KARABAĞLAR BELEDİYESİ
İZMİR

T.C.
KARABAĞLAR BELEDİYESİ
BİLGİ İŞLEM MÜDÜRLÜĞÜ

BİLGİ GÜVENLİĞİ POLİTİKALARI KILAVUZU

2016

1. ÖNSÖZ

A. BİLGİ GÜVENLİĞİ

A.1. TEMEL İLKELER

A.1.1. Bilgi Güvenliği Politikası
A.1.2. Bilgi Güvenliği Organizasyonu
A.1.3. Bilgi Güvenliği İhlâl Yönetimi
A.1.4. Bilgi Güvenliği Denetimleri
A.1.5. Bilgi Güvenliği Politikaları Kılavuzu
A.1.6. Kılavuzun Uygulanması
A.1.7. Bilgi Güvenliği Eğitimleri
A.1.8. Bilgi Güvenliği Standartları

B. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

B.1.RİSK NEDİR
B.1.1. Riskin tanımı
B.1.2. Risk türleri
B.1.3. Risk ve risk yönetimi
B.1.4. Risk yönetimi nedir / ne değildir?
B.1.5. Kurumsal risk yönetimi

B.2 BT RİSK YÖNETİMİ
B.2.1 Standart Risk Sınıfları
B.2.2. Risk Yönetim Stratejisi
B.2.2.1. Engeller
B.2.2.2. BT Risk Yönetimi Stratejisi
B.2.2.3. Zayıflık-Tehdit Örnekleri
B.2.2.4. Zayıflık ve Tehditlerin Kontrolle Eşleştirilmesi

B.3. SORUMLULUKLAR
B.3.1. Üst Yönetim
B.3.2. Chief Information Officer(CIO)
B.3.3. Sistem ve Bilgi Sahibi
B.3.4. İş Yöneticileri
B.3.5. Bilgi Güvenliği Yöneticileri
B.4. BT RİSK YÖNETİMİ KATEGORİLERİ
B.4.1. BT Risk Alanları
B.4.1.1 BT Yönetişim/Strateji Riski
B.4.1.2 BT Beceri/İnovasyon Riski
B.4.1.3 BT Mimari Riski
B.4.1.4 İş Sürekliliği Riski
B.4.1.5 Uyum / Yasa Riski
B.4.1.6 BT Kaynak Riski
B.4.1.7 Tedarikçi Yönetimi Riski
B.4.1.8 Üçüncü Taraflarla İlişki Riski
B.4.1.9 Proje/Geliştirme Riski
B.4.1.10 Değişiklik Gerçekleştirme Riski
B.4.1.11 BT İtibar/Vatandaş Memnuniyet Riski
B.4.1.12 Bilgi Riski
B.4.1.13 BT Güvenlik Riski
B.4.1.14 Online / Web Riski

B.5. BT RİSK KATEGORİLERİ
B.6. BT RİSKLERİNİN İŞ RİSKLERİ İLE İLİŞKİLENDİRMESİ
B.6.1. Risk Etki Kategorileri
B.6.1.1. Operasyonlar
B.6.1.2. Teknoloji
B.6.1.3. Yasal
B.6.1.4. İtibar
B.7. BT RİSK YÖNETİMİ YAŞAM DÖNGÜSÜ
B.7.1. 1.Aşama Bt Altyapı Süreçlerinin Anlaşılması
B.7.2. 2.Aşama-Bt Risk Modelinin Geliştirilmesi
B.7.2.1. BT Yönetişimi
B.7.2.2. BT Strateji Planlama
B.7.2.3. Mimari
B.7.2.4. Proje Yönetimi
B.7.2.5. BT Operasyonları
B.7.2.6. Süreklilik Yönetimi
B.7.3. 3.Aşama - Riskin Ölçeklendirilmesi
B.7.3.1. Risk Faktörleri
B.7.3.2. Risk Değerlendirmesi
B.7.4. 4.Aşama – Risk Profilinin Oluşturulması
B.7.5. 5.aşama – Takvim ve Kaynak Belirlenmesi

B.8. BT RİSK YÖNETİMİNİN TEKNOLOJİK BEKLENTİLERİ
B.9. RİSK KAPSAMININ BELİRLENMESİ
B.10. OLAY TESPİTİ
B.11. RİSK YANITLAMASI
B.12. RİSK AKSİYON PLANININ OLUŞTURULMASI VE İZLENMESİ
B.13. BELEDİYE BİLGİ SİSTEMLERİ YÖNETİMİNDE ESAS ALINACAK İLKELER

