T.C.
KARABAĞLAR BELEDİYESİ
BİLGİ İŞLEM MÜDÜRLÜĞÜ

BİLGİ GÜVENLİĞİ POLİTİKALARI KILAVUZU

2016

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.

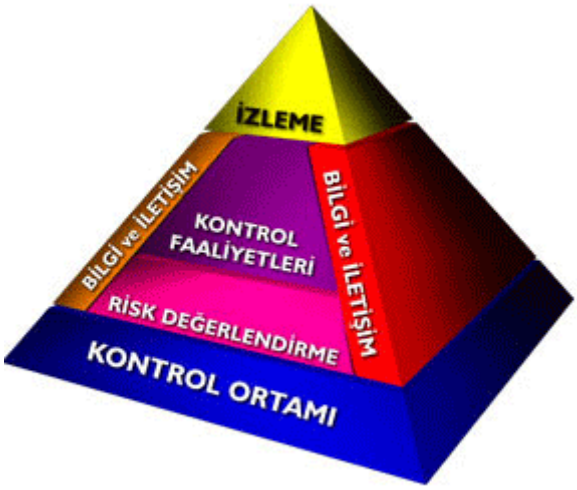
A.1.8. Bilgi Güvenliği Standartları

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.

B. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

Ülkemizde Kamu Mali Yönetim ve Kontrol Sistemini yeniden düzenleyen 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ve buna ilişkin ikincil mevzuat COSO modelini esas alan İç Kontrol Sisteminin kurulmasını hedeflemektedir.

COSO Küpü (COSO Cube): İç kontrol unsurlarının, iç kontrolün amaçları ve idarenin faaliyetleriyle ilişkisini gösterir. Birimler, hedefler ve iç kontrolün unsurları, bir küpün farklı yüzeylerini oluşturur ve ayrılmaz bir bütündür. Tüm faaliyet ve birimler; faaliyetlerin etkinliği ve verimliliği, bilgilerin güvenilirliği, mevzuata uygunluk ve kurum varlıklarının korunmasını hedeflerine ulaşmak amacıyla COSO modelinde yer alan iç kontrolün beş unsurundan yararlanır.



COSO PİRAMİDİ

Şekil 1 (COSO MODELİ)

COSO Modeli (COSO Model): COSO (The Committee of Sponsoring Organisations of the Treadway Commission) tarafından hazırlanan ve bir kurumun günlük faaliyetleri sırasında kurum içerisindeki mevcut ve olması gereken asgari iç kontrol uygulamalarının sistematik bir şekilde değerlendirilmesine imkân sağlayan bir iç kontrol modelidir. COSO Modeli iç kontrol sistemlerine ilişkin standartların temelini oluşturmaktadır. Modele göre iç kontrol sisteminin ana hedefleri; organizasyonun günlük işlemlerinde etkinlik ve verimliliği, kurum içerisinde üretilen her türlü bilginin doğruluğu ve güvenilirliğini, gerçekleştirilen işlemlerin mevzuata uygun olmasını ve kurum aktiflerinin ve varlıklarının korunmasını sağlamaktır.

COSO Pramidi (COSO Pyramid): İç kontrol unsurlarının birbirleriyle ilişkisini gösterir. Kontrol ortamı kurumun içerisinde faaliyet gösterdiği ana kontrol yapısı olup diğer unsurlara temel teşkil eder. Kontrol faaliyetleri ve risk değerlendirme yapılırken bilgi ve iletişim kanalları kullanılarak gözetimin ihtiyaç duyduğu bilgiler sağlanır. Sistem yönetim, personel ve iç denetçiler tarafından izleme yapılarak geliştirilir.

B.1.RİSK NEDİR

İşletme yönetiminde, iş süreçlerinde ve pay ve menfaat sahipleri ile ilişkilerde; eşitlik, şeffaflık, hesap verebilirlik ve sorumluluk yaklaşımıyla işletme faaliyetlerinin etkinlik ve verimliliği, raporlama güvenilirliği, düzenlemelere uygunluk, pay ve menfaat sahiplerinin hak ve çıkarlarının korunması için güvence sağlayan yaklaşım ve ilkeleri ifade eder.

B.1.1. Riskin Tanımı

- Risk, tehditlerin bir organizasyonun strateji ve hedeflerine ulaşmasında engel teşkil etmedeki etkisi ve olasılığıdır.
- Risk potansiyel bir değer kaybı ya da kazancın optimum sınırların altında kalmasıdır.
- Kısacası, risk bir şirketi mevcut varlıklarını korumaktan ya da hisse değeriniarttırmaktan
- Alıkoyan her şeydir.
- Risk pozitif ve negatif sonuçları kapsar. Pozitif sonuçlar doğuran risk fırsatları,negatif sonuçlar doğuran risk tehditleri olarak değerlendirilir.
- Kurum getiri için riskleri göze almalıdır.

B.1.2. Risk Türleri

- Getirisi olmayan risk (Unrewardedrisk)
- İyi yönetildiğinde herhangi bir getiri sağlamayan, ancak kurumların özellikle yasalarla düzenlenmiş yükümlülüklere uyması ve belirli sorumlulukların yerine getirilmesi ile ilgili risklerdir. Finansal tabloların yanlış oluşturulması ya da mevzuata aykırı hareket edilmesi bu tür risklere örnektir.
- Getirisi olan risk (Rewardedrisk)
- Gerektiği gibi yönetildiğinde kuruma fayda ya da çıkar sağlayan risklerdir. Birleşme ve devralmalar, yeni ürün geliştirme, yeni piyasa ve iş modelleri bu risk tipine örneklerdir.

B.1.3. Risk ve Risk Yönetimi

RİSK
Risk kurum genelindeki seçimler ve kararlar sonucunda karşılaşılacak kayıp ve kazançlara ilişkin belirsizliklerdir.

RİSK YÖNETİMİ
Alınan kararların etkilerini belirleme,ölçeklendirme,azaltma ve ölçmeyi mümkün kılarak organizasyonlarda istikrar sağlayan bir mekanizmadır..

B.1.4. Risk Yönetimi Nedir / Ne Değildir?

Risk Yönetimi:

Kontrol fonksiyonudur

- İcranın bir parçasıdır
- Stratejik karar almanın ilk adımıdır
- Kültür değişimidir
- Aynı zamanda bir fırsat yönetimidir

Ancak,

- Yeni veya bir ölçüye kadar yapılmayan
- Sadece olumsuzlukları öne çıkaran
- Pratik olmayan öneriler geliştiren
- İmaj maksatlı yapılan
- Kendi başına problemleri çözebilecek bir fonksiyon

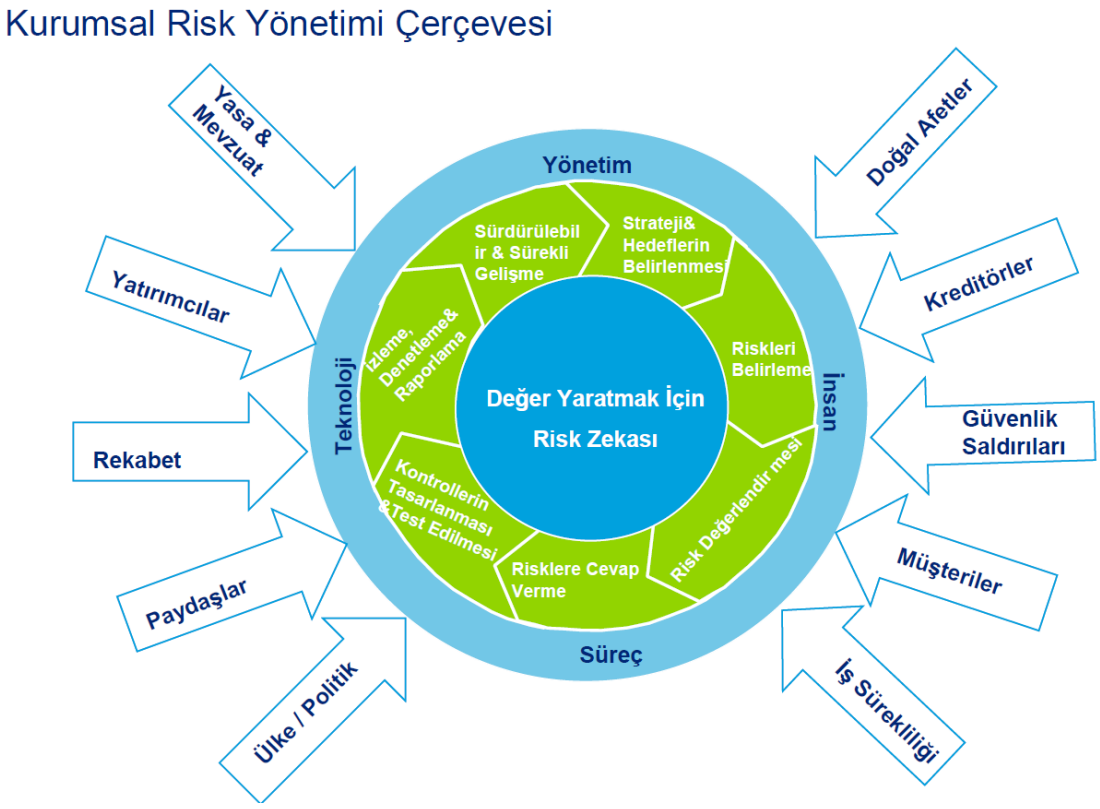
DEĞİLDİR.

B.1.5. Kurumsal Risk Yönetimi

"Kurumsal Risk Yönetimi, kurumu etkileyebilecek potansiyel olayları tanımlamak, riskleri kurumun risk alma iştahına uygun olarak yönetmek ve kurum hedeflerine ulaşması ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; kurumun yönetim kurulu, üst yönetimi ve diğer tüm çalışanları tarafından etkilenen ve stratejilerin belirlenmesinde kullanılan ve kurumun tümünde uygulanan sistematik bir süreçtir."

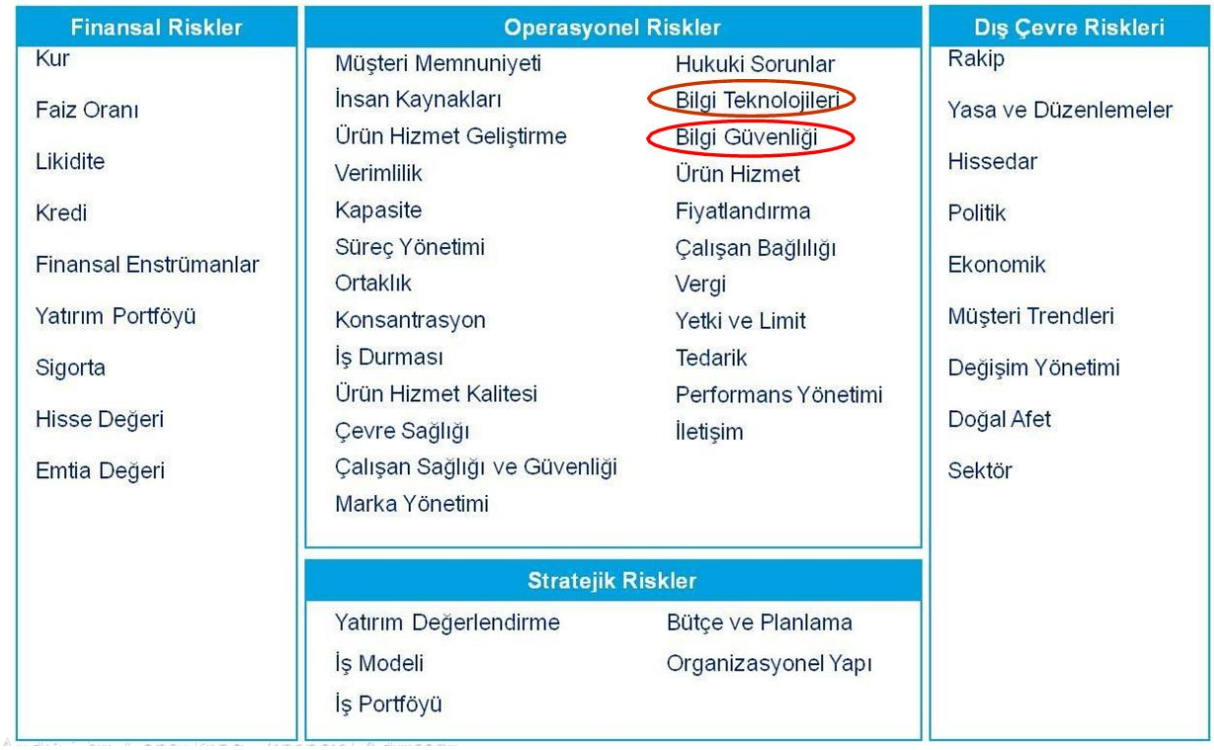
Kurumsal Risk Yönetimi

- Kurumsal risk yönetimi kurumlarda süregelen ve devam eden bir süreçtir.
- Sadece fonksiyon bazında değil, kurumun tamamında uygulanır.
- Tüm aksiyonların hissedarlarının risk alma isteği ile uyumlu olmasını sağlar.
- Sadece tehlikelerden korunma değil, değer yaratma odaklıdır.
- Strateji belirlemede kullanılır.
- Tüm risklerin uygun bir şekilde yönetildiğine dair makul bir güvence sağlar.
- Sonuç değil, sonuca ulaşmak için kullanılan bir araçtır.

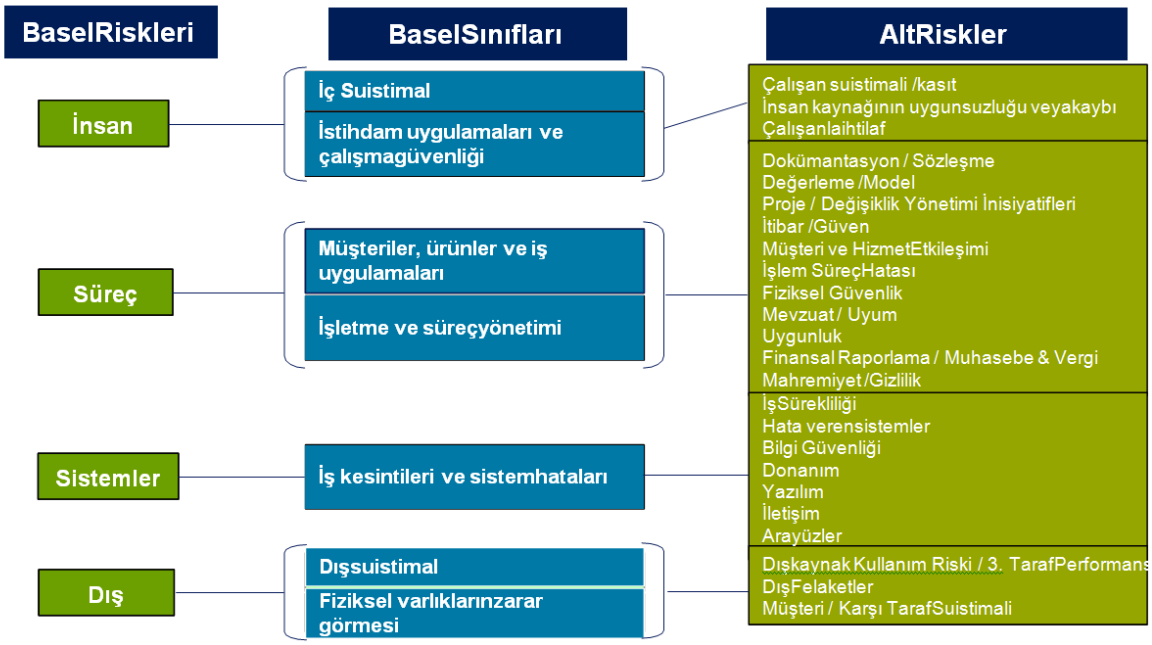


B.2 BT RİSK YÖNETİMİ

Bilişim Teknolojileri riski,BT ortamındaki durumdan kaynaklanan (BT varlıkları,organizasyonu, süreçleri, yönetişimi) herhangi bir hatadan organizasyonun zarara maruz kalma potansiyelidir.



B.2.1 Standart Risk Sınıfları



B.2.2. Risk Yönetim Stratejisi

B.2.2.1. Engeller

- İç BT Politikaları
- Kurumsal Risk Yönetimi vizyonu eksikliği – BT'e yer verilmemesi
- BT Risk Yönetimi Tanımı

B.2.2.2. BT Risk Yönetimi Stratejisi

- BT Risk Yöneticisi (IT CRO) atama
- Bu kişiyi CIO ve CRO'a bağlama
- BT Risk Yönetimi için tüzük oluşturulması
- BT Risk Gösterge Tablosu & Raporlama – BT KPI ile KRI Dengesi
- Risk Yönetimi – Risk analizi, kabulü, sahipliği ve bakımı

B.2.2.3. Zayıflık-Tehdit Örnekleri

Zayıflık	Tehdit-Kaynak	Tehdit–Aksiyon
İşten ayrılan personelin kullanıcı adlarının sistemden silinmemesi/bloke edilmemesi	İşten ayrılanpersonel	Kurum ağına ulaşması ve kurumsal bilgilereerişmesi
Kurum güvenlik duvarlarının gelen telnet'lere izin vermesi ve XYZ sunucusuna "misafir" kullanıcı adı ile ulaşılabilmesi	Yetkilendirilmemiş kullanıcılar (hacker'lar, işten ayrılan çalışanlar, bilişim suçluları,teröristler)	XYZ sunucusuna telnet ile erişim ve "misafir" kullanıcı adı ile sistem dosyalarınaulaşması
Tedarikçinin, sistem güvenlik tasarımında açıklar belirlemesi, yeni yamaların sistemeuygulanmaması	Yetkilendirilmemiş kullanıcılar (hacker'lar, memnun olmayan çalışanlar, bilişim suçluları, teröristler)	Bilinen sistem zayıflıklarını kullanarak kritik sistem dosyalarına yetkisiz erişimler

B.2.2.4. Zayıflık ve Tehditlerin Kontrolle Eşleştirilmesi

(1) Risk (Zayıflık-Tehdit)	(2) Risk Seviyes	(3) Önerilen Kontroller	(4) Aksiyon Önceliği	(5) Seçilen Kontroller	(6) Gereken Kaynaklar	(7) Sorumlu Ekip/Kişiler	(8) Başlangıç BitişTarihi	(9) Bakım Gereksinimi/Görüşler
Kurumgüvenlik duvarlarınıngelen telnet'lereizin vermesi veXYZ sunucusuna "misafir"kullanıcı adı ileulaşılabilmesi	Yüksek	• Gelen telnet'eizin verilmemesi • Hassaskurumsal dosyalara"herkes" erişiminin kaldırılması • "misafir"kullanıcı adınınkaldırılması veyaparolasının zorlaştırılması	Yüksek	• Gelentelnet kaldırılması • Dosyalara "herkes" erişiminin kaldırılması • "misafir" kullanıcı adının kaldırılması	Sistemi tekrar konfigüre etmek vetest etmek için10 saat	• XYZ sunucusu sistem yöneticisi • Güvenlik duvarı yöneticisi	xx.xx.xxxx–xx.xx.xxxx	Sistemgüvenliğinin düzenligözden geçirilmesi veXYZ sunucusunauygun güvenliğin sağlandığınıntest edilmesi

1. Riskler (Zayıflık-Tehdit), risk değerlendirme sürecinin çıktısıdır.

2. Belirlenmiş her bir risk için risk seviyesi risk değerlendirme sürecinin çıktısıdır.

3. Önerilen kontroller risk değerlendirme sürecinin çıktısıdır.

4. Aksiyon önceliği risk seviyesine ve müsait durumdaki kaynaklara (maddi, insan, teknoloji) göre belirlenmektedir.

5. Seçilen kontroller, önerilen kontroller arasından belirlenmektedir.

6. Gereken kaynaklar, seçilen kontrolleri uygulamaya almak üzere belirlenmektedir.

7. Sorumlu ekip ve kişiler, yeni veya geliştirilen kontrolleri uygulayacak kişilerdir.

8. Başlangıç ve bitiş tarihi, yeni veya geliştirilen kontrollerin hangi tarihlerde uygulanacağını belirtir. Bakım gereksinimi, yeni veya geliştirilen kontrollerin uygulanması sonrasında ihtiyaç duyulacak çalışmalardır.

B.3. SORUMLULUKLAR

B.3.1. Üst Yönetim

İş hedeflerine ulaşmak için kaynakların doğru kullanıldığını takip eder ve risk analizi sonuçlarından karar verme sürecinde faydalanırlar.

B.3.2. Bilgi İşlem Müdürlüğü

BT planlamasından, bütçesinden ve performasından sorumludur. Kararları, etkin bir risk yönetim programına dayanarak alırlar.

B.3.3. Sistem ve Bilgi Sahibi

Organizasyonel varlıkların fonksiyonel sahipleri olarak iş birimi yöneticileridir. Varlıkların bütünlüğünün, gizliliğinin ve kullanılabilirliğin temel sorumlularıdır.

B.3.4. İş Yöneticileri

Organizasyonun hedeflerine ulaşması için maliyet etkin kararlar almakla sorumlu kişilerdir. Risk yönetimi sürecindeki sorumlulukları, iş ile ilişkili kontrollerin uygulanmasını sağlamaktır.

B.3.5. Bilgi Güvenliği Yöneticileri

Risk Yönetimi sürecinde bilgi güvenliği ile ilişkili programların gerçekleştirilmesinden sorumludur.

B.4. BT RİSK YÖNETİMİ KATEGORİLERİ

B.4.1. BT Risk Alanları

1. *BT Yönetişim/Strateji Riski*
2. *BT Beceri/İnovasyon Riski*

3. *BT Mimari Riski*
4. *İş Sürekliliği Riski*
5. *Uyum Riski*
6. *BT Kaynak Riski*
7. *Tedarikçi Yönetim Riski*
8. *Üçüncü Taraf İlişkileri Riski*
9. *Proje/Geliştirme Riski*
10. *Değişiklik Riski*
11. *BT İtibar/Müşteri Memnuniyet Riski*
12. *Bilgi Riski*
13. *BT Güvenlik Riski*
14. *Online/Web Riski*

B.4.1.1 BT Yönetişim/ Strateji Riski:

Kurum BT stratejilerinin iş gereksinimleri ile tutarlı olmaması, iş gereksinimlerini karşılamaması, değişikliğe uygun olmaması, düzenli ve sık sık organizasyonla paylaşılmaması, iş ile uyumunda eksiklikler olması riskidir. Bu durumda, BT iş ile ilişkisi olmayan bir birim olarak algılanır.

B.4.1.2 BTBeceri/ İnovasyon Riski:

Kurumun bulunduğu pazar, endüstri ve etkileşim ortamında ilerlemesi için BT'nin yeni hizmet teknolojilerini uygulayamaması riskidir. BT'nin yeni teknolojilere adapte olmakta başarısız olması durumunda, Kurum pazar ve endüstrideki değişikliklere uyum sağlayabilmek için baskı altında kalacak ve rekabetçi ortamda iş performansını en uygun duruma getiremeyecektir.

B.4.1.3 BT Mimari Riski:

İş birimlerinin mevcut ve gelecekteki ihtiyaçlarını etkin bir şekilde desteklemek için, BT'nin etkin, standart hale getirilmiş ve sürdürülebilir bilgi teknolojileri altyapısına (donanım, ağ, yazılım, insan ve süreç) sahip olmaması riskidir.

B.4.1.4 İş Sürekliliği Riski:

BT ile ilişkili kritik operasyonların ve süreçlerin devam ettirilmesi için gerekli organizasyonel beceri riskidir. Kritik bilgi veya sistemlerin erişilebilir olmaması durumunda, Kurum kar eden operasyonlarını devam ettirememe riski ile karşılaşır.

B.4.1.5 Uyum / Yasa Riski:

BT organizasyonunun, dış gereksinimler ve kurumsal yönetişim politikaları/uygulamaları ile uyum sağlayamama riskidir. Bu risklere, hukuksal ve

sözleşmeye dayalı yükümlülükler ve yasal konular dahildir.

B.4.1.6 BT Kaynak Riski:

İnsan ve finansal kaynakların hazır olmaması ve planlanmaması veya verimsiz bir şekilde kullanılması riskidir. Bu riske, BT sistemleri hakkındaki bilgilerin personel değişiklikleri ile korunmaması da dahildir.

B.4.1.7 Tedarikçi Yönetimi Riski:

BT organizasyonunun, BT tedarikçileri, dış kaynak kullanımlar, sözleşmeli personel ve hizmet sağlayıcılar ile ilişki kurarken karşılaştığı risklerdir.

B.4.1.8 Üçüncü Taraflarla İlişki Riski:

Dağınık bir iş ortamında diğer kuruluşlarla ilişki kurarken ve bilgi paylaşırken karşılaşılan risklerdir. İş ortakları ve dış paydaşlarla iletişim kurmak,hassas bilgilerin gizliliğinin ihlal edilmesi ve yasal riskleri oluşturacaktır.

B.4.1.9 Proje/Geliştirme Riski:

BT'nin kötü proje planlama ve yönetimi sebebiyle karşılaştığı risklerdir. Bu risklere, iş ihtiyaçlarını karşılayan uygulamaların geliştirilmesi için bir biri ile ilişkili ve iyi anlaşılmış sürecin bulunmaması veya aksine çok fazla kontrolün olması sebebiyle BT'nin uygulamaları zamanında kullanıma alma becerisinin kaybedilmesi de dahildir.

B.4.1.10 Değişiklik Gerçekleştirme Riski:

BT' de teknoloji ortamının değiştirilmesini yönetmek için uygun olmayan gözetim ve süreçlerin bulunması riskidir. Buradaki en büyük risk,BT sistemleri ve uygulamaları üzerinde yetkilendirilmemiş veya kötü test edilmiş değişikliklerin oluşturacağı bütünlük ve erişilebilirlik problemidir.

B.4.1.11 BT İtibar/Vatandaş Memnuniyet Riski:

BT' nin iş taleplerini, hizmet seviye anlaşmalarını ve müşteri destek çağrılarını uygun olmayan bir şekilde karşılaması riskidir. BT itibar riski, nasıl hizmet verildiğidir.

B.4.1.12 Bilgi Riski:

BT'nin hassas ve düzenlenmiş kurumsal bilgiyi uygun olmayan bir şekilde kontrol etmesidir. Bilgi risk yönetimi, risk ve fırsatların yönetilmesi amacıyla organizasyonel bilginin belirlenmesi, sınıflandırılması ve kontrol edilmesi için çabalamaktadır.

B.4.1.13 BT Güvenlik Riski:

BT' nin teknik mimari zayıflığı ve organize suç,hacker, zararlı yazılım (virüs, solucan vb.) gibi saldırılara maruz kalmasıdır.

B.4.1.14 Online / Web Riski:

BT' nin Web varlığını oluşturma, işletme ve koruma için karşılaştığı risklerdir. Bu risklere web dünyasındaki itibar, hackleme, mahremiyet, markalaşma ve uyum dahildir.

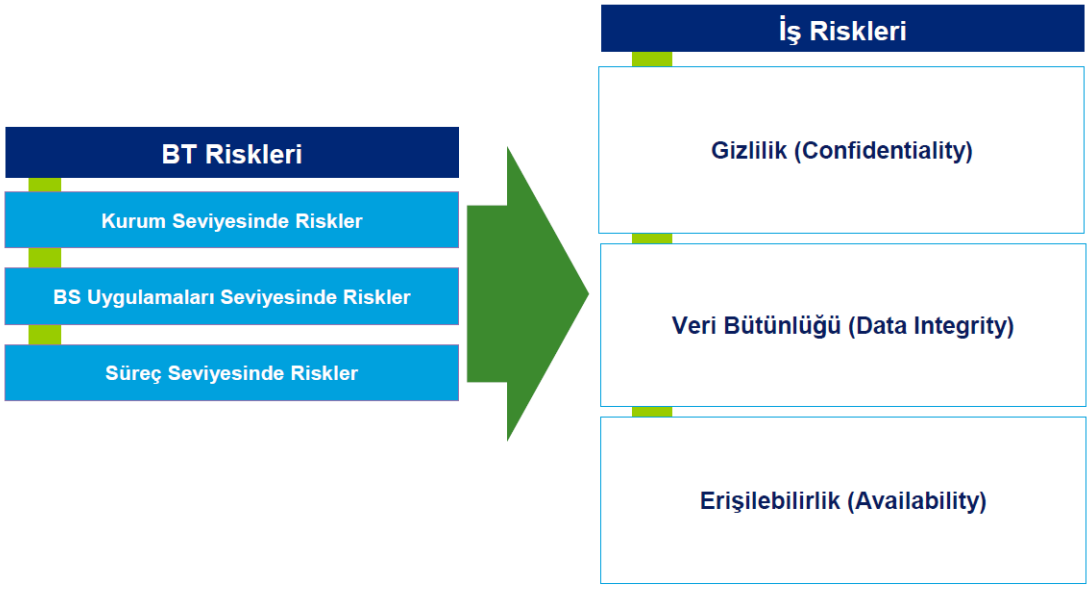
B.5. BT RİSK KATEGORİLERİ

BT riskleri üç seviyede düşünülmelidir:

- Kurum seviyesinde (organizasyonun geneli için),
- Bilgi sistemleri uygulamaları seviyesinde (uygulamalar tarafından desteklenen iş süreci işlemleri için), Süreç seviyesinde (uygulama ve veri bütünlüğünü destekleyen genel bilgisayar kontrol alanları için)

B.6. BT RİSKLERİNİN İŞ RİSKLERİ İLE İLİŞKİLENDİRMESİ

BT riskleri iş risklerini doğurmakta ve iç kontrol ortamına etki etmektedir.



