****

**KABUL EDİLEBİLİR KULLANIM POLİTİKASI**

# DOKÜMAN KONTROLÜ

**DOKÜMAN KODU:** NB.BG.POL.04

**DOKÜMAN ADI:** KABUL EDİLEBİLİR KULLANIM POLİTİKASI

|  |  |  |
| --- | --- | --- |
| **Hazırlayan** | **Kontrol Eden** | **Onaylayan** |
| İsim: Elif Müge TUSKAN | İsim: Mahsun YAZGAN | İsim: İsmail AY |
| Görevi: BGYS Bilgi Teknolojileri Sorumlusu  Bilgisayar Mühendisi | Görevi: BGYS Teknik Yöneticisi  Bilgi İşlem Müdürü | Görevi: BGYS Kurul Başkanı  Belediye Başkan Yardımcısı |
| İmza: | İmza: | İmza: |
| Tarih: | Tarih: | Tarih: |

**GİZLİLİK SINIFI:** Kurum İçi

VERSİYON TARİHÇESİ:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versiyon** | **Revizyon Tarihi** | **Hazırlayan** | **Onaylayan** | **Açıklama** |
| 1 | - | Mahsun YAZGAN  BGYS Teknik Yöneticisi | İsmail AY  BGYS Kurul Başkanı | Bilgi Güvenliği Kabul Edilebilir Kullanım Politikası ile ilgili 2020 yılı itibariyle çalışmalar başlatılmıştır. |

**DAĞITIM LİSTESİ:**

Tüm Narlıdere Belediyesi Çalışanları

İçindekiler

[DOKÜMAN KONTROLÜ 2](#_Toc50560675)

[1. AMAÇ 5](#_Toc50560676)

[2. KAPSAM 5](#_Toc50560677)

[3. GENEL KURALLAR 5](#_Toc50560678)

[3.1. Bilgisayar Kullanım İlkeleri 5](#_Toc50560679)

[3.2. Kişisel Kullanım Politikası 6](#_Toc50560680)

[3.3. Kişisel Bilgisayar Tahsisi Politikası 6](#_Toc50560681)

[3.4. Narlıdere Belediyesi Kaynaklarının Yasalara ve Etik Prensiplerine Uygun Kullanımı 6](#_Toc50560682)

[3.5. Konfigürasyon ve Güvenlik Ayarları 7](#_Toc50560683)

[3.6. Narlıdere Belediyesi’ne Ait Olmayan Bilgisayarlar 7](#_Toc50560684)

[3.7. Ofis Araç Gereçlerinin Fiziksel Güvenliği 7](#_Toc50560685)

[3.8. Güvenlik Olay ve Zafiyetlerinin Raporlanması 7](#_Toc50560686)

[4. HESAP VEREBİLİRLİK 7](#_Toc50560687)

[4.1. Hesap Verebilirlik 7](#_Toc50560688)

[4.2. Kullanıcı Kimliği 8](#_Toc50560689)

[4.3. Parola (Şifre) Kriterleri 8](#_Toc50560690)

[5. İNTERNET KULLANIMI 8](#_Toc50560691)

[5.1. Kurumsal ve Kişisel Bilgilerin İnternet Üzerindeki Web Sitelerine Verilmesi 8](#_Toc50560692)

[5.2. İnternetten Dosya İndirme 8](#_Toc50560693)

[5.3. Kurum İnterneti’nin Amacı Dışında Kullanılması 9](#_Toc50560694)

[5.4. İnternet Üzerinden Peer to Peer – P2P Ağ Oluşturma ve Dosya Paylaşımı 9](#_Toc50560695)

[6. MESAJLAŞMA KULLANIMI 9](#_Toc50560696)

[6.1. İzin Verilen Mesajlaşma Çözümleri 9](#_Toc50560697)

[6.2. E-posta Kullanımı 9](#_Toc50560698)

[6.3. Mesajlaşma Mahremiyeti 10](#_Toc50560699)

[6.4. Kimlik Hırsızlığı (Phishing) Saldırıları, Mesaj Ekleri Politikası, İstenmeyen (Spam) E-postalar ve Yasak Kullanımlar 10](#_Toc50560700)

[6.5 E-Posta Yedekleme İşlemleri 11](#_Toc50560701)

[7. OFİS EKİPMANLARI, BASILI DOKÜMANLAR VE TAŞINABİLİR VERİ SAKLAMA ARAÇLARI 11](#_Toc50560702)

[7.1. Yazıcılar ve Fotokopi Makineleri 11](#_Toc50560703)

[7.2. İhtiyaç Kalmayan Basılı Dokümanların İmha Edilmesi 11](#_Toc50560704)

[7.3. Taşınabilir Veri Saklama Araçları 11](#_Toc50560705)

[8. İZLEME VE KAYIT AKTİVİTELERİ, MAHREMİYET 12](#_Toc50560706)

[8.1. Narlıdere Belediyesi Sistemlerinde Saklanan Narlıdere Belediyesi Sistemleri Aracılığı ile İletilen Verilerin Mahremiyeti 12](#_Toc50560707)

[8.2. Kayıtlar 12](#_Toc50560708)

[9. GENEL VERİ KORUMA VE SINIFLANDIRMA SORUMLULUKLARI 12](#_Toc50560709)

[9.1. Bilgi Paylaşımı, Veri Sahipliği ve Sınıflandırılması 12](#_Toc50560710)

[9.2. Kurumsal Verinin Saklanması 12](#_Toc50560711)

[9.3. Narlıdere Belediyesi Dizüstü Bilgisayarları 12](#_Toc50560712)

[9.4. Narlıdere Belediyesi Ofisi Dışına Gönderilen Bilgisayarlar ve Veri Saklama Araçları 13](#_Toc50560713)

[9.5. Narlıdere Belediyesi Ağına Uzaktan Erişim 13](#_Toc50560714)

[9.6. Temiz Masa, Temiz Ekran Politikası 13](#_Toc50560715)

[9.7. Telefon Görüşmeleri 13](#_Toc50560716)

[10. İHLALLER VE YAPTIRIMLAR 14](#_Toc50560717)

[11. DİĞER HUSUSLAR 14](#_Toc50560718)

[11.1. Daha Fazla Bilgi İçin 14](#_Toc50560719)

[12. KISALTMALAR VE TANIMLAR 15](#_Toc50560720)

# AMAÇ

Bu politikanın amacı, çalışanlara kurum bilgisayarlarının kullanımı için gerekli yol gösterici bilgiyi sağlamak, Kuruma ait bilgisayar ve ilgili cihazların kullanımıyla ilgili kısıtlamaları ve düzenlemeleri belirlemek ve belirlenmiş olan kurallara mukavemet gösterilmesi ya da uyulmaması halinde kurum tarafından gerekli yaptırımların gerçekleştirilmesidir.