C. POLİTİKALAR

C.1. İnsan Kaynakları ve Zafiyetleri Yönetimi
C.2. Fiziksel ve Çevresel Güvenlik
C.3. Ekipman Güvenliği
C.4. İşletim Sistemleri ve Son Kullanıcı Güvenliği
C.4.1. İşletim Sistemleri Güvenliği
C.4.2. Son Kullanıcı Güvenliği
C.5. Parola Güvenliği
C.6. Kriptolama Yönetimi
C.7. İnternet ve Elektronik Posta Güvenliği
C.8. Sunucu ve Sistem Güvenliği
C.9. Ağ Cihazları Güvenliği
C.9.1. Ağ Cihazları Güvenlik Politikası
C.9.2. Kablosuz Ağlar Güvenliği
C.10. Mal ve Hizmet Alımları Güvenliği
C.11. Uygulama Yazılımları Güvenlik Yönetimi
C.11.1. Yazılım Geliştirme Politikası
C.11.2. Belgelendirme Politikası
C.12. Güvenlik Yazılım ve Donanımları Yönetimi
C.13. Bilgi Güvenliği Teknolojileri Güvenliği
C.13.1. Yazılım Güvenliği
C.13.2. Donanım Güvenliği

C.14. Mobil Cihazlar Güvenliği
C.15. İletişim ve İşletim Güvenliği
C.16. Kullanıcı Hesabı Açma, Kapatma Yönetimi
C.17. Erişim Yönetimi ve Erişim Kaydı Tutulması
C.17.1. Erişim Yönetimi
C.17.2. Kayıt Tutulması (Log tutulması)
C.18. Uzaktan Erişim Yönetimi
C.19. Acil Erişim Yetkilendirme Yönetimi
C.20. Veri Merkezi Standartları ve Yönetimi
C.21. Veri Tabanı Güvenliği
C.22. Kaydedilebilir Taşınır Materyaller Güvenliği
C.23. Bilgi Sistemleri Edinim Geliştirme ve Bakımı
C.24. Yedekleme ve İş Sürekliliği Yönetimi
C.24.1. Veri Yedekleme
C.24.2. İş Sürekliliği Yönetimi
C.25. Bilgi Kaynakları Atık ve İmha Yönetimi
C.26. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri
C.27. Değişim Yönetimi
C.28. İhlal Bildirim ve Yönetimi
C.29. Bilgi Güvenliği İzleme ve Denetleme Yönetimi
C.30. Bilgi Güvenliği Testleri
C.31. Acil Durum Yönetimi
C.32. Bilgi Güvenliği Ulaştırma Güvenliği Yönetimi
C.33. Sosyal Mühendislik Zafiyetleri
C.34. Sosyal Medya Güvenliği

D.KISALTMALAR

E.SÖZLÜK

F. KAYNAK

ÖNSÖZ

Günümüzde kurumlar bilgilerinin büyük bir kısmını elektronik ortamda bulundurmakta ve bu bilgileri bilişim sistemleri altyapısı kullanarak işlemektedir. İş ve işlemlerin elektronik ortama taşınması, kamu hizmetlerinin etkinleştirilmesi, yasa dışı faaliyetlerin tespit edilebilmesi ve önlenmesine yönelik olarak kişisel bilgilerin de elektronik ortamda bulunması ve işlenmesi yoğun bir şekilde artmıştır. Ancak bu durum, kişisel bilgilerin sahiplerinin isteği dışında ilgisiz ve yetkisiz tarafların eline geçmesi, kişisel bilgi sahibini rahatsız edecek veya onlara zarar verecek şekilde yasa dışı olarak kullanılması ve kişi mahremiyetinin ihlali tehlikesini de doğurmaktadır. Dolayısı ile gelişen bilişim teknolojileri bilgi güvenliği olgusunu da beraberinde önce ihtiyaç sonra zorunluluk haline getirmiştir.

Bilgi güvenliği politikaları, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür.

A. BİLGİ GÜVENLİĞİ

Bilgi Güvenliği kurumun bilgi varlıklarının aşağıdaki özelliklerinin korunması olarak tanımlanır:

a) Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması,

b)Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması,

c)Kullanılabilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması.