B.6.1. Risk Etki Kategorileri

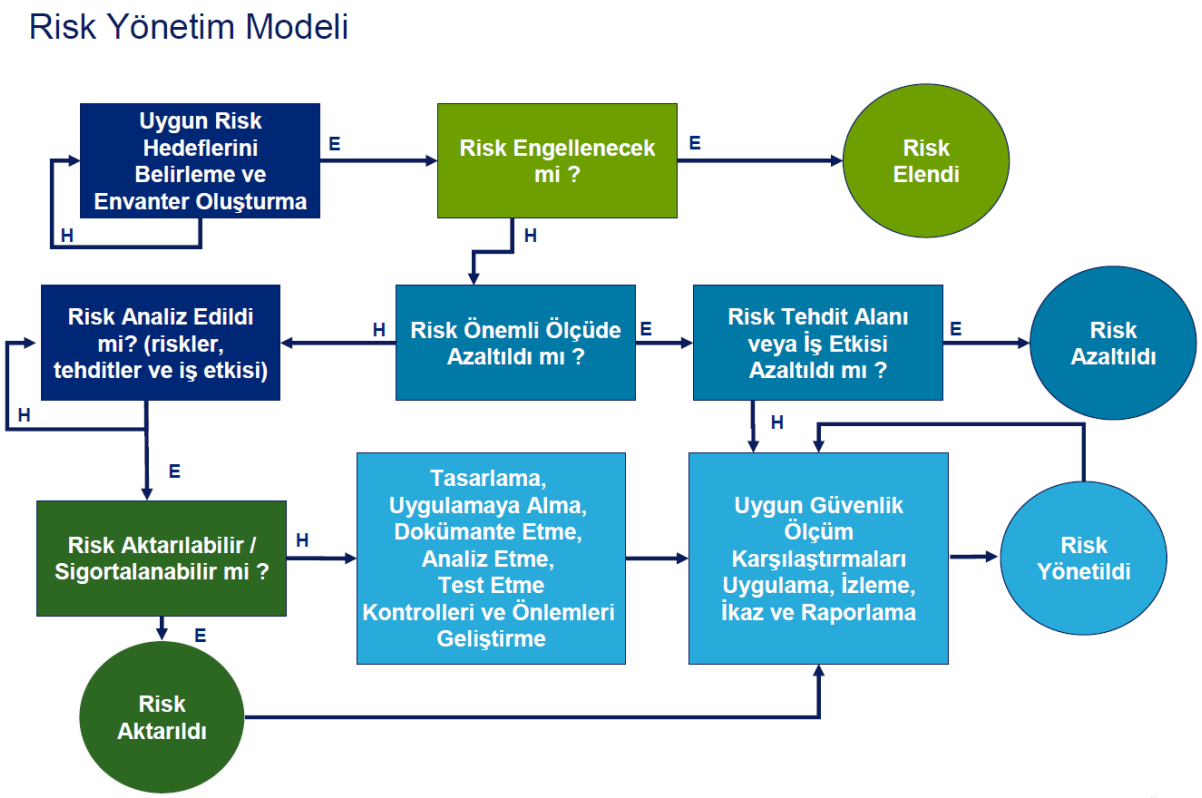
B.6.1.1. Operasyonlar: İş hizmetleri sunumunu destekleyen fonksiyonlar (mekan veya alan tahsisi, personel, satınalma, finansal, iletişim vb.)

B.6.1.2. Teknoloji: BT altyapısını destekleyen bilgi varlıkları (güvenlik, donanım, yazılım, ağ veya iletişim sistemleri)

B.6.1.3. Yasal: Kanunlara dayalı zorunluluklardan oluşan parametreler, mevzuat, politika veya üst yönetim kararları

B.6.1.4. İtibar: Hizmetlerin nasıl sunulduğu hakkında genel kamuoyu düşüncesi (bütünlük, kredibilite, güven, müşteri memnuniyeti, imaj, medya ilişkileri)

B.7. BT RİSK YÖNETİMİ YAŞAM DÖNGÜSÜ



B.7.1. 1. Aşama BT Altyapı Süreçlerinin Anlaşılması

Ana Aktiviteler

- Bilgi Toplama:
  - Kurumsal hedef ve stratejiler
  - Organizasyonel yapı ve değişiklikler
  - Kritik iş süreçleri ve merkezler
  - Geçmiş dönem denetim bulguları
  - Mevcut risk analiz dokümanları
  - Sektörel riskler ve sorunlar
- Kurumsal yapının toplanan veriler ışığında değerlendirilmesi

Çıktılar

- Profil
  - İş Hedefleri
  - Organizasyonel yapı
  - İş ve BT süreçleri, lokasyonları
- Ön risk bilgileri
  - Mevcut analizler
  - Sektörel riskler

Ana Aktiviteler	Aktivite 1: İstenecek Dokümanların Listelesinin Hazırlanması	Aktivite 2: BT Hedef, Amaç ve Stratejisinin Anlaşılması	Aktivite 3: BT Genel Kontrol Yapısının Anlaşılması	Aktivite 4: BT Süreç ve Altyapısının Anlaşılması	Aktivite 5: Trend / Endüstriyel Risklerin Belirlenmesi	Aktivite 6: Altyapı – BT Süreçlerinin Eşleştirilmesi
Dokümanlar / Çıktılar	Doküman Listesi Ön Bilgiler Talep Edilen Dokümanlar için Takip Listesi	BT Profili BT Strateji Dokümanı BT Yıllık Plan BT Bütçesi Büyük Projeler	Kurumsal Kontrol Noktaları BT Yönetişim Dokümanları BT Politika Prosedürler BT Risk Kontrol Matrisleri	Temel BT Süreçleri Uygulama Listesi Altyapı Envanteri Veri Merkezleri	Risk & Kontrol Dokümanları Yasal Zorunluluklar Sektörel Riskler	BT Süreçleri-Altyapı Eşleştirilmesi

B.7.2. 2. Aşama BT Risk Modelinin Geliştirilmesi

Ana Aktiviteler

- İş süreçleri sahipleri ile birlikte risk çerçevesinin belirlenmesi:
  - Risk çerçevesi kapsamının belirlenmesi
  - Etki, olasılık ve zafiyet kriterlerinin belirlenmesi
- Risk çerçevesinin onaylanması

Çıktılar

- Risk çerçevesi
  - BT yönetişimi
  - BT süreçleri
  - Operasyon
- BT risk tanımları
- Risk değerlendirme kriterleri:
  - Etki
  - Olasılık
  - Zafiyet

Ana Aktiviteler	Aktivite 1: BT Risk Çerçevesinin Belirlenmesi	Aktivite 2: Kriterlerinin Belirlenmesi	Aktivite 3: Risk Çerçevesinin Onaylanması	Aktivite 4: Risklerinin Belirlenmesi
Dokümanlar / Çıktılar	BT Risk Çerçevesi Kategoriler: • Yönetişim / Strateji Planlama • BT Süreçleri • Altyapı	Kriterler (Etki, zafiyet, olasılık) Risk Değerlendirme Yaklaşımı	BT Risk Modeli	Risk Kataloğu

BT Risk Çerçevesi, öngörülen risklerin belirli kategoriler altında toplanarak, tüm BT süreçleri ile ilgili risklerin değerlendirilmesini sağlar.

- BT Risk Değerlendirme Yöntemi üzerinde anlaşılır.
- Paydaşlar ile BT risk değerlendirmesi sonuçları paylaşılır.
- Tüm riskleri içeren bir risk kataloğu hazırlanır.

Risk Kataloğu				
#	Sahibi	Sınıfı	Risk İfadesi	Olasılığı
1	Bilgi Güvenliği Sorumlusu	Bilgi Varlıkları	Sistem yöneticisinin CEO e-postalarını okuması ve rakiplere bilgi vermesi	Düşük
2				

ÖRNEK BT RİSKLERİ –YÖNETİŞİM SEVİYESİ

B.7.2.1. BT Yönetişimi:

B.7.2.1.1. Misyon: BT misyonu dokümante edilmemiştir veya mevcut değerleri korumaya ve yeni katma değer yaratmaya yönelik değildir.

B.7.2.1.2. BT–İş Birimleri Uyumu: BT ile iş birimleri arasındaki hedefler uyumlu olmadığı için BT etkin bir katma değer sağlayamamaktadır.

B.7.2.1.3. Politika: Politika ve prosedürler tanımlanmamış ya da dokümante edilmemiştir. Mevcut yazılı politika ve prosedürler etkin bir dağıtım mekanizmasıyla birimlerle paylaşılmamıştır. Politika ve prosedürlerin farkındalığında eksiklikler bulunmaktadır.

B.7.2.2. BT Strateji Planlama:

B.7.2.2.1 BT Planlama: Bilgi sistemleri strateji ve planları kurumsal stratejik hedeflerle tam uyumlu değildir.

B.7.2.2.2 Bütçe, Metrik ve Kontroller: BT bütçeleri yönetim tarafından onaylanmamaktadır. Bütçedeki gerçekleşme farklılıkları kontrol edilmemekte ve sebepleri araştırılmamaktadır. Metrik ve kontroller tanımlanmamıştır.

B.7.2.3. Mimari:

B.7.2.3.1 Teknoloji Planlama: BT organizasyonu, kuruma ve süreçlere katma değer sağlayacak teknolojileri takip edememekte ve zamanında kullanmaya başlayamamaktadır.

B.7.2.3.2 Gelişen Teknolojiler: BT organizasyonu gelişen teknolojileri takip edememekte, ortaya çıkan yeni fırsat ve önerileri değerlendirememektedir.

B.7.2.3.3 Tedarikçi / Ürün Seçimi: BT tedarikçi ve ürünlerinin seçimi,yönetimin belirlediği standartlar dahilinde yapılamamaktadır.

B.7.2.3.4 Entegrasyon &Konsolidasyon: Sistemlerin entegrasyonu etkin değildir, sistemlerin etkileşimi istenilen düzeyde değildir.

B.7.2.4. Proje Yönetimi:

B.7.2.4.1 Proje Yönetim Hayat Döngüsü: Projelerin planlamasında, kaynak ayrılmasında, yürütülmesinde ve zamanında tamamlanması için belirli bir metodoloji geliştirilmemiştir.

B.7.2.4.2 Yazılım Geliştirme Hayat Döngüsü: BT yazılım geliştirme projeleri yönetimin belirlediği standartlara göre yürütülmemektedir.

B.7.2.4.3 Proje Risk (Geçiş Öncesi) Değerlendirme: BT projeleri, Kalite Güvence birimleri, İç Denetim ve/veya Yönetim tarafından geçiş öncesi incelenmemektedir.

B.7.2.5. BT Operasyonları

B.7.2.5.1 Çevre Yönetimi: İş ve BT hedeflerininin kullanılabilirlik ve performans değerleri için diğer tüm BT ihtiyaçları (donanım, yazılım, bilgisayar ağı, veri merkezleri, araçların) izlenmemektedir.

B.7.2.5.2 Veri Saklaması/Yedeklemesi: Üst Yönetim ve kullanıcılar veri yedeklemesi ve saklanması ile ilgili uygun planlama yapmamaktadır. Veri kaybolması riskinin azaltılması amacı ile yedeklemeler uzak bir lokasyonda tutulmamaktadır.

B.7.2.6. Süreklilik Yönetimi

B.7.2.6.1 İŞ-Etki Analizi: Kurum geneli için geçerli olan bir süreklilik planı hazırlanmamış yada iş-etki analizine göre yapılmamıştır.

B.7.2.6.2 Süreklilik Planı Geliştirme/Güncelleme: Süreklilik Planı mevcut değildir yada gözden geçirilmemekte veya iş ortamındaki değişiklikleri yansıtmamaktadır.

B.7.2.6.3 Test Edilmesi: Üst Yönetim süreklilik planını düzenli olarak test etmemekte, test sonuçlarını dokümante etmemekte ya da planı geliştirmemektedir.

B.7.3. 3. Aşama - Riskin Ölçeklendirilmesi

Ana Aktiviteler

- Mülakat, çalışma toplantıları ve anketlerle risklerin değerlendirilmesi:
  - Üst yönetim
  - Orta seviye yönetim
  - İş birimleri ve BT birimleri yöneticilerine anketler yapılması
- Risk derecelendirmesi ve haritasının çıkarılması

Çıktılar

- Risk Haritası ("MARCI")
  - Risklerin etki ve zafiyetlere göre değerlendirilmesi
- Mülakat toplantı notları
- Anket sonuçları

Ana Aktiviteler	**Aktivite 1:** Risk Değerlendirme Süreci Katılımcıların Belirlenmesi	**Aktivite 2:** Mülakat, Çalışma Toplantıları ve Anketlerin Yapılması	**Aktivite 3:** BT Risklerinin Önceliklendirilmesi	**Aktivite 4:** Risklerin Yönetim Tarafından Değerlendirilmesi
Dokümanlar / Çıktılar	Mülakat, Çalışma Toplantıları ve Anket Katılımcılarının Belirlenmesi Anket ve Mülakat Formlarının Belirlenmesi	Duyuru e-postaları Mülakatlar Çalışma Toplantıları Materyalleri Anketler Anket, Mülakat ve Formların Belirlenmesi	Risk Değerlendirme Sonuçları Risk Haritası	Uyarlanmış Risk Değerleri

B.7.3.1. Risk Faktörleri

Varlıkların ve sahiplerinin belirlenmesi, gizlilik, bütünlük ve erişilebilirlik değerlerinin verilmesi

Varlık Grubu	Varlık	G	B	E
Bilgi / veri	Maaş bilgileri			
Donanım	Domain Controller			
Yazılım ve uygulamalar	Ana bankacılık uygulaması			
İletişim cihazları	Güvenlik Duvarı			
Taşınabilir veri saklama ortamları	Yedekleme kartuşları			
Dokümanlar	Faturalar			
Personel	Veritabanı Yöneticisi			
Bilgi işlem merkezleri	Olağanüstü Durum Merkezi			

Zayıflık	Bir varlık üzerinde gizlilik, bütünlük ve/veya erişilebilirliğin kaybedilmesine neden olabilecek açıklık	Kullanıcılar ve sunucular aynı ağ içerisinde yer almaktadır ve kullanıcılar sunuculara erişebilmektedir.
Tehdit	Varlığın gizlilik, bütünlük ve/veya erişilebilirliğinin kaybedilmesine neden olabilecek olay	Kullanıcılar bilinçli veya bilinçsiz olarak kritik servislere müdahale edebilir.
Risk	Tehditin zayıflığı istismar etmesiyle ortaya çıkabilecek sonuç	Hizmet kesintisi gerçekleşebilir.
Kontrol	Riskin etkisini azaltan düzenleme ve/veya aksiyonlar	Güvenlik duvarı ve sanal ağlar kullanılarak erişim kısıtlaması sağlanmalıdır.

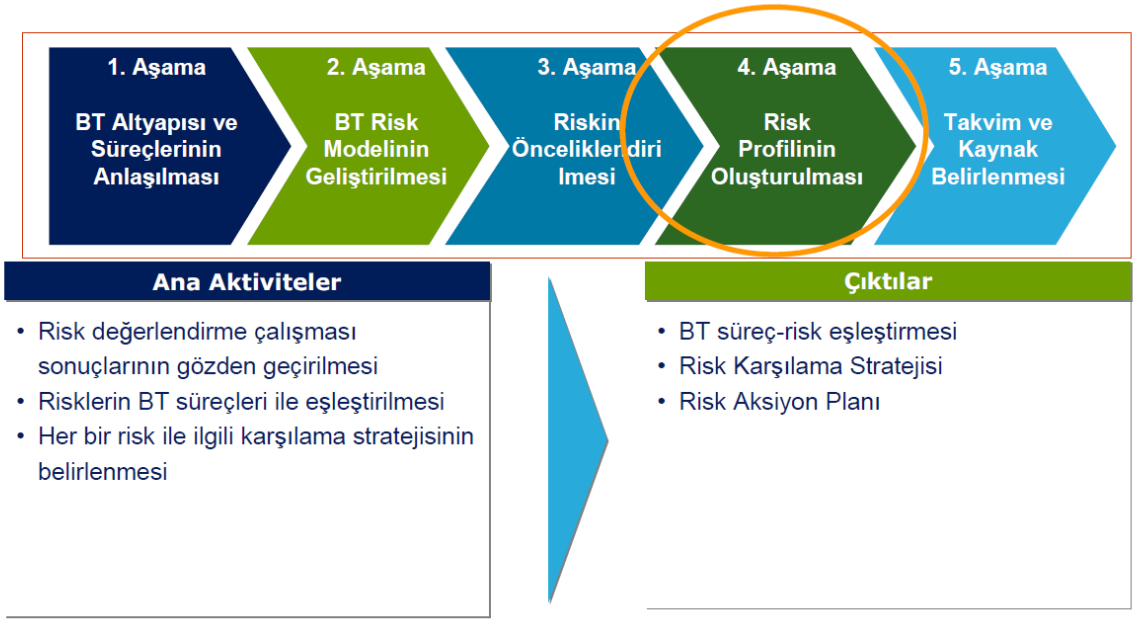
B.7.3.2. Risk Değerlendirmesi

Riske Maruz Kalma Olasılığı (Tehdit)	Zayıflık: Düşük	Zayıflık: Orta	Zayıflık: Yüksek
Düşük	Çok Düşük	Düşük	Orta
Orta	Düşük	Orta	Yüksek
Yüksek	Orta	Yüksek	Çok Yüksek

Risk Seviyesi (İş Etkisi)	Riske Maruz Kalma Olasılığı: Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
Düşük	1	2	3	4	5
Orta	2	3	4	5	6
Yüksek	3	4	5	6	7

Varlık	İş Etkisi (G / B / E)			Zayıflık	Tehdit	Risk
Web Uygulama Sunucusu				Varsayılan kullanıcı hesapları aktif durumdadır.	İnternetteki saldırganlar uygulamaya erişebilir.	Veriler yetkisiz kişilerce değiştirilebilir.
VoIP Telefonlar				Görüşmeler şifrelenmeden iletilmektedir.	Kurum çalışanları görüşmeleri dinleyebilir.	Kişisel ve gizli kurumsal bilgiler ifşa olabilir.

B.7.4. Aşama – Risk Profilinin Oluşturulması



Risk Karşılama, riskin etkisini azaltmak üzere Üst Yönetimin uygulattığı sistematik metodolojidir. **Risk karşılama için seçenekler aşağıdaki gibidir:**

B.7.4.1 Riski Kabullenme: Potansiyel riski kabul ederek devam etmektir. Kontroller uygulanarak risk daha az bir seviyeye getirilmeye çalışılır.

B.7.4.2 Riskten Kaçınma: Riskin oluşmasına neden olan durumu ortadan kaldırarak riskten kaçınmaktır.

B.7.4.3 Risk Sınırlama: Bir zayıflık ile ilgili çalışarak tehdidin etkisini azaltmak amacıyla

kontroller uygulamaktır. (Tespit edici veya kurtarıcı kontroller gibi)

B.7.4.4 Risk Planlama: Kontrolleri önceliklendiren, uygulayan ve yürüten bir risk karşılama planı geliştirilmesi ile riskin yönetilmesidir.

B.7.4.5 Risk Aktarımı: Zararın azaltılmasını sağlayacak seçeneklerin kullanılması ile riskin transfer edilmesidir.

Üst Yönetim

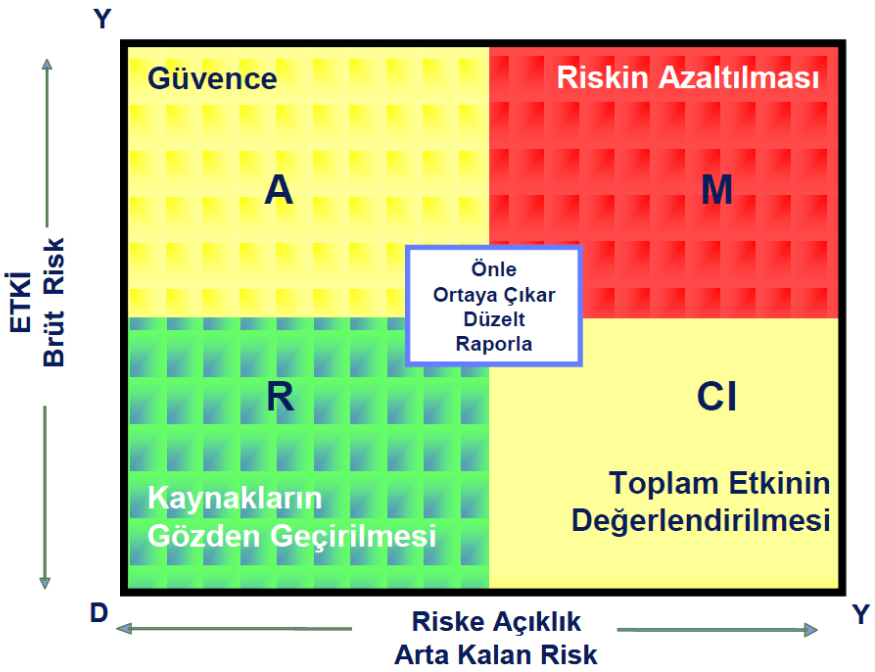
- Öncelikleri ve endişeleri nedir?
- Hangi riskler yüksek önceliklidir?
- Hangi riskler kabul edilmektedir?
- Hangi kontroller etkin değildir?
- Hangi riskler müdahale gerektirir?

RiskProfili

#	Doğal Risk Seviyesi	Kontrol	Kalan Risk Seviyesi	Hedef Risk Seviyesi	Öncelik	Aksiyon
1	Yüksek	Kont1	Düşük	Düşük	Düşük	Kabul
2	Orta	-	Orta	Düşük	Yüksek	Müdahale

Risk Haritası Genel Alanları

Risk Karşılama yaklaşımı “MARCI” şemasında risklerin yerleştiği alana göre belirlenir.



B.7.5. Aşama – Takvim Ve Kaynak Belirlenmesi

Ana Aktiviteler

- İlgili Aksiyon Sorumluları ve Üst Yönetimi ile gerekli niteliklerin, araçların belirlenmesi
- Risk azaltma çalışmaları takviminin oluşturulması ve kaynakların belirlenmesi

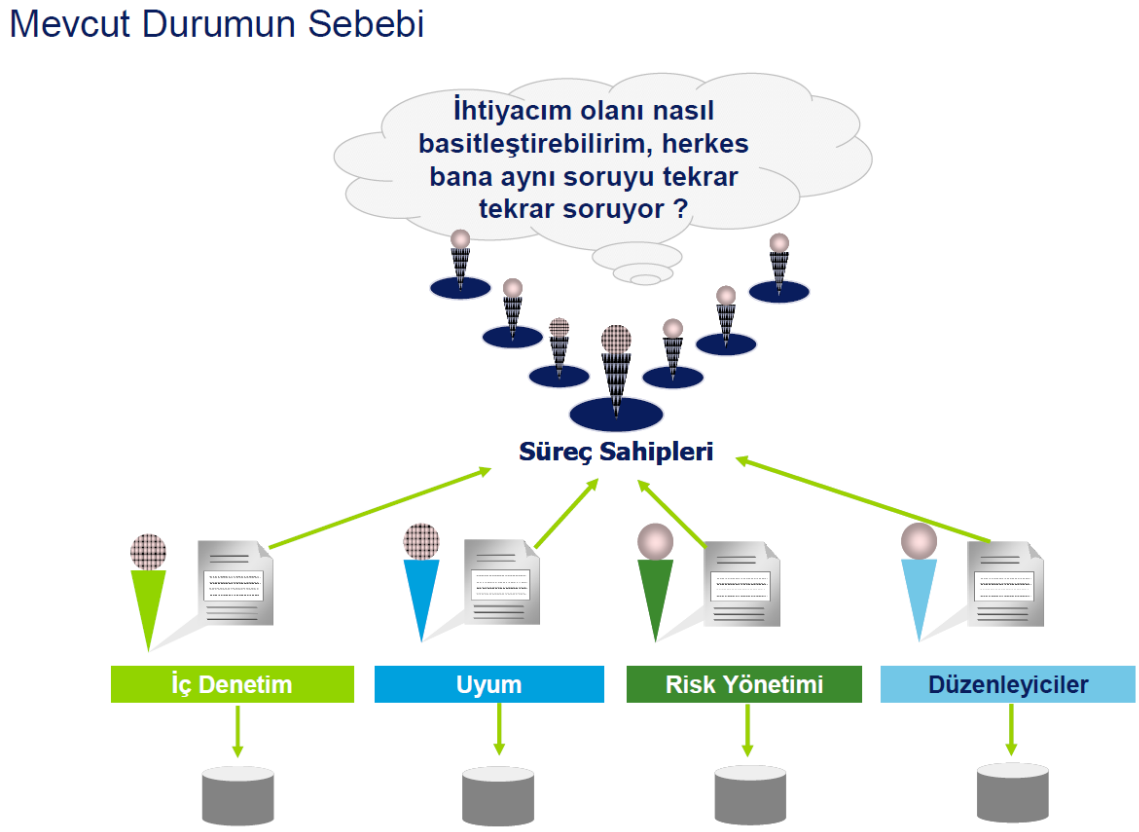
Çıktılar

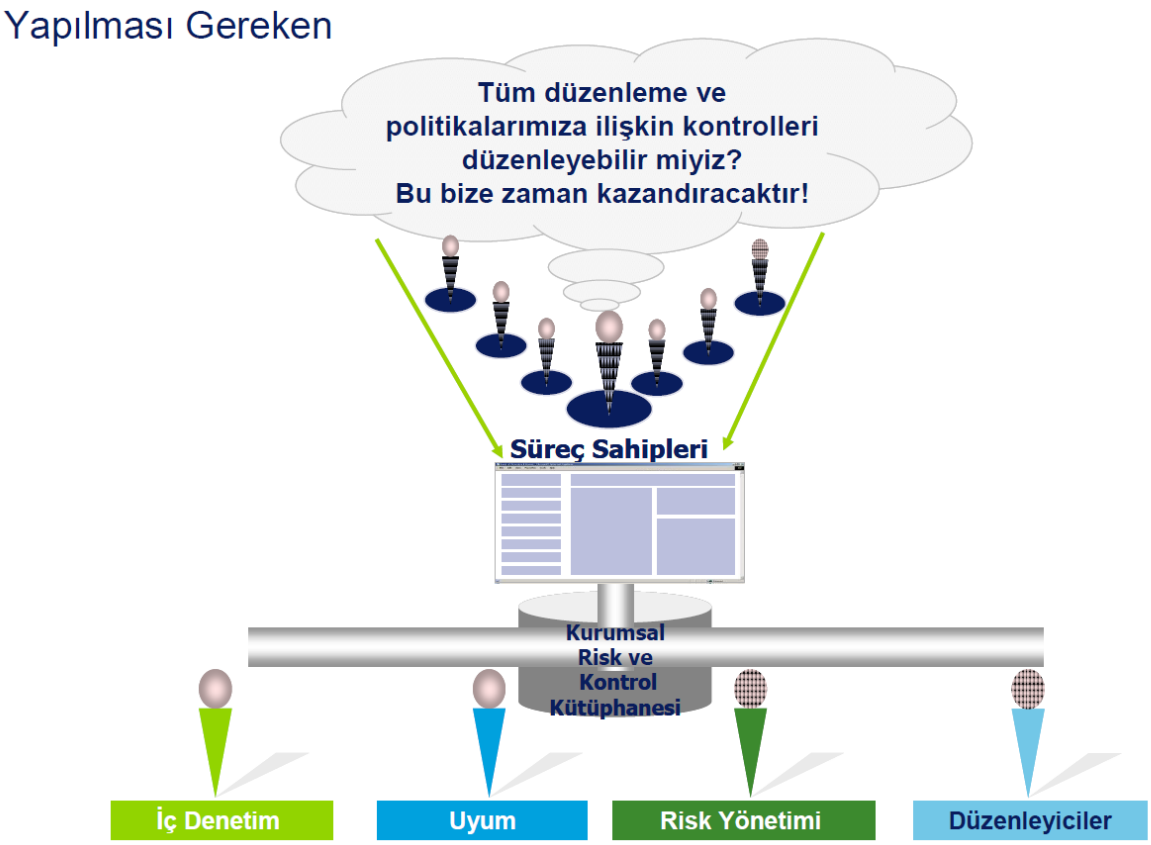
- Detaylı aksiyon planı:
  - Risk değerlendirmesi ile aksiyon planının eşleştirilmesi
  - Takvim
  - Kaynak & Eğitim Listesi

Risk Aksiyon Planı

Riskler	Yanıtlar	Sorumlu	Tamamlanma Tarihi	Durum
1,2	Oracle Veritabanında Değişiklik Kontrollerinin Uygulanması	Veritabanı Yöneticisi	XX.XX.XXXX	Açık
3	Sistem odası günlük erişim raporlarının, şüpheli aktiviteler ve anormallikler için gözden geçirilmesi	BT Yöneticisi, Sistem odası Sorumlusu	XX.XX.XXXX	Açık

B.8. BT Risk Yönetiminin Teknolojik Beklentileri





B.9. Risk Kapsamının Belirlenmesi

Uygun sonuçların elde edilmesi için risk değerlendirme çerçevesinin uygulama kapsamının belirlenmesi amaçlanmaktadır.