# KAPSAM

Narlıdere Belediyesi Kabul Edilebilir Kullanım Politikası tüm Narlıdere Belediyesi çalışanlarını kapsar. Politika maddeleri hem ofis içindeki hem de ofis dışındaki kullanım için geçerlidir. Ayrıca bazı alanlarda Narlıdere Belediyesi personelinin sorumluluğunda çalışan 3. parti çalışanları için de kabul edilebilir kullanım kuralları bu politika ile tanımlanmaktadır.

# GENEL KURALLAR

* Bilgisayar masası üzerinde yiyecek ve içecek bulundurulmamalıdır. Eğer klavye üzerine sıvı bir madde dökülürse klavye hemen ters çevrilmeli, kurumaya bırakılmalıdır.
* Kasa, klavye ve fare haftada bir kez hafif nemli bir bez (kolonyalı mendil vb.) ile temizlenmelidir. Monitörün ekran temizliği mutlaka kuru bez ile yapılmalıdır. Aksi halde ekranda lekeler oluşmaktadır.
* Bilgisayarların çalışabilmesi için gereken elektriğin sağlıklı olması şarttır. Kullanıcılar sahip oldukları bilgisayarlarını en yakın prize takmadan önce prizleri kontrol ettirmelidir. Eğer binada Kesintisiz Güç Kaynağı (UPS) var ise UPS kullanılmalıdır.
* Sürekli tekrarlanan arızalarda, büyük bir olasılıkla kullanıcı kusuru söz konusudur. Bu konuda ısrar edilmesi halinde, kullanıcıya yaptırımlar uygulanabilecektir.
* Kullanıcının tanımadığı kişilerden gelen ve özellikle eki olan elektronik postalar açılmadan silinmelidir.
* Sadece Kurum tarafından sağlanan bilgisayar teçhizatı (yazıcı, tarayıcı, dijital kamera, USB kart okuyucuları, CD yazıcılar, taşınabilir sabit disk, Flash disk/hafıza kartı) bilgisayara bağlanabilir. Bunlardan başka hiçbir donanımı yöneticinin haberi olmaksızın kurum bilgisayarında kullanılmayacaktır.
* Çalışan personel bilgisayar giriş şifresini kendisi belirlemekle yükümlüdür. Şifrenin unutulması halinde yalnızca sistem yöneticisi ile ilgili kullanıcı temasa geçerek şifrenin resetlenmesi işlemine onay vermek suretiyle şifre değiştirme işlemi gerçekleştirilir.
* Kullanıcı bilgisayarında tutulmuş olan tüm verilerden sorumludur.

# Bilgisayar Kullanım İlkeleri

Müdürlüklerimizde/Birimlerimizde; aşağıdaki maddelerde bahsedilen faaliyetlere izin verilmez.Kullanıcı bu maddelerin ihlali durumunda hakkında idari işlem yapılabileceğini ve tüm sorumluluğun kendisinde olduğunu kabul eder.

* Oyun oynamak,
* Film izlemek,
* Sesli bir biçimde müzik dinlemek,
* Toplum genel ahlak kurallarına uymayan web sayfalarına bakmak,
* Internet etik kurallarına uymayan e-mail göndermek,
* Kurum içinde kullanılan standart yazılımlar dışında herhangi bir yazılım kullanmak,

# Kişisel Kullanım Politikası

Narlıdere Belediyesi bilgisayar ve iletişim sistemlerinin kişisel kullanımı, gerekli olduğu durumlarla kısıtlanmaktadır. Kişisel kullanım, e-posta zincirlerinin yayılmasına yardımcı olmak veya yaratmak, uygunsuz veri ve resim alışverişi yapmak, kumar oynamak ve politik aktivitelere katılmak gibi hareketleri içeremez. Narlıdere Belediyesi Bilgi İşlem Müdürlüğü ortak paylaşım sunucularında saklanan iş dışı kişisel dosyaları haberli bir şekilde silme hakkına sahiptir.

# Kişisel Bilgisayar Tahsisi Politikası

Narlıdere Belediyesi çalışanlarına, görev tanımları gereği Bilgi Teknolojileri donanımları tahsis edilip, gerekli teknik destek sağlanmaktadır.

Tahsis edilecek donanım, her çalışana, İK biriminden gelen onaya istinaden görev tanımına veya kurum tarafından belirlenmiş kullanım kriterlerine uygun olarak verilmektedir. Her seviyedeki çalışana normal kullanım ihtiyaçları çerçevesinde standart uygulamaların bulunduğu donanım tahsis edilmektedir. İleri seviye konfigürasyona sahip donanım, standart donanımın kullanıcının ihtiyacını karşılayamadığı özel durumlarda ve ilgili Birim Yöneticisi ve Bilgi İşlem Müdürü onayı ile verilebilmektedir.

Kullanım süresi içinde kişinin kullanıcı profilindeki herhangi bir değişiklik sebebiyle kullanmış olduğu Bilişim malzemelerinin değiştirilmesi gündeme gelirse, mevcut kullanmış olduğu cihazlar(bilgisayar,yazıcı,tarayıcı vb.) kurum içinde başka bir uygun kullanıcıya verilmektedir.

# Narlıdere Belediyesi Kaynaklarının Yasalara ve Etik Prensiplerine Uygun Kullanımı

Narlıdere Belediyesi personeli, internet kullanımı ve sesli haberleşme aktiviteleri dahil olmak üzere, tüm bilgi sistemleri ve iletişim imkanlarının kullanımında ve bu imkanların sağlanmasında, başta 5651 numaralı yasa olmak üzere ilgili Türkiye Cumhuriyeti yasalarına, uluslararası hukuka ve genel etik kurallarına uymakla yükümlüdür. Kullanıcılar, bilgisayarlarında bulunabilecek standart iş ve ofis uygulamaları dışındaki yazılımlar (Narlıdere Belediyesi Bilgi İşlem Müdürlüğü teknik personeli tarafından kurulmuş işletim sistemi, virüs koruma, ofis uygulamaları, iş uygulamaları vb. dışındaki yazılımlar) için telif hakkı koruma düzenlemelerine uymakla şahsen sorumludur.

