KONAK BELEDİYESİ

BİLGİ GÜVENLİĞİ POLİTİKASI

a. Tanım;

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

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

1. Gizlilik
2. Bütünlük
3. Erişilebilirlik

Bu kavramları biraz daha açacak olursak

Gizlilik

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

Bütünlük

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

Erişilebilirlik

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

b. Kapsam;

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

c. Amaç;

Kurum yönetimi:

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

d. Politika İhlali ve Yaptırımlar;

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, ilgililer hakkında adli ve idari yasal işlemler yapılabilecektir. Kurumumuza ait Bilgi Güvenliği Politikası oluşturulmuş olup bu politika kapsamında hazırlanmış olan talimatlar aşağıda gösterilmiştir.

Kurumsal Bilişim sistemlerinin güvenliğinde herhangi bir aksamaya mahal verilmemesi için genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında çalışanlarımızın da bu hususta titizlikle uyması gereken bu kurallara bütün kurum çalışanları uymak zorundadır.

1. E-Posta Kullanma Kuralları

1.1. Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
1.2. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
1.3. Kişisel kullanım için İnternet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
1.4. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
1.5. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
1.6. Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, fikri mülkiyet içeren malzeme vb.) gönderemezler.
1.7. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
1.8. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
1.9. Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.
1.10. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodlar içerebilirler.
1.11. Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.
1.12. Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre (kişisel klasörler) çekilmelidir.
1.13. Belediyemiz çalışanları gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Yasadışı ve hakaret edici e-posta haberleşmesi yapılması durumunda yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilir ve kullanıcı hakkında yasal ve idari işlemler başlatabilir.
1.14. Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren yetkililerle temasa geçip durumu haber vermekle yükümlüdürler.
1.15. E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma, işten ayrılma sebepleriyle kurumdaki değişikliğinin ilgili Müdürlük tarafından Bilgi İşlem Müdürlüğüne en kısa zamanda bildirilmesi gerekmektedir.

2. Şifre Kullanma Kuralları

2.1. Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her üç ayda birdir.
2.2. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
2.3. Kuruma ait uygulamalarda kullanılan parolalar iş arkadaşları da dâhil olmak üzere kimse ile paylaşılmamalı, parolalar yazılı olarak post-it ya da not kâğıtlarına yazılarak pano, bilgisayar ekranı, klavye gibi donanımlara yapıştırılmamalıdır.

2.4. Şifrelemede, küçük ve büyük karakterlere (örnek, a-z, A-Z), hem digit hem de noktalama karakterleri ve ayrıca harflere (örnek, 0-9, !'^+%&/()=?_;*) sahip olmalıdır.
2.5. En az altı adet alfa nümerik karaktere sahiptir.
2.6. Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
2.7. Aile isimleri kullanılmamalıdır.
2.8. Herhangi bir kişiye telefonda şifre verilmemelidir.
2.9. E-posta mesajlarında şifre yazılmamalıdır.
2.10. Şifreler aile bireyleriyle paylaşılmamalıdır.
2.11. Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
2.12. Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.
2.13. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

3. Antivirüs Politikası

3.1. Bütün bilgisayarlarda kurumun lisanslı antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.
3.2. Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem Müdürlüğüne haber verilmelidir.
3.3. Zararlı programları (örneğin, virüsler, solucanlar, truva atı, e-mail bombaları vb) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.
3.4. Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını sisteme kuramaz.

4. İnternet Kullanım Politikası

4.1. Hiçbir kullanıcı peer-topeer ve tünel bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örneğin; Zen Mate, KaZaA, iMesh, Gnutella, Napster, Aimster, Madster, FastTrak, eMule,.vb)
4.2. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde Skype, Messenger vb. mesajlaşma ve sohbet programları gibi chat programları kullanılmamalı ve chat programları üzerinden dosya alışverişinde bulunulmamalıdır.
4.3. Hiçbir kullanıcı internet üzerinden Multimedia Streaming (Video, mp3 yayını ve iletişimi) yapamayacaktır. Bu internet erişiminde bant genişliği harcadığı için diğer kullanıcıların veriye erişiminde sorunlar yaratmaktadır.
4.4. Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.
4.5. İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek ve bilgisayarlarda saklamak yasaktır.
4.6. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz kullanılamaz
4.7. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

4.8. Bilgisayar İşletim Sistemlerine zarar verdiği için internet üzerinden ekran koruyucu, yamalar, masaüstü resimleri, yardımcı, tamir edici program olduğu belirtilen araçlar gibi her türlü dosya ve programların indirilmesi ve/veya kurulması yasaktır. Üçüncü şahısların kurum içerisinden interneti kullanmaları Bilgi İşlem Müdürlüğünün izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.

4.9. Bilgi İşlem Müdürlüğü, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir. Gerekli durumlarda internet üzerinde kısıtlamalar yapabilir.

5. Genel Kullanım Politikası

5.1. Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.
5.2. Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır.
5.3. Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
5.4. Kurumda domain (çalışma alanı) yapısı varsa mutlaka login olunmalıdır. Bu durumda, domain' e bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.
5.5. Bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Müdürlüğüne haber verilmelidir.
5.6. Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur.
5.7. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.
5.8. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packetsniffing, packetspoofing, denial of service vb.) eylemlere girişmemelidir.
5.9. Port veya ağ taraması yapılmamalıdır.
5.10. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.
5.11. Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.
5.12. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Müdürlüğünü onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
5.13. Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.
5.14. Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD' leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.
5.15. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
5.16. Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, odamızın bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilemez.
5.17. Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde USB flash bellek ve/veya harici hard disk gibi taşınabilir medya bırakmamalıdır.
5.18. Personel telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranmalıdır. Gizlilik içeren bilgiler, telefonlarda dışarıya ses açık olarak görüşülmemelidir.
5.19. Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliği ile sorumludur.
5.20. Bilgi İşlem Müdürlüğü tarafından yetkili kişiler kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel kişisel bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.
5.21. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

5.22. Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
5.23. Kurumda Bilgi İşlem Müdürlüğünün bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb.) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.
5.24. Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.
5.25. Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez
5.26. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
5.27. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Müdürlüğüne haber verilmelidir.
5.28. Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.

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

Nilüfer ÇINARLI MUTLU
Mimar
Belediye Başkanı