- Risk değerlendirmede iç ve dış kapsam, değerlendirmenin hedefi ve hangi risklerin değerlendirileceği kriterleri göz önüne alınmalı
- Risk kapsamı, Kurumun risk yaklaşımı olarak anlaşılmalı
- Prosedürler genel BT risk değerlendirmelerinde ve ayrıca proje risk değerlendirmelerinde kullanılacak standartları içermeli

B.10. Olay Tespiti

Kurumun, iş, yasal, düzenleyici, teknolojik, ticari ortak, insan kaynağı ve operasyonel durum hedeflerine ve operasyonlarına potansiyel negatif etkisi olan olayların (önemli bir zayıflığı kullanan gerçek bir tehdidin) belirlenmesi amaçlanmaktadır.

- Tespit edilen riskler bir risk kütüğüne kaydedilmeli ve buradan yönetilmeli
- BT risk kayıtlarında tehditlerin ilişkisi, tehdide açıklık miktarı ve etkinin önemi bulunmalı
- Tehdit unsuru olabilecek potansiyel olayları belirlemek için kullanılan süreçler oluşturulmalı
- Tüm BT süreçleri risk analizine dahil edilmeli
- Değişik vakalarda ve etki tespit aktivitelerinde uygun işlevler arası ekipler görev almalı

B.11. Risk Yanıtlaması

Düzenli olarak risklerin oluşumunu azaltan maliyet etkin kontroller sağlamak için tasarlanmış bir risk karşılama sürecinin geliştirilmesi ve yönetilmesi amaçlanmaktadır.

Risk yanıtlama süreci kaçınma, azaltma, paylaşma veya kabul etme gibi risk stratejilerini belirlemeli, sorumlulukları atamalı ve risk tolerans seviyelerini göz önüne almalıdır.

Her bir risk için belirlenen strateji Üst Yönetim tarafından onaylanmalıdır.

B.12. Risk Aksiyon Planının Oluşturulması Ve İzlenmesi

Yararlı olarak belirlenmiş risk yanıtlarının gerçekleştirilmesi için maliyetlerin, kazanımların ve sorumlulukların belirlenmesini içeren kontrol aktivitelerinin tüm seviyelerinin önceliklendirilmesi ve planlanması amaçlanmaktadır.

- BT risk aksiyon planı oluşturulmalı, planın sahipliğine ve yönetilmesine ilişkin sorumluluklar belirlenmeli
- Tüm önerilen aksiyonlar ve kabul edilen kalan riskler onaylanmalı
- Onaylanan aksiyonlar uygun süreç sahibi tarafından sahiplenilmeli
- Aksiyon planının işleyişi izlenmeli ve sapmalar Üst Yönetime raporlanmalı

Bu standard, risk değerlendirme, güvenlik tasarımı ve gerçekleştirme, güvenlik yönetimi ve yeniden değerlendirmeyi yöneten bu kılavuzlardaki prensipleri gerçekleştirmek için sağlam bir model sağlar.

- **BGYS'nin kurulması için aşağıdakiler yapmalıdır:**
  - BGYS kapsamını ve sınırlarını tanımlama
  - BGYS politikası tanımlama
  - Risk değerlendirme yaklaşımını tanımlama
  - Riskleri tanımlama
  - Riskleri çözümleme ve derecelendirme
  - Risklerin işlenmesi için seçenekleri tanımlama ve değerlendirmE
  - Risklerin işlenmesi için kontrol amaçları ve kontrolleri seçme
  - Sunulan artık risklere ilişkin yönetim onayı edinme
  - BGYS'yi gerçekleştirmek ve işletmek için yönetim yetkilendirme edinme
  - Uygulanabilirlik Bildirgesi hazırlama

BGYS dokümantasyonu aşağıdakileri kapsamalıdır:

- Risk değerlendirme metodolojisinin bir tanımı
- Risk değerlendirme raporu
- Risk işleme planı

Bilgi Güvenliği Yönetiminde

- Süreç hedefleri arasında BT risklerinin uygun şekilde yönetilmesi de yer almaktadır.
- İş ve BT riskleri ve yönetimi süreç kapsamı içerisindedir.
- Bilgi Güvenliği Yönetişiminin 6 temel çıktısından birisi Risk Yönetimidir:
  - Üzerinde uzlaşılmış bir risk profili
  - Risk Yönetimi önceliklerinin farkındalığı
  - Risk Karşılama
  - Risk Kabul

B.13. Belediye Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler

- Belediye, Belediyecilik faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri ölçmek, izlemek, kontrol etmek ve raporlamak üzere gerekli önlemleri alır.
- Bilgi sistemlerine ilişkin risklerin yönetilmesi, bilgi sistemleri yönetiminin önemli bir bileşeni olarak ele alınır.
- Belediye, risk yönetim politika ve süreçlerini, bilgi teknolojilerinin kullanımına bağlı olarak gözden geçirip, buradan kaynaklanacak risklerin yönetimini kapsayacak şekilde yeniler.
- Bilgi teknolojilerinden kaynaklanan risklerin operasyonel risk kapsamında değerlendirilmesinin yanı sıra bu risklerin belediyecilik faaliyetlerinden kaynaklanan diğer risklerin de bir çarpanı olabileceğinden, bilgi teknolojilerinden kaynaklanan riskleri de içeren bütünleşik bir risk yönetim yaklaşımı tüm belediyecilik faaliyetleri için benimsenir, bilgi teknolojilerinin takibi ve gözetimine ilişkin çalışmalardan edinilen verilerin belediyenin bütünsel risk yönetim çerçevesinin bir parçası haline gelmesi sağlanır.
- Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla geliştirilen politika ve prosedürlerin gerekleri, belediyenin organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözetim ve takip gerçekleştirilir.

C-POLİTİKALAR

C.1. İnsan Kaynakları ve Zafiyetleri Yönetimi

C.1.1. Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde tutulmamalıdır.

C.1.2. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.

C.1.3. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.

C.1.4. İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) imha edilmelidir.

C.1.5. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim edilmelidir.

C.1.6. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

C.1.7. Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

C.1.8 EBYS veya MIS yazılımları üzerinden kişiyle ilgili bir işlem yapıldığında(izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.

C.1.9 EBYS, MIS yazılımları, mail, telefon ve Active Directory için müdürlükler arası yer değiştirme, nakil ve emekliye ayrılanlar İnsan Kaynakları Ve Eğitim Müdürlüğü tarafından Bilgi İşlem Müdürlüğüne yazı ile bildirilmelidir.

C.2. Fiziksel ve Çevresel Güvenlik

Fiziksel ve çevresel güvenlik, işyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.

C.2.1. Fiziksel Güvenlik Sınırı;

C.2.1.1 Bilgi işlem Müdürlüğünü ve kritik öneme sahip Sistem Odasını korumak amacıyla kart kontrollü ve şifre panelli giriş sistemi yapılmalıdır.

C.2.2. Fiziksel Giriş Kontroller

C.2.2.1 Kurum içerisinde sistem odası ve network odalarına sadece yetkili personelin girişine izin verilmelidir.

C.2.2.2 Hassas bilgilerin bulunduğu alanlar (kimlik doğrulama kartı ve PIN koruması gibi yöntemlerle) yetkisiz erişime kapatılmalıdır.

C.2.3. Ofislerin ve Odaların Güvenliğinin Sağlanması;

C.2.3.1 Ofisler ve odalarla fiziksel güvenlik önlemleri alınmalıdır.

C.2.3.2 Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmalıdır.

C.2.3.3 Kritik tesisler kolayca ulaşılamayacak yerlere kurulmuş olup giriş çıkış alanları korunmalıdır.

C.2.3.4 Bilgi işlem merkezlerinin konumunu içeren dâhili/harici telefon rehberleri halka kapalı olmalıdır.

C.2.4. Harici ve Çevresel Tehditlerden Korunma;

C.2.4.1 Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karsı fiziksel koruma tedbirleri alınmalıdır.

C.2.4.2 Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir

yerde konuşlandırılmalıdır.

C.2.4.3 Komşu tesislerden kaynaklanan potansiyel tehditler göz önünde bulundurulmalıdır.

C.2.5. Güvenli Alanlarda Çalışma;

C.2.5.1 Kayıt cihazlarının güvenli alanlara sokulması yasaklanmalıdır.

C.2.5.2 Kullanılmayan güvenli alanlar kilitli olarak tutulmalıdır.

C.2.5.3 Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara çalışma sorumlusu birimin görevlendirdiği personel nezaret etmelidir.

C.2.5.4 Güvenli bölgelere örneğin sistem odasına yapılan girişler kayıt altına alınmalıdır.

C.2.5.5 Güvenli çalışma alanlarındaki personel veya bu alanda yürütülmekte olan çeşitli faaliyetlerde bulunan personel ve üçüncü parti çalışanları için "ihtiyacı kadar bilme" prensibi uygulanmalıdır.

C.2.5.6 Bilgi işlem servisleri ile dağıtım ve yükleme alanları ve yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmiş olmalıdır.

C.3. Ekipman Güvenliği

C.3.1. Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğünün bozulmalarına ya da yok olmalarına sebep olabilir. Tüm bu veya daha fazla tehditleri yok edebilmek için aşağıda yer alan belli başlı temiz masa kurallarına ilişkin önlemler alınmalı ve bu önlemler çalışanlar tarafından uygulanmalıdır.

C.3.2. Belli başlı temiz masa kuralları;

C.3.2.1 Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir. Bu bilgi ve belgelerin kilitli yerlerde muhafaza edilmelidir.

C.3.2.2 Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terk edilecekse ekran kilitlenmelidir.

C.3.2.3 Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulundurulmamalıdır.

C.3.2.4 Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.

C.3.2.5 Faks makinelerinde gelen giden yazılar sürekli kontrol edilerek makinede yazı bırakılmamalıdır.

C.3.2.6 Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), PCler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

C.3.2.7 Kısa süreli ayrılmalarda dahi, cep telefonu, PDA, USB bellek, harici harddisk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılmamalıdır.

C.3.3. Ekipman Yerleşimi ve Koruması;

C.3.3.1 Ekipmanların, gereksiz erişimlerin asgari düzeye indirilecek şekilde yerleştirilmesine özen gösterilmelidir.

C.3.3.2 Nem, sıcaklık, hava sirkülasyonu gibi parametreler izlenmelidir.

C.3.3.3 Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanmalıdır.

C.3.3.4 Bilgi işlem müdürlüğüne ait cihazların yakınında yeme, içme ve sigara içmek yasaklanmalıdır.

C.3.3.5 Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır.

C.3.3.6 Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmelidir.

C.3.3.7 Paratoner kullanılmalıdır.

C.3.3.8 Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme konularını düzenleyen kurallar olmalıdır.

C.3.4. Destek Hizmetleri;

C.3.4.1 Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde tutulmaya çalışılmakta aylık periyotlarda iklimlendirme cihazlarının bakımları yapılmalıdır.

C.3.4.2 Belediyemiz içerisinde genel kullanımda olan ups sistemine ek olarak sunucu kabinetleri içerisinde ek ups sistemi bulunmalı ve sistem jeneratör ile desteklenmelidir.

C.3.4.3 Belediyemiz içerisinde oluşturulan network altyapısında kullanılan aktif cihazlarımız yedekli yapıda çalışmakta olup yaşanacak arıza yalnızca ilgili switch cihazının bağlı bulunduğu lokasyonu kapsayacak ve diğer tüm kullanıcılar yaşanan kesintiden etkilenmeden çalışmadan devam edebilecek yapıda kurulmalıdır.

C.3.4.4 Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

C.3.5. Kablolama Güvenliği;

C.3.5.1 Güç ve iletişim kablolarının fiziksel etkilere ve dinleme faaliyetlerine karşı korunması için önlemler alınmalıdır.

C.3.5.2 Kablolar kapalı ve erişime müdahalesi zor alanlardan çekilmelidir.

C.3.5.3 Karışmanın ("interference") olmaması için güç kabloları ile iletişim kabloları ayrılmalıdır.

C.3.5.4 Hatalı bağlantıların olmaması için ekipman ve kablolar açıkça etiketlenmiş ve işaretlenmiş olmalıdır.

C.3.5.5 Alternatif yol ve iletişim kanalları mevcut olmalıdır.

C.3.5.6 Fiber optik altyapı yapılandırılmalıdır.

C.3.5.7 Bağlantı panelleri ve odalara kontrollü erişim altyapısı kurulmalıdır.

C.3.6. Ekipman Bakımı;

C.3.6.1 Ekipman, bakım için kurum dışına çıkarılırken kontrolden geçirilmelidir.

C.3.6.2 Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılmalıdır.

C.3.6.3 Bakım sadece yetkili personel tarafından yapılmalıdır.

C.3.6.4 Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutulmalıdır.

C.3.6.5 Ekipman bakım için kurum dışına çıkarılırken kontrolden geçirilmelidir.

C.3.6.6 İçindeki hassas bilgiler silinmelidir.

C.3.6.7 Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınmalı ve takip edilmelidir.

C.3.7. Kurum Dışındaki Ekipmanın Güvenliği;

C.3.7.1 Kurum alanı dışında bilgi işleme için kullanılacak ekipman için idare tarafından yetkilendirme yapılıyor olmalıdır.

C.3.7.2 Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına, seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir.

C.3.7.3 Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulmalıdır.

C.3.7.4 Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenmelidir.

C.3.8. Ekipmanın Güvenli İmhası ya da Tekrar Kullanımı;

Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format işlemlerinin yapılarak hard disklerin fiziksel imhası sağlanmalıdır.

C.3.9. Varlıkların Kurumdan Çıkarılması;

C.3.9.1 Ekipman, bilgi veya yazılımın yetkilendirme olmadan tesis dışına çıkarılmamasını sağlayan kontrol mekanizması oluşturulmalıdır.

C.3.9.2 Kurum varlıklarının yetkisiz olarak kurum dışına çıkarılıp çıkarılmadığını saptamak için denetleme yapılmalıdır.

C.3.9.3 Kurum çalışanları bu tip denetlemelerden haberdar olmalıdır.

C.4. İşletim Sistemleri ve Son Kullanıcı Güvenliği

C.4.1. İşletim Sistemleri Güvenliği

C.4.1.1 Kurum son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar vermekte ve bu işletim sistemine uygun yazılım donanım sistemlerinin kurulumunu temin etmelidir.

C.4.1.2 Kurum, işletim sistemlerinin güncel ve güvenli olması için güncelleme ve yama çalışmaları yapılmalıdır.

C.4.1.3 Her bilgisayarda etki alanı kimlik doğrulamasını sağlamalıdır.

C.4.1.4 Kurum, mevcut envanteri haricindeki donanımların kurum bilgisayarlarında kullanımını engellemelidir.

C.4.1.5 İşletim sistemlerinde kurulumda gelen yönetici hesaplarının (Administrator, root) kaba kuvvet saldırılarına karşı korunmuş olması, Microsoft ürünlerinde pasif hale getirilmesi, Linux tabanlı ürünlerde root hesabına ssh erişiminin engellenmesi sağlanmalıdır.

C.4.2. Son Kullanıcı Güvenliği

C.4.2.1. Son kullanıcılar sistemlere, etki alanları dâhilinde kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanmalıdır.

C.4.2.2. Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmekte ve internete çıkabilmelidir.

C.4.2.3. Son kullanıcıların yetkileri, içinde bulundukları grup politikasına göre Active Directory ile belirlenmelidir.

C.4.2.4. Son kullanıcıların aktiviteleri, 5651 Sayılı kanuna uygun olarak loglanarak kayıt altına alınmalıdır.

C.4.2.5. Güvenlik zafiyetlerine karşı, son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır.

C.4.2.6. Son kullanıcılar bilgisayarlarında ki ve sorumlusu oldukları cihazlarda ki bilgilerin düzenli olarak yedeklerini almalıdır. Kurum için önem arz eden resmi nitelikte ve kuruma ait bilgilerin sunucular üzerinde oluşturulmuş müdürlük klasörlerinde tutulması gereklidir.

C.4.2.7. Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.

C.4.2.8. Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde USB flash bellek ve/veya harici hard disk gibi removable media (taşınabilir medya) bırakmamalıdır.

C.4.2.9. Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır.

C.4.2.10. Kullanıcı bilgisayarlarında, güncel anti virüs bulunmalıdır.

C.4.2.11. Kurum, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulamalıdır.

C.4.2.12. Kurum, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişikleri merkezi grup politikalarıyla engellemelidir.

C.4.2.14. Temiz masa, temiz ekran ilkesi benimsenmeli ve hayata geçirilmelidir.

C.5. Parola Güvenliği

C.5.1. Güvenliğin oluşturulacağı birim için kullanılan programlarda uygulanan parola standardı belirlenmelidir.

C.5.2. Bilgi Güvenliği Yetkilisinin devreye girmesi ile parola standardı belirlenerek uygulanmaya başlanmalı, geliştirilerek aşağıdaki yapıya çekilmesi konusunda plan yapılmalıdır.

C.5.2.1 Parola en az 6 karakterden oluşmalıdır.

C.5.2.2 Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içermelidir.

C.5.2.3 Büyük ve küçük harfler bir arada kullanılmalıdır.

C.5.3. Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

C.5.3.1 Kişisel ve aile bilgileri gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi)

C.5.3.2 Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır. Herhangi bir dilde argo,lehçe olmamalıdır.

C.5.3.3 Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

C.5.4. Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.

'B' yerine 8	'Z' yerine 2	Örneğin Balıkçıl-Kazak 8a1lkç1l-Ka2ak
'I', 'i', 'L', 'l' yerine 1	'O' harfi yerine 0	
'S' yerine 5 'G' yerine 6	'g' verine 9	Solaryum! 501aryum

Güçlü parola yöntemleri

C.5.5 Kullanıcı seviyeli şifreler en az ayda bir kez değiştirilmelidir.
C.5.6 Şifreler e-posta iletilerine veya herhangi bir elekronik forma eklenmeme ve kağıda yazılmamalıdır.
C.5.7 Herhangi bir kişiye telefonla şifre verilmemelidir.
C.5.8 E-posta mesajlarına şifre yazılmamalıdır.
C.5.9 Şifreler, hiçbir şekilde iş arkadaşlarına verilmemelidir.
C.5.10 Bir kullanıcı adı ve şifresi birden fazla bilgisayarlarda kullanılmamaya özen gösterilmelidir.
C.5.11 Bilgi güvenliği çerçevesinde yapılan kontrol çalışmalarında şifre kırma ve tahmin etme operasyonları belli aralıklar ile Bilgi İşlem Müdürlüğü yetkili personelince yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse ve kırılırsa kullanıcıya şifresinin değiştirilmesi talep edilecektir.

C.6. Kriptolama Yönetimi

C.6.1. Kriptografik kontroller aşağıdaki maksatlarla kullanılır;

C.6.1.1 Gizlilik: Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelemenin kullanılması,

C.6.1.2 Bütünlük/Güvenilirlik: Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzaların veya mesaj doğrulama kodlarının kullanılması,

C.6.1.3 İnkar edilemezlik: Bir olay veya faaliyetin oluşumu veya oluşmadığının kanıtını elde etmek için kriptografik tekniklerin kullanılması.

C.6.2. Personelin gönderdiği maillerde, hiçbir şekilde yönetici, kullanıcı gibi hesap şifreleri bulundurulmamalıdır.

C.6.3. İşletim sistemi üzerinde saklanan kullanıcı ve yönetici hesabı şifrelerinin kriptolu olarak saklandığı belirli zaman aralıklarında kontrol edilmelidir.

C.6.4. Sunuculara kriptolu bağlantı ile bağlanılmalı, kripto kullanmayan yöntemler tercih edilmemelidir. Düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portlar gerekirse kapatılmalıdır.
C.6.5. Kripto kullanımı ile hangi iş bilgisinin korunacağı ile ilgili genel prensipler belirlenmelidir.

C.6.6. Taşınabilir ortam, cihaz ve iletişim hatlarında iletilen hassas bilginin korunması için şifreleme mekanizmalarının kullanımı belirlenmelidir.
C.6.7 İçerik denetimi üzerinden yapılan kontrollerde şifrelenmiş bilgi kullanımının etkileri değerlendirilmelidir.

C.6.8 Kriptografik anahtarların korunması, şifrelenmiş bilginin kaybolması, tehlikeye düşmesi veya hasar görmesi durumunda tekrar geri alınması ile ilgili metotları içeren anahtar yönetimi uygulanmalıdır.

C.6.9 Politikanın uygulanması, anahtar üretimini de içeren anahtar yönetimi ile ilgili görevler ve sorumluluklar belirlenmelidir.

C.6.10. Anahtar yönetiminde göz önüne alınacak hususlar aşağıda belirtilmiştir;

- Farklı kriptografik sistemler ve farklı uygulamalar için anahtar üretimi,

- Açık anahtar sertifikası üretimi ve elde edilmesi,
- Anahtarın alınmasını müteakip nasıl faaliyete geçirileceği dâhil kullanıcılara anahtar dağıtımı,
- Yetkili kullanıcıların anahtar erişiminin sağlanmasını da kapsayan anahtarların saklanması,
- Anahtarların ne zaman ve nasıl değiştirileceğinin kurallarını da kapsayan anahtarların değişimi ve güncellenmesi,
- Güvenliği tehlikeli bir duruma düşmüş anahtarlar,
- Anahtarların geri alımı ve kullanılmaz hale getirilmesini kapsayan anahtarın yürürlükten kaldırılması (Ör. Anahtarın güvenliğinin tehlikeli bir duruma düşmüş olması veya kullanıcının kuruluştan ayrılması durumları),
- İş süreklilik yönetiminin bir parçası olarak kaybolan veya bozulan anahtarların kurtarılması (Örn: Kriptolanmış bilginin kurtarılması),
- Anahtarların arşivlenmesi,
- Anahtarların imhası,
- Anahtar yönetimi ile ilgili faaliyetlerin izleme kayıtlarının (log) tutulması.

C.7. İnternet ve Elektronik Posta Güvenliği

C.7.1. Kullanıcıya resmi olarak tahsis edilen e-posta adresini, kişisel kullanım için ve internetteki listelere üye olunması durumunda kurum e-posta adresini kullanmamalıdır.

C.7.2. İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.

C.7.3. Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.

C.7.4. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; taciz, suistimal, küçük düşürücü, hakaret edici ve alıcının haklarına zarar vermeye yönelik öğeleri içeren e-posta mesajları gönderilemez. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yöneticisine haber verilmelidir.

C.7.5. İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta adresi bu mesajlarda kullanılamaz. Ancak iş gereği üye solunması yararlı internet haber grupları için yöneticisinin onayı alınarak Kurumun sağladığı resmi e- posta adresi kullanılabilir.

C.7.6. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.

C.7.7. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.

C.7.8. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip veya rar formatında) mesaja eklenmelidir.

C.7.9. Kurumumuz ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

C.7.10. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.

C.7.11. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e- postalar alındığında başkalarına iletilmeyip, Bilgi İşlem Müdürlüğüne haber verilmelidir.

C.7.12. Spam, zincir, sahte vb. zararlı olduğu d üşünülen e-postalara yanıt verilmemelidir.

C.7.13. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi, propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

C.7.14. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.

C.7.15. Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir. Bu nedenle; kullanıcı şifre kullanılmalı ve e-posta erişimi için

donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

C.7.16. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın derhal silmeli ve Bilgi İşlem Müdürlüğüne haber vermelidir.

C.7.17. Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajlara zamanında yanıt vermelidir.

C.7.18. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinerek tehdit unsuru olduğu düşünülen e-postalar Bilgi İşlem Müdürlüğüne haber verilmelidir.

C.7.19. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e- postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Bilgi İşlem Müdürlüğüne haber vermelidir.

C.7.20. Kullanıcı, kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemini kullanmamaya özen göstermelidir.

C.7.21. Elektronik postalar Müdürlük ve kullanıcı olarak 2 farklı şekilde oluşturulmuştur. Müdürlük e- postaları IMAP, Kullanıcıların e-postaları ise POP3 olarak saklanmaktadır. Bu nedenle; kullanıcılar iş ile ilgili belge ve bilgileri müdürlük mail adreslerine göndermelidirler. Ayrıca kullanıcılar e-posta adreslerine gelen mesajları uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayarlarındaki bir kişisel klasöre çekilmelidir.

C.7.22. Bir yıl 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, nakil, işten ayrılma ve emekli olma sebepleriyle kurumdaki değişikliğin İnsan Kaynakları ve Eğitim Müdürlüğünden en kısa zamanda yazı ile bildirilmesi gerekmektedir.

C.7.23. Yasa dışı ve hakaret edici e-posta haberleşmenin yapılmasının tespiti durumunda Bilgi İşlem Müdürlüğü yetkili kişileri önceden haber vermeksizin e-posta mesajlarını denetleyebilir ve kullanıcı hakkında yasal ve idari işlemler başlatabilir.

C.7.24. Kullanıcılara oluşturulmuş olan internet çıkış düzeyi üzerinden kullanıcılar interneti kullanmalıdırlar. Alternatif bir yol üzerinden izin verilmeyen sitelere ulaşmaya çalışan kullanıcılar tespit edildiği takdirde, gerekli yasal işlem yapılmalıdır.

C.7.25. Kullanıcılar sistem veri trafiğini, sistemin log almasını ve sistem üzerinde konulmuş olan kuralları aksatacak yazılımların kullanmaması gerekmektedir.

C.7.26. Antivirüs programının güncellenme özelliği her zaman açık olmalı ve belirli aralıklarla, olaylara bağlı olarak bilgisayarımızı taratılmalıdır. Antivirüs programını asla kapatmamalıyız.

C.7.27. Karşıdan yüklediğimiz veya yükleyeceğimiz öğeyi,dosyayı.. virus taramasından geçirmeliyiz.

C.7.28. Güvenlik duvarı kullanılmalıdır.

C.7.29. İşletim sistemi güncellenmelidir.

C.7.30. Düzenli aralıklarla boş ve kimliği belirsiz e-posta ya da spam, phishing mesajlar geliyorsa Bilgi İşlem Müdürlüğü'ne bilgi verilmelidir.

C.8. Sunucu ve Sistem Güvenliği

C.8.1.Sunucu Güvenlik Politikaları;

C.8.1.1 Kuruma hizmet veren tüm uygulama sunucuları ve disk üniteleri Bilgi İşlem veri merkezlerinde veya idarece uygun görülen güvenli fiziksel alanlarda konumlandırılmalıdır.

C.8.1.2 Farklı lokasyonlarda konumlandırılmış yerel sunucuların Karabağlar Belediyesi Özel Ağına bağlanması güvenli bağlantı ile sağlanmalıdır.

C.8.1.3 Servislere erişimler kaydedilmeli ve servis erişimleri, erişim kontrol yöntemleri ile sağlanmalıdır.

C.8.1.4 Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları, anti virüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir.

C.8.1.5 Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, uygulama sahipleri tarafından test mekanizmasından geçirilmeli, onaylanmalı sonra uygulanmalıdır. Test sürecinden başarılı bir şekilde geçen değişiklikler Bilgi İşlem Müdürlüğü onayı ile uygulamaya alınır.

C.8.1.6 Sistem yöneticileri kullandıkları bilgisayarlarda 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır.

C.8.1.7 Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

C.8.1.8 Kurumda bulunan sunucuların yönetiminden, ilgili sunucu yönetimi için yetkilendirilmiş personel sorumludur. Yetkilendirme Bilgi İşlem Müdürlüğü tasarrufunda yapılmalıdır. Görevinden ayrılan personelin tüm erişim yetkileri anında iptal edilmelidir.

C.8.1.9 Sunucu kurulumları, konfigürasyonları, sunucu işletim sistemi yedeklemeleri, yamaları, güncellemeleri Bilgi İşlem Müdürlüğü tarafından yapılmalıdır.

C.8.1.10 Sunuculara ait bilgilerin yer aldığı envanter veri tabanı oluşturulmalıdır.

C.8.1.11 Sunucuların yazılım ve donanım bakımları sistemden sorumlu teknik personel yada üretici firma tarafından belirlenmiş aralıklarla yapılmalıdır.