Diğer kullanıcıların kimlik doğrulama ve erişim kontrol araçlarını (VPN, fiziksel geçiş kontrol kartı, vb.) ele geçirmeye çalışmak, Narlıdere Belediyesi kaynaklarına zarar vermek ya da üçüncü taraflara Narlıdere Belediyesi kaynaklarını kullanarak zarar vermek etik kurallarına ve yasalara aykırı olup, kabul edilemez. Kullanıcılar teknik olarak mümkün olsa bile iş sorumlulukları gereği erişim ihtiyacı olmayan kaynaklara erişmemelidirler. Kullanıcılar bu hususlarda bir zafiyet fark ederse Bilgi İşlem Müdürlüğünü bilgilendirmekle yükümlüdür.

Tüm iletişimde genel prensip olarak kurumsal ve genel etik ve nezaket kurallarına uyulmalıdır. Ayrıca iletişim sırasında kurum çalışanlarına, vatandaşlara ve diğer taraflara zarar verecek hakaret içeren ifadeler kullanılamaz. Narlıdere Belediyesi bilgi kaynaklarının personel tarafından yasal olmayan şekilde kullanımı halinde gerekli hukuki işlemler başlatılacaktır.

# Konfigürasyon ve Güvenlik Ayarları

Kullanıcılar teknik olarak mümkün olsa bile bilgisayarlarındaki güvenlik ayarlarının düzeyini düşürmemelidir. Güvenlik ayarlarına örnek olarak; İşletim sistemi güncelleme ayarları, virüs programı ayarları, BIOS ayarları ve diğer donanımsal ve yazılım güvenlik ayarları sayılabilir. Kullanıcılar bilgisayarlar üzerinde yeni kullanıcı oluşturamaz ve mevcut kullanıcıların hakları ve kullanıcı gruplarını değiştiremez. Eğer iş ihtiyaçları gereği konfigürasyon ve güvenlik ayarlarının değiştirilmesi gerekiyor ise Bilgi İşlem Müdürü’nün onayına başvurulur, onay verilmesi durumunda gerekli konfigürasyon ve güvenlik ayar değişiklikleri gerçekleştirilir.

Virüslere ve zararlı yazılımlara karşı güvenliğin sağlanabilmesine yönelik olarak aşağıdaki önlemler alınmalıdır.

* Kullanılan bilgisayarda hazırlanmamış her tür bilgi teknolojileri medyası (CD, disket, teyp, vb.) virüs kontrolü yapıldıktan sonra kullanılmalıdır.
* Güncel virüs yazılımı Bilgi İşlem Müdürlüğü tarafından sağlanmakla beraber Narlıdere Belediyesi kullanıcıları, bilgisayarlarındaki anti virüs yazılımının aktif olmasından sorumludur.
* İlgisiz ya da şüpheli mesajlar açılmamalı ve bilgisayardan silinmelidir. Şüpheli durumlarda Bilgi İşlem Müdürlüğü bilgilendirilmelidir.

# Narlıdere Belediyesi’ne Ait Olmayan Bilgisayarlar

Narlıdere Belediyesi’ne ait olmayan bilgisayarlar sadece iş gereği ve Bilgi İşlem Müdürü’nün onayı ile Narlıdere Belediyesi ofis ağına bağlanabilirler. Narlıdere Belediyesi’ne ait olmayan bilgisayarlarda Bilgi İşlem Müdürlüğü teknik kontroller uygulama ve ayar değişiklikleri yapma / yaptırma hakkına sahiptir.

# Ofis Araç Gereçlerinin Fiziksel Güvenliği

Sistem odası içerisine yiyecek, içecek gibi gıda maddeleri ile girmek yasaktır. Kritik sunucular sadece yetkili kişilerin erişebileceği şekilde sistem odasında tutulmaktadır. Kullanıcıların doğrudan sorumluluğunda veya ortak kullanımda olan bilgisayarlar ve diğer ofis araçlarını olumsuz etkileyebilecek çevresel etkenlere karşı (sıcaklık, nem, aşırı toz, v.b. gibi) Bilgi İşlem Müdürlüğü bilgilendirilmelidir.

# Güvenlik Olay ve Zafiyetlerinin Raporlanması

Kullanıcılar günlük işlerini yaparken güvenlik olaylarına ve zafiyetlerine karşı duyarlı olmalıdır. Fark edilen her zafiyet, riskin gerçekleşmesi zayıf bir olasılık olsa bile en kısa zamanda Bilgi İşlem Müdürlüğüne bilgi verilmelidir. Bu duruma örnek olarak, kullanıcı bilgisayarlarında virüs bulunmasından şüphelenilmesi, kullanıcı parolasının başkaları tarafından öğrenilmiş olmasından şüphelenilmesi veya erişim araçlarının (VPN, fiziksel geçiş kontrol kartı, vb.) kaybedilmesi / çalınması, dizüstü veya avuç içi bilgisayarların kaybedilmesi / çalınmas ve hizmet kesintisi gibi beklenmeyen durumlar verilebilir. Dizüstü bilgisayarların, kritik öneme sahip dokümanların ve veri saklama cihazlarının kaybı veya çalınması durumunda en kısa zamanda Bilgi İşlem Müdürlüğü bilgilendirilmelidir.

# HESAP VEREBİLİRLİK

# Hesap Verebilirlik

Kullanıcıya atanmış erişim araçları hiçbir şart altında teknik personel dahil kimseyle paylaşılamaz. Erişim araçlarına örnek olarak; parola, VPN, fiziksel geçiş kontrol kartı, vb. verilebilir. Bilgi İşlem Müdürlüğü personeli hiçbir zaman kullanıcılardan şifrelerini ve PIN kodlarını söylemelerini, yazılı iletmelerini isteyemez. Eğer kullanıcılar erişim ile ilgili konularda destek için telefon ile iletişim kuruyorsa, özellikle karşı tarafın araması durumunda, arayan kişinin kimlik doğrulamasını yapmalıdır. Şüpheli telefon aramaları veya mesajlar, edinilmesi mümkün olan detay bilgiyle birlikte Bilgi İşlem Müdürü’ne raporlanmalıdır.

# Kullanıcı Kimliği

Kullanıcıların Narlıdere Belediyesi sistemleri üzerinde kendilerine ait olmayan kullanıcı kodlarını (veya genel anlamıyla kimliklerini) kullanmaları, yasaktır. Bu çerçevede e-posta iletilerindeki gönderen kısmında bir kimlik bilgisi bulunmaktadır ve bu alanın yanıltıcı biçimde değiştirilmesi yasaktır. Her kullanıcı için ayrı bir “kullanıcı hesabı” oluşturulmuştur. Kullanıcılar, ortak hesap kullanımından kaçınmalı, kendisine özel oluşturulmuş kullanıcı hesabı ile işlemlerini gerçekleştirmeli, kendisine ait bir kullanıcı hesabı yok ise Bilgi İşlem Müdürlüğü’nden kullanıcı hesabı oluşturulması için talepte bulunmalıdır.