A.1. TEMEL İLKELER

- Tüm Müdürlükler kendi sorumluluk alanlarındaki veri işleme ve güncelleme işlemleri ile ilgili alanlara veri işleyecek kişilerden ve yetkilendirmelerinden sorumludurlar.
- Her kullanıcı tamim ve taahhütname ile gönderilen çalışma alanları ile ilgili hususlara uymak ile yükümlüdür.
- Kullanıcı, güvenlik tehditlerini bilmek, önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmekten sorumludur.
- Kullanıcılar, bilgi sistem ve ekipmanlarının kullanımında birbirlerinin haklarına saygı göstermekle yükümlüdürler.
- Kullanıcı, idarece yapılmış olan risk değerlendirmelerinde kendileriyle ya da çalışma alanlarıyla ilgili öngörülen tedbirlere uymak zorundadır.
- Kullanıcı, güvenliği, bilgi sistem ve ağlarının önemli bir unsuru olarak değerlendirmelidir.
- Kurumlar hedeflenmek sureti ile içerden ya da dışarıdan yapılacak siber saldırılara karşı kurumsal sorumluluk ve yetkiler çerçevesinde gerekli tedbirler alınmalıdır.
- İdare bilgi güvenliği yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.

İdare, bilgi sistem ve ağlarının güvenliklerini incelemeli ve yeniden değerlendirmelidir. İnceleme ve yeniden değerlendirme neticesinde, güvenlik ile ilgili politika, uygulama, önlem ve prosedürlerde gerekli değişiklikleri zamanında yapmakla yükümlüdür.

A.1.1. Bilgi Güvenliği Politikası

Belediyemiz, T.C. Anayasası ve kanunlar çerçevesinde yürütmekte olduğu iş ve işlemlerin işleyen süreçlerinde ilçemiz sınırları içerisinde belediye hizmetleri ile ilgili tüm süreçlerde çalışmakla yükümlendirilmiş bir kurum olma hüviyeti ile Belediyemizde hizmet alan her bir vatandaşa karşı sorumlulukları olan kuruluşlardan birisidir. Her bir vatandaşın Belediyemize müracaat ettiğinde en gizli ve mahrem sayılabilecek bilgilerine dair erişebilen kaydedebilen bir kuruluştur. Bu nedenle kurumumuz kayıt altına alınan bireyin her türlü veri ve bilginin kendisine emanet edilmiş bir değer olduğu düşüncesiyle kendisini bu sorumluluğun yerine getirilmesinde mükellef olarak görmektedir. Ayrıca kurumumuz kişi verilerinin ve bilgilerinin korunması ve güvenliği ile alakalı her türlü "teknik idari ve

hukuki yöntemi" kullanmak sureti ile emanetinde bulunan tüm bilgi sistemleri kaynaklarını "bilgi güvenliği ana politikası çerçevesinde" korumakla ve bu hususta tüm tedbirleri almakla yükümlü olduğunun bilincindedir.

Tüm belediyemizde üretilen bilginin de en üst seviyelerde güvenlik anlayışı içerisinde korunması gerektiği bilinci ile hareket eden Karabağlar Belediyesi misyon ve vizyonuna bağlı kalarak Bilgi Güvenliği konseptinin esasını oluşturan basılı ve elektronik ortamdaki bilgilerin yasal mevzuat ışığında ve risk metotları kullanılarak "gizlilik, bütünlük ve kullanılabilirlik" ilkelerine göre yönetilmesi amacıyla;

- Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmek,
- Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,
- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
- Bilgi Güvenliği Yönetim Sistemini sürekli gözden geçirmek ve iyileştirmek,
- Bilgi Güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmek,

ana politikalar olarak öngörülmektedir.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuyu da kapsar.

Bilgi güvenliği bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir. Kurum çalışanları, yüklenici firma personeli, stajyerler, diğer kurum çalışanları, ziyaretçiler, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir. Kullanıcılar, bilgi güvenliği bilinçlendirme sürecindeki en büyük ve önemli hedef kitledir. Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir. Yöneticiler, bilgi güvenliği bilinçlendirme ve eğitimi sürecinin gereklerine personelinin uymasını sağlamakla sorumludurlar.

Başarılı ve etkin işleyen bir bilgi güvenliği bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekmektedir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür.

Sonuç olarak Bilgi Güvenliği Politikasının amacı bilgi varlıklarını korumak, bilginin ve verinin gizliliğini sağlamak, bütünlüğünü bozmaya çalışacak yetkisiz kişilerin erişimine karşı korumak ve böylece Belediyemiz güvenini ve itibarını sarsacak durumları bertaraf etmektir.