C.8.2. Sahip olma ve sorumluluklar ile ilgili kurallar;

C.8.2.1 Kurum'da bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel sorumludur.

C.8.2.2 Sunucu kurulumları, konfigürasyonları, işletim sistemi yedeklemeleri, yamaları, güncellemeleri sadece sistem sorumluları tarafından yapılmalıdır.

C.8.2.3 Tüm bilgiler Bilgi İşlem Müdürlüğü tarafından belirlenmiş kişi(ler) tarafından güncel tutulmalıdır.

C.8.2.4 Sunucular ile ilgili, yüklenici firmalar ile yapılacak çalışmalarda, ilgili sunucuyla yetkilendirilmiş personel eşlik etmelidir.

C.8.3. Genel yapılandırma kuralları;

C.8.3.1 Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri Bilgi İşlem Müdürlüğü talimatlarına göre yapılmalıdır.

C.8.3.2 Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

C.8.3.3 Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.

C.8.3.4 Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve anti virüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir. Anti virüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır.

C.8.3.5 Sistem yöneticileri kurum bilgisayarlarında 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.

C.8.3.6 Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.

C.8.3.7 Sunucular üzerinde lisanslı yazılımlar kurulmalıdır.

C.8.3.8 Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

C.8.4. Sunucu gözlemleme kuralları;

C.8.4.1 Kritik sistemlerde, uygulamalar kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.

C.8.4.2 Günlük tape backuplar en az 1(bir) ay saklanmalıdır.

C.8.4.3 Aylık fiili backuplar en az 6(altı) ay saklanmalıdır.

C.8.4.4 Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanmalıdır.

C.8.4.5 Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.

C.8.4.6 Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.

C.8.4.7 Port tarama atakları düzenli olarak yapılmalıdır.

C.8.4.8 Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü yapılmalıdır.

C.8.4.9 Denetimler, Bilgi İşlem Müdürlüğü tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.

C.8.4.10 Sunucuların bilgileri yetkilendirilmiş kişi tarafından tutulmalı ve güncellenmelidir.

C.8.5. Sunucu işletim kuralları;

C.8.5.1 Sunucular, sıcaklık ve nem değerleri düzenlenmiş; elektrik, ağ altyapısı kuvvetli; tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulmalıdır.

C.8.5.2 Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

C.8.5.3 Sistem odalarına giriş ve çıkışlar kontrol edilmelidir.

C.9. Ağ Cihazları Güvenliği

C.9.1. Ağ Cihazları Güvenlik Politikası

C.9.1.1. Ağ cihazlarının IP ve Mac adres bilgileri envanter dosyasında yer almalıdır.

C.9.1.2. Cihazlar üzerinde yerel kullanıcı hesapları açılmamalıdır.

C.9.1.3. Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanmalıdır.

C.9.1.4. Kurumun belirlemiş olduğu SNMP community string'leri kullanılmalıdır. Bu bilgi sadece yetkilendirilmiş kişiler tarafından bilinmelidir. Ayrıca SNMP v3 kullanılmasına dikkat edilmelidir.

C.9.1.5. İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.

C.9.1.6. Yönlendirici ve anahtarlar Ağ Yönetimi kontrolünde olmalıdır.

C.9.1.7. Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin dışında üretim ortamına taşınmalıdır.

C.9.1.8. Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.

C.9.1.9. Cihazlara yetkili kişiler dışında cihazın başında olarak erişilmesini önlemek amacıyla Console(Konsol) portu için de "enable şifresi" gibi kodlanmış ayrı bir parola verilmelidir.

C.9.1.10. Cihazları yönetecek kurum içindeki kişiler için cihaz üzerinde "enable şifresinden" farklı olarak kullanıcı adı, parola ve yetki seviyesini belirleyen privilege numarası tanımlanmalıdır.

C.9.1.11. Cihazlar Sistem odası gibi yerlerde kilitli kabinlerde konumlandırılmalıdır. Sistem odası dışında kalan cihazlar yine uygun kabinlerde kapalı dolap ya da kilitli kabinlerde muhafaza edilmelidir.

C.9.2. Kablosuz Ağlar Güvenliği

C.9.2.1. Wi- Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802. lx erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.

C.9.2.2. Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.

C.9.2.3. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

C.9.2.4. Varsayılan SSID isimleri kullanılmamalıdır. SSID ayar bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vb.

C.9.2.5. Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir.

C.9.2.6. Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından kurumun tüm internet bant genişliğinin tüketilmesi engellenmelidir.

C.9.2.7. Erişim cihazlarının bağlantısının sağlanması için, kullanılan yönetim cihazı üzerinde bağlantı talebinde bulunan kullanıcılar yönetim cihazının yerleşik Firewall'u üzerinden ağa dâhil olmalıdırlar.

C.9.2.8. Kullanıcı bilgisayarlarında kişisel anti-virüs ve güvenlik duvarı yazılımları yüklü olmalıdır.

C.9.2.9. Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir

C.9.2.10. Kablosuz erişim noktalarının aktif cihazlara giden kablolamasında fiziksel güvenliğe dikkat edilmelidir.

C.9.2.11. Kurum çalışanlarının kullandığı ile misafirler için olan SSID'ler farklı olmalıdır.

C.9.2.12. Kablosuz ağ cihazlarına erişim sadece yetkili kişiler tarafından SSH ile ya da cihaz başında console (konsol) ile yapılmalı, http ve telnet kapatılmalıdır. Ayrıca kablosuz cihazlara erişim için de "enable ve console (konsol) şifresi" oluşturulmalıdır.

C.10. Mal ve Hizmet Alımları Güvenliği

C.10.1. Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.

C.10.2. Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

- Bilgi güvenliği politikası,
- Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,
- Gerekli fiziki koruma için kontrol ve mekanizmalar
- Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,
- Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,
- Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,
- Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,
- Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,
- Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,
- Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,
- Uygun olduğu yerde personel transferi için hüküm,
- Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,
- Açık bir raporlama yapısı ve anlaşılan raporlama formatı,
- Değişim yönetimi sürecinin açıkça belirlenmesi,
- Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,
- İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,

- Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,
- Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,
- Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,
- Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,
- Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,
- Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,
- Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,
- Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,
- Anlaşmayla ilgili tarafların yükümlülükleri,
- Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı)
- Fikri mülkiyet hakları,telif hakkı ve herhangi bir ortak çalışmanın korunması,
- Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,
- Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,
- Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda acil durum planı olmalıdır.
- Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi,
- Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

C.10.3. Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.

C.10.4. Bilgi güvenliği yönetimi dış kaynaklı ise anlaşmalarda üçüncü tarafın güvenlik garantisinin yeterliliğini nasıl ele alındığı anlaşmada belirtilmelidir. Risk değerlendirmede tanımlandığı gibi, risklerdeki değişiklikleri belirlemek ve başa çıkmak için güvenliğin nasıl adapte edileceği ve sürdürüleceği ele alınmalıdır.

C.10.5. Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesinti süresi, acil durum planlaması yönetmelikleri ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde; kuruluş değişiklikleri yönetmek için uygun süreçlere ve anlaşmaların yeniden müzakere edilmesi ya da fesh edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.

C.10.6. Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

C.10.7. Genellikle anlaşmaların esasları kuruluşlar tarafından geliştirilmiştir. Bazı durumlarda anlaşmaların üçüncü taraflarca geliştirilmesi ve kuruluşa empoze edilmesi durumu olabilir. Kuruluşlar, kendi yapılarına üçüncü taraflarca empoze edilecek anlaşmalarda kendi güvenliklerinin gereksiz yere etkilenmesini engeller.

C.10.8. Gizlilik Taahhütnameleri

C.10.8.1 Gizlilik veya ifşa etmeme anlaşmaları yasal olarak uygulanabilir terimleri kullanarak gizli bilgileri korumanın gerekliliğini ele almalıdır. Gizlilik veya ifşa etmeme anlaşmaları için aşağıdaki unsurlar dikkate alınmalıdır:

- Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),
- Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dahil olmak üzere anlaşma süresi,
- Anlaşma sona erdiğinde yapılması gereken eylemler,

- Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi,
- Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,
- Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı
- Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesinin bildirimi ve raporlama prosesi,
- İade veya imha anlaşmasına bırakılacak bilgi için terimler,
- Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.

C.10.8.2 Bir kuruluşun güvenlik gereksinimlerine dayalı olarak, diğer unsurlarla bir gizlilik veya ifşa etmeme anlaşması gereklidir.

C.10.8.3 Gizlilik ve ifşa etmeme anlaşmaları uygulandığı yerin geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.

C.10.8.4 Gizlilik ve ifşa etmeme anlaşmaları için gerekler periyodik olarak veya gerekleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.

C.10.8.5 Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korumalı ve imzalayanın, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtmelidir.

C.10.8.6 Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçları doğrultusunda farklı şekillerde kullanılmalıdır.

C.11. Uygulama Yazılımları Güvenlik Yönetimi

C.11.1. Yazılım Geliştirme Politikası

C.11.1.1. Mevcut sistem yazılımları üzerine kurulacak, kullanılacak yeni bir yazılım veya mevcut sisteme yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

C.11.1.2. İdare sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

C.11.1.3. Uygulama yazılımlarının kurum içerisinde mi hazırlanacağı yoksa satın mı alınacağının belirlenmesi, uygun bir şekilde tanımlanmalıdır.

C.11.1.4. Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

C.11.1.5. Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

C.11.1.6. Yazılım geliştirme ve temin politikalarına uygun olmayan, ulusal ve uluslararası yazılım geliştirme standartları çerçevesinde geliştirilmemiş ve kurum talebi olmaksızın üretilmiş olan yazılımların kurumsal sistemler üzerine entegre edilmesine izin verilmemelidir.

C.11.1.7. Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.

C.11.1.8. Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

C.11.1.9. Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

C.11.1.10. Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.

C.11.1.11. Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

C.11.1.12. Yazılımlar sınıflandırılmalı/etiketlenmeli ve envanterleri çıkarılarak bir yazılım

kütüğünde muhafaza edilmelidir.

C.11.1.13. 3. Taraflarca geliştirilen yazılımın proje yönetimi, yazılım geliştirme, test ve kabul esasları tanımlanmalıdır.

C.11.1.14. Kurumsal yazılım geliştirme esasları yayınlanmışsa ona uygun geliştirme talep edilmelidir. Fonksiyon isimlendirme, yorum kullanımı, kullanılan yazılım dili vb.

C.11.1.15. Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

C.11.1.16. Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

C.11.1.17. Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

C.11.1.18. Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması engellenmelidir.

C.11.2. Belgelendirme Politikası

C.11.2.1. Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.

C.11.2.2. İş akışları uygun şekilde belgelenmelidir.

C.11.2.3. Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.

C.11.2.4. Girdi türleri ve girdi form örnekleri belgelenmelidir.

C.11.2.5. Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.

C.11.2.6. Çıktı form örnekleri ve çıktıların kimlere dağıtılacağı belgelenmelidir.

C.11.2.7. Programların nasıl test edildiği ve test sonuçları belgelenmelidir.

C.11.2.8. Bütün program değişikliklerinin detayları belgelenmelidir.

C.12. Güvenlik Yazılım ve Donanımları yönetimi

C.12.1. Bu sunuculara sistem biriminin admin/root yetkisi bulunmalıdır. Yapılacak tüm işlemler sistem güvenlik birimi nezaretinde yürütülmelidir. Kuruma ait sunucularda, sadece yetkili kişilerin erişebileceği administrator/root yetkisi bulunmalıdır.

C.12.2. Kuruma ait sunucular üzerinde bulunan,tüm kullanıcı hesapları (administrator ve root hesaplarıda dahil olmak üzere)güçlü şifreler ile korunmalıdır.

C.12.3. Yapılacak tüm işlemler düzgün bir şekilde dokümante edilmeli ve ilgili birim sorumlularına iletilmelidir.

C.12.4. Güvenlik amaçlı erişim logları, merkezi log sisteminde tutulmalı ve izlenmelidir.

C.12.5. Güvenlik yazılım ve donanımlarının logları, her bir yazılım ve donanım için belirlenen disk alanlarında tutulmalı ve ilgili birim tarafından yönetilmelidir.

C.12.6. Güvenlik donanımları, yetkisiz kişiler tarafından erişilememesi için gerekli güvenlik tedbirleri alınmış sistem odalarında tutulmalıdır.

C.12.7. Güvenlik donanımlarının konfigürasyon yedekleri düzenli olarak alınmalı ve bir back-up sunucusunda tutulmalıdır.

C.12.8. Kurumda kullanılan güvenlik yazılım ve donanımları en güncel ve stabil yamaya (patch) sahip olmalıdır.

C.12.9. Kurumda kullanılan güvenlik donanımları, harici izleme yazılım ya da donanımları ile

izlenmeli ve cihazlarda oluşan sorunlar sms ve/veya eposta aracılığı ile ilgili sorumlulara iletilmelidir.

C.12.10. Kurumun tüm istemcileri ve sunucuları anti-virüs yazılımına sahip olmalıdır.

C.12.11. İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.

C.12.12. Sistem yöneticileri, anti-virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.

C.12.13. Kullanıcı hiç bir sebepten dolayı anti-virüs yazılımını bilgisayarından kaldırmamalıdır.

C.12.14. Anti-virüs güncellemeleri anti-virüs sunucusu ile yapılmalıdır. Sunucular internete sürekli bağlı olmalı, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, anti-virüs sunucusu tarafından anti- virüs güncellemeleri otomatik olarak yapılmalıdır.

C.12.15. Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarların internet bağlantılarını kesebilme opsiyonuna sahip olmalıdır.

C.12.16. Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.

C.12.17. Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.

C.12.18. Optik Media ve harici veri depolama cihazları anti-virüs kontrolünden geçirilmelidir.
C.12.19. Antivirüs yazılımı yüklü olmayan kullanıcı bilgisayarları domain ortamına alınmamalı ve Bilgi İşlem Müdürlüğü Erişim Birimine bilgi verilmelidir.
C.12.20. Sistemin log almasına engel olabilecek yazılımlar (.exe uzantılı portable özellikte yazılımlar) kurum içerisinde kullanılmamalı ve dağıtımı yapılmamalıdır.
C.12.21 Sistem tarafından kullanıcı bilgisayarlarına kurum içerisinde kullanılan lisanslı ve güncel antivirüs yazılımı dışında bir yazılım kullanılmasına engel olunmalı,kullanıcıların antivirüs yazılımlarını bilgisayarlarından kaldırmalarına engel olunacak kurallar geliştirilmelidir.

C.13. Bilgi Güvenliği Teknolojileri Güvenliği

C.13.1. Yazılım Güvenliği

C.13.1.1. Kurum içerisinde kullanılan tüm bilgisayarların zararlı yazılımlara karşı en güncel anti virüs yazılımına sahip olmalıdır.

C.13.1.2. Bilgisayarlarda kullanılan anti virüs yazılımları düzenli olarak güncellenmelidir.

C.13.1.3. Bilgisayarların üzerinde kullanılan işletim sistemleri düzenli olarak güncelleştirilmelidir.

C.13.1.4. Bilgisayarlar üzerinde korsan yazılımlar bulundurulmamalıdır.

C.13.1.5. Kurum için hazırlanacak uygulamalar güvenlik zafiyetlerini en aza indirmek için güvenli yazılım yaşam döngüsüne uygun olarak tasarlanmalıdır.

C.13.1.6. Geliştirilen yazılımlar gizlilik, bütünlük ve erişebilirlik şartlarına uygun olmalıdır.

C.13.1.7. Yazılım geliştirme sürecinde, giriş doğrulama, yetkilendirme, kimlik doğrulama, konfigürasyon yönetimi, hassas bilgi, kriptografi,parametre manipülasyonu, hata yönetimi ve kayıt tutma ve denetimi kriterleri dikkate alınmalıdır.

C.13.1.8. Yazılım geliştirme süreci boyunca, gerekli bütün testler eksiksiz şekilde yapılmalıdır.

C.13.1.9. Kurum için geliştirilen uygulamalar ve satın alınan yazılımlar, güvenlik zafiyetlerine neden olmamak için en son stabil yamalara ve güncelleştirmelere sahip olmalıdır.

C.13.1.10. Uygulamalar geliştirilme süreçlerinde gerçek ortamda uygulanmadan önce test sunucularında test edilmelidir. Uygulamalar gerçek ortamda kurumun uygun bulduğu mesai saatleri dışında bir zaman diliminde devreye alınmalıdır.

C.13.1.11. Kurum için geliştirilen uygulamalar, uluslararası kabul görmüş standartlara bağlı dokümante edilmelidir. Uygulama için yazılmış olan dokümanlar uygulama ile beraber kuruma teslim edilmelidir.

C.13.2. Donanım Güvenliği

C.13.2.1. Kuruma ait sistemler ve sunucular dışarıdan gelebilecek saldırılara karşı, güncel teknolojilere sahip donanımsal firewall cihazları ile korunmalıdır.

C.13.2.2. Kurum çalışanlarının internete çıkışlarının kontrol edilerek, zararlı ve kurum politikasına uymayan sitelere erişimlerinin engellenmesi için proxy cihazları ile korunmalıdır.

C.13.2.3. Kuruma ait uygulamaların güvenli bir şekilde çalışması ve uygulamalara gelebilecek saldırıların engellenmesi için Web Application Firewall (Web Uygulama Güvenlik Duvarı) ile korunmalıdır.

C.13.2.4. Kurum ile dış dünya arasında ki yazışmalar bir eposta sunucusu ile kontrol edilmelidir. SPAM, virüs, kurum politikalarına uygun olmayan içerikler engellenmelidir.

C.13.2.5. Kurumda ki güvenlik cihazları sürekliliğin sağlanması için cluster (yedekli yapıda) bulunmalıdır.

C.13.2.6. Kurumda kullanılan güvenlik cihazlarının loglarının düzenli olarak alınması ve encrypt (şifreli) olarak saklanması gerekmektedir.

C.13.2.7. Kurumda kullanılan bütün güvenlik cihazlarının konfigürasyon yedekleri periyodik olarak alınmalı, doğru şekilde etiketlenerek saklanmalıdır.

C.13.2.8. Kurumda kullanılan bütün sistem ve güvenlik donanımları, kurumun ihtiyaçlarına bağlı olarak sadece izin verilen erişimlere göre konfigüre edilmelidir.

C.14. Mobil Cihazlar Güvenliği

Bilgiyi taşımanın kolay bir yolu laptop ve akıllı telefonlar gibi mobil cihazlardır. Bu cihazlarda bulunan hassas bilgiler ve erişim yetkileri de düşünüldüğünde mobil cihazlarda güvenliğin dikkat edilmesi gereken bir konu olduğu anlaşılmaktadır.

C.14.1. Mobil cihazlara erişimde mutlaka parola kullanılmalıdır.

C.14.2. Mobil cihazınızda ne tür bilgiler sakladığının farkında olunmalı, hassas ve gizli bilgileri mümkün olduğunca mobil cihazınızda bulundurulmamalıdır.

C.14.3. Verilerin yedekleri alınmalı ve güncel bir kopyası farklı bir yerde saklanmalıdır.

C.14.4. Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

C.15. İletişim ve İşletim Güvenliği

C.15.1. Bilgi sistemlerinin iletişim ve işletim görev ve sorumlulukları kuruluşun varlıklarının yetkisiz veya kasıtsız olarak değiştirilmesi ve yanlış kullanılmasını engellemek maksadıyla ayrılmalıdır. Hiçbir personel denetimsiz veya yetkisiz olarak sistemlere erişemez ve sistemleri değiştiremez.

C.15.2. Bilgi İşleme ve İşletim yönetimi aşağıda belirtilen konuları kapsar;

- Bilgi işleme ve bulundurma gereksinimlerinin belirlenmesi,
- Bilginin yedeklenmesi,
- En erken işe başlama ve en geç işi tamamlama zamanlarının belirlenmesi,
- Sistem kullanım kısıtları hata mesajlarını yöneten talimatların oluşturulması,
- Beklenmeyen işletim ve teknik sorunlar karşısında destek irtibatları belirlenmesi,
- Güvenli çıktı alma talimatlarının hazırlanması,
- Sistem hatası durumunda yeniden başlatma ve kurtarma süreçlerinin belirlenmesi,
- Sistem izleme kayıtlarının yönetiminin planlanması ve uygulanması.

C.15.3. Uygulama geliştirme, test ve operasyonel sistemlerinin ayrılması;

C.15.3.1 Yazılımın geliştirme sistemlerinden uygulama sistemlerine aktarımı kuralları belirlenmeli ve dokümante edilmelidir.

C.15.3.2 Geliştirme ve uygulama yazılımları ayrı işlemcilerde, ayrı sistemlerde, ayrı etki alanlarında veya kütüphanelerde çalıştırılmalıdır.

C.15.3.3 İhtiyaç olmadığı durumlarda operasyonel sistemlerde derleyici, editör, ve diğer geliştirme araçları bulundurulmaz.

C.15.3.4 Test sistemi operasyonel sistemle mümkün olduğunca aynı sistem olmamalıdır.

C.15.3.5 Kullanıcılar test ve uygulama sistemlerinde farklı kullanıcı tanımları kullanmalıdır.

C.15.4. Üçüncü taraflardan hizmet alımı esnasında gereken aktarımlar (bilgi, bilgi işleme imkânları ve taşınan diğer unsurlar) planlanmalı ve güvenlik daima göz önünde bulundurulmalıdır. Üçüncü taraf hizmetlerinin izlenmesi ve gözden geçirilmesi kapsamında;

C.15.4.1 Hizmet performans seviyesinin anlaşmaya uyumlu olduğu izlenmelidir.

C.15.4.2 Üçüncü tarafça hazırlanan hizmet raporları gözden geçirilmeli, anlaşmada belirtildiği şekilde geliştirme toplantıları yapılmalıdır.

C.15.4.3 Alınan hizmete ilişkin üçüncü taraf tarafından tutulan güvenlik olayları kayıtları, operasyonel sorunlar, hatalar, hizmet kesintileri gözden geçirilmelidir.

C.15.4.4 Varsa tespit edilen sorunlar yönetilmeli ve çözülmelidir.

C.15.5. Üçüncü taraf hizmetlerinde yapılan değişikliklerde;

- Ağdaki değişimler,
- Yeni teknolojilerin kullanımı,
- Yeni ürünlerin daha yeni sürüm ve baskılara uyumu,
- Yeni geliştirme araç ve ortamları,
- Hizmetlerin verildiği fiziksel yerin değişimi göz önüne alınmalıdır.

C.15.6. Üçüncü taraflardan hizmet alımlarında değişiklik olması durumunda; kuruluş tarafından yapılan değişikliklerde;

- Sunulan hizmetteki gelişmeler,
- Yeni uygulama ve sistemlerin geliştirilmesi,
- Kurumun politikalarındaki değişiklik ve güncellemeler,
- Güvenliği geliştirmek ve bilgi güvenliği olaylarını çözmek için geliştirilen yeni kontroller göz önüne alınmalıdır.

C.15.7. Bilgi işlem teçhizatının kapasite yönetimine ilişkin olarak anahtar konumundaki sistem kaynaklarının kullanım durumu sistem yöneticileri tarafından sürekli izlenir, her yeni veya devam eden faaliyetin kapasite gereksinimi belirlenir. Sistemden en uygun şartlarda verim almak için sistem ayarları sürekli kontrol edilir. Gelecekteki sistem ihtiyaçları, ileriye yönelik planlanan yeni iş uygulamaları ve mevcut kapasite göz önüne alınarak değerlendirilir.

C.15.8. Ağ güvenliği;

C.15.8.1 Mümkün olduğu takdirde ağdan sorumlu personel bilgisayar işletiminden sorumlu personelden ayrı görevlendirilmelidir.

C.15.8.2 Uzak cihazların yönetimiyle ilgili sorumluluklar belirlenmelidir.

C.15.8.3 Halka açık ağ veya kablosuz ağlardan iletilen verinin bütünlüğünü sağlayacak tedbirler alınmalıdır.

C.15.8.4 Güvenlikle ilgili olayların kaydedilmesini sağlayıcı uygun izleme yöntemleri kullanılmalıdır.

C.15.8.5 Hizmet kalitesini artırmak ve bilgi işleme altyapısının sürekli kontrolünü sağlamak için yönetim faaliyetleri yakından koordine edilmelidir.

C.15.8.6 Ağ hizmetlerinin güvenli bir şekilde verildiği düzenli olarak izlenmelidir.

C.14.8.7 Ağ güvenliği için yetkilendirme, kriptolama, bağlantı kontrolü vb. güvenlik tedbirleri uygulanmalıdır.

C.15.8.8 Gerekli görüldüğünde ağ kullanımına sınırlar getirilmelidir.

C.15.9. Taşınabilir ortamların yönetimi;

C.15.9.1 Tüm ortamlar üretici talimatında belirtildiği şekilde emniyetli ve güvenli ortamda saklanmalıdır.

C.15.9.2 Ortamın saklama kapasitesinden daha uzun bir süre saklanmasına ihtiyaç duyulan bilgi, aynı zamanda farklı bir ortam üzerinde de saklanmalıdır.

C.15.9.3 Veri kayıplarını engellemek maksadıyla taşınabilir ortamları izlenmelidir.

C.15.9.4 Çıkarılabilir ortam sürücüleri sadece iş ihtiyaçları için kullanılabilir hale getirilmelidir.
C.15.9.5 İhtiyaç kalmadığında tekrar kullanılabilir ortamların içeriği tekrar düzeltilemeyecek hale getirilmelidir.
C.15.9.6 Gerek görüldüğünde kurumdan taşınan ortam için yetkilendirme yapılır ve kayıt altına alınmalıdır.

C.15.10. Ortamın imha edilmesi;

C.15.10.1 Hassas bilgi içeren ortamlar yakılarak, silinerek, parçalanarak güvenli ve emniyetli bir şekilde yok edilmelidir.

C.15.10.2 Üzerindeki hassas bilgiyi ayırmaktan çok ortamları toplu olarak güvenli bir şekilde imha etmek daha kolay olabilmekte olup, bu durum imha aşamasında göz önüne alınmalıdır.

C.15.10.3 Birçok kurum atık toplama ve imha etme hizmeti vermekte olup, böyle bir kurumun seçimi durumunda güvenlik açısından uygun kontroller geliştirilmelidir.

C.15.10.4 Mümkün olduğu takdirde imha işlemi kayıt altına alınmalıdır.

C.15.11. Bilgi işleme süreci aşağıda belirtilen hususları kapsar;

C.15.11.1 Yetkisiz personelin erişimini önlemek için erişim kısıtlamaları konulmalıdır.
C.15.11.2 Bilgi belirlenen sınıflandırma seviyesine işlenmeli ve etiketlenmelidir.
C.15.11.3 Veriyi alan yetkililer kayıt altına alınmalıdır.
C.15.11.4 Girdi verisinin tamlığı, işlemenin uygun şekilde tamamlandığı ve çıktı doğrulamasının yapıldığı garanti edilmelidir.

C.15.11.5 Çıktı için havuzda bekleyen verinin hassasiyetine göre korunması sağlanmalıdır.

C.15.11.6 Üreticininbelirlediği özelliklere göre ortamların saklanması sağlanmalıdır.

C.15.11.7 Kopyalanan ortamların yetkili alıcının dikkatini çekmek için açık bir şekilde işaretlenmesi sağlanmalıdır.
C.15.11.8 Yetkili alıcı listeleri ile dağıtım listelerinin belirli aralıklarla gözden geçirilmesi sağlanmalıdır.

C.15.12. Sistem dokümantasyonunun güvenliği;

C.15.12.1 Sistem dokümantasyonu güvenli bir ortamda saklanmalıdır.

C.15.12.2 Sistem dokümantasyonuna erişim uygulama sahibi tarafından yetkilendirilmeli ve minimum seviyede tutulmalıdır.

C.15.13. Bilgi değişim esasları;

C.15.13.1 Bilgi değişiminin kopyalanması, değiştirilmesi, yanlış yönlendirilmesi ve imhasından korunması sağlayıcı tedbirler alınmalıdır.

C.15.13.2 Elektronik iletişim kullanılarak iletilen bilginin zararlı kodlara karşı korunması için tedbir alınmalıdır.

C.15.13.3 Elektronik iletişimin uygun kullanımına ilişkin politika ve prensipler geliştirilmeli ve yayınlanmalıdır.

C.15.13.4 Çalışanlar, sözleşme tarafları ve diğer kullanıcıların kurumu karalayıcı, sıkıntıya sokucu, ardı ardına zincir posta, haksız kazanç sağlama gibi faaliyetlere katılmama sorumlulukları ortaya konulmalıdır.

C.15.13.5 İletilen elektronik bilginin eklentilerinin korunmasına yönelik tedbir alınmalıdır.

C.15.13.6 Kritik ve hassas bilgi, yazıcılar, vb.cihazlar üzerinde bırakılarak yetkisiz kişilerin erişmelerine imkân verilmemelidir.

C.15.13.7 Personel faks makinelerinin dikkatsiz kullanımının bilgi güvenliği açısından verebileceği zararlar konusunda bilinçli olmalıdır.