Bilgi İşlem Müdürlüğü uzun süre boyunca kullanılmayan hesapları kapatma hakkına sahiptir. 6 ay süreyle kullanılmayan hesaplar kapatılabilir ve ilgili kullanıcının dosyaları silinebilir.

# Parola (Şifre) Kriterleri

Narlıdere Belediyesi sistemleri, teknik olarak mümkün olan durumlarda, parola karmaşıklık ve değişiklik kontrollerini teknik olarak uygulayacak biçimde yapılandırılmaktadır. Kullanıcılar parola kriterlerinin teknik olarak zorlanmasının mümkün olmadığı durumlarda aşağıdaki belirtilen kriterlere uymakla yükümlüdür.

* Minimum şifre uzunluğu 7 karakter olmalıdır.
* Şifre yapısı; alfanümerik, büyük ve küçük harfler ve en az bir özel karakter (bunlardan en az üçü sağlanmalıdır) şeklinde olmalıdır.
* 30 günde bir defa şifre değişikliği yapılmalıdır.
* 10 hatalı giriş denemesinden sonra kullanıcı hesabı kilitlenmektedir.
* Kullanıcı şifrelerinde İngilizce karakter haricinde karakter kullanılmamalıdır.
* Şifre oluşturulurken başkaları tarafından kolay tahmin edilebilecek tarih, isim ve benzeri tanımlar kullanılmamalıdır.
* Şifre girişi sırasında başkalarının izlemediğinden emin olunmalıdır.
* Bilgisayarların açılış şifreleri, internet ortamında başka amaçlarla kullanılan şifrelerle aynı olmamalıdır.
* Kullanıcı şifresi kişiye özeldir ve başkaları ile paylaşılmamalıdır.
* Bilgisayar başında bulunulmayacağı durumlarda şifre korumalı ekran kilitleme sistemleri aktif duruma getirilmeli veya bilgisayar kapatılmalıdır.

# İNTERNET KULLANIMI

# Kurumsal ve Kişisel Bilgilerin İnternet Üzerindeki Web Sitelerine Verilmesi

Kullanıcılar internet üzerindeki tartışma gruplarına, sohbet odalarına ve diğer forumlara şirket adres ve telefon bilgilerini, personel isimlerini, ünvanlarını, e-posta adreslerini ve diğer kişisel bilgilerini iş gereksinimleri ve kanuni gereklilikler dışındaki durumlarda aktarmamalıdır.

# İnternetten Dosya İndirme

Kullanıcılar iş gereksinimleri için internetten veri dosyaları indirebilir, ancak bu işlemden önce anti-virüs imzaları ve işletim sistemi yamalarının güncelliğini kontrol etmelidir.

# Kurum İnterneti’nin Amacı Dışında Kullanılması

Kullanıcı, internet ortamındaki haber gruplarında, sohbet ortamlarında; hakaret, pornografi ve diğer yasadışı aktivitelerde bulunamaz. Belediyeye ait ağ ve sunucu bilgisayarlar uygunsuz, müstehcen, rahatsız edici görüntülerin üretilmesi ve dağıtılması amacıyla kullanılamaz.

Kullanıcı, kamu kurum veya kuruluşları ile gerçek/tüzel kişiler hakkında karalama ve benzeri yayın yapamaz, yapılması için özendirici olamaz. İftira mahiyetinde, gerçek dışı, sıkıntı ve rahatsızlık verici, gereksiz korku yaratacak materyalin üretim ve dağıtımını yapamaz.

Kullanıcı, internet ortamında dile getirdiği tüm fikir, düşünce, ifade ve yazıların kendisine ait olduğunu, Bilgi İşlem Müdürlüğü’nün hiçbir şekilde sorumlu olmadığını kabul eder.

Suç teşkil edecek, yasal açıdan takip gerektirecek, ülke çapında ya da uluslararası düzeyde yasalara ters düşecek bir durum yaratan ya da teşvik eden, her tür ve şekilde iletim dahil olmak üzere; her türlü yasadışı, tehditkar, rahatsız edici, hakaret, küfür veya iftira içeren, küçük düşürücü, kaba, pornografik, rahatsız edici ya da ahlaka aykırı olan web sitelerini ziyaret etmek yasaktır.

# İnternet Üzerinden Peer to Peer – P2P Ağ Oluşturma ve Dosya Paylaşımı

İnternet üzerinden P2P ağlara katılım ve dosya paylaşımı yasaktır. Eğer internet üzerinden P2P ağ oluşumu veya dosya paylaşımı iş amaçları için gerekli ise, Bilgi İşlem Müdürü’nün yazılı onayı alınmalıdır.

# MESAJLAŞMA KULLANIMI

# İzin Verilen Mesajlaşma Çözümleri

İş amaçlı kullanılabilecek mesajlaşma çözümleri, şirket e-postası ve anında mesajlaşma sistemleridir. Her Narlıdere Belediyesi kullanıcısına “adsoyad@narlidere-bld.gov.tr” formatlı bir e-posta adresi verilmektedir.Narlıdere Belediyesi için çalışan 3. parti firma çalışanlarına “adsoyad@narlidere-bld.gov.tr” uzantılı bir e-posta adresi verilemez.

Emeklilik veya istifa yolu ile ayrılan çalışanlar ayrılış tarihleri itibariyle “adsoyad@narlidere-bld.gov.tr” uzantılı eski e-posta adresi ile mesaj gönderemezler. Ancak iş sürekliliğinin olumsuz etkilenmemesi açısından dışarıdan eski adreslere gelen mesajların geçici bir süre ile alınması Bilgi İşlem yöneticisinin vereceği karara bağlı olarak mümkün olabilir.

# E-posta Kullanımı

Elektronik mesajlaşma kuralları, yazılı ve yüz yüze olmak üzere aynı özellikleri taşırlar. Yüz yüze iletişimin mümkün olmadığı durumlarda elektronik mesajlaşma kullanılır. Adres listesinde yer alan gruplara mesaj gönderilirken alıcıların tamamının gönderilecek mesajı almak isteyeceğinden emin olunmalıdır. Mesajın doğrudan muhatabı ve gerekiyor ise aksiyon alması gereken kişiler “TO” alanına, bir aksiyon alması gerekmeyen ve sadece bilgilendirme amacı ile mesaj gönderilen kişiler “CC” alanına yazılmalıdır. Mesajlara eklenecek dosyaların büyüklükleri önemlidir. Özellikle grafikler ve resimler çok yer tutacağından dikkat edilmeli ve mümkünse göndermeden önce sıkıştırılmalıdır. Elektronik mesajlar için belirlenmiş sınır 50 Mb’dır. Bu büyüklüğü geçen elektronik mesajlar yollanamayacak ve alınamayacaktır.

