BANDIRMA
BELEDİYESİ

BİLGİ GÜVENLİĞİ POLİTİKASI

Bandırma Belediyesi
Bilgi Güvenliği Politikası

1.Tanım

Bilgi, Kurumda süreçlerin devamlılığı için sahip olunan, kurum için önem taşıyan ve en iyi şekilde korunması gereken, en önemli kurum varlıklarındandır.

Bilgi Güvenliği, oluşturulan, derlenen, işlenen, kullanılan bilgilerin saklanması ve korunmasıdır.

Bilgi Güvenliği Politikası, Kurum içindeki bilgilerin (basılı, yazılı, dijital, sözel) tehditlere karşı korunmasını düzenleyen uygulamalar ve kurallar bütünüdür. Üç temel unsuru içerir.

a. **Gizlilik (Confidentiality)**

   Bilginin yetkisiz kişilere kapalı olması, gizliliğinin gözetilmesi,

b. **Bütünlük (Integrity)**

   Bilginin yetkisiz kişilerce değiştirilmemesi, silinmemesi ve tahrip edilmemesi,

c. **Erişilebilirlik (Availability)**

   Bilginin olması gereken yerde kullanıma hazır, yetkili kişilerce erişilebilir ve kullanılabilir olmasıdır.

2. Amaç

Bu Bilgi Güvenliği Politikasının amacı; Bandırma Belediyesi Bilgi İşlem Müdürlüğü'nün, Bandırma Belediyesi'nde kullanılan bilgi varlıklarının gizliliği bütünlüğü ve sadece yetki verilen kişilerce erişilebilirliği sağlanarak; kazara ya da kasten oluşabilecek bilgi güvenliği tehditleri, ihlal ve zafiyetleri konusunda alacağı tedbir, uygulama ve kuralları, Kurum personellerine ve Üçüncü kişilere (yazılım, donanım, teknik destek sağlayıcıları ve tedarikçiler) bildirmek ve duyurmaktır.

3. Kapsam

Bu politika, Bandırma Belediyesi 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.

4. Politika İhlali ve yaptırımlar

Bilgi Güvenliği politikası, prosedür ve talimatlara uyulmaması halinde, ilgililer hakkında adli ve idari yasal işlemler yapılacaktır.

5. Politika

Bilgi kaynakları, sistemler, tesisler ve cihazlar gibi T. C. Bandırma Belediyesi açısından büyük önem taşıyan varlıklardır. Bilgi varlıklarını ve kaynaklarını kullanan veya bilgi sağlayan herhangi bir kişi, bilgi varlıklarını korumakla yükümlüdür.

Ortak bilgi varlıklarını kullanan tüm çalışanların, gereken duyarlılığı göstermesi ve diğer meslektaşlarını, kurum çalışanlarını ve kurumsal değerleri gözeterek hareket etmesi beklenir.

Kurumsal değerlerin gereği olarak gizliliğe önem verilir, her türlü kişisel bilgi en yüksek güvenlik standartlarına sahip sistemlerle korunur. Bilginin sahibi istemedikçe, yetki verilmedikçe veya yasal gereklilikler oluşmadıkça bilgi paylaşılmaz.

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.

Kurumumuza ait Bilgi Güvenliği Politikası oluşturulmuş olup bu politika kapsamında hazırlanmış olan talimatlar aşağıda gösterilmiştir.

1. Şifre Kullanma Kuralları

1.1. Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, program, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her üç ayda birdir.

1.2. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemeli ve kaydedilmemelidir.

1.3. Şifreler başkası ile paylaşılmamalı, kağıtlara yada elektronik ortamlara yazılmamalıdır.

1.4. Şifrelemede, küçük ve büyük karakterlere (örnek, a-z, A-Z), hem sayısal hem de noktalama karakterleri ve ayrıca harflere (örnek, 0-9, !'^+%&/()=?_;*) sahip olmalıdır.

1.5. En az altı(6) adet alfa nümerik karaktere sahiptir.

1.6. Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.

1.7. Aile isimleri kullanılmamalıdır.

1.8. Herhangi bir kişiye telefonda şifre verilmemelidir.

1.9. E-posta mesajlarında şifre yazılmamalıdır.

1.10. Şifreler aile bireyleriyle paylaşılmamalıdır.

1.11. Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.

1.12. Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.

1.13. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

2. E-Posta Kullanma Kuralları

2.1. Çalışanlar kurum ile ilgili çalışmalarında kurumun dışındaki e-posta hesaplarını kullanamazlar.

2.2. Kurumsal e-posta olmayan kişisel e-posta hesapları (gmail, Hotmail, yahoo mail vs.) gibi e-posta sistemlerinden kurumsal yazışma yapılmamalıdır.

2.3. Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.

2.4. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

2.5. Kişisel kullanım için İnternet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

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

2.7. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

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

2.9. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

2.10. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.

2.11. Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

2.12. 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.

2.13. Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.

2.14. Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre (kişisel klasörler) çekilmelidir.

2.15. E-posta adresine sahip kullanıcının herhangi bir sebepten (emekli olma, işten ayrılma gibi nedenlerle) kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem birimine bildirilmesi gereklidir.

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 bulundurmak, oluşturmak ve dağıtmak yasaktır.

3.4. Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını sisteme kuramaz.

3.5 E-posta ile gelen spam, zincir ve junk e-mailleri silinmelidir

3.6 Bilinmeyen ve şüpheli kaynaklardan asla dosya indirmeyin.

3.7 Bilinmeyen kaynaklardan gelen taşınabilir bellek, disk ve CD'lere virüs tarama yapılmalıdır.

4. İnternet Kullanım Politikası

4.1. Hiçbir kullanıcı peer-to peer, Proxy, VPN tünel bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örneğin;Zen Mate, KaZaA, iMesh, Gnutella, Napster, Aimster, Madster, FastTrak, eMule,. vb)

4.2. Bigisayarlar 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 ve 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. Bandırma Belediyesi'ne ait Kurumsal Sosyal Medya hesapları haricinde hiçbir kullanıcı sosyal medya hesabı kullanmamalıdır.

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

5. Uzaktan Erişim Politikası

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

5.2. İnternet üzerinden kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. Bu, veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec , L2TP, SSL, PPTP vs. protokollerinden birini içermelidir.

5.3. Uzaktan Erişim sağlayacak Kurum personeli, Bandırma Belediyesi Bilgi İşlem Müdürlüğü'ne yazılı izin ile bildirmelidir.

5.4. Uzaktan Erişim ve Destek sağlayacak sözleşmeli, sözleşmesiz, bakım anlaşması olan veya olmayan kurum dışı firmalar, Bilgi İşlem Müdürlüğü'ne yazılı veya e-posta yoluyla erişim izni istemelidir.

6. Genel Kullanım Politikası

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

6.2. Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.

6.3. Kurumda domain (çalışma alanı) yapısı varsa mutlaka login olunmalıdır. Bu durumda, domain' e bağlı olmayan bilgisayarların yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.

6.4. Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Müdürlüğüne haber verilmelidir.

6.5. 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.

6.6. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.

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

6.8. Port veya ağ taraması yapılmamalıdır.

6.9. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.

6.10. Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.

6.11.Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Müdürlüğünü onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

6.12. Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.

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

6.14. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.

6.15. Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, Belediye'mizin bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilemez.

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

6.17. 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.

6.18. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

6.19. Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

6.20. Kurumda Bilgi İşlem Müdürlüğünün bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb.) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.

6.21. 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.

6.22. Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez

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

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

6.25. 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.

Dursun MİRZA

Belediye Başkanı