C.15.13.9 Personel, yetkisiz bilgi toplamayı engellemek için demografik veri, e-posta adresleri, kişisel bilgi vb. kayıt edilmemesi konusunda bilinçli olmalıdır.

C.15.13.10 Telefonla görüşürken hassas bilginin ifşa edilmemesi, bilginin dinlenmemesi için tedbir alınmasına dikkat edilmelidir.

C.15.13.11 Personel faks ve fotokopi makinelerinin arıza yapması halinde hafızalarında bilgi kaldığı, onarılmayı müteakip bu bilginin basıldığı veya iletildiği konusunda bilinçli olunmalıdır.

C.15.13.12 Riskleri göz önüne alarak kablosuz iletişim kullanımı ile ilgili kurallar belirlenmelidir.

C.15.13.13 Bilginin gizliliği, bütünlüğü ve güvenilirliğini korumak için kriptografik tekniklerin kullanımı değerlendirilmelidir.

C.15.13.14 Ulusal ve uluslararası mevzuat dâhilinde tüm mesajları kapsayan iş yazışmalarının saklanması ve imhası ile ilgili kurallar belirlenmelidir.

C.15.13.15 Yetkisiz personel tarafından tekrar dinlenebileceğinden, yanlışlıkla numara çevrilebileceğinden hassas bilgi otomatik cevap kayıtlarına, iletişim sistemlerine konulmamalıdır.

C.15.14. Dış taraflarla yapılacak bilgi değişim anlaşmalarında aşağıda belirtilen hususlar göz önüne alınır;

C.15.14.1 Bilgi gönderme ve alımının kontrolü için sorumluluklar belirlenmelidir.

C.15.14.2 Gönderenin, gönderim ve alımla ilgili bilgilendirilmesi sağlanmalıdır.

C.15.14.3 İnkâr edilemezlik ve izlenebilirlik garanti edilmelidir.

C.15.14.4 Paketleme ve transfer için asgari teknik standartlar belirlenmelidir.

C.15.14.5 Emanet anlaşmaları yapılmalıdır.

C.15.14.6 Kurye belirleme standartları belirlenmelidir.

C.15.14.7 Bilginin kaybolması gibi bilgi güvenliği olaylarındaki sorumluluklar tayin edilmelidir.

C.15.14.8 Bilginin uygun şekilde korunduğunu garanti etmek maksadıyla karşılıklı mutabık kalınmış bir etiketleme sisteminin hassas ve kritik bilgi üzerinde kullanılması sağlanmalıdır.

C.15.14.9 Veri koruma, telif hakları ve lisans uyumlulukları için sorumlulukların sahibi belirlenmelidir.

C.15.14.10 Kriptografik anahtarlar gibi hassas bilginin korunmasında ihtiyaç duyulacak özel kontroller belirlenmelidir.

C.15.15. Fiziksel ortamların taşınması;

C.15.15.1 Güvenilir taşıma şekli ve kuryeler kullanılmalıdır.

C.15.15.2 Kuryelerin kimliğini kontrol eden süreçler geliştirilmelidir.

C.15.15.3 Paketleme, içeriğin fiziksel hasarlardan yeterince korunmasını sağlayacak şekilde yapılmalıdır.

C.15.15.2 Yönetim tarafından yetkili bir kurye listesi belirlenmelidir.

C.15.15.5 Hassas bilgi, kilitli kapların kullanılması, elden teslim, kurcalanmaya karşı korunmalı, gerekirse farklı yollardan parçalı olarak gönderim yöntemleri kullanılarak açığa vurulması veya değiştirilmesi önlenmelidir.

C.15.16. Elektronik mesajlaşma;

C.15.16.1 Mesajların yetkisiz erişim, değiştirilme veya hizmet engelleme saldırısından koruma, mesajın doğru adreslemesi ve iletiminin sağlanması, servisin genel güvenirliği ve kullanılabilirliği, elektronik imza vb. hukuki sebepler, anlık mesajlaşma veya dosya paylaşımı gibi halka açık dış servisleri kullanmadan önce onay elde etme, halka açık ağ erişimlerinde daha güçlü kimlik denetimi yapma konuları göz önüne alınır.

C.15.16.2 Uzmanlar arasında e-posta ile iletilen kritik bilgiler mutlaka şifrelenmelidir.

C.15.17. Çevrimiçi işlemlerle ilgili güvenlik açısından aşağıdaki hususlar dikkate alınır;

- İşlem içerisinde yer alan her iki tarafın elektronik imzalarının kullanımı,
- Her iki tarafın kullanıcı yetkilendirmelerinin doğru olduğu ve doğrulandığı, işlemlerin güvenli olduğu, her iki tarafın gizliliğinin sağlandığı,
- Tüm tarafların iletişiminin şifrelenmesi,
- Tüm tarafların iletişim protokollerinin güvenli olması,
- İş detaylarının saklandığı yerin herkes tarafından erişilemeyen bir yerde bulunması,
- Uçtan uca elektronik imzanın kullanıldığı güvenli bir yetkilendirme,
- Bilgi sistemlerinde herkese açık bilginin değiştirilmeden arşivlenmesi.

C.15.18. Erişim kontrolüne ilişkin olarak sistem kayıtları asgari aşağıdaki hususları kapsar;

- Kullanıcı tanımları,
- Sisteme giriş-çıkış tarihi, zamanı gibi ana faaliyetler,
- Terminal kimliği ve mümkünse yeri,
- Başarılı ve ret edilen sisteme erişim girişimleri,
- Başarılı ve ret edilen veri ve diğer kaynaklara erişim girişimleri,
- Sistem konfigürasyonundaki değişiklikler,
- Ayrıcalıkların kullanımı,
- Sistem olanakları ve uygulamalarının kullanımı,
- Erişilen dosyalar ve erişim türü,
- Ağ adresleri ve protokoller,
- Erişim kontrol sisteminin verdiği uyarılar,
- Anti virüs ve saldırı önleme sistemleri gibi koruma sistemlerin başlatılması ve sonlandırılması.
- Ağ üzerinde;yetkilendirmede yapılan güncellemelerde kayıtların önceki durumları ayrıca log'lanır ve arşivlenir.

C.16. Kullanıcı Hesabı Açma, Kapatma Yönetimi

C.16.1. Kullanıcı hesabı tanımlanması için 1 yöntem uygulanır.

C.16.1.1 Bağlı bulunulan müdürlüklerden resmi yazı yazılması şeklinde yapılmalıdır.

C.16.1.2 Kullanıcı hesabı kapatma talebi gelmesine istinaden dondurulur ve dondurulmuş hesaplar klasöründe bir sene süresince yasal takip ihtiyaçlarına binaen saklanır ve bir sene sonunda silinmelidir.

C.17. Erişim Yönetimi ve Erişim Kaydı Tutulması

Veri tabanlarına erişen kullanıcıların yapmış oldukları işlemler loglanmalı, gerektiğinde erişim yetkilisinin kayıt silme logları da listelenebilir olmalıdır.

C.17.1. Erişim Yönetimi

C.17.1.1. Kurumun erişim sağlanacak sunucularına admin/root yetkili yönetici kullanıcılar, sudo ve runas yetkili kısıtlı yönetici kullanıcılar ve dış dünyadan erişen, uygulamayı kullanan kullanıcılardan oluşmaktadır.

C.17.1.2. Sunuculara uzak erişim için IP/SEC ya da SSL VPN kullanılmalıdır. Mümkünse kullanıcıların erişimi için SSLVPN tercih edilmelidir. Erişim Birimi tarafından sağlanmalıdır.

C.17.1.3. Sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlar erişim verilmelidir.

C.17.1.4. Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.

C.17.1.5. Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir.

C.17.1.6. Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, ssh-key) ile yapılmalıdır.

C.17.1.7. Kullanıcıların sunucu yönetim için sağlanan erişimde erişim kısıtlı erişim yetkileri tanımlanmalıdır.

C.17.1.8. Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir. Erişim Birimi tarafından bu işlem sağlanmalıdır.

C.17.1.9. Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, sistem gurubuna teslim edilmelidir. Erişim birimi nezaretinde ve tarafından yürütülmelidir.

C.17.1.10. Sunucu servislerinin yönetim işlemleri merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır.

C.17.1.11. Kurumun yedekleme sistemlerine sadece memur ya da danışman yetkili kişi erişim yapmaktadır. Firmaların yapacakları tüm işlemler erişim birimi nezaretinde yürütülmelidir.

C.17.2. Kayıt Tutulması (Log tutulması)

C.17.2.1. Kurumun güvenlik cihazlarına ait loglar güvenlik birimi tarafından yönetilmeli ve değerlendirilmelidir.

C.17.2.2. Kurumun veri tabanlarına ait loglar database admin tarafından yönetilmeli ve değerlendirilmelidir.

C.17.2.3. Kurumun network cihazlarına ait loglar Bilgi Ağları Birimi tarafından yönetilmeli ve değerlendirilmelidir.

C.17.2.4. Tüm sunuculara ve servislere sağlanan tüm yönetici erişimleri uzak ve merkezi bir kayıt sunucusuna gönderilmelidir.

C.17.2.5. Merkezi kayıt sunucusu üzerinde yapılan analizler sonucunda başarısız erişimler raporlanmalıdır.

C.17.2.6. Merkezi kayıt sunucusu üzerinde alınan başarısız erişim istekleri uyarı olarak Bilgi İşlem Müdürüne gönderilmelidir.

C.17.2.7. Merkezi kayıt sunucusu üzerindeki başarılı girişler de istatiksel veriler halinde raporlanabilmelidir.

C.17.2.8. Merkezi kayıt sunucusu üzerindeki kayıt verileri belirli tarih aralığında tutulmalı ve istenildiğinde raporlanabilir olmalıdır.

C.17.2.9. Merkezi kayıt sunucusu kayıtlar üzerinde yaptığı analizler doğrultusunda saldırı ve normal olmayan durumları tespit edip, Bilgi İşlem Müdürüne uyarı gönderebilmelidir.

C.18. Uzaktan Erişim Yönetimi

C.18.1. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.

C.18.2. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması,erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir.

C.18.3. Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one-time password authentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir.

C.18.4. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

C.18.5. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

C.18.6. Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.

C.18.7. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.

C.18.8. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

C.18.9. Uzak erişimde yapılan tüm network hareketleri loglanmalıdır.

C.18.10. Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.

C.18.11. Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.

C.18.12. VPN ile erişecek olan kullanıcı VPN Erişim formunu doldurmak zorundadır.

C.18.13. Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi)kurumun ihtiyacına göre limitlenmelidir.

C.19. Acil Erişim Yetkilendirme Yönetimi

C.19.1. Acil erişim yetkilendirme gerektiren durumlarda uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.

C.19.2. Kurum bünyesindeki bütün dahili sunucuların, ağ güvenliği ve şebeke cihazları ile veri tabanı yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur.

C.19.3. Kurum bünyesindeki yazılım ve veri güvenliğini sağlarken yetkilendirilmiş sistem yöneticisi Güvenliği sağlamaktan sorumlu Bilgi Ağları Birimi sorumluları birlikte uyumlu çalışarak sağlamak zorundadır.

C.19.4. Sunuculara ve cihazlara acil erişim yetkilendirilmesi gereken durumlarda; kurum içi kullanıcı, yetkilendirilmiş sistem yöneticisine başvurarak sistem üzerinde yetki istemelidir.

C.19.5. Veri tabanına acil erişim yetkilendirilmesi gereken durumda; kurum içi kullanıcı için erişim yetkilendirmesinde bağlantının yapılabilmesi için yetkilendirme ayarı Bilgi Ağları Birimi sorumluları tarafından gerçekleştirilir.

C.19.6. Başka birimlerden alınması gereken erişim yetkisinin sorumluluğu, isteği yapan birimin yetkilendirilmiş yöneticisinin sorumluluğundadır.

C.19.7. Kritik sistemlerde veri güvenliğini sağlamak için sistem yöneticisi gerekli güvenlik tedbirlerini almalıdır. Güvenliği sağlamak için gereken durumlarda başka birimler ile birlikte çalışmalıdır.

C.20. Veri Merkezi Standartları ve Yönetimi

C.20.1. Kurumun veri merkezinde yedek enerji ve soğutma sistemleri olmalıdır.

C.20.2. Kurumun veri merkezi (Sistem odaları) yangın söndürme sistemlerine sahip olmalıdır. Yangın söndürme çözümleri veri merkezinde bulunan elektronik cihazlara ve personel sağlığına zarar vermeyecek şekilde olmalıdır. Bu yüzden bu özelliğe sahip gazlar kullanılmaktadır. Yangın söndürmede FM200, FE25, Argon ve Novec 1230 gazları kullanılmalıdır.

C.20.3. Veri Merkezi 7/24 güvenlik kameraları ile gözetlenmeli ve kayıt altına alınmalıdır. Veri Merkezinde bulunan iklimlendirme sistemlerinden sızan su sızıntıları, sıcaklık, yangın, voltaj değişimleri ve içeride bulunan havanın neminin izlenmesi amacıyla anlık bilgilendirme yapabilen sistemler ile takip edilmelidir. Bu bilgilendirmeler mail ve ya sms yoluyla sorumlu kişiye iletilebilmelidir.

C.20.4. Kurumun veri merkezi olarak kullanılacak odalarda dışarıya açılan pencere veya kapı (balkon kapısı) bulunmamalıdır. Girişler için sadece tek kapı bulunmalıdır ve bu kapıda da gerekli güvenlik tedbirleri (biometric giriş, card-reader, şifre paneli) alınmış olmalıdır. Veri Merkezine yetkisiz personelin girişi engellenmelidir.

C.20.5. Veri Merkezine yapılacak tüm giriş ve çıkışlar kayıt altına alınmalıdır. İlgili personel tarafından, giriş yapan kişilerin bilgileri ayrıca log'lanmalıdır. (Sistem odası giriş çıkış listesinin imzalanması vb.). Veri Merkezi 7/24 güvenlik kameraları ile gözetlenmeli ve kayıt altına alınmalıdır.

C.20.6. Veri merkezinde çalışacak personeller Veri Merkezi yönetimi konusunda yetkin olmalı ve gerekli durumlarda ilgili personele teknik ve farkındalık eğitimleri verilmelidir.

C.20.7. Veri merkezinde bulunan bütün güvenlik, acil durum ve iklim sistemlerinin periyodik bakımları yapılmalı ve bu bakımlar dokümante edilmelidir.

C.20.8. Veri merkezi içerisinde, sunucu yönetimi uzak masaüstü veya SSH gibi protokoller kullanılarak yapılmalıdır.

C.20.9. Veri merkezi içerisinde, acil durumlarda ya da felaket anında ki görev ve sorumluluklar belirlenerek dokümante edilmelidir.

C.20.10. Veri Merkezi Zemin Döşemesi kablo kanallarına ve soğuk hava akışına imkân verecek şekilde uygun bir yükseklikte (asgari 20 cm) yapılmalıdır.

Kullanılacak döşeme malzemeleri kabinlerdeki tam dolu olma durumu göz önünde tutularak 1000 kg kadar basınca dayanabilecek sağlamlıkta seçilmelidir.Zemin altında karoları tutan destek ayakları mümkün olduğunca kabin ayaklarının basacağı noktaların altına veya yakınına konarak kabin yüklerinin taşınması kolaylaştırılmalıdır. Kabinlerin sallanması gibi ihtimallere karşı bu ayaklar yerlerinden kolayca oynamayacak ve birbirine destek olabilecek şekilde yerleştirilmelidir.

C.20.11. Veri Merkezinde, sunucu kabinler ve kablolama işleri aşağıdaki standartlar çerçevesinde olmalıdır.

C.20.11.1. UTP, fiber ve enerji kablolarını birbirinden ayırmak için kanallar kullanılmalıdır. Kablolar birbirinin manyetiğinden etkilenmemelidir. Yanmaz kablolar tercih önceliğine sahip olmalıdır.

C.20.11.2. Kablo sonlandırmaları olabildiğince sağlıklı yapılmalı gerekirse sonlandırma yapıldıktan sonra kabloda performans ölçme cihazlarıyla test yapılmalıdır.

C.20.11.3. Manyetik alanın yüksek olacağı yerlerde mutlaka fiber kablo kullanılmalı,

manyetik alandan etkilenmediği için böyle noktalarda verileri fiber ile taşımalıdır.

C.20.11.4. Kablolar döşenirken kıvrılmalara izin verilmemeli, 90 derecelik keskin dönüşler daha yumuşak şekilde yapılmalıdır. Kabloların kırılmalarını veya dışlarındaki muhafazasına zarar verecek keskin kenarlar üzerinden geçmelerini engelleyecek malzemeler kullanılmalıdır.

C.20.11.5. Kabinler yerde sabit ayaklarda durmaları küçük sarsıntılarda ileri geri hareket etmelerini engelleyecek bir yapı oluşturulmalıdır. Deprem gibi durumlarda devrilme yer değiştirme gibi ihtimaller düşünülerek yerleşim yapılmalı, kablo bağlantıları çok gergin tutulmamalıdır.

C.20.11.6. Kabin kapakları yetkisiz personel tarafından açılmamalıdır.

C.20.11.7. Gerek elektrik gerek data kablolarında mutlaka ana bağlantıların yedekli olarak çekilmesine önem verilmelidir. Kabloların yedekliliğinin yanında yedek kabloların sistem odasına farklı bir güzergâhtan girişlerinin sağlanmalıdır.

C.20.11.8. Sunucular doğru şekilde etiketlenmeli, sunucu kabinleri çalışma yapılmadığı zamanlarda kilitlenmelidir. Sunucu kabinlerinde kablolamalar düzgün ve kolayca ayırt edilecek şekilde yapılmalıdır. Bütün kablolar ayrı ayrı etiketlenmelidir.

C.20.11.9 Veri merkezi kurulumunda ve kurulum sonrasında periyodik olarak gerekli testler yapılmalı ve yapılan bu testler dokümante edilmelidir.

C.21. Veri Tabanı Güvenliği

C.21.1. Veri tabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.

C.21.2. Veri tabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.

C.21.3. Veri tabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.

C.21.4. Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.

C.21.5. Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır. Belirli aralıklarla yedekten geri dönme senaryoları ile backupların güvenirliği test edilmelidir.

C.21.6. Veri tabanı yedekleme planları dokümante edilmelidir. Hangi veri tabanının, hangi yöntem ile hangi gün ve saatte yedeğinin alındığını içermelidir.

C.21.7. Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile çelik kasa gibi güvenli ortamlarda encrypted olarak saklanmalıdır.

C.21.8. Veri tabanı erişim politikaları kimlik doğrulama ve yetkilendirme usulleri çerçevesinde oluşturulmalıdır.

C.21.9. Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil DurumYönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.

C.21.10. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

C.21.11. Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.

C.21.12. Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

C.21.13. Bilgi saklama medyaları kurum dışına çıkartılmamalıdır.

C.21.14. Sistem dokümantasyonu güvenli şekilde saklanmalıdır.

C.21.15. İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.

C.21.16. Veri tabanı sunucusu sadece ssh, rdp, ssl ve veri tabanının orijinal yönetim yazılımına açık

olmalı; bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır.

C.21.17. Uygulama sunucularından veri tabanına rlogin vb. şekilde erişilememelidir.

C.21.18. Veri tabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfın açılması durumunda ilgili yetkililer bilgilendirilmelidir.

C.21.19. Ara yüzden gelen kullanıcılar bir tabloda saklanmalı, bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş(encrypted) olmalıdır.

C.21.20. Veri tabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılmalıdır. Root veya admin şifresi tanımlı kişi/kişilerde olmalıdır.

C.21.21. Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.

C.21.22. Veri tabanlarında yönetici yetkisine sahip (sysdba, sysoper, admin vb.) kullanıcı haklarına hangi kullanıcıların sahip olduğu kontrol edilmelidir.

C.21.23. Veri tabanlarında kullanıcı oluşturulabilmesi için üst idare tarafından hazırlanacak bir taahhütname doldurulmalıdır. Üst idare'ye resmi yazı ile başvurulmalıdır. Veri tabanındaki herhangi bir nesne için yapılacak yetki talepleri, ilgili nesnenin sahibi olan birim sorumlusundan veya proje yöneticisinden yazılı olarak veya e-posta yoluyla yapılmalı ve telefon ile teyit edilmelidir.

C.21.24. Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.

C.21.25. En üst düzey veri tabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.

C.21.26. Veri tabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.

C.21.27. Veri tabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar kullanılmalıdır.

C.21.28. Veri tabanı sunucularına ancak yetkili kullanıcılar erişmelidir.

C.21.29. Veri tabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler ara yüzden sağlanmalıdır.

C.21.30. Veri tabanı kullanıcılarının mesai saatleri içerisinde deployment yapmaları engellenmelidir.

C.21.31. Veri tabanı sunucularına giden veri trafiği ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için mümkünse şifrelenmelidir.

C.21.32. Bütün şifreler düzenli aralıklarla değiştirilmelidir. Şifre belirleme konusunda "Parola Güvenliği Politikası" esas alınmalıdır.

C.21.33. Sisteme giriş denemelerinde maksimum yanlış şifre giriş değeri belirlenmeli, bu değerin aşılması durumunda belirli bir süre kullanıcı hesabı kapatılmalıdır.

C.21.34. Veri tabanı kullanıcıları belirli aralıklarla incelenmeli ve veri tabanının kendi oluşturduğu veya sonradan oluşturulan ama kullanılmayan kullanıcı hesapları belirlenmeli ve kilitlenmelidir.

C.21.35. Veri tabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

C.21.36. Alınan veri tabanı yedekleri disklerdeki doluluk oranına bağlı olarak en azından en son full yedek ve devamındaki incremental yedekleri olacak şekilde saklanmalıdır.

C.21.37. Veri tabanı yedeklerinin başarılı bir şekilde alınıp alınmadığı bilgisi, yedekleme işleminin sonunda otomatik olarak e-posta yoluyla veri tabanı yöneticilerine gönderilmelidir.

C.21.38. Veri tabanı tablo erişim hakları belli aralıklarla denetlenmelidir.

C.21.39. Uygulama kullanıcısı üzerinden gelen DB sorgularının sorguyu yapan uygulama kullanıcısı ile eşleştirilmesi için gerekli altyapı/kodlama sağlanmalıdır.

C.22. Kaydedilebilir Taşınır Materyaller Güvenliği

C.22.1. Taşınacak veri eğer usb disk ile taşınacaksa bu usb diskin tehdit unsuru olan bir yazılım içermediğine emin olunmalıdır.

C.22.2. Usb disk biçimlendirdikten sonra veriyi kopyalanmalıdır. Aksi takdirde içerisinde tehdit unsuru olan casus yazılımlar usb disk içindeki verinin silinmesine veya başkalarını eline geçmesine neden olabilir.

C.22.3. Taşınacak verinin de tehdit unsuru içeren herhangi bir yazılım içermediğine emin olunmalıdır.

C.22.4. Veriyi ister usb disk isterse de cd, dvd ortamında taşınsın kesinlikle şifrelemelidir.

C.22.5. Veriyi usb disk ile taşıyorsak; bunları bilgisayara takarken usblerin sağlıklı çalıştığından emin olmalıyız. Aksi taktirde aygıtımızın bozulmasına neden olabilir.

C.22.6. Usb diskleri bilgisayardan çıkartırken aygıtı düzenli şekilde çıkart dedikten sonra bilgisayardan çıkartmalıyız aksi taktirde aygıtımız bozulabilir.

C.22.7. Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.

C.22.8. Cd ve dvdlerde veri saklamak için ise kaliteli medyalar kullanmalı, düşük hızla yazdırmalı, alt yüzeye mümkün olduğunca temas etmemeli, nemli, ışık almayan ortamlarda cdleri çok fazla sıkıştırmadan saklamalıdır.

C.22.9. Kötü amaçlı kimselerin bilgilerimize ulaşmasını engellemek için taşınabilir materyallerimizi güvenilir şekilde muhafaza etmeliyiz. Gerekirse kilitli dolaplarda veya çelik kasalarda muhafaza edilmelidir.

C.22.10. Taşınır materyaller çalışma masasında veya bilgisayarda güvensiz şekilde bırakılmamalıdır. Yanımızda, kaybedebileceğimizden dolayı mümkün olduğunca taşınmamalıdır. Eğer taşınıyorsa veri kesinlikle şifrelenmelidir.

C.23. Bilgi Sistemleri Edinim Geliştirme ve Bakımı

C.23.1. Bakanlık politikalarına uygun ihtiyaçlar hızlı ve güvenli bir şekilde sağlanmalıdır.

C.23.2. Yatırım yapılan teknolojilerde üretici bağımsız ve yaygın ürünler tercih edilmelidir.

C.23.2. Bilgi sistemleri ihtiyaçları tam, sorunsuz karşılayacak ürünler tercih edilmelidir.

C.23.3. Tüm bilgi sistemleri ihtiyaçları, kapasite planlaması yapılarak tespit edilmelidir. Gerekli ihtiyaçlar ivedilikle yönetime sunulmalıdır.

C.23.4. Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.

C.23.5. Firma teknik destek elemanlarının bakım yaparken "Karabağlar Belediyesi Bilgi Güvenliği Politikaları" na uygun davranmaları sağlanmalı ve kontrol edilmelidir.

C.23.6. Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.

C.23.7. Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" uygulanmalıdır.

C.23.8. Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.

C.23.9. Sistem bakımlarından sonra bir güvenlik açığı oluştuğundan şüphelenilmesi durumunda "Bilgi Güvenliği Politikaları" uyarınca hareket edilmelidir.

C.23.10. Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için bütçe ayrılmalıdır.

C.23.11. Yüklenici teknik destek elemanlarının bakım yaparken bu kılavuza uygun davranmaları sağlanmalı ve kontrol edilmelidir.

C.23.12. Bilgi sistemleri edinimi ve sistem geliştirmede güvenlik gereksinimi analizi;

C.23.12.1 Kontrol gereksinimlerinin belirtimi bilgi sistemi içerisindeki otomatik kontrolleri ve manüel kontrolleri kapsar. Aynı kontroller iş ihtiyaçları için geliştirilen veya sipariş edilen yazılım paketleri için de dikkate alınmalıdır.

C.23.12.2 Güvenlik gereksinimleri ve kontroller bilgi varlıklarının iş değerini ve güvenlik kaybı veya güvenlik hatalarından kaynaklanan potansiyel iş kayıpları göz önüne alınarak düzenlenmelidir.

C.23.12.3 Bilgi güvenliği için sistem gereksinimleri ve güvenliği uygulama süreçleri bilgi sistemleri projelerinin ilk aşamalarında entegre edilmelidir. Tasarım aşamasında oluşturulan kontrollerin uygulanması ve geliştirilmesi sistemlerin kurulması veya kurulması aşamasından sonraki aşamalardaki uygulanmasından daha az maliyetli olacaktır.

C.23.12.4 Eğer ürünler sipariş edilmiş ise bir test ve edinim süreci takip edilir. Üreticiler ile yapılan sözleşmeler belirlenmiş güvenlik gereksinimlerini karşılamalıdır. Güvenlik fonksiyonlarının gereksinimleri karşılamadığı noktada, satın almadan önce riskler belirlenmeli ve ilgili kontroller oluşturulmalıdır.

C.23.13. Uygulama yazılımlarında giriş verisinin geçerlemesi;

C.23.13.1 Sınır dışı değerler, veri alanlarındaki geçersiz karakterler, kayıp veya eksik veri, üst ve alt değer sınırlarının aşımı, yetkisiz veya tutarsız kontrol verisi gibi hataları gidermek için kontroller yapılmalıdır.

C.23.12.2 Anahtar alanların veya veri dosyalarının geçerliliğini ve bütünlüğünü korumak için içeriklerinin periyodik olarak gözden geçirilmesi sağlanmalıdır.

C.23.13.3 Geçerleme hatalarına karşılık olarak izlenecek süreçler belirlenmelidir.

C.23.13.4 Makul girdi verisinin test süreçleri uygulanmalıdır.

C.23.13.5 Veri girişi ile görevlendirilen personelin sorumlulukları belirlenmelidir.

C.23.13.6 Veri giriş prosesi için izleme (log) kayıtları tutulmalıdır.

C.23.13. Uygulama yazılımlarında iç işleyişin kontrolü;

C.23.12.1 Veri değişikliklerini işlemek için ekleme, değiştirme ve silme fonksiyonları kullanılmalıdır.

C.23.13.2 Programların yanlış sırada çalışmasını veya önceki programın hataya düşmesi durumunda sıradaki programın çalışmasını önlemek maksadıyla kontroller yapılmalıdır.

C.23.13.3 Tampon belleğin aşırı işlem/taşma durumunu kullanarak yapılan ataklara karşı koruma sağlanmalıdır.