Narlıdere Belediyesi, e-posta sistemini kullanırken aşağıdaki koşulları kabul etmiş sayılırsınız.

Aşağıda sayılan koşullara uyulmaması halinde sorumluluk tamamen kullanıcıya aittir. Bu nedenle Bilgi İşlem Müdürlüğü; kaynaklanabilecek doğrudan veya dolaylı sonuçların yol açabileceği hiçbir zarardan sorumlu değildir. Birimlerde görevli tüm personeller kendilerine verilen e-posta ve bu e-posta ile gönderilen içerikten sorumludur.

**GeneL Kurallar**

* Kullanıcı, hizmet hakkının sadece kendisine ait olduğunu, bu hakkın kullanımına ilişkin özel ve gizli şifresini ve kullanıcı adını ve/veya kodunu başkasına kullandırmayacağını ve devretmeyeceğini, başkası tarafından öğrenilme şüphesi dahi olsa derhal değiştireceğini, aksi takdirde yapılan tüm işlemlerin sorumluluğunun kendine ait olacağını, kendisi kullanmadığı iddiasında bulunmayacağını kabul eder.
* Kullanıcı, E-posta ile dile getirdiği tüm fikir, düşünce, ifade ve yazıların kendisine ait olduğunu, Bilgi İşlem Müdürlüğü’nün hiçbir şekilde sorumlu olmadığını kabul eder.
* Kullanıcı, göndereceği elektronik posta mesajlarında; hakaret, pornografi, toplumun genel ahlak anlayışına aykırı ve diğer yasadışı herhangi bir amaç güden aktivitelerde bulunamaz.
* Narlıdere Belediyesi’ne ait sistem ve ağ güvenliğinin ihlal edilmesi, servis kalitesini etkileyecek, bozacak, karışıklık yaratacak faaliyetlerde bulunulması yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Bilgi İşlem Müdürlüğü bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa yasa uygulayıcı ile işbirliği yapar.

# Mesajlaşma Mahremiyeti

Narlıdere Belediyesi içerisinde kullanılan anlık mesajlaşma sistemi üzerinden yapılan tüm elektronik iletişimin kişiye özel olacağı garantisi verilemez. Kullanıcılar elektronik ortamdaki her türlü iletişimlerinin kötü niyetli kişilerin saldırılarına maruz kalabileceğini bilmelidirler. Bu nedenle kritik kurum bilgilerini içeren iletişimin, hem iletişim hattında hem de ulaştığı alıcı noktasında gizlilik ve bütünlüğünün korunabilmesi için şifreleme yöntemleri ile yapılması gereklidir. Kullanıcılar gizlilik ihtiyacı olan iletişimleri için teknik çözüm konusunda Bilgi İşlem Müdürlüğüne başvurmalıdırlar.

# Kimlik Hırsızlığı (Phishing) Saldırıları, Mesaj Ekleri Politikası, İstenmeyen (Spam) E-postalar ve Yasak Kullanımlar

Narlıdere Belediyesi, kurum kullanıcılarının e-posta adreslerine gelen istenmeyen e-posta ve virüs eklentilerine karşı teknik önlemler uygulamaktadır. Buna rağmen son kullanıcılar saldırı yöntemlerinin yeni olması ya da korunma yöntemlerinin hatalı çalışabilmesi veya bazı durumlarda bu yöntemlerin bazı saldırılara karşı yetersiz kalmaları sebebi ile genel e-posta güvenlik kurallarına uymalıdır. Kullanıcıların;

* Kişileri rahatsız edici, müstehcen, politik ve dini propaganda yapan veya kurumsal değerlere aykırı içerikler taşıyan elektronik mesajları yaratmak veya dağıtmak ve bu sitelerdeki diyaloglarda yer almak,
* İnternet aracılığı ile rastgele, tehdit edici ve saldırgan yazı/mesaj göndermek,
* Şans mektupları veya zincir mektuplarını içeren mesajları yaratmak veya dağıtmak,
* Telif hakkı yasalarına uygun olmayan bilgileri içeren mesajları ve eklerini oluşturmak veya dağıtmak,
* Kaynağının izni olmadan bir mesajı ve ekini değiştirerek veya kopyalayarak dağıtmak,
* Şifre güvenliğine aykırı olarak şifrelerin herkes tarafından görülmesini sağlamak gibi aktivitelerde bulunmaları yasaktır.

Bunlara ek olarak, e-posta içinde gelen bağlantılara tıklayarak (kullanıcı kodu ve parolası başta olmak üzere) kişisel bilgilerini girmemeli, HTML formatında gelen e-postalardaki resimleri görüntülemek için indirmemeli, e-posta içindeki herhangi bir bağlantıya tıklamamalı, güvenilir kaynaklardan gelmeyen e-postalardaki eklentileri indirmemeli ve gönderen kısmındaki bilginin yanıltıcı olabileceğini unutmamalıdır.

E-posta içindeki herhangi bir bağlantıya tıklamak veya e-posta içindeki resimleri görüntülemek üzere indirmek, istenmeyen e-postanın var olan bir kullanıcıya ulaştığı bilgisini saldırgana verir. Ayrıca resim indirme veya linki ziyaret etme işlemi resim işleyici uygulamalardaki açıklardan dolayı bilgisayarınızın zarar görmesine veya “Cross Site Scripting – XSS” adı verilen istemci tarafında çalışan betiklerin kötü niyetle kullanılmasına ve oturum hırsızlığı saldırılarına imkân verebilir.

# 6.5 E-Posta Yedekleme İşlemleri

Kurumsal mailler pop3 protokolü üzerinden sağlanmaktadır. Maillerin yedeklerini almak kullanıcının sorumluluğundadır.

# OFİS EKİPMANLARI, BASILI DOKÜMANLAR VE TAŞINABİLİR VERİ SAKLAMA ARAÇLARI

# Yazıcılar ve Fotokopi Makineleri

Kullanıcılar gizlilik gereksinimi yüksek bir dokümanı yazdırırken, bilginin yetkisi olmayan kişiler tarafından görülmesini veya ele geçirilmesini engellemek için yazdırma esnasında yazıcının yanında bulunmalıdır. Kullanıcılar, gizlilik gereksinimi olsun veya olmasın makineye sıkışmış dahi olsa orijinal ve kopya doküman nüshalarını yazıcı ve fotokopi makinelerinde terk etmemelidirler. Telif hakkı Narlıdere Belediyesi’ne ait olmayan dokümanların Narlıdere Belediyesi yazıcı ve fotokopi makinelerinde çoğaltılması yasaktır. Yazıcı ve fotokopi makineleri kişisel işler için kullanmak yasaktır.

