladım.

Personelin;
İmzası :

T.C. Kimlik/Pasaport No:

Adı ve Soyadı :

Unvanı :

Bölümü :

Tarih :

Bu form Tuzla Belediyesi Bilgi Güvenliği Politikasının okunduğu, anlaşıldığı ve kabul edildiğinin onaylandığı bir dokümandır. Tuzla Belediyesi kurumunun yönetim temsilcisi ve en üst düzey yöneticisi bu politikanın uygulanabilirliğinden sorumludur.