C.23.14. İç işleyiş ile ilgili kontrol listeleri aşağıdaki hususları dikkate almalıdır;

- İşlem güncellemelerinden sonra veri kütüklerini dengeleyen ve düzenleyen oturum süresince veya toplu kipte yürütülen kontroller,
- Önceki kütük kapatmalarına karşı açma dengelemelerini kontrol etmek için programların çalışması esnasında, kütük güncellemeleri bazında ve programlar bazında yapılan dengeleme ayarları,
- Sistem tarafından üretilen girdi verisinin doğrulanması,
- Merkezi ve uzak sistemler arasında indirilen veya karşı tarafa yüklenen veri veya yazılımın bütünlüğü, yetki durumu ve diğer güvenlik seviyesinin kontrolü,
- Kayıtların ve kütüklerin özetleme algoritmalarının toplamları,
- Uygulama programlarının doğru zamanda çalıştığının kontrolü,
- Programların doğru sırada çalışması, hata durumunda çalışmanın kesilmesi ve sorun çözülünceye

kadar çalışmanın durdurulduğunun kontrolü,
- İşlev kapsamındaki faaliyetlerin izleme kayıtlarının (log) yaratılması,
- Uygulamalarda yetkilendirme ve mesaj bütünlüğünün korunması, bu maksatla uygun kontrollerin belirlenmesi.

C.23.15. Uygulama yazılımlarında çıkış verisinin geçerlemesi;

C.23.15.1 Çıktı verisinin uygunluğu kontrol edilmelidir.

C.23.15.2 Tüm verinin işlenmesini sağlanmalıdır.

C.23.15.3 Bilginin doğruluğunu, tam olduğunu, hassasiyetini ve sınıflandırmasını belirtmek maksadıyla yeterli bilgi sağlanmalıdır.

C.23.15.4 Çıktı geçerleme testleri uygulanmalıdır.

C.23.15.5 Çıktı geçerleme testlerinin izleme kayıtları (log) tutulmalıdır.

C.23.15.6 Karabağlar Belediyesi bilgi sistemlerindeki çıktıların doğruluğunun taşıdığı hayati önem daima göz önünde bulundurulmalıdır.

C.23.16. Operasyonel sistemlerdeki arızaları en aza indirmek ve güvenli işletim için aşağıdaki hususlara dikkat edilmelidir;

C.23.16.1 Yazılım uygulamaları ve program kütüphanelerinin güncellemesi eğitimli personel tarafından uygun yönetim yetkisi alında yapılmalıdır.

C.23.16.2 Operasyonel sistemler sadece onaylanmış çalıştırılabilir kodları tutar, bu sistemlerde geliştirme kodları veya derleyiciler bulunmamalıdır.

C.23.16.3 Uygulama ve operasyon sistem yazılımları geniş kapsamlı ve başarılı testlerden sonra sisteme yüklenmelidir. Bu testler kullanılabilirlik, güvenlik, diğer sistemler üzerindeki etkiler ve kullanım kolaylığı testlerini içerir ve ayrı sistemlerde uygulanmalıdır. Karşılık gelen program kaynak kütüphanelerinin güncellenmesi sağlanmalıdır.

C.23.16.4 Sistemin konfigürasyonu dokümante edilmeli, uygulanan yazılımların kontrolü için bir konfigürasyon kontrol sistemi oluşturulmalıdır.

C.23.16.5 Değişiklikler yürürlüğe girmeden önce bir geri kurtarma stratejisi belirlenmelidir.

C.23.16.6 Operasyonel program kütüphanelerinin güncellenmesinde izleme kayıtlarının (audit log) tutulması sağlanmalıdır.

C.23.16.7 Beklenmedik durumlar için uygulama yazılımlarının önceki versiyonlar saklanmalıdır.

C.23.16.8 Veri arşivlendiği sürece yazılımların eski versiyonları, gerekli bilgi, parametreler, prosedürler, konfigürasyon detayları ve destek yazılımları ile birlikte arşivlenmelidir.

C.23.17. Operasyonel verinin test verisi olarak kullanılırken güvenliğinin sağlanması;

C.23.17.1 Operasyon sistemi için kullanılan erişim kontrol usulleri test uygulama sistemlerinde de kullanılır.

C.23.17.2 Test sistemine operasyon bilgisinin her kopyalanışında ayrı bir yetkilendirme yapılmalıdır.

C.23.17.3 Test tamamlanmayı müteakip operasyonel bilgi test sisteminden hemen silinmelidir.

C.23.17.4 Operasyonel bilginin kopyalanması ve kullanımının izleme kayıtları (audit log) tutulmalıdır.

C.23.17.5 Karabağlar Belediyesi Bilgi sistemlerinde saklanan veriler asla test maksatlı olarak kullanılamaz.

C.23.18. Program kaynak kodlarına erişimin kontrolü;

C.23.18.1 Mümkün olduğu takdirde programların kaynak kütüphaneleri operasyonel

sistemler üzerinde tutulmaz.

C.23.18.2 Programların kaynak kodları ve kaynak kodu kütüphaneleri kontrol altında bulundurulmalıdır.

C.23.18.3 Destek personeli program kaynak kodu kütüphanelerine sınırsız erişim yetkisine sahip olamaz.

C.23.18.4 Program kaynak kütüphanelerinin, ilgili öğelerin ve program kaynaklarının programcılara yayımı uygun yetkiler alındıktan sonra yapılmalıdır.

C.23.18.5 Program listeleri güvenli bir ortamda saklanmalıdır.

C.23.18.6 Program kaynak kütüphanelerine erişimlerin izleme kayıtları (log) tutulmalıdır.

C.23.18.7 Program kaynak kütüphanelerinin bakımı, kopyalanması sıkı değişim kontrolleri ile kontrol altında bulundurulmalıdır.

C.23.19. Değişim kontrolleri aşağıda belirtilen hususları içermelidir;

C.23.19.1 Kararlaştırılmış yetki seviyelerinin kaydı tutulmalıdır.

C.23.19.2 Değişikliklerin yetkili kullanıcılar tarafından yapılması sağlanmalıdır.

C.23.19.3 Değişikliklerin mevcut durumu tehlikeye atmaması için kontroller ve bütünlük süreçleri gözden geçirilmelidir.

C.23.19.4 İyileştirme gerektiren yazılımın tamamı, bilgi, veri tabanı varlıkları ve donanım belirlenmelidir.

C.23.19.5 İşin başlamasından önce resmi bir onay alınmalıdır.

C.23.19.6 Yetkili kullanıcıların uygulamadan önce değişiklikleri üstlenmeleri sağlanmalıdır.
C.23.19.7 Her değişiklikten sonra sistem dokümantasyonunun güncellenmesi, eski dokümantasyonun arşivlenmesi veya imha edilmesi sağlanmalıdır.

C.23.19.8 Tüm yazılım güncellemeleri için sürüm kontrolü sağlanmalıdır.

C.23.19.9 Tüm değişiklik gereksinimlerinin izleme kayıtları (log) tutulmalıdır.

C.23.19.10 Operasyon dokümanlarının uygun bir şekilde değiştirilmesi sağlanmalıdır.

C.23.19.11 Değişiklik uygulamalarının iş süreçlerini bozmayacak şekilde uygun zamanda yapılması sağlanmalıdır.

C.23.20. İşletim sistemindeki değişikliklerden sonra uygulamaların teknik olarak gözden geçirilmesi;

C.23.20.1 Uygulama kontrollerinin ve bütünlük prosedürlerinin işletim sistemi değişikliklerinden zarar görmediğini garanti etmek için gözden geçirilmesi sağlanmalıdır.

C.23.20.2 Yıllık destek planı ve bütçenin işletim sistemi değişikliğinden kaynaklanan gözden geçirme ve sistem testlerini karşılaması sağlanmalıdır.

C.23.20.3 İş süreklilik planlarında uygun değişikliklerin yapılması sağlanmalıdır.

C.23.21. Yazılım paketlerinde değişiklik yapıldığında aşağıdaki hususlar dikkate alınmalıdır;

C.23.21.1 Yazılım içindeki kontroller ve bütünlüğün tehlikeye düşme riski değerlendirilmelidir.

C.23.21.2 Telif hakkı sahibinin izninin alınıp alınmayacağı belirlenmelidir.

C.23.21.3 İhtiyaç duyulan değişikliklerin üreticiden standart program güncellemesi olarak alınma ihtimali değerlendirilmelidir.

C.23.21.4 Eğer kurum değişiklikler sonucunda ileriki bakımlar için sorumlu olacaksa bunun etkisi değerlendirilmelidir.

C.23.22. Bilgi sızma risklerini kısıtlamak maksadıyla aşağıdaki hususlar dikkate alınmalıdır;

C.23.22.1 Saklı bilgi için gönderilen iletişimin ortamının taranması sağlanmalıdır.

C.23.22.2 Üçüncü tarafların sistem ve iletişim durumlarından muhtemel bilgi çıkarmalarını azaltmak için bu durumlar maskelenir veya değiştirilmelidir.

C.23.22.3 Yüksek seviyede bütünlük sağlayan sistem ve yazılımlar kullanılmalıdır.

C.23.22.4 Mevcut mevzuat ve düzenlemeler çerçevesinde personel ve sistemin düzenli olarak gözlenmesi sağlanmalıdır.

C.23.22.5 Bilgisayar sistemlerindeki kaynak kullanımı izlenmelidir.

C.23.23. Dışarıdan (dış kaynaktan) sağlanan yazılım geliştirme ile ilgili olarak aşağıda belirtilen konular dikkate alınmalıdır;

- Lisans anlaşmaları, kod mülkiyeti, telif hakları,
- Yürütülen işin kalitesi ve doğruluğuna ait sertifikasyon,
- Üçüncü tarafın başarısız olması durumunda alınacak tedbirler,
- Yapılan işin kalite ve doğruluğunun izlenmesi için yetki,
- Kodun kalitesi ve güvenlik fonksiyonelliği için sözleşme gereksinimleri,
- Kurulumdan önce zararlı ve trojan kodları tespit etmek için test etme.

C.23.24. Teknik açıklıkların kontrolü;

C.23.24.1 Açıklıkları gözleme, açıklık risk belirlemesi, yamalar, varlıkların izlenmesi, gerekli koordinasyon sorumluluklarıdâhil teknik açıklıkların yönetimiyle ilgili görevler ve sorumluluklar belirlenmelidir.

C.23.24.2 Teknik açıklıkları belirlemek ve bunlarla ilgili farkındalığı sağlamak için kullanılacak kaynaklar belirlenmelidir. Bu kaynaklar envanter değişikliklerinde veya yeni kaynaklar bulunduğunda güncellenmelidir.

C.23.24.3 Potansiyel teknik açıklık bildirimlerine reaksiyon göstermek için bir zaman çizelgesi oluşturulmalıdır.

C.23.24.4 Potansiyel bir teknik açıklık ortaya çıktığında ilgili riskler ve alınacak tedbirler belirlenmeli böyle bir tedbir açıklık olan sistemlerin yamalanması veya diğer kontrolleri içerebilmelidir.

C.23.24.5 Teknik açıklığın belirlenmesinin aciliyetine bağlı olarak alınan tedbir değişim yönetimiyle ilgili kontrollere göre veya güvenlik ihlali durumunda uygulanacak süreçlere göre devam ettirilmelidir.

C.23.24.6 Eğer yama mevcutsa yamanın oluşturabileceği riskler ile teknik açıklığın riskleri karşılaştırılmalıdır.

C.23.24.7 Yamalar yüklenmeden önce etkinliğini ve tolerans gösterilemeyecek yan etkilerini ortaya koymak maksadıyla test edilmelidir. Eğer yama mevcut değil ise açıklıkla ilgili servisler ve imkânlar kapatılmalı, ağ sınırlarına güvenlik duvarı kurulması gibi erişim kontrolleri ilave ve adapte edilmeli, mevcut atakları önlemek ve tespit etmek için izleme artırılmalı ve açıklığın farkındalığı artırılmalıdır.

C.23.24.8 Uygulanan tüm prosedürler için izleme kaydı (log) tutulmalıdır.

C.23.24.9 Yüksek riskli sistemler öncelikle belirlenmelidir.

C.24. Yedekleme ve İş Sürekliliği Yönetimi

C.24.1. Veri Yedekleme

C.24.1.1. Veri yedeklemesi kurumun kritik BT işlemlerinden birisidir. Kurum politikasında yedekleme konusu mutlaka yer almalı ve veri yedeklemesi için yönetim prensiplerini ortaya koyan bir politika bulunmalıdır. Kurum verisinin yedekleme işlemleri yedekleme politikasına göre yerine

getirilmelidir.

C.24.1.2. Kurumun bütün verisinin, kurum çapında kullanılan sunucu işletim sistemlerinin ve uygulamaların tamamının yedeği uygun ve düzenli olarak alınmalıdır.

C.24.1.3. Yedekleme sistemi iş sürekliliği planında yer alan veri yedekleme ihtiyacını karşılamalıdır.

C.24.1.4. Yedeği alınacak veri ve uygulamalar için sınıflandırma yapılmalı ve her bir sınıf için kabul edilmeli veri kaybı süresi belirlenmelidir.

C.24.1.5. Kabul edilir veri kaybı süresi yönetim tarafından onaylanmalıdır.

C.24.1.6. Yedekleme işlemlerinin sağlanması için yedekleme politikasına uygun olarak bir yedekleme planı oluşturulmalıdır.

C.24.1.7. Yedekleme işlerine ait kayıtlar tutulmalıdır.

C.24.1.8. Başarısız olan yedekleme işleri takip edilmeli ve yedeği alınamamış verinin yedeği alınmalıdır.

C.24.1.9. Yedekleme medyalarının kopyaları alınarak ana sistem odasına zarar verebilecek felaketlerden etkilenmeyecek kadar uzakta ve güvenli olarak depolanmalıdır.

C.24.1.10. Yedeklenmiş verinin düzenli aralıklarla geri döndürme testi yapılmalıdır.

C.24.1.11. Yedekleme altyapısı, yedekleme ve geri döndürme işlemleri için talimatlar hazırlanmalıdır.

C.24.1.12. Yedeklemesi alınacak bilginin seviyesi belirlenmelidir.

C.24.1.13. Yedekleme kopyalarının doğru ve tam kayıtları ve dokümante edilmiş geri yükleme süreçleri sağlanmalıdır.

C.24.1.14. Yedeklemenin türü (tam yedekleme/değişen kayıtların yedeklenmesi), yedeklemenin sıklığı iş gereklerine, güvenlik gereksinimlerine ve bilginin kritiklik derecesine göre belirlenmelidir.

C.24.1.15. Yedeklerin bir kopyası doğal afetlerden ve olası tehlikelerden korumak maksadıyla ana merkezden uzak bir merkezde saklanmalıdır.

C.24.1.16. Yedekleme bilgisine uygun seviyede fiziksel ve çevresel koruma sağlanmalıdır.

C.24.1.17. Herhangi bir tehlike durumunda kullanımını sağlamak maksadıyla yedekleme bilgisi düzenli olarak test edilmelidir.

C.24.1.18. Geri yükleme süreci düzenli olarak kontrol ve test edilmelidir.

C.24.1.19. Gizliliğin önemli olduğu durumlarda yedeklemelerin kriptolu olarak alınması göz önünde bulundurulmalıdır.

C.24.1.20. Yedekleme medyaları etiketlenmeli ve hangi medyada hangi yedeğin bulunduğuna dair kayıtlar tutulmalıdır.

C.24.2. İş Sürekliliği Yönetimi

C.24.2.1. Kuruluşun karşılaşabileceği risklerin olasılığı, zaman içerisindeki etkisi, kritik iş süreçleri belirlenmelidir.

C.24.2.2. Kritik iş süreçleri kapsamındaki varlıklar belirlenmelidir.

C.24.2.3. Hangi bilgi güvenliği olaylarının iş sürekliliğinde kesintilere neden olduğu ve etkisi araştırılmalıdır.

C.24.2.4. Operasyonel risk yönetiminin olabileceği gibi tüm iş sürekliliği sürecinin bir parçasının sigorta ettirilmesi değerlendirilmelidir.

C.24.2.5. Önleyici ve zararı azaltıcı ilave kontroller uygulanmalıdır.

C.24.2.6. Belirlenmiş bilgi güvenliği gereksinimleri için yeterli finansal, kurumsal, teknik ve

çevresel kaynakların tahsis edilmesi sağlanmalıdır.

C.24.2.7. Personel güvenliği, bilgi işleme tesisleri ve kurumsal varlıkların korunması garanti altına alınmalıdır.

C.24.2.8. Uygulamaya konulan plan ve süreçlerin düzenli olarak test edilmesi ve güncellenmesi sağlanmalıdır.

C.24.2.9. Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme;

C.24.2.9.1 İş sürekliliği prosedürleri ile tüm sorumluluklar belirlenmelidir.

C.24.2.9.2. Kabul edilebilir bilgi ve hizmet kayıpları belirlenmelidir.

C.24.2.9.3. İş operasyonlarının kurtarılması ve yeniden başlatılması için prosedürler uygulanmalıdır.

C.24.2.9.4. Kabul görmüş işlev ve prosedürler dokümante edilmelidir.

C.24.2.9.5. Planlar test edilmeli ve güncel bulundurulmalıdır.

C.24.2.9.6. Kriz yönetimi dâhil kabul görmüş işlev ve prosedürlerle ilgili personel eğitilmelidir.

C.24.2.10. İş sürekliliği planlarını test etme;

C.24.2.10.1. Farklı senaryoların masa üstü testleri (örnek kesintiler kullanılarak iş kurtarma düzenlemelerinin tartışılması) yapılmalıdır.

C.24.2.10.2. Simülasyonlar (özellikle insanların olay/kriz yönetimindeki rolleri ile ilgili eğitimleri) gerçekleştirilmelidir.

C.24.2.10.3. Teknik kurtarma testleri (bilgi sistemlerinin etkin olarak geri yüklenmesinin sağlanması), yapılmalıdır.

C.24.2.10.4. Alternatif bir yerde geri yükleme (iş süreçlerinin kurtarma operasyonlarına paralel olarak esas yerden uzakta çalıştırılması) test edilmelidir.

C.24.2.10.5. Üreticilerin hizmetleri ve kolaylıkları (haricen sağlanan hizmet ve ürünlerin sözleşme hükümlerini karşılamasının sağlanması) test edilmelidir.

C.24.2.10.6. Tam bir tatbikat (kuruluşun, personelin, malzemenin, tesislerin ve süreçlerin kesintilerin üstesinden gelme durumunun test edilmesi) gerçekleştirilmelidir.

C.24.2.10.7. Karabağlar Belediyesi bilgi sistemlerinde iş sürekliliğinin sağlanmasının taşıdığı hayati önem göz önüne alınarak alınacak tedbirler eksiksiz yerine getirilmelidir.

C.25. Bilgi Kaynakları Atık ve İmha Yönetimi

C.25.1. Karabağlar Belediyesi Müdürlükleri hizmetleri kapsamında oluşturacakları arşivden sorumludur. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.

C.25.2. Resmi evrakların yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır.

C.25.3. Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.

C.25.4. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek

lokasyon belirlenmelidir.

C.25.5. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.

C.25.6. Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.

C.25.7. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.

C.25.8. Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.

C.25.9. Hacimsel küçültme işlemi için parçalanmalıdır.

C.25.10. Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.

C.25.11. Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

C.26. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri

C.26.1. Kurum içerisinde bilgi güvenliği teknik ve farkındalık eğitimleri İnsan Kaynakları ve Eğitim Müdürlüğünce yıllık bir plan çerçevesinde yapılmalıdır.

C.26.2. Yıllık planlar çerçevesinde bilgi güvenliği teknik ve farkındalık eğitimleri gerçekleştirilmelidir.

C.26.3. Sunulan bilgi güvenliği teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülmeli ve eğitim etkililiği hususunda değerlendirme yapılmalıdır. Ayrıca katılım tutanağı düzenlenmelidir.

C.26.4. Kurumların teknik işlerinde (Bilişim faaliyetleri), uygulama geliştirme, sistem güvenliği kapsamında hizmet veren personellerin kişisel gelişimlerinin devamlılığı konusunda eğitimler düzenlenmelidir.

C.26.5. Eğitime katılım formları muhafaza edilmelidir.

C.26.6. Eğitim faaliyetleri işlemlerinin, kurum içerisinde nasıl yürütülmesi gerektiği hususunda bir prosedür geliştirilmelidir.

C.27. Değişim Yönetimi

C.27.1. Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.

C.27.2. Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.

C.27.3. Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümante edilmelidir.

C.27.4. Değişiklikler gerçekleştirilmeden önce kurumun ilgili biriminden onay alınmalıdır.

C.27.5. Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.

C.27.6. Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.

C.27.7. Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.

C.27.8. Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmeli ve dokümante edilmelidir.

C.27.9. Değişiklik yönetimini işletmek için bir talep yönetim sistemi kurmak ve işletmek önemlidir. Talebin nasıl alınacağı ve değerlendirileceği gibi esaslar tanımlanmalıdır.

C.27.10. Değişiklik onayının, "hangi kontroller ne şekilde yapıldıktan sonra verileceği" tanımlanmalıdır.

C.27.11. Değişiklik öncesi test süreci tanımlanmalıdır.

C.27.12. Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler tanımlanmalıdır.

C.28. İhlal Bildirim ve Yönetimi

C.28.1. Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

C.28.2. Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

C.28.3. Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.

C.28.4. Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.

C.28.5. İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

C.28.6. Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin süreci başlatılması için dosya İnsan Kaynakları ve Eğitim Müdürlüğüne gönderilir.

C.28.7. Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.

C.28.8. Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf ederek tedbirler alınır.

C.28.9. Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme,tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.

C.28.10. İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.

C.28.11. Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.

C.28.12. Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.

C.28.13. İnsan Kaynakları ve Eğitim Müdürlüğünce dosya Başkanlık Olur'u ile Teftiş Kurulu Müdürlüğüne gönderilir.

C.28.14. Teftiş Kurulu Müdürlüğünce Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

- Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
- Kanıtın niteliği ve tamlığını gösteren ağırlığı.

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, mevzuat veya sözleşmede belirtilen yaptırımlar biri uygulanabilir.

C.29. Bilgi Güvenliği İzleme ve Denetleme Yönetimi

C.29.1. Bilgi Güvenliği Sistemi düzenli olarak denetlenmesi sağlanmalıdır.

C.29.2. Kurum yetkilileri tarafından Bilgi Güvenliği İç Denetimleri yapılmalıdır.

C.29.3. Hazırlanacak Bilgi Güvenliği İç Denetim soru listeleri hazırlanmalıdır.

C.29.4. Denetim yapacak personelin Bilgi Güvenliği konusunda yetkilendirilmiş kurumlardan iç denetim eğitimi almaları, denetime katılacak kişilerin iç denetçi sertifikasının olması gerekir.

C.29.5. İç denetimler için bütün birimleri kapsayacak şekilde denetim planı hazırlanmalıdır.

C.29.6. Denetim sonuçları iç denetim raporu şeklinde hazırlanmalı ve üst yönetime sunulmalıdır.

C.29.7. Denetimlerde tespit edilen bulgular için çözüm önerileri geliştirilmelidir.

C.29.8. Bir sonraki yapılacak iç denetimlerde, bir önceki tespit edilen bulguların çözümlenip çözümlenmediği hususunda takip yapılmalıdır.

C.30. Bilgi Güvenliği Testleri

C.30.1. Kılavuzda belirtilen standartların uygulanmasının kontrolleri hususunda yıllık plan yapılmalı, bu plan ile takvim günleri belirlenmelidir.

C.30.2. Belirlenen yıllık plana uygun olarak kullanıcı seviyesinde, yöneticiler seviyesinde, sistem yürütücü ekip seviyesinde, makineler seviyesinde, network seviyesinde gerekli kontroller, testler yapılmalıdır.

C.30.3. Yapılan kontrol, testler sonucunda çıkan sonuçlar puanlandırılarak raporlanmalıdır. Rapor içeriğindeki ilgili bölümlerin puanlandırma seviyesine göre gerekli hallerde ek farkındalık eğitimleri, seminerler verilmelidir. Makine ve network sistemi için gerekli görülen ek ayar düzeltmeleri yapılmalıdır.

C.30.4. Puanlandırma sisteminin oluşturulmasında sahadan Bilgi Güvenliği Kılavuzuna uygun olarak oluşturulmuş formlara belirlenecek personel tarafından veri bildirimleri girdirilmeli ve bu formlara uygun olarak yılın belirlenecek zamanlarında formlara uygun olarak oluşturulacak puanlamaların fiziksel kontrolleri sağlanmalıdır.

C.30.5. Yapılacak kontroller ve testler ISO 27001 sistemine, TÜBİTAK UEKAE, Siber Güvenlik Enstitüsü standartlarına bağlı kalınarak yürütülmelidir.

C.31. Acil Durum Yönetimi

A-ACİL DURUM EYLEM PLANININ AMACI VE KAPSAMI:

Acil Durum Eylem Planlaması, herhangi bir şekilde iş yapılırken, kesintiye neden olabilecek, özellikle ekipmandan kaynaklanabilecek aksiliklere karşı önlem alınmasıdır. Sorunların yada felaketlerin, tüm kaynaklar göz önünde bulundurularak iş aktivitelerine yada iş süreçlerine etkilerinin boyutlarının, olası çeşitli senaryoların ve müdahale ekibinin önceden belirlendiği,büyük çaplı bir plandır.

Bir felaket, deprem, sel ya da hortum gibi bir doğal afet olabileceği gibi su basması, enerji problemi, yangın, patlama ya da sabotaj gibi farklı biçimlerde de gerçekleşebilir. Felakete etki eden faktörleri şu şekilde sıralayabiliriz;

A)Çevre Faktörü:

1 Savaş
2 Biyolojik ve kimyasal saldırı
3 Nükleer saldırı
4 Bombalama, sabotaj, terörizm

D)İş Faktörü

1 Yangın
2 Patlama
3 Kimyasal sızıntılar
4 Radyoaktif kaçaklar

B)Doğa Faktörü:

1 Deprem
2 Sel veya su baskını
3 Fırtına

C)İnsan Faktörü:

1 Sabotaj
2 Ayaklanma
3 Kırıp girme, tahrip etme

Olağanüstü Durumlarda Karşılaşılabilecek Sorunlar

Olağanüstü durumlarda karşılaşılabilecek olası sorunlar şu şekillerde olabilir:

1. Veri kaybı
2. Enerji kaybı
3. Telekomünikasyon/ iletişim ağı hizmetlerinin kaybı
4. Sistemlerin/uygulamaların kaybı
5. Hizmet sağlayıcıların devre dışı kalması
6. Çalışma alanlarının zarar görmesi, kullanılamaması
7. Kritik/ anahtar personele ulaşılamaması
8. Can kaybı ve yaralanmalar

1 – ULAŞTIRMA:

Afet sırasında işyeri şoförü, fork-lift ehliyeti olan tüm işçiler (sadece fork-lift kullanmak için) ve güvenlik elemanları, her türlü ulaştırma işleminde görevlidirler.

2– GECE GÖREVLERİ:

Afet sırasında işyerinde gece vardiyası varsa yukarıdaki ekip üyelerindeki çalışanlar derhal görevlerinin başına geçerler. Güvenlikten sorumlu işçiler başta servis müdürü olmak üzere tüm gerekli kişilere ve/veya kurumlara haber verir.

B. ACİL DURUM OPERASYONUNUN KAPSAMI VE YÖNETİMİ

1 – KRİZ MERKEZİNİN OLUŞUMU YETKİ VE SORUMLULUKLARI

Amaç bölümünde belirtilen istenmeyen olayların vukuunda toplantı odasında bir kriz masası teşkil edilecektir.

Kriz yönetim görevleri:

1-Öncelikli olarak işyerini besleyen enerji kaynaklarını keser.

2-Yangın çıkma olasılığı olan bölgeleri kontrol eder.

3-Elektrik kaynaklarını keser.

4-Yangın çıkma olasılığı olan bölgeleri belirler ve kontrol eder.

5-Kriz merkezi ile iletişim:Görevli ekip dışında kalan herkes acil çıkışları kullanarak ana toplanma yerine gelirler.Yaralı olanlar ilk yardım ve arama kurtarma ekibini oldukları yerde beklerler.

6-Arama kurtarma ekibinin binalara girmesine karar verir.

7-İşyeri dışındaki birimlerle iletişimi sağlar.(hastane,itfaiye,sivil savunma,il acil durum amirliği)

8-İşçilerle iletişimi sağlar.Toplanma yerine giderek açıklamalarda bulunur.

9-İşyerinden çıkışları veya sığınma amaçlı işyerine girişleri organize eder.

10-Enerji kaynaklarının kesilmesini sağlar.

11-İşyeri ulaşımını organize eder.