A.1.2. Bilgi Güvenliği Organizasyonu

Bilgi Güvenliği ana sorumlusu olarak kurumumuz içerisinde Bilgi İşlem Müdürlüğü, görevlendirilmiştir.

A.1.2.1. Bilgi İşlem Müdürlüğü görevleri;

- Bilgi güvenliği politika ve stratejilerini belirler,
- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlanması amacı ile İnsan kaynakları ve Eğitim Müdürlüğü ile iletişime geçer,
- Bilgi güvenliği faaliyetleri ve kontrollerinin tüm kurum içerisinde koordine edilmesini sağlar.

A.1.3. Bilgi Güvenliği İhlâl Yönetimi

Bilgi güvenliği olaylarının rapor edilmesi;

Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan idari uygulama planı oluşturulur.

Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği ihlal raporu hazırlanır.

Güvenlik ihlaline neden olanlar hakkında, hukuki süreç başlatılır.

Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan Bilgi İşlem Müdürlüğüne mümkün olan en kısa sürede rapor ederler.

A.1.4. Bilgi Güvenliği Denetimleri

- Bilgi İşlem Müdürlüğü bilgi güvenliği denetimlerini yapar.
- Bilgi güvenliği denetimlerini yapacak personel Bilgi İşlem Müdürlüğü tarafından belirlenir.
- Senaryoları idarece önceden onaylanmak kaydıyla "bilişim güvenliği testleri" yapılabilir.
- Bilgi Güvenliği ile ilgili çalışmaların doğruluk ve güvenirliğini test etmek amacı ile danışmanlık hizmetleri ile penetrasyon testleri yaptırılır.

A.1.5. Bilgi Güvenliği Politikaları Kılavuzu

- Kılavuz; Karabağlar Belediyesi Bilgi İşlem Müdürlüğü tarafından bilgi güvenliğinin sağlanması ile ilgili; yönetsel, teknik, idari, hukuki süreçlerin tüm detaylarının yer alacağı bir doküman olarak hazırlanır.
- Kılavuzun ilk versiyonu Başkan onayı ile yürürlüğe girer, daha sonraki versiyonlar Başkan Yardımcısı onayı ile yürürlüğe konulur.
- Kılavuz; periyodik olarak, teknolojik gelişmeler paralelinde gözden geçirilerek revize edilir ve elektronik ortamda yayınlanacak bir rehber doküman olarak hazırlanır.
- Kapsam maddesinde belirtilen Belediye ve bağlı birimleri unsurları Kılavuzda yer alan hususlara uymakla yükümlüdürler. Gerekli hallerde Bilgi İşlem Müdürlüğünce teknik destek talepleri karşılanır. Belediyemiz internet ana sayfası üzerinde bilgi güvenliği alanı oluşturur. Bu alan üzerinde bilgi güvenliği konularında üretilen ulusal ve uluslararası kılavuz, rapor, bilgi notu, tez vb. dokümanlara erişim sağlar.
- Bilgi İşlem Müdürlüğü, Bilgi Güvenliği Terimleri Sözlüğü hazırlar ve internet üzerinden yayına sunar.
- Bilgi güvenliği amaçlarının gerçekleşmesi için hazırlanan başka ilgili politikalarla, standartlarla, prosedür ve talimatlarla desteklenecektir.

A.1.6. Kılavuzun Uygulanması

Kılavuzun uygulanması ile ilgili olarak; yöneticiler hazırlayacakları bilgi güvenliği planları içerisinde "Kılavuza Uyumlaşma Takvimi " hazırlar ve kılavuzun uygulanması ile ilgili gerekli idari tedbirleri alır.

A.1.7. Bilgi Güvenliği Eğitimleri

Belediyemizde yapılacak tüm eğitimler İnsan Kaynakları ve Eğitim Müdürlüğünce planlanıp gerçekleştirilmektedir. Müdürlüğümüzce Bilgi güvenliği konusunda yapılması planlanan eğitimler İnsan kaynakları ve Eğitim Müdürlüğünden talep edilmektedir.

A.1.8. Bilgi Güvenliği Standartları

Bilgi İşlem Müdürlüğü bilgi güvenliği çalışmalarının standartlaştırılması ve çalışmalara sistematik bir anlayış entegre edilmesi yaklaşımı ile ulusal ve uluslararası bilgi güvenliği standartlarına uyumlaşma ve sertifikasyonun gerçekleştirilmesi yönünde çalışmalar yapar.