# İhtiyaç Kalmayan Basılı Dokümanların İmha Edilmesi

İmha edilecek tüm hassas dokümanlar, doküman parçalayıcı makine ile parçalanmalıdır. Gizlilik gereksinimi olmayan diğer dokümanlar ofis içi veya dışında rastgele bölgelerde bırakılmamalı ve kağıt atık geri dönüşüm kutularına atılmalıdır.

# Taşınabilir Veri Saklama Araçları

Taşınabilir olmaları nedeniyle çalınma tehdidiyle karşı karşıya olan taşınabilir veri saklama araçlarının, özellikle kritik veri barındırmaları durumunda fiziksel güvenliği kullanıcıların sorumluluğundadır. Verinin saklanma ihtiyacı sona erdiğinde veriler saklama cihazından silinmeli, CD gibi tek kullanımlık medyaların kullanımı durumunda medya imha edilmelidir.

# İZLEME VE KAYIT AKTİVİTELERİ, MAHREMİYET

# Narlıdere Belediyesi Sistemlerinde Saklanan Narlıdere Belediyesi Sistemleri Aracılığı ile İletilen Verilerin Mahremiyeti

Narlıdere Belediyesi, kendi sistemleri üzerinde saklanan ve Narlıdere Belediyesi sistemleri aracılığı ile iletilen tüm bilgileri inceleme hakkını saklı tutar. Kullanıcılar, Narlıdere Belediyesi sistemleri üzerinde saklanan veya Narlıdere Belediyesi sistemleri aracılığı ile iletilen kişisel bilgileri hakkında mahremiyet beklentisi içinde olmamalıdır.

# Kayıtlar

Narlıdere Belediyesi, iç ve dış saldırılara karşı katmanlı güvenlik anlayışı gereği geliştirdiği loglama (denetim izi tutma) stratejisini uygulamaktadır. Bu loglama stratejisi özellikle kullanıcı faaliyetlerini izleme amacına yönelik olmamakla birlikte, kullanıcıların uygulamalar ve Narlıdere Belediyesi bilgi ağı üzerinde gerçekleştirdiği faaliyetler kayıt altına alınmaktadır. Kullanıcılar, Narlıdere Belediyesi sistemleri üzerinde veya Narlıdere Belediyesi sistemlerini kullanarak yasal mevzuata veya kurum içi kurallara aykırı davranışlarından şüphe edilmesi halinde Narlıdere Belediyesi yönetiminin resmi talebi üzerine kullanıcıların bilgi sistemleri üzerindeki faaliyetlerinin izlenebileceğinin bilincinde olmalıdır.

# GENEL VERİ KORUMA VE SINIFLANDIRMA SORUMLULUKLARI

# Bilgi Paylaşımı, Veri Sahipliği ve Sınıflandırılması

Kurum içi bilgi paylaşımı sadece görev gereği ilgili veriye ulaşması gereken kullanıcılar arasında olabilir. Kamu kurumları ve üyeler ile bilgi paylaşımı bu irtibat görevini yerine getirmek üzere atanmış personel tarafından gerçekleştirilmelidir.

Kullanıcılar kendileriyle ilgili iş verilerinin sahibi olup, bu varlıkların korunmasından nihai olarak sorumludur. Veri sahipleri kendileriyle ilgili iş verilerinin sınıflandırılmasından ve gerektiğinde yeniden sınıflandırılmasından sorumludur. Verinin elektronik ortamda saklanabileceği gibi, basılı doküman halinde de saklanabileceği unutulmamalıdır.

# Kurumsal Verinin Saklanması

Kullanıcılar sahibi oldukları iş verilerinin yasal yükümlülükler veya iş gereklerinden doğan saklanma süre ve şart ihtiyaçlarını Bilgi Güvenliği Yöneticisi’ne bildirmekle yükümlüdür. Basılı dokümanlar üzerinde bulunan veriler de bu maddenin kapsamı içindedir. Genel prensip olarak üzerinde çalışılan dosyalar ve kritik olmayan dosyalar kişisel bilgisayarlarda saklanabilir. Ancak kritik dosyalar üzerinde çalışılmadığı durumlarda kişisel bilgisayarlara ek olarak sunucularda yedeklenmeli ve saklanmalıdır. Kullanıcılar ortak paylaşım alanları dışındaki verilerinin güvenliğinden ve yedeklenmesinden sorumludur.

# Narlıdere Belediyesi Dizüstü Bilgisayarları

Kullanıcılar, hassas kurum verilerini Narlıdere Belediyesi dizüstü bilgisayarlarında saklamaktan kaçınmalıdır. Bu cihazların kullanıcıları özellikle halka açık mekanlarda cihazlarını terk edemez ve cihazların fiziksel güvenliğini sağlamakla yükümlüdürler. Kullanıcılar kendilerine tahsis edilen dizüstü bilgisayarları kullanmadıkları durumlarda kilitli dolap veya çekmecelerde saklamalıdırlar. Uçak, otobüs gibi halka açık ulaşım araçlarında taşınabilir cihazlar baş üstü bagajlarına değil koltuk altına konulmalıdır. Havaalanı, tren ve otobüs garlarında taşınabilir cihazları güvenlik kontrollerinden geçirilirken sürekli olarak izlemeli ve göz teması kesilmemelidir. Taşınabilir cihazlar Narlıdere Belediyesi’ne uzaktan erişim için kullanılıyorsa, erişim için kullanılan kullanıcı adı ve parola bilgileri bilgisayar üzerinde herhangi bir dosya içinde saklanmamalıdır.

# Narlıdere Belediyesi Ofisi Dışına Gönderilen Bilgisayarlar ve Veri Saklama Araçları

Eğer kişisel bilgisayarlar veya bu bilgisayarlara ait depolama birimleri tamir veya hibe amacı ile kurum dışına gönderilecekse, bu bilgisayarların kullanıcıları ve Bilgi İşlem teknik personeli bilgisayar üzerinde bulunan hassas verilerin silinmesi ve gerekiyorsa yedeklenmesinden nihai olarak sorumludur.