12-Tüm güvenlik faaliyetlerine karar verir.(Afetin çeşidine göre işçileri korumak için gerekli tedbirler)

13-Kriz merkezinde bulunacak malzemeler:

- 1 adet masa
- 1 adet telefon (dış hatlara erişimi olan) (dahili tel:……)
- Acil durum eylem planları ve gerekli tüm telefon numaraları
- İşyerinin detaylı projesi
- Pilli radyo ve pil
- 10 metre telefon kablosu
- 1 adet megafon
- 2 adet emniyet şeridi
- 10 adet kırmızı tükenmez kalem
- Not kağıtları
- İl için acil durum telefon numaraları
- Müdahale ekibi listeleri

2 – YANGIN SÖNDÜRME EKİBİNİN YETKİ VE SORUMLULUKLARI

Ekip, yangın durumunda derhal devreye girer. Toplanma yerinde toplanırlar. Yangın yeri amiri ve/veya ekip başının talimatlarıyla yangına müdahale eder. Ekip üyeleri işletmeyi,yangın risklerini ve yangın söndürme malzemelerinin yerini iyi bilmelidir.Yangın tüpleri ve hortumlarının yerlerini gösteren bir planda bulunmalıdır.

Ekip Lideri: Kargaşa ve paniğe izin vermeden, ekibini sevk ve idare ederek yangına müdahaleyi sağlatır. Ekip başı, yanma ürünlerini ve yangın yerindeki tehlikeleri iyi bilmelidir. Yangın ihbarı olduğunda, yanan yerdeki yangına,hangi söndürücü ile nereden müdahale edileceğini söylemeli ve uygulatmalıdır.

Keşifçi / Nozulcu: Mevcut koruyucu teçhizatlarını giymiş olarak yangın mahallindeki ilk müdahale ile birlikte, yangının keşfini yapar. Neyin yandığını nerelere ve ne kadar hızla yayılabileceği, nereden ve hangi söndürücüyle müdahale edilmesi gerektiği ile ilgili keşif değerlerini ekip liderine bildirir. Bu esnada ekipteki diğer personelin getirdiği söndürücülerle yangına müdahale ederken, yangını kontrol altına almaya ve söndürmeye çalışır.

Hortumcu / Takımcı: Görevi,yangına direkt müdahale eden keşifçi /nozulculara söndürücü malzeme iletmektir.Yangın sınıfına göre ve ekip amirlerinin direktifi doğrultusunda su,köpük,kuru kimyevi toz ve CO_2 vb. söndürücülerin yerlerini iyi bilmelidirler.Su ile yapılan söndürme çalışmalarında yangın söndürme dolaplarından hortumu ve vanayı açar,keşifçi ise vanayı kapatmak üzere hazır bekler.

Hortumcu / Takımcılarının birincisi,keşifçi / nozulcunun hemen arkasında yer alır.Hortumları,takımları takip ederken keşifçinin / nozulcunun can güvenliğinden de sorumludur.Yine yangın mahallinde ihtiyaç duyulabilecek balta,merdiven,kazma, kanca,vb. mekanik yardımcıları ulaştırmak hortumcu / takımcıların görevidir.

3 – KURTARMA EKİBİNİN YETKİ VE SORUMLULUKLARI

a) Ekibin üyeleri afetten sonra toplandıkları yerden,hemen kriz merkezine intikal ederler.

b) Kriz merkezine intikal eden arama-kurtarma ekiplerinden ikişer kişilik gruplar oluşturulur,

c) Arama-kurtarma yapacakları bölgeye giderler.

d) Afet mahallinde,mahsur kalan personel başta olmak üzere,kıymetli evrak, para, vb. malzemeyi kurtarır

e) Ekip personeli yaralıyı kurtarma ve taşıma tekniklerini çok iyi bilmelidir.

f) Yangınla bağlantılı olan kapı,valfleri açıp-kapatmak,yangın mahalli civarında boşaltılması gereken yerlerdeki malzemeleri öncelik derecesine göre toplayıp, paketlemek ve güvenli bir yere nakledilmesini sağlamakla görevlidir.

g) Ekip personeli,görevinin gerektirdiği kurtarma ve taşıma tekniklerini iyi bilmeli, ayrıca kurtarma teçhizatı ile araç-gereçlerini işletme riskine uygun olarak bulundurup,uygun yerlerde muhafaza etmelidir.

h) Gerektiğinde kriz masasından takviye arama-kurtarma, ilk yardım ekibi ve teknik malzeme isterler.

ı) Tahliye süresince tüm kitlenin koşmadan ve paniklemeden tahliye olması için yönlendirmede bulunurlar

i) Tüm görev bölgesi elden geçene kadar arama-kurtarma çalışmalarını sürdürürler

j) Gerektiğinde kriz merkezi, görev yerlerini ve ekipleri değiştirebilir

4 - İLK YARDIM EKİBİNİN YETKİ VE SORUMLULUKLARI

Görevi,afet anında işyeri mahallinde yaralanan kişilere ilk yardım yapmak ve en yakın sağlık merkezine ulaştırılmalarını sağlamaktır.Öncelikle yangında boğulma, kanama ve kırıklar konusundaki ilk yardım teknikleri,ekipte görevli her personel tarafından çok iyi bilinmelidir.

a) Tahliye süresince tüm kitlenin koşmadan ve paniklemeden tahliye olması için yönlendirmede bulunurlar.

b) Ana toplanma alanına, ilk yardım malzemelerini getirerek yaralılara müdahale ederler.

c) Yürüyebilen yaralıları ilk yardım merkezine götürür (doktor odası), yürüyemeyecek durumda olan yaralılar için kriz merkezine haber verirler.

d) Yaralılarla ilgilenir, hastaneye sevk edilmesi gereken yaralıları saptar, kriz merkezi ile ilişkiye girerler.

5 - KORUMA VE GÜVENLİK EKİBİNİN YETKİ VE SORUMLULUKLARI:

a. Olağanüstü hallerde (yangın, deprem, sel, sabotaj vs.) işletmelerin güvenlik tedbirlerini arttırır.

b. İşyeri mahallinde araç ve personel trafiğini düzenler.
c. Yardıma gelen itfaiye, ambulans ve güvenlik güçlerine (jandarma, polis) kılavuzluk eder.
d. İşyeri mahallinden veya civarından tahliye edilen malzemeyi emniyetle koruma altına alır.
e. Kapılarda görevli olan güvenlik ekibi, afetten hemen sonra tahliye kapılarından çıkışı olaylaştırmak için kapı önü birikmelerini önler.
f. Deprem gibi afetlerde artçı şoklar olabileceği için dışarı çıkanların tekrar içeri girmemelerini sağlarlar
g. Tehlikeli bölgelere veya korunması gereken yerlere emniyet şeridi çeker.

6-SIZINTI EKİBİ YETKİ VE SORUMLULUKLARI

a. Kimyasal maddelerin bulunduğu depo,boru ve ekipmanlarında herhangi bir kaçak olmadığını kontrol eder.
b. Tehlikeli olabilecek sahayı şeritlerle belirler, bu bölgeye personelin yaklaşmasını önler.
c. Tehlikeli maddenin zehirli parlayıcı, patlayıcı olması durumuna göre gerekli ikaz ve önlemleri aldırır.

7-ELEKTRİK VE MEKANİK BAKIM EKİBİ

a. Acil durumlarda mekanik ve elektrikle ilgili arızaların giderilmesini ve tehlikelerin ortadan kaldırılmasını sağlamak.
b. Elektrik panolarının ayda bir sağlamlığının kontrolünü yapmak.
c. Su baskını sonucu ortamda biriken suyun boşatılması mekanik ekibin görevidir. Fakat su basan kısma girmeden önce o bölümüm elektriği elektrik ekibi tarafından kesilecektir.
d. Acil durumlarda asansörde insan olmadığı tespit edildikten sonra elektrik enerjisini kesmek.

8-TRAFİK VE ÇEVRE GÜVENLİĞİ EKİBİ

a. Acil durumlarda çevre güvenliğini sağlayacak ve trafiği yönlendirecektir.
b. Acil durumda olay yeri etrafının emniyet şeridiyle çevrelenmesi, olay yerine dışarıdan
c. herhangi bir şekilde insanların girişinin engellenmesi ve toplanma mahallindeki insanların güvenliğinin sağlanmasında sorumludur.

9-AŞIRI SOĞUK VE GAZ EKİBİ

- Herhangi bir kar yağışı sonrası ana yolların açılması ve şantiye yolların açılmasını sağlayarak genel ihtiyaç malzemelerinin şantiye bünyesine gelmesini sağlayacaktır.

C.YANGIN SÖNDÜRME EKİBİNİN YETKİLERİ, SORUMLULUKLARI VE YANGINLARDAN KORUNMA

KISIM I - AMAÇ :

İşyerinde çıkacak yangınları önleme ve yangınlardan korunma hizmetleri hususunda alınacak tedbir ve yapılacak işlerin tespitidir.

KISIM II - YANGINLARIN SEBEPLERİ VE SINIFLANDIRILMASI :

- **Yangın Sebepleri:**Yangının oluş nedenlerini birkaç başlık halinde düşünüp incelemek mümkündür.
- **Korunma Tedbirlerinin Olmaması:**Yangınların çıkmasındaki en büyük neden korunma tedbirlerinin alınmaması bir başka deyişle korunmanın olmamasıdır.Bu tedbirler amaca uygun malzeme kullanımı,teknik talimatlara uygun makine,cihaz ve teçhizat kullanılması gibi çok geniş kapsamlıdır.Can ve mal güvenliğine yönelik koruma tedbirleri gibi görünen bu önlemler yangın güvenliğinin sağlanmasında da temel faktörlerden biridir.İhtiyaç elektrik gücüne uygun kablo çekilmesi,doğalgazın kaçağının olmayacak şekilde bağlanması,soba boru ve bacaların temizlenmesi gibi bir çok örnek sayılabilir.

- **Tedbirsizlik:**Kullanılan madde ve malzemelerin yangına sebebiyet verebilecek özelliklerinin bilinmemesi veya depolama yakınlarında sigara içilmesi ve izmaritinin atılması vs. başlı başına bir yangın nedenidir.Örneğin ocağa bağlanan doğalgaz tüpünde gaz kaçağı kontrol edileceğini bilmemek veya gaz kaçağının kontrolünün çakmak,kibrit vb. alevle değil de sabun köpüğü ile yapılacağını bilmemek,tavan arası ve çatıya kolay ve çabuk tutuşabilecek eşyalar koymak,gibi örnekler gösterilebilir.
- **İhmal:**Yangından korunma tedbirleri olduğu ve bu tedbirleri bildiği halde üşenme,tembellik veya bir şey olmaz şeklindeki adamsendecilikte yangının çıkış nedenlerinden biridir.Örneğin benzin,tiner vb. maddelerle boya,temizlik gibi çalışmalar yapılırken sigara içmenin tehlikeli ve yasak olduğu bilinmesine rağmen içilmesi.Keza kullanılan elektrikli cihazların fişlerinin prize tam oturmayıp boşluk yapması ve olacak spark ile kablonun ısınıp tutuşacağının bilindiği halde kullanılması.Sıvı yakıt depo ve tanklarında gas-free yapılmadan kaynak vb. İşlem yapılması şeklinde çoğaltılabilir.
- **Kasıt ve Sabotaj:**Bilerek zarar vermeye dayanan kundakçılıkta denilen bu yolla büyük can ve mal kaybına neden olan yangınlar çıkarmaktadır.Kişilerde davranış bozuklu,bazı suçluluk duyguları ve politik nedenlere dayanan kasıt ve sabotaj sansasyonel bir haber yaratma amacıyla da yapılmakta olduğu görülmüştür.Önlenebilmesi ise düşmanca tavra neden olacak uygulamaları kaldırırken fiziki

güvenlik sistemlerinin artırılması ve güvenlik güçleri ile işbirliği yapılması ile mümkün olabilir.

- **Kaza:** Zaman zaman istem dışı bazı olaylarda yangına neden olmaktadır. Ancak bu kendiliğinden gelişen bazı olaylar başlangıçta yeterli önlemlerin alınmaması sonucu olabildiği gibi bilgisizliğinde rol oynadığını görmekteyiz. Temelde bunlar olmaksızın kazaların rol açtığı yangınlarda olmaktadır. Örneğin;Trafik kazaları araç yangınlarına,iş kazaları makine ve bina yangınlarına,soba vb. elektrikli cihazlarda meydana gelen arıza ve kazalar ise bina yangınlarına sebep olmaktadırlar.
- **Doğal Afetler:** Doğal afet olarak kendiliğinden ortaya çıkan yangınlardır. Örneğin;Yıldırım,deprem,lav (yanardağ),çiğ,sel rüzgar gibi afetler sonucu meydana gelen yangınlardır.
- **Hayvanlar:** Evlerde beslenen kedi ve köpeklerin kazalara sebep olarak yangın vesilesi oluşturduğu gibi kemirgen hayvanların tesisatları kemirmesi (fare-elektrik kablosu) ve tilki,tavşan vb. hayvanlarda yangın bölgesinde tutuşarak kaçarken başka bölgelerde yangınlara sebep olmaktadır.Özellikle orman yangınlarında ve endüstriyel işletmelerde bu tip yangınlar görülmektedir.

Yangın Sınıfları:

Yangınların bir birinden farklı davranışlar, gösterdiği görülmektedir.Her yangının oluşumu,gelişimi farklı farklı tezahür etmesine rağmen bu farklılığın yanıcı maddeden kaynaklandığı bilinmektedir.Bu nedenle yangın;yanıcı maddenin fiziksel özelliklerine göre dört kategoride incelenmektedir.

A Sınıfı Katı Yanıcı Maddeler Yangını (ADİ YANGINLAR):

Artık olarak karbon tabakası bırakan ve genelde korlu olarak yanan katı yanıcı maddelerin tutuşması ile oluşan yangınlardır. Metallerin dışındaki yanıcı katı maddeleri kapsar.Odun,kağıt,tekstil maddeleri,kauçuk bazı örneklerdir.Bu yanıcılar için için yanmaya devam etme özelliklerine sahiptirler.Yani yanma yüzeyde sınırlı olmayıp maddenin iç hücrelerine doğru devam etmektedir.Naftalin,zift gibi yanarken eriyen A sınıfı içinde değerlendirilen yanıcılarda vardır.Bu tip yanıcılarda yanma derinliklere nüfuz edemeden yüzeyde oluşur.

B Sınıfı Sıvı Yanıcı Maddeler Yangını (AKARYAKIT YANGINLARI):

Yanıcı sıvıların oluşturduğu bu yangınlar genellikle petrol türevi ve bitkisel yağların tutuşması ile oluşan yangınlardır.Ancak B sınıfı yangınları yine yanıcı madde özelliklerine göre kendi içinde de üç kategoride düşünmek doğru bir değerlendirme olur.Birincisi su ile karışmayan ham petrol,benzin,gaz yağı,makine yağları,laklar vb. sıvılar.İkincisi su ile hemen karışan(suda çözülen)alkol vb. sıvılar.Üçüncüsü ise katran,asfalt,gres vb. ağır yağlardır.B sınıfı yangınlarda yanma yüzeydedir.Yani ısınan sıvıdan çıkan buharlar yanar.

C Sınıfı Gaz Yanıcı Maddeler Yangını (GAZ YANGINLARI):

Yanabilen gazların oluşturduğu yangınlardır.Doğalgaz vb. gaz yanıcılar bu sınıfa örnek bazı gazlardır.C sınıfı yangınlarda yanma gazın sızdığı yüzeydedir.Gaz basıncının atmosfer basıncından fazla olduğu yerlerde böyle devam eder.Gaz ve atmosfer basıncının eşit olduğu yerlerde yanma bütün bölgede devam eder.Gaz, depo vb. kapalı yerlerde ise bu durumda yanma bölgesindeki hızlı yanma basıncını yenecek açıklık (havalandırma) yoksa patlama kaçınılmazdır.

D Sınıfı Hafif Metal Yangınları:

Özel yangınlar olarak da nitelendirilen D sınıfı yangınlar gelişen teknoloji ile endüstriyel çevrelerde görülmeye başlayan yangınlardır. Bu yangınlar magnezyum, alüminyum, sodyum, zirkonyum vb. hafif metallerin yanması ile oluşur.

YANGIN SÖNDÜRME PRENSİPLERİ :

Yangının sınıfı ne olursa olsun söndürme prensipleri ortaktır. Bu prensip yanmayı meydana getiren üç unsurdan yanıcı maddeyi, oksijen veya ısıyı ortadan kaldırmaktır.

YANICI MADDEYİ YOK ETMEK	ISIYI YOK ETMEK	OKSİJENİ YOK ETMEK
-Yanıcı maddeyi ortadan kaldırmak	-Su ile soğutmak	-Örtmek
-Yanıcı maddeyi ısıdan ayırmak	-Yanıcı maddeyi dağıtmak	-Boğmak
-Ara boşluğu meydana getirmek	-Kuvvetli üflemek	-Oksijeni azaltmak

Yanıcı maddeyi ortadan kaldırmak: Kırıp parçalamak,ayırmak veya sıvı akıcıyı kesmek suretiyle yanıcı maddeleri bazen ortadan kaldırmak mümkün olsa da, yanıcıların ağır ve taşınmaz mallar olduğu düşünülürse her zaman uygulama alanı bulunmayabilir.

Isıyı ortadan kaldırmak: Her yanıcı maddenin bir yanma ısısı olduğuna göre,yanan maddeleri bu ısının altına kadar soğutmak yangını söndürmek için iyi bir yöntemdir.

Oksijeni ortadan kaldırmak: Yangın mahalline ağır ve yanmaz gazlarla airesol sıvılar sevk etmek havada bulunan yaklaşık %21 oranındaki oksijen azaltılarak ortadan kaldırılmasını sağlar.

KISIM III - YANGINLARA KARŞI KORUNMA TEDBİRLERİ :

A-GENEL ÖNLEMLER :

1. İşyeri kapıları, pencereleri,havalandırma menfezleri belirli bir basınç karşısında dışarıya doğru açılacak şekilde olacaktır.
2. İşyerinde bulunan yangın su tankı,yangın pompası ile işletme elektrikleri kesilse dahi sabit sulu yangın devresi,jeneratör ile sürekli beslenecektir..
3. Yangın hortumları ve su tesisatları yangın amacı dışında,bahçe sulamak ve çevre temizlemek gibi maksatlarla kullanılmayacaktır.
4. Merkezi yangın istasyonları, yangın dolapları (Yangın hidrant ve muslukları dahil) seyyar yangın söndürme cihazları vb. sabit söndürme sistemleri, otomatik ve manuel alarm/ikaz sistemleri, gibi yangın malzeme ve yerlerinin ön ve yanları asla kapatılmayacaktır. Yerlerinin görünmesi ve her an kullanıma hazır bulundurulması ön planda tutulacaktır.
5. Yangın dolapları üzerine **"YANGIN"** kelimesi yazılmış olacak,hemen altında o dolabın sıra numarası bulunacaktır.Dolap üzerlerine talimatları asılacaktır.
6. Yangın hidrantlarının anahtarları bir zincir vs. ile hidrant bedeni üzerine asılacaktır.
7. Kapalı hacimlere dağıtılan seyyar yangın söndürücü tüpler en az 20 metre uzaktan görülecek şekilde yerleştirilmiş ve tüp üzerine yangın dolaplarında olduğu gibi numaralandırılacaktır.
8. Elle taşınabilen seyyar yangın söndürücü tüpleri, mümkünse duvar/direk üzerine yerden 105-125 cm. yüksekliğe asılacaktır. Ancak; asılma imkanı yoksa paslanmayı önlemek üzere tüp altlarına tahta/plastikten altlık konulacaktır.
9. İşyerindeki yangına hassas yerler (Kalorifer kazan dairesi, akaryakıt tesisleri, tehlikeli maddeler için ambar/depo vs.) ayrı bölmeler olarak yapılacaktır.
10. Acil Durum Eylem Planı içerisinde hazırlanması gereken Yangından Korunma Talimatının ilgili bölüm sorumluları ve maddelerin içeriğini takip edecek görevliler belirlenecektir. Böylece görevlerin sahipsiz ve boşlukta kalması önlenecektir.

B- İDARİ BİNALARDA ALINACAK ÖNLEMLER : (Büro/Ofis,Salon, vs.)

1. İdari bina yangın dolabı, alarm-ikaz, algılama sistemi, kamera sistemi ve seyyar yangın söndürme cihazları ile korunacaktır.
2. İdari binada bilgi işlem odası duman detektörü sistemi ile korunacaktır.
3. Çöp kutuları kontrollü olarak ve dolmasını beklemeden her gün akşam boşaltılacaktır.
4. Sigara izmaritlerinin gelişi güzel atılması önlenecek, kül tablaları zaman zaman ve emniyetli olarak boşaltılacak, yanan izmarit olmadığından emin olunacaktır.

5. Çöp ve sigara izmaritleri bina dışındaki saç varil/kutulara konulacaktır.
6. Isıtma amaçlı soba veya elektrikli ısıtıcıların kullanma zorunluluğu olduğu hallerde bu cihazların riziko şartlarına uygunluğu sağlanmalıdır. Yaşam mahalleri içerisinde LPG tüpü kullanılmayacaktır.
7. Mesai bitiminde elektrik, gaz, soba, kalorifer vs. emniyet hususları kontrol edilerek odalar/bölümler terk edilecektir.
8. Bütün oda kapıları numaralandırılacaktır. Oda anahtarlarına 3x3 cm. ebadında ve üzerinde oda numarası yazılı madeni etiket takılacaktır. Bu anahtarlar oda kapıları kilitlendikten sonra ilgilisince bekçi ve aynı maksatla görevlendirilen personele ait odalardaki anahtar dolabına takılmak üzere teslim edilecektir.
9. Yangından korunması gereken para, kıymetli evrak ve eşyalar önem derecesine göre kasa veya özel kilitli bölmelerde muhafaza edilecektir.
10. Yangın mahallerinde kurtarılması gereken eşya,dolap ve kasa üzerine "**YANGINDA İLK ÖNCE KURTARILACAKTIR**" yazılı etiketler konulacaktır.

11. Yangın anında kıymetli evrakın tahliye edilmesi için buralarda ve merkezi bir yerde brandadan yapılmış ağzı bağlanabilir olan yeteri kadar büyüklükte çuval/torbalar bulundurulacaktır.

C-ARŞİVLERDE ALINACAK ÖNLEMLER:

Arşivlerde alınacak önlemler TS 12115'e uygun olacaktır. Bu maksatla;

1. Aşiv kapılarına 7x15 cm. ebatlı içten ve dıştan camlı gözetleme pencereleri açılmalı ve yalnız gündüz ve sorumlu memurların refakatinde girilecektir.
2. Isıtmak için ne tip olursa olsun asla soba kullanılmayacak, keza aydınlatma sadece elektrikle yapılacaktır.
3. Mesai bitiminde görevli memur tarafından arşiv dairesinin elektrikleri ana şalterden kesilecek, kapıları kilitlenecektir.Güvenlik görevlileri / nöbetçileri kontrollerini kapı pencerelerinden yapacaklardır.
4. Arşiv malzemesini tahliye edebilecek kadar ağzı bağlanabilir branda torbalar uygun yerde bulundurulacaktır.

D- TERASTA/ÇATI KATLARI/ARALARINDA ALINACAK ÖNLEMLER:

1. Çatı aralarına asla elektrik tesisatı yapılmayacaktır / çekilmeyecektir.
2. Çatı aralarına çıkan kapılar sürekli kilitli tutulacaktır. Giriş - çıkış için seyyar veya sabit merdiven bulundurulacak, ancak sorumlusunun bilgi ve kontrolü ile giriş – çıkış sağlanacaktır.
3. Çatı arasında onarım, bakım vs. yapılması gerektiğinde; Çatı arasında sigara içilmeyecek, aydınlatma için pille çalışan el fenerleri ve akü ile çalışan seyyar aydınlatma lambaları haricinde kibrit, çakmak, mum, gaz lambası vs. kullanmayacaktır. Bu uyarı sorumlular tarafından çalışanlara tekrar hatırlatılacak, hatta talimat olarak imza karşılığı tebliğ edilecektir.(Tutanak yangın işleri dosyasında muhafaza edilmelidir.)
4. Çatı aralarındaki onarımlarda kaynak ve kesme işleri yapılacaksa o işletmede görevlendirilen iş emniyet veya yangın güvenlik personeli tarafından seyyar yangın söndürme cihazı ve yangın dolabından açılacak su hortumu ile çalışma süresince yangın emniyeti alacaktır.
5. Çatı aralarında yanıcı, parlayıcı/patlayıcı malzemeler muhafaza edilmeyecektir, depo, yatakhane vs. maksatla kullanılmayacaktır.

E- ELEKTRİK TESİSATI VE TEÇHİZATINDA ALINACAK ÖNLEMLER:

1. İşyerinde yapılacak elektrik tesisatları "03.12.2003 tarih ve 25305 sayılı resmi gazetede yayınlanan elektrik iç tesisatı yönetmeliği ve fenni şartnamesi " standartlarına uygun olarak ve yasal yetkiye sahip teknik personele yaptırılacaktır. Kuvvetli akım tesisatının kuruluş ve işletilmesi esnasında "30.11.2000 tarih ve 24246 sayılı resmi gazetede yayınlanan Elektrik Kuvvetli Akım Tesisleri Yönetmeliği" ve "21.08.2001 tarih ve 24500 sayılı resmi gazetede yayınlanan Elektrik Tesislerinde Topraklamalar yönetmeliği" kurallarına uygunluk sağlanacaktır.
2. Elektrikli cihaz ve teçhizlerin bulunduğu mahallerde yanma ve parlamalara karşı kullanılmak üzere tercihen halokarbon, karbondioksit veya kuru kimyevi toz sıralamasına uygun olarak seyyar yangın söndürme cihazları ve/veya sabit söndürme sistemleri kullanılacaktır. İşletme personelince elektrik/elektronik sistemlerindeki yangınlarda su ve sulu söndürücüler kullanılmayacaktır.
3. İşyerinin elektrik tesisat durumları kendi mühendis, teknisyen veya ustaları tarafından en az yılda bir kez kontrol edilecektir.Teknik arızalar ilgililerce onarılacak,kontrol ve arıza onarım sonuçları rapor halinde tanzim edilerek muhafaza edilecektir.
4. Geçici bile olsa gelişi güzel bağlantılarla elektrik kablosu çekilmeyecek, tesisat yapılmayacaktır.
5. İşyerinin elektrik tesisat projeleri cam çerçeveli olarak ilgili şefliğin odasında asılı bulundurulacaktır.
6. İşyerinindeki elektrik kutularında otomatik sigorta kullanılacaktır.
7. İşyeri içindeki muhtelif elektrik pano ve sigorta kutularının önleri asla kapatılmayacaktır.
8. İşyerininde kullanılan elektrikli cihazlarda priz-fiş uyumuna dikkat edilecek tam temas etmeyen, bozuk olan priz-fiş kullanılmayacaktır.
9. İşyerinde meydana gelebilecek yangınlarda hangi kısmın elektriklerinin kesileceğine olay yerindeki elektrik görevlisi ve bölge itfaiye yetkilisi müştereken karar verecektir.
10. Acil olaylarda elektriklerin kesilmesi işlemini trafo merkezlerindeki nöbetçi elektrik sorumlusu yapacak,zorunlu olmadıkça yangın sistemleri durdurulmadan çalıştırılacaktır.
11. Yangın alarm sistemleri en geç altı ayda bir periyodik test ve bakım kontrolüne tabii tutulacaktır.
12. Otomatik yangın ihbar, alarm ve söndürme sistemlerini yapan firmalarda dünya standartlarına uygun nitelikte üretim,montaj ve bakım yapmaları aranacak,TSE ile ilgili esaslar bulunduğu takdirde bu dikkate alınacaktır.
13. İşyeri bütün bu tedbirlere ilaveten **"İşçi Sağlığı ve İş güvenliği Tüzüğünün"** elektrik tesisatlarında alınacak güvenlik tedbirlerini yerine getirilecektir.

F- ISITMA ARAÇLARINDA ALINACAK ÖNLEMLER :

1. Kazan dairesinin baca ve boruları sık sık temizletilecek, kurum toplama / birikmesi önlenecektir. Temizlik tarihleri kazancı defterine kaydedilecektir.
2. Baca tesisatı TS 2165'deki esaslara uygun olacak,baca duvarlarının dış yüzeylerinin sıvanması ise TS 1481'e uygun olacaktır.
3. Aynı bacayı kullanan iki ayrı odanın baca delikleri birbiriyle karşılaşmayacak, birinin diğerine göre yüksekliği en az 25 cm olacaktır.
4. Soba altlarında, yanlarında ve etrafında kolay tutuşabilen yanıcı maddeler bulundurulmayacaktır. (Yedek gaz bidonu, kağıt vs.)
5. Kazan daireleri TS 1257 ve TS 2736'ya,sıvı yakıt tankları ise TS 712 ve TS 2192'ye uygun olacaktır.
6. Ocak, kazan vs. üzerindeki temizliklerde gaz,benzin,motorin gibi akaryakıt ürünleri,solvent ve alkol kullanılmayacaktır.
7. Kazan dairesi 2x12 kg.lık otomatik söndürme cihazı ile korunacak, ayrıca; gaz kaçak ve algılama detektörü bulunacaktır.

