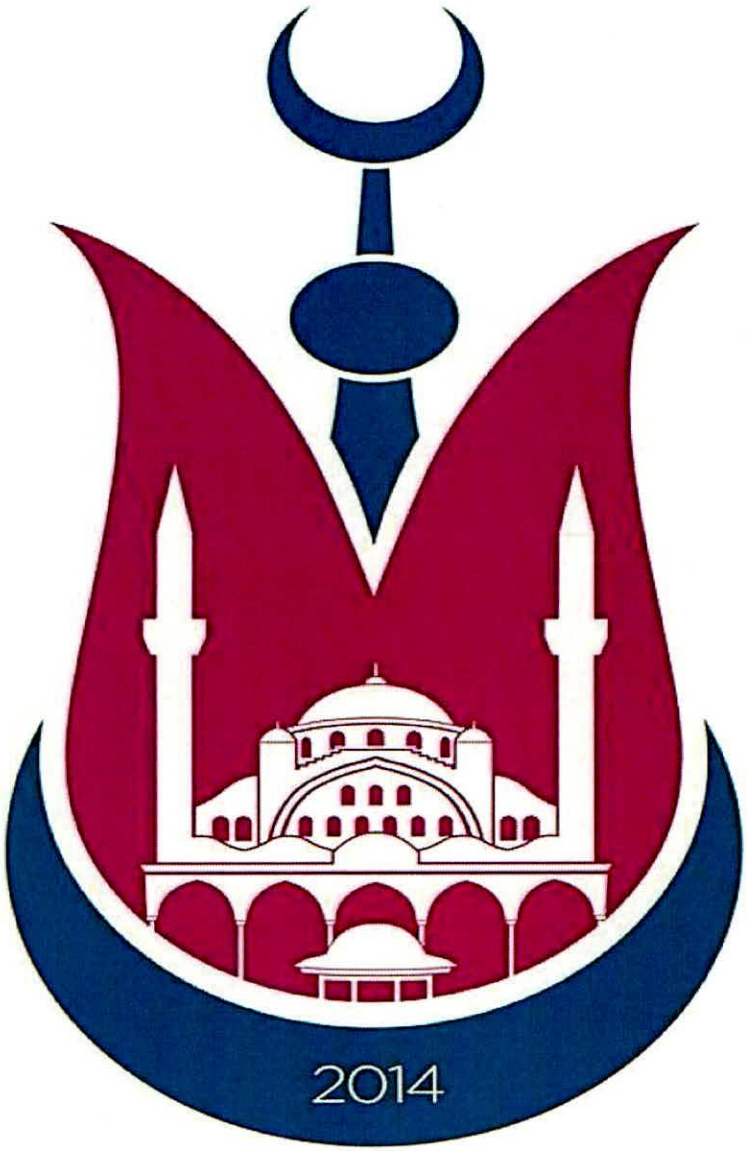

ŞEHZADELER BELEDİYESİ

BİLGİ GÜVENLİĞİ POLİTİKASI

A. Genel Amaç

Bilgi güvenliği politikasının amacı, Şehzadeler Belediyesi'nin bilgi varlıklarını korumak, bu varlıkların gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak ve bu amaç doğrultusunda gerekli önlemleri alarak riskleri minimize etmektir. Bu politikanın temel hedefleri şunlardır:

- **Gizlilik**: Bilginin yetkisiz kişilerce erişilmesini önlemek.
- **Bütünlük**: Bilginin doğruluğunu ve tamlığını korumak, yetkisiz değişiklikleri önlemek.
- **Erişilebilirlik**: Bilginin gerektiğinde yetkili kullanıcılar tarafından erişilebilir olmasını sağlamak.

Bilgi güvenliği politikası ayrıca yasal ve düzenleyici gereksinimlere uyumu sağlamayı, güvenlik ihlallerine karşı önlemler geliştirmeyi ve çalışanların bilgi güvenliği farkındalığını artırmayı da hedefler. Bu politikalar, bilgi varlıklarının korunmasını sağlamak için stratejiler, prosedürler ve sorumluluklar belirler.

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. Bilgi Güvenliğinin Çerçevesi

Şehzadeler belediyesinde kurumun bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes için;

- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kurum bilgilerinin gizliliğini korur.
- Bilgi güvenli ortamlarda yedeklenir.
- Risk düzeylerine göre güvenlik önlemleri alınır.
- Bilgi güvenliği ihlalleri raporlanır ve gereken tüm aksiyonlar alınır.
- Kurum içi bilgi kaynakları bağlı bulunduğu mevzuatta veya yaptığı sözleşmelerde açıkça belirlenen haller dışında üçüncü kişilerle hiçbir surette paylaşılmaz.
- Kurum bilişim kaynakları T.C. yasalarına, bunlara bağlı kanun ve yönetmeliklere aykırı faaliyetler amacı ile kullanılamaz.