# Narlıdere Belediyesi Ağına Uzaktan Erişim

Narlıdere Belediyesi ağına uzaktan erişmesi gereken kullanıcılar erişim için sıra dışı bir neden yoksa Narlıdere Belediyesi dizüstü bilgisayarlarını kullanmalıdırlar. Kullanıcılar uzaktan erişim araçlarını (VPN) koruma konusunda hassasiyet göstermelidir. Uzaktan erişim kimlik doğrulama için kullanılan cihazların üzerine Narlıdere Belediyesi veya kullanıcıyla ilgili bir erişim bilgisi (telefon numarası, sunucu adı, IP adresi, kullanıcı kodu, vb.) yazılmamalı / yapıştırılmamalıdır. Eğer sıra dışı bir durum için Narlıdere Belediyesi bilgisayarı dışında bir bilgisayardan uzaktan erişim yapılması gerekiyorsa Bilgi İşlem Müdürü’nün onayı alınmalıdır. Kullanıcılar, Narlıdere Belediyesi bilgisayarı dışında bir bilgisayar kullanmak zorunda olduklarında Bilgi İşlem sorumlusunun önereceği kontrolleri uygulamakla yükümlüdür (çalışılan bilgisayar üzerinde iz bırakmamak için sanallaştırma (virtualization) yazılımı kullanmak, kullanılan bilgisayarın kişisel koruma duvarının olması, şifre hatırlama seçeneğinin seçilmemiş olması, anti-virüs imzalarının ve işletim sisteminin güncel olması, vb.).

Narlıdere Belediyesi dışından, Narlıdere Belediyesi sistemine herhangi bir üçüncü partinin uzaktan erişmesi gerekiyor ise Bilgi İşlem Müdürü’nün onayı dahilinde süreli ve sadece ilgili sunuculara ait VPN erişimi tanımlanmalı ve gizlilik sözleşmesi imzalanmış olmalıdır.

# Temiz Masa, Temiz Ekran Politikası

Kullanıcılar masaları başında olmadıklarında hassas bilgi içeren basılı dokümanları masa üstünde bırakmamalıdırlar ve bilgisayar ekranlarını açık terk etmemelidirler. Hassas bilgi içeren basılı dokümanlar kullanılmadıklarında masadan kaldırılmalı ve gerekiyorsa kilit altında tutulmalıdır. Kullanıcılar kurum dışında basılı doküman, bilgisayarlar ve veri saklama cihazlarının fiziksel güvenliği konusunda kurum içerisine göre daha hassas davranmalı, asla kontrolsüz biçimde açıkta bırakmamalıdır. Kurum dışında bilgisayar ekranından veya basılı dokümanlardan hassas bilgilerin başkalarınca izlenme riskinin daha yüksek olduğu unutulmamalı, halka açık mekânlarda hassas bilgiler görüntülenmemelidir ya da bu gibi durumlarda ekran koruyucu filtreler kullanılmalıdır. Restoranlar ve bina içerisindeki ortak alanlar gibi halka açık mekânlarda iş ile ilgili konular konuşulurken dikkat edilmeli ve başka kişilerin duyabileceği durumlarda konuşma yapılmamalıdır.

# Telefon Görüşmeleri

Narlıdere Belediyesi çalışanları özellikle şirket dışında hassas bilgi içeren telefon görüşmesi yapmamaya gayret etmelidir. Hassas bilgilerin iletişimini gerektiren bir görüşme yapılması gerekiyorsa, cep telefonları diğer şahıslara / kurumlara ait telefonlara, kapalı ve yalnız bulunulan mekânlar açık ve kalabalık mekânlara tercih edilmelidir. Gelen aramalarda arayanın kimliğinden emin olunamaması halinde ya da kritik bilgilerin dağıtımını güvence altına almak için geri arama yapılarak arayanın kimlik doğrulaması yapılmalıdır.

Bu politikalara uyulmaması durumunda ilgili kişi ve yöneticileri Narlıdere Belediyesi Bilgi Güvenliği Yöneticisi tarafından uyarılacak ve tekrarı halinde kişi hakkında idari işlem yapılacaktır.

# İHLALLER VE YAPTIRIMLAR

Narlıdere Belediyesi’ne ait sistem ve ağ güvenliğinin ihlal edilmesi, servis kalitesini etkileyecek, bozacak, karışıklık yaratacak faaliyetlerde bulunulması yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Bilgi İşlem Müdürlüğü bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa yasa uygulayıcı ile işbirliği yapar.

Suç teşkil edecek, yasal açıdan takip gerektirecek, ülke çapında ya da uluslararası düzeyde yasalara ters düşecek bir durum yaratan ya da teşvik eden, her tür ve şekilde iletim dahil olmak üzere; her türlü yasadışı, tehditkar, rahatsız edici, hakaret, küfür veya iftira içeren, küçük düşürücü, kaba, pornografik, rahatsız edici ya da ahlaka aykırı olan bilgi postalamak veya iletmek yasaktır.

Kullanıcılar kurum bilgisayarlarını kullanırken tüm iş ve işlemlerinde 5846 Sayılı Fikir ve Sanat Eserleri Kanunu ile 5651 Sayılı “İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLENMESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCADELE EDİLMESİ HAKKINDA KANUN”a uygun hareket etmekle yükümlüdür.

# DİĞER HUSUSLAR

# Daha Fazla Bilgi İçin

Kullanıcılar gerektiğinde bu politikada belirtilen konular hakkında daha fazla bilgi / destek almak için Bilgi İşlem Müdürlüğüne danışmalıdır.