D. Politika İhlali ve Yaptırımları

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, ilgililer hakkında adli ve idari yasal işlemler yapılabilecektir.

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.

Bilgi Güvenliği gereklerinin yerine getirilmediği, politika ve prosedürlerin ihlal edildiği durumlarda disiplin süreci işletilecektir. Güvenlik ihlali gerçekleştirdiği kesinleşen personel için bağlı bulunduğu mevzuat çerçevesinde;

- Uyarı,
- İhtar,
- Para cezası,
- Geçici uzaklaştırma,
- Kesin uzaklaştırma,
- Tazminat davası açma,
- Açılan tazminat davalarının sonuçlarının rücu edilmesi,
- Cezalarının birinin veya birden fazlasının uygulanması yaptırımları uygulanabilecektir.

Sürdürülebilirliği sağlamak için bilgi güvenliği ihlalleri kayıt altına alınacak, kayıt altına alınan Bilgi Güvenliği ihlallerine bağlı olarak düzeltici-iyileştirici faaliyet planlanarak takip edilecektir.

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

1. İnternet Kullanım Politikası

- 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.
- Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.
- Kurum bilgisayarlarında tüm kullanıcıların, internet ve program erişim yetkilendirmelerinin, yürütülen işler göz önünde bulundurularak yapılması sağlanacaktır.
- İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek ve bilgisayarlarda saklamak yasaktır.
- İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz kullanılamaz.
- Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
- 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 dâhilinde gerçekleştirilebilecektir.
- Bilgi İşlem Müdürlüğü, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir. Gerekli durumlarda internet üzerinde kısıtlamalar yapabilir.

2. E-posta Güvenliği

- Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Kişisel kullanım için İnternet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
- Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, fikri mülkiyet içeren malzeme vb.) gönderemezler.
- Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
- Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
- Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.
- 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.
- Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.
- Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre (kişisel klasörler) çekilmelidir.
- 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.
- 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.
- Altı ay süre ile kullanılmayan e-posta kutuları Bilgi İşlem Müdürlüğü tarafından kaldırılabilir. Kurumdan ayrılan personel kurumsal e-posta sistemini kullanamaz. E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma, işten ayrılma sebepleriyle kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem Müdürlüğüne en kısa zamanda bildirilmesi gerekmektedir.

3. Antivirüs Politikası

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

4. Şifre Kullanım ve Belirleme Kuralları

- Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az üç ayda bir değiştirilmelidir.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Şifreler başkası ile paylaşılmamalı, kâğıtlara ya da elektronik ortamlara yazılmamalıdır.
- Şifrelemede, küçük ve büyük karakterlere (örnek, a-z, A-Z), hem digit hem de noktalama karakterleri ve ayrıca harflere (örnek, 0-9,.!'^+%&/()=?_;*) sahip olmalıdır.
- Aynı harfin farklı karakterlerle değiştirilmesi (örneğin, "a" yerine "@" kullanmak) şifrenin karmaşıklığını artırabilir.
- Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
- Aile isimleri kullanılmamalıdır.
- Herhangi bir kişiye telefonda şifre verilmemelidir.
- E-posta mesajlarında şifre yazılmamalıdır.
- Şifreler aile bireyleriyle paylaşılmamalıdır.
- Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
- Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.

5. Genel Kullanım Politikası

- Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.
- Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
- Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Müdürlüğüne haber verilmelidir.
- Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.
- Port veya ağ taraması yapılmamalıdır.
- Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.
- Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.
- Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Müdürlüğünü onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
- Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.
- Kurum içi bilgisayar yer değişikliği yapıldığında mutlaka bilgi işlem müdürlüğüne bilgi verilmelidir.

- Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD' leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.
- Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
- Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliği ile sorumludur.
- 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.
- Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
- Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- Kurumda Bilgi İşlem Müdürlüğünün bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb.) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.
- 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.
- Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
- Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Müdürlüğüne haber verilmelidir.
- Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.

Şehzadeler Belediyesi yönetimi olarak **Bilgi Güvenliği Politikası**'nın uygulanmasında kontrolünde ve güvenlik ihlalleri durumunda gerekli yaptırımın sağlanmasında yönetim tarafından desteklenerek takip edileceğini beyan ederim.

Hakan ŞİMŞEK
Belediye Başkanı A.
Belediye Başkan Yardımcısı