# KISALTMALAR VE TANIMLAR

|  |  |
| --- | --- |
| **Betik (Script)** | Uygulamaları denetlemek için kullanılan bir programlama dilidir. Betikler doğrudan kaynak kodundan çalıştırılır. İlk betik dilleri genelde yığın dilleri veya iş denetim dilleri olarak adlandırılırdı. İlk betik dilleri geleneksel düzenle, derle, bağla, çalıştır işlemlerini kısaltmak için yaratılmıştı. Bu şekilde oluşturulmuş bir dosya doğrudan işletim sistemi komut satırından çağrılarak tek adımda ardışık komutlar çalıştırılabilir. Bu tür dosyalarda güvenlik açısından kullanıcı adı ve parola bilgisinin kayıtlı olmaması gerekir. |
| **Cross Site Scripting -XSS** | Bilgisayar güvenlik açığıdır. HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır. Genelde cross site scripting açıkları, saldırganın sistemi deneme-yanılma yaparak bulması ile ortaya çıkmaktadır. Açığın bulunması ile saldırgan, başka bir alan adından, açığın bulunduğu alan adı ve sayfanın bilgilerini, oturum ayrıntılarını ve diğer nesne değerlerini çalabilir. |
| **P2P Ağ** | Peer-to-peer ya da P2P olarak tanımlanır. Peer eş, denk demektir. İki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür.  Eşler, sunucuları veya sabit bilgisayarlar tarafından merkezi koordinasyon ihtiyacı olmadan, işlemci gücü, disk depolama veya ağ bant genişliği gibi kendi kaynaklarının bir kısmını, doğrudan diğer ağ katılımcıları için kullanılabilir yapabilir. |
| **Internet Explorer Güvenlik Alanları (Security Zones)** | Internet Explorer tüm web sitelerini dört güvenlik bölgesinden birine atar: Internet, Yerel intranet, Güvenilen Siteler ve Yasak Siteler. Bir web sitesine atanan bölge, bu site için kullanılan güvenlik ayarlarını gösterir. İnternet sitelerinin dinamik içerik sunma ihtiyacı ve tarayıcıların daha fonksiyonel olmaları amacıyla Applet, ActiveX,VBScript, Java Script vb. teknolojiler geliştirilmiştir. Ancak bu fonksiyonellik zaman içinde ortaya çıkan zayıflıklar kullanılarak kötüye kullanılmış / kullanılmaktadır. |
| **İstenmeyen (Spam) E-posta** | İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi Spam olarak adlandırılır. Spam çoğunlukla ticari reklam niteliğinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacına yöneliktir. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajın alıcıları veya taşıyıcı, servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır. |
| **Jenerik / Ortak Hesap** | Sistem yazılımları ve bazı sunucu ve uygulama yazılımları varsayılan kurulumları ile belli jenerik kullanıcıları erişim kontrolü için yaratır. Bu kullanıcı hesaplarına jenerik hesaplar denir. Ortak hesap kullanımı aynı kullanıcı hesabının farklı kullanıcılar tarafından kullanılmasıdır. Bu durum hesap verebilirliğe zarar verir. |
| **Koruma Duvarı (Firewall)** | Ağ servisleri belli protokoller üzerinden, bu protokollerden ikisi olan TCP/UDP servisleri de belli portları kullanarak hizmet verir. Genel güvenlik prensibi olarak sadece gerekli sunucuların ve gerekli servislerin (protokol ve port tanımlarıyla) sunulması gerekir. Sadece gerekli servislerin sunulması, ağların güvenlik ihtiyaçlarına göre bölümlenmesi, sadece gerekli sunucuların (teknik olarak IP adreslerinin) hizmetlerine sadece istenen kullanıcılar tarafından ulaşımın sağlanması için bir kontrol cihazı (veya yazılımı) olarak koruma duvarları kullanılır. |
| **Parola (Şifre)** | Kimlik doğrulamada kullanıcı adına ek olarak kullanılan ve sadece kullanıcısı tarafından bilinmesi gereken karakterler bütünüdür. |
| **Phishing (Yemleme)** | Phishing (Yemleme) saldırısında amaç (kimlik bilgileri, kart numarası gibi) kişisel bilgilerin ele geçirilebilmesi olup, temelde bir sosyal mühendislik yöntemi olan sahte e-posta ve Web sayfalarının kullanılmasıyla gerçekleştirilir. Phishing'de dolandırıcılar, tüketicilere tanınmış bir firmadan geliyormuş izlenimi verilmiş bilgi güncelleme talebi vb. içeren e-postalar göndermektedir. Bu e-postalarda genellikle cevap için e-postanın içindeki linkin (Web sayfası için kısa yol) tıklanarak gerekli siteye geçilebileceği belirtilmektedir. Ancak, verilen talimat uygulandığında gidilen site dolandırıcılar tarafında hazırlanmış ve gerçeğini taklit eden sahte bir Web sayfası olmaktadır. Bu sahte sitede elde edilen bilgiler mahiyetine göre daha sonra çeşitli dolandırıcılık faaliyetlerinde kullanılabilmektedir. Phishing yönteminde bankaların kimliğinin kullanmasının yanında mağazalar veya e-ticaret kurumlarının ve İnternet servis sağlayıcıların kimliklerinin de kullanıldığı görülmektedir. |
| **Sanallaştırma (Virtualization) Yazılımları** | Sanallaştırma yazılımları bir işletim sistemi yazılımını veya bir uygulamayı üzerinde çalıştığı donanım veya işletim sisteminden soyutlar. İşletim sisteminin soyutlanmasındaki temel amaç aynı anda tek donanımın kaynakları kullanılarak birden fazla işletim sisteminin ve doğal olarak hizmetlerinin kullanılmasıdır. Teknik olarak işletim sistemi sanallaştırma yöntemi ile aynı yöntem kullanılmamakla birlikte sanallaştırma desteği sağlayan uygulamalar da o uygulama ile yapılan işlemlerin geri kalan sistem dosyalarına etki etmesini engeller ve uygulama kapatıldığında kullanım sırasında gerçekleşen tüm değişiklikler yok olur. Böylece o bilgisayar üzerinde yapılan işlemlerin başkaları tarafından öğrenilmesine yol açacak kalıntıların bulunmaması sağlanmış olur. |
| **Anti-Virüs ve Virüs İmzaları** | Genel olarak kötü niyetli yazılım (malware) olarak adlandırılan virüs, trojan, worm, spyware ve adware yazılımlarının ortak noktası bilgisayar kullanıcılarının (veya daha genel tanımıyla sistem sahiplerinin) bilgi ve onayı olmadan sistemlere girme, bilgi çalma veya zarar verme amacına yönelik olarak yaratılmış olmalarıdır. Virüsler kendilerini kopyalamak için başka bir çalıştırılabilir dosyaya kendini eklemeye ihtiyaç duyarken worm kendi başına ağ üzerinden diğer bilgisayarlara bulaşabilir. Trojan, genel olarak farklı ve kullanıcının isteyerek yüklediği bir uygulamaya eklenip, istenen uygulamanın çalıştırılması ile bulaşır. Spyware bulaştığı bilgisayarda yapılan aktiviteleri kaydedip, başka bir sisteme kullanıcının bilgi ve onayı olmadan gönderir. Adware bulaştığı bilgisayara istenmeyen pazarlama materyallerini indirir ve gösterir. Diğer kötü niyetli yazılımlar arasında rootkit’ler, backdoor’lar, bot’lar, keylogger’lar ve dialer’lar sayılabilir. Anti-virüs yazılımları bu tür yazılımları erişim sırasında veya taramalar sırasında saptar ve günümüzde vazgeçilmez bir güvenlik katmanı oluşturur. Anti-virüs yazılımları kötü niyetli yazılımları tespit etmek için birer virüs imza veritabanı kullanır. Sürekli olarak yeni kötü niyetli yazılımlar ortaya çıktığından bu imzaların güncelliği son derece önemlidir. |