G- SİGARA VE GÜNEŞ IŞINLARI İÇİN ALINACAK ÖNLEMLER :

1. İçerisinde hava kabarcığı bulunan cam,ayna,cam küreler ve şişeler mercek görevi yaparak güneş ışınını bir noktada toplamak suretiyle yangın çıkmasına sebep olabilirler.Bu nedenle bu tip camların kolay tutuşabilen pamuk,selüloit, viskon gibi yanıcı ve parlayıcı maddelerin depo edildiği ambarlara takılmaması uygundur.Zorunlu takılanlar ise içten ve dıştan boyanarak emniyete alınmalıdır
2. İşyerinde sigara içilebilecek yerler tahsis edilmeli ve bunların dışında sigara içilemeyeceği tüm personele tebliğ edilmelidir.Sigara içilmesi tehlikeli olan yerlere **"SİGARA İÇMEK YASAKTIR"** levhaları takılmalıdır.Ancak bu yasağa uyulmasının sağlanması ilgililerce takip edilmelidir.
3. Sigara içme mahallerine içi kum/çakıl dolu özel kül tablaları/kutuları konulmalıdır.Söndürülmemiş izmaritlerin gelişi güzel atılması önlenmelidir.
4. Ofis,büro ve çalışma odalarına kül tablaları,koridorlara ise içi kum/çakıl dolu kutular konulmalıdır.Kül tablalarının kağıt sepetleri yerine bu kutulara boşaltılması sağlanmalıdır. Kutulardaki izmaritler ise özel olarak toplanıp atılmalıdır.
   Ambarlarda depolanan malzeme ve miktarı ne olursa olsun,sigara içilmemelidir.Kibrit, çakmak yakılmamalıdır.
5. Park-bahçe ve Piknik/dinlenme sahalarında gelişi güzel ateş yakılması,cam şişe atılması, kontrolsüz sigara içilmesi kesinlikle önlenmelidir.Özellikle yaz aylarında ve işletme sahasındaki büyük yangın rizikosu sık sık hatırlatılmalıdır.

H- GARAJ VE ARAÇ BAKIM/TAMİR ATÖLYELERİNDE ALINACAK ÖNLEMLER :

Garaj/Otopark ile ilgili alınacak önlemler TS 11922'ye uygun olmalıdır.

1. İşletmelere ait her araçta tonajı ve amacına uygun seyyar yangın söndürme cihazı bulundurulacaktır.
2. Araçların içinde,bagajında vs. yerlerinde plastik kaplarda yedek vb. amaçla benzin,motorin vs. yakıt taşınacaktır.Yakıt taşıma zarureti olduğunda bu amaçla yapılmış özel madeni kaplarda taşınacaktır.
3. Garaj ve bakım/tamir atölyelerinde yakıt depolanmaktan kaçınılmayacak,yakıt bulundurulması için mutlak zaruret varsa uygun kaplarda ve az miktarda keza araçlardan uzak bir yerde tutulmalı ve **"DİKKAT TEHLİKE-SİGARA İÇMEYİNİZ"** şeklinde uyarı levhası takılmalıdır.
4. Muhtemel araç arızalarına yetkili kişilerce müdahale yapılmalıdır.Özellikle kışın zor çalışan araçların altında ateş yakılmamalı,ısıtma için pürmüz vs. kullanılmamalıdır.Araçlarda herhangi bir çalışma,onarım halinde akünün pozitif (+) ucu çıkartılmalıdır.Şarj edilen akü yakınlarına sigara ve ateşle yaklaşılmamalıdır.

I- İMALAT/ÜRETİM BÖLÜMÜNDE ALINACAK ÖNLEMLER :

1. İmalathaneler her sektör için kendi özelliğine uygun olarak değerlendirilmelidir. Özellik arz eden sektörel risklerin dışında ortak ilke olarak tek katlı olmalı, üretim şekline ve amacına uygun olarak tercihen çatıdan havalandırılabilir ve aydınlatılabilir olmalıdır.
2. Yapılacak işe göre standartlara uygun malzeme ve takım kullanılmasına özen gösterilmelidir.(Örneğin;oksifuelgaz kesme ve kaynak hortumları TSE veya uluslararası normlarda olmalı,yapıştırılmış ve bantlanmış hortumlar standartlara uygun kabul edilmemelidir).İmalathanelerde kullanım vs. sonucu kirlenen üstübü,paçavra gibi temizlik malzemeleri rasgele atılmayıp özel olarak yapılmış madeni bidon/kaplara konulmalıdır.
3. Üretim yeri,kullanılan hammadde,üretim şekli,üretilen mamul maddenin özelliklerine bağlı riskleri karşılayacak şekilde,sayıda ve tipte seyyar yangın söndürme cihazı konulmalıdır.

4. İmalathanelerdeki makine,cihaz,takım vs. alet ve edevatlar imalatçı firmanın kullanma kılavuzuna uygun olarak çalıştırılmalı ve emniyet tedbirleri alınmalıdır.
5. İşletmelerde kaynak/kesme işlemleri güvenli alanlarda yapılmalıdır.Bütün yanıcı maddeler yatay olarak en az 20 metre uzaklığa çekilmeli ve 10 metre civarındaki duvarlarda kıvılcım sıçramasına karşı delik olmadığı görülmelidir. Koruyucu teçhizat (Elbise-eldiven-gözlük vs.) giyilmeli,kaynak/kesme tamiratların üretim saatleri dışında yapılmalı,yangın gözcüsü konulmalı, çevredeki yanıcı,parlayıcı,patlayıcı maddelerin tespiti vs. ile bir kaynak kesme işleri talimatı hazırlanıp ilgililere tebliğ edilmeli ve işlerliği takip ve kontrol edilmelidir.
6. İmalathanelerde üretim cinsi,özelliği ve safhalarına uygun ve her üretim alanındaki kendi riziko şartlarına bağlı olarak toz toplama sistemleri konulmalıdır.Toz toplama sistemleri vakum sistemi olmalıdır.Vakum yerine asla basınçlı hava kullanılmamalıdır.Vakum toz toplama torbaları sık sık değiştirilmelidir.

J- AMBAR/DEPOLARDA ALINACAK ÖNLEMLER :

1. Depolama ilgili alınacak önlemler TS 10661,10663,10882,10976,11369 ve 11528'e uygun olmalıdır.
2. Depo alanı yangın dolabı,seyyar yangın söndürme cihazları,kapalı devre kamera sistemi, alarm-ikaz sistemi,algılama sistemi ile korunmalıdır.
3. Çalışma saatleri sonunda görevlisi tarafından gezilen ambar/depo elektrikleri kesilerek (ana şalterden kapatılır) kapıları kilitlenmeli ve anahtarları gece bekçi güvenlik görevlisine teslim edilmelidir.Kapının mühürlenmesi gerekiyorsa bu işlem sorumlu ambar görevlisi ile bekçi/güvenlik görevlisi tarafından birlikte yapılmalıdır.Ambar/depoda ambalaj maddeleri, ambalajlı ham ve mamul maddeleri ile yanıcı özellikteki ambalajsız maddeler riziko şartlarına uygun olarak istiflenmelidir.(Üretim safhalarında riziko ve önlemleri TSE veya uluslar arası normlarda olmalıdır.)Depo/ambarlar istiflenen malzeme özelliklerine uygun olarak seyyar yangın söndürme cihazları ile donatılmalıdır.Depo/ ambarlar riziko şartlarına uygun olarak tabii ve cebri olarak havalandırılmalıdır.
4. Ambar/depoların açılış ve kapanışlarını gösterir bir talimat işletme müdürlüklerince hazırlatılarak ambar/depoların görünür bir yerine asılmalıdır.Açılış ve kapanışlar bu talimata uygun olarak yapılmalıdır.

K- LABORATUARLARDA ALINACAK ÖNLEMLER :

1. Laboratuarlar ile ilgili alınacak önlemler TS 9705'e uygun olmalıdır.
2. Laboratuarlar çok iyi havalandırılmalıdır.
3. Laboratuarlar yangının yayılmasını önlemek üzere küçük bölümlere ayrılmalıdır.

L- CAN EMNİYETİ İÇİN ALINACAK İLAVE ÖNLEMLER :

Kaçış yolu bir yapının herhangi bir noktasından yer seviyesine kadar olan devamlı ve engellenmemiş yolun tamamıdır.Kaçış yoluna engelleyici bir şey konulmamalı, çıkış kapatılmamalıdır.Bu güvenliğin sağlanması bina sorumlusu veya güvenlik görevlisinin sorumluluğundadır.

1. İşletme idari bölümlerde **"EXIT"** şeklinde acil çıkış aydınlatmalar mevcut olmalıdır.
2. Acil çıkış kapıları asla kilitli tutulmamalı,herhangi bir çarpma anında açılacak durumda olmalıdır.
3. **UYARI:**Asansörler asla kaçış yolu olarak kullanılmamalıdır.Yangın merdiveni olarak düşünülmemelidir.

4. Binalarda çıkışa giden koridor,galeri,balkon,çatı vs. olmalıdır.Kapalı alandaki çıkış/kaçış koridorunun azami uzunluğu 30 m olmalıdır.Ancak sprinklerle korunan kaçış yolu uzunluğu 45 metre kadar olmalıdır.
5. Binaların kaçış yolları elektrikler kesilse dahi çok iyi aydınlanacak şekilde dizayn edilmelidir. Merdivenler,koridorlar,köşe,merdiven sahanlığı,kapı vs. görülebilmelidir.

M- DOĞALGAZ VE TESİSATI İLE İLGİLİ ALINACAK ÖNLEMLER :

1. Acil durumlarda kapatılacak Ana Kesme Vanasının yerini mutlaka öğrenin.
2. Can ve mal güvenliğiniz için doğalgaz yetkililerin bilgisi dışında tesisatta değişiklik yapmayın.
3. Tehlike anları haricinde Ana Kesme Vanasını kapatmayın.
4. Mecburi hallerde kapatılan Ana Keme Vanası sadece yetkili görevliler tarafından açılacaktır.
5. Havalandırma menfezlerini iptal etmeyin,kapamayın veya yerlerini değiştirmeyin.
6. Doğalgaz cihazlarının bakım ve onarımlarını yetkili servislere yaptırın.
7. Gaz Alarm detektörlerinin sesli uyarısının akabinde gaz akışı otomatik olarak kesilir.
8. Acil durumlarda elektrik cihazlarını çalıştırmayın,aydınlatma düğmesi açıksa kapatmayın,kapalıysa açmayın.
9. Ortamı havalandırın.
10. Doğalgazın 187 no'lu acil telefonunu arayın,açık adres ve bilgi vererek yardım isteyin.

KISIM IV- YANGIN VUKUUNDA YAPILACAK İŞLER :

A-YANGIN, ÇALIŞMA SAATLERİ İÇİNDE OLURSA:

1. Herhangi bir yangın meydana geldiğinde işletme personeli toplanma yerinde bölümlere ayrılarak kısa sürede mevcut alınmalı,işletme içinde kalan personel mevcudu çıkarılmalıdır.İlk müdahale söndürme ekibi tarafından şehir itfaiye gelinceye kadar yapılmalıdır.
2. Eğer haberleşme telefon ile yapılıyorsa,İtfaiyeye (110) telefonla,irtibat kurulamıyorsa,ulaşım ve pasaparola ekiplerinden birer kişi bir araçla İtfaiyeye haber vermelidir.
3. Ekip personeli itfaiye ile koordine halinde çalışmalıdır.

B-YANGIN, ÇALIŞMA SAATLERİ DIŞINDA OLURSA :

1. Yine aynı işlemler takip edilmeli,farklılık gerektiren durumlar göz önünde tutulmalıdır.(İşletme yetkilisinin bulunmaması,elektrik sorunu vs.) Herhangi bir yangın meydana geldiğinde işletme personeli toplanma yerinde bölümlere ayrılarak kısa sürede mevcut alınmalı,içeride kalan personel mevcudu çıkarılmalıdır.

C-YANGIN İŞYERİ YAKININDA OLURSA :

1. Yangın komşu işletmelerde olursa protokol gereği emir beklemeksizin ehil personel yardım için olay yerine en kısa zamanda gelmelidir.Çağrıldığı takdirde gelmeyenler hakkında yasal işlem yapılmalıdır.
2. Gerekli olan malzemeler işletmeye tutanakla verilerek olay sonrası geri temin edilmelidir.

KISIM V - PLANIN TATBİK ŞEKLİ :

1. Bu plan **İzmir Karabağlar Belediyesi** tarafından uygulanır.
2. Bu planda **İzmir Karabağlar Belediyesi İşçi Sağlığı ve Güvenliği Kurulu'nun** müsaadesi alınmadan herhangi bir değişiklik yapılmaz.
3. Bu planda yayınlandığı tarihten itibaren yürürlüğe girer.

YANGINLA MÜCADELE TEŞKİLATI VE GÖREVLERİ

YANGIN AMİRİNİN GÖREVLERİ :

1. Yangınla mücadeleyi sevk ve idare eder,paniğe mani olur.
2. Yangın alarmını duyar duymaz yangın mahalline gider; yangın yerini keşfe çalışır ve uygun söndürme sistemini belirler.
3. Yangın bölgesinde mücadeleye başlamış olan yangın söndürme personelinin çalışmalarını izler. Yangın yeri; şekli ve şartlarına göre gerekli tertip,tedbir ve düzenlemeler veya takviyeler için emirler verir.
4. Yangının biran evvel kontrol altına alınarak söndürülmesine çalışır.
5. Yangınla mücadele personelinin güvenli çalışmasını temin eder.
6. Yangına gelen itfaiye ekibine bilgi aktararak yangın yeri amirliği görevini itfaiye müdürü veya adına yetkili itfaiye ekip şefine devreder.
7. Ekipleri ve gelen itfaiyenin uyumlu ve koordineli çalışmasını sağlar.

YANGIN AMİR YARDIMCISININ GÖREVLERİ :

1. Yangınla mücadelede yangın amirine yardım eder, yangının başka bölgelere atlamasına mani olur.
2. Su ile yangın mahalline yakın olan binaların çatı ve duvarlarını diğer eşyaları ıslattırarak soğutur, alevlere karşı su ile sis perdesi yaptırır.
3. Yangına henüz maruz kalmamış fakat yangın sıcaklığından etkilenebilecek stok tanklarını ve tüpleri soğutur. Çevre kontrolünü sağlar.

HABER İLETME EKİBİNİN GÖREVLERİ:

Kuruluşu: Ayrıca yangın mahallinde ekipler arası ve ekipler ile yangın amiri arasında haberleşmeyi sağlamak üzere haber taşıma (Pasaparola) personeli görevlendirilir.Keza telefon santral personeli Haberleşme ekibi olarak sınıflandırılabilir.Görevi;

1.Alarmla birlikte yangın bölgesine koşar,yangın amirinin daima yanında bulunur.

2.Yangın amirinden alacağı emirleri ast kademelere,ast kademelerden gelecek haberleri yangın amirine iletir.Haber iletmek için pilli megafonu yanında taşır.

3.Ast kademelerle daima göz irtibatında bulunur.

HABERLEŞME EKİBİNİN GÖREVLERİ:

1.Yangın alarmının duyulması ile dahili ve harici bütün telefon konuşmalarını keser.

2.Baştan itibaren yanında bulunan önemli kademelerin telefon numaralarını arayarak yangını bildirir ve öncelikle itfaiye olmak üzere yardım ister.Dış kargaşalıkların önlenmesi için jandarma ve emniyet teşkilatları ile temasa geçer.

3.Yangın devam ettiği süre içinde kendisine verilen ilgili telefonlara bilgi verir.

4.Yaralıların tedavisi için hastanelerle temas ederek yatak ve ön hazırlıkları sağlar.

5.Yangın amirinin emirlerini yerine getirir.

6.Yangın sonunda temasa geçtiği bütün numaralara bilgi verir.

7.Yangın veya tatbikat sonunda yaptığı işlerle ilgili tesis müdürüne bilgi verir.

8.Haberleşmede tesis gizlilik durumuna riayet etmesi esastır.

YANGIN SÖNDÜRME EKİBİ GÖREVLERİ:

9 kişiden meydana gelen söndürme ekip/ekipleri kurulur.Ekip şefliğini bir teknisyen veya usta başının yaptığı söndürme ekibinin görevi;yangın çıkmasını önleyici tedbir almalarına ilaveten ekip olarak çıkabilecek yangınlara ilk müdahaleyi yaparak söndürmek veya itfaiye teşkilatı gelinceye kadar büyümesini önleyecek tedbir ve tertipleri almaktır.Bu ekiplerde görev alan personele işletme yetkililerince uygun zamanlarda yangın ve söndürme yöntemleri hususunda eğitim verilir/yaptırılır.

1.İkaz ve alarm haberleriyle birlikte yangınla mücadele plan ve talimatları uygulamaya konulur.

2.Ekip Amiri/şefinin talimatı ile yangın mahalline sevk edilen ekip tarafından yangına hemen müdahale edilir.

3.Yangına mücadele civardaki yangın söndürme cihazları ile yapılır.

4.Yangına müdahale ederken önce can emniyeti göz önünde bulundurulmalıdır.

5.İtfaiye yangın mahalline intikal edinceye kadar yangının çevreye sirayeti ve genişlenmesinin önlenmesine çalışılmalıdır.

6.İtfaiye gelince tesisin yangın söndürme ekibi İtfaiye Müdürü/vekili talimatına göre görevine devam eder.

7.Can kurtarma faaliyetleri ve enkaz kaldırmasına yardımcı olacaktır.

KURTARMA VE TAHLİYE EKİBİ GÖREVLERİ:

Kuruluşu: Her vardiyada çalışan personel arasından tefrik edilen 2-4 kişiden kurulan bir ekiptir.Görevi;Yangın, deprem,su baskını vs. olağan üstü durumlarda can ve malzeme kurtarılmasını temin etmektir.(Mal tahliyesinde malzeme vs. paketlemek/ taşımak üzere emre intizar personelden istifade edilir.)Bu maksatla kurtarma ekibinde görev alan personel özellikle yangından can ve mal kurtarılması,depremden kurtarma konularında eğitilmelidir.

1.İkaz ve alarm haberiyle birlikte tesisin toplanma bölgesinde toplanacaktır.

2.Yangın Amiri talimatı ile yangın mahallinde kurtarılacak can ve mal varsa kurtarır.

3.Yangın mahallinde açılacak / kapatılacak valf - kapı vs. varsa verilen talimata göre gerekeni yapar.

4.Kurtarılacak malzeme ve eşyayı yangın yerinden uzaklaştırmak üzere öncelik sırasına göre toplama/ paketleme yapar.

5.Enkaz altında kalanların kurtarılmasında diğer personele kılavuzluk yapar.

6.Yangın amiri talimatları ile söndürme, koruma ve trafik / kılavuzluk ve ilk yardım ekipleri ile koordineli olarak görev yapar.

KORUMA VE TRAFİK/KILAVUZ EKİBİ GÖREVLERİ:

3 kişiden kurulan bir ekiptir. Görevi;

1.Alarmın duyulması ile birlikte tesisin giriş / çıkış yolunu trafiğe kapatır. Lüzumsuz giriş ve çıkışları önler.

2.Yangın mahalline gelen ekiplere yol gösterir.

3.Yangına çağrılan itfaiye,polis,jandarma,ilkyardım,elektrik vs. kuvvetlerin dışındaki trafiği önler.

4.Yangın yerinde trafik düzenini sağlar.

5.Yangın mahallinden kurtarılarak tahliye edilen malzemelerin muhafaza edilmesini sağlar.

6.Yangın Amiri talimatı ile Söndürme, Kurtarma/Tahliye Koruma/Trafik Kılavuz ve ilkyardım ekibiyle koordineli olarak görevini yürütür.

İLK YARDIM EKİBİ GÖREVLERİ:

6 kişiden kurulu bir ekiptir. Görevi;Yangın,deprem,su baskını vs. olağanüstü durumlarda meydana gelebilecek yaralanma ve kaza olaylarında yaralıları doktora ulaşıncaya kadar,o anki durumun daha kötüye gitmesini önlemek için mevcut malzemelerle ilk müdahaleyi yaparak en yakın sağlık kuruluşuna sevk etmektir.Bu maksatla ilk yardım ekibinde görev alan personel kırıklar,kanamalar,elektrik çarpmaları,boğulmalar,yanma ürünleri ve yanıklara yapılacak ilk yardımlar konusunda eğitilmelidir.Unutulmamalıdır ki;ilk yardımı yapan kimse doktorun yerini alamaz / tutamaz.Görevi,

1.Yangın alarmının duyulması ile birlikte sağlık ilkyardım malzemeleri ve sedyeleri ile derhal tesisin toplanma bölgesine gider ve ilkyardıma hazır olur.

2.İlkyardımı yaparken seri,dikkatli ve kaidelere uygun hareket eder.

3.Yaralılar taşınırken sarsmamaya dikkat edilir.

4.Yangın başlangıcında yaralanan ve hastalananlara ilk yardımı yapar; gerekenleri hastaneye sevk eder.

5.Gerekirse mevcut araçlardan istifade ile yaralıyı en yakın ilkyardım merkezine nakleder.

6.Yangın amirine bağlı olarak diğer ekiplerle koordine içerisinde görevini yürütür.

YANGIN EKİPLERİNDE KOORDİNE:

Yangınla yapılan mücadelenin arzu edilen başarıya ulaşabilmesi için görevli her ekibin hem personel olarak kendi içinde hem de diğer ekiplerle koordineli ve uyumlu çalışması esastır.Ekipte görevli bir personelin yeterliliği kafi değildir.Her personelin görevini yapabilme kabiliyeti ekibin gücünü ortaya koyacağından müşterek çalışma ruhu aşılanmalı ve geliştirilmelidir.Yangın yerinde bir amir bulunmalı diğer bütün ekip şefleri yangın amiri ile koordineli çalışmalıdır.Böylece kargaşalık önlenirken yangınla mücadelede daha kısa zamanda etkinlik sağlanacaktır.Bir yangın söndürme organizasyonunda bütün ekiplere birden ihtiyaç duyulmasa bile genel bir işlem sırası aşağıdaki gibidir.

1. Yangın ihbarı ile birlikte yangın mahallinin elektrikleri kesilir.
2. Yangına uygun söndürücü ile müdahaleye başlanır.
3. Personel toplanma yerine alınarak mevcut alınır.
4. Varsa kurtarma işlemi ve ilkyardım yapılır.
5. Yangın mahalli ve işletmenin fiziki güvenlik önlemleri artırılır.
6. Gerekiyorsa tahliye işlemi yapılır.
7. Sürekli olarak çevre kontrolü yapılarak yangının yayılması önlenir.
8. Yangın mahallinde infilak ve yayılmayı önlemek üzere duman tahliyesi yapılır.
9. Yangına su sıkılıyorsa diğer ünitelere geçişi önleyecek direyn,bariyer vs. tedbirler alınır.

YANGIN ÖNLEME ÇEK LİSTESİ (ÖN BİLGİLER):

Evlerimizde,iş yerlerimizde ve çevremizde oluşabilecek yangınları nasıl önleyebiliriz?

1. Sigarayı hiç içmemenizi öneririz ama hiç olmazsa;yatakta sigara içmeyiniz. Sigarayı söndürmeden gelişigüzel yerlere atmayınız.Kül tablasındaki sigaraları söndüğünden emin olmadan çöpe boşaltmayınız.Yasaklanmış yerlerde sigara içmeyiniz.
2. Ütü,elektrik sobası gibi cihazların işi bitince fişini çıkartınız.Kullandığınız elektrik malzeme ve cihazların TSE'li olmasına dikkat ediniz.
3. Sigortalara tel sarmayınız,otomatik sigortaları tercih ediniz.Aynı prize birden fazla cihaz takmayınız.
4. Çok nemli (banyo vb.) yerlerde aydınlatma lambasını fanus içine alınız.
5. Çocuklarınızın kibrit,çakmak vb. yakıcı ve yanıcı maddelerle oynamasına engel olunuz.
6. Bodrum ve tavan aralarına gelişi güzel şekilde yanıcı madde koymayınız.
7. Temizlik yangını önler.Bacalarınızı her yıl temizletiniz.Sıvasız,hatalı inşa edilmiş bacaları kullanmayınız.
8. Her kat,her oda,her kazan için müstakil baca kullanınız.
9. Soba borularınızdaki,kazan borularındaki kurumları sık sık temizleyiniz/ temizletiniz.
10. Sobanızı tutuşturmak için benzin,tiner gibi kolay yanıcı sıvı maddeleri kullanmayınız.
11. Yakıldıktan sonra sönen sobalara da sıvı yanıcı dökmeyiniz.Soba boruları çevresinde çamaşır kurutmayınız.
12. Sobadan sıçrayabilecek kıvılcımlara karşı önlem alınız.Bacasız şofben kullanmayınız.
13. Piknik tüplerini geniş tabanlı tava-tencere ısıtmak için kullanmayınız.
14. Isıtma cihazlarının altında,yanında ve yakınında kolay yanıcı madde bulundurmayınız.
15. LPG tüplerini dik tutunuz,donmalara karşı açık alevle ısıtmayınız.Tüp değişiminde contaları değiştiriniz.
16. LPG ve Doğalgazla çalışan soba ve kalorifer mahallerini iyi havalandırınız. Gaz kokusu aldığınızda,gaz kaçağına karşı kıvılcım çıkabilecek hareketlerden kaçınınız.Kibrit,çakmak yakmayınız,elektrik anahtarlarına dokunmayınız ve buzdolabını açmayınız.Bunun yanında ağzınızı-burnunuzu ıslak bir mendille kapatarak dışa açılan balkon vb. kapı-camları açınız.LPG kullanılan mahalli hayali toz-çöp vs. düşünerek açtığınız kapıya doğru süpürünüz.
17. LPG için tabandan,doğalgaz (NLG) için tavan veya yakın kısımlarından havalandırma delikleri bırakın.Çünkü LPG havadan ağır olup yere çöker. NLG ise havadan hafif olduğu için yukarıda,tavan kısmında toplanır.

18. LPG tüplerini bodrum gibi yerlerde bulundurmayınız. Bu mahallerde kullanım zarureti varsa,mutlaka gaz alarm detektörü kullanınız.
19. Binanızda gereksiz şekilde yanıcı malzemeden dekor-süsleme yapmayınız, yapmanız halinde ise yanmaz malzemeyi tercih ediniz. Ahşap yapıları (kapı-pencere-dolap-raf vs.) yanmaz boya ile boyayınız.
20. İkaz, yangın riskini azaltır.Aile bireylerinizi ve komşularınızı ikaz ediniz.Acil ve önemli telefonları yazılı olarak el altında bulundurunuz.
21. Evinizde ve işyerinizde mutlaka yangın söndürme tüpü bulundurunuz
22. Mesai saatleri sonunda ve mesai saatleri dahilinde açıkta yanıcı bir şey bırakmayınız.
23. Bina çıkış kapılarını her an açılmaya elverişli, koridorları açık bulundurunuz.
24. Yangın pompalarını her an çalıştırmaya hazır bulundurunuz.
25. Öncelikle görevliler ve fabrikadaki bütün çalışanlar yangın söndürücülerin nasıl kullanılacağını öğreniniz.

YANGIN SIRASINDA ÖNERİLER:

1.Soğukkanlılık muhafaza edilmeli;paniğe kapılmadan,yangın yeri ile birlikte, ”**YANGIN”** diye bağırılmalıdır.

2.Yangın ikaz sistemi kullanılarak yangın zili veya yangın çanı ile alarm verilmelidir.

3.Yetkili şahıslara derhal haber verilmelidir.

4.Yangın görülen yerlerin acele tahliyesi sağlanıp kapalı alanlarda hava cereyanını azaltmak için kapılar kapalı tutulmalıdır.

5.Yangına ilk müdahale yapılmalı, yangının havayla teması mümkünse kesilmelidir.

6.İtfaiyeye haber verilmelidir.

7.Binanın sorumlusu olan şahsa yokluğunda Koruma ve Trafik/Kılavuz Ekip Amirine durum bildirilmelidir.

8.İtfaiye ekibi canlının ve eşyanın tahliyesine yardım etmelidir.

9.Kurtarma ekibi tahliye edilen canlının ve eşyanın kurtulmasını sağlamalıdır.

10.Koruma ekibi tahliye edilen canlının ve eşyanın güvenliğini sağlamalıdır.

11.Koruma ekibi trafiği düzenlemeli,kargaşalığı önlemelidir.

12.İlk Yardım Ekibi hazır durumda bulunmalı,yaralı ve baygın olanlara ilk müdahaleyi yapmalıdır.

TAHLİYE SIRASINDA ÖNERİLER:

1.Tahliyenin yapılacağı bina ve sahadakilere olay duyurulur ve **“PANİĞE KAPILMAYINIZ”** anonsu yapılır.

2.Büronuzu boşaltırken kapı ve pencereleri hava cereyanını azaltmak için **“KİLİTLEMEDEN KAPATINIZ”**

3.Çalışma yerlerinizi telaşa kapılmadan terk ediniz ve beraberinizde önemli evrak vs. almayı unutmayınız.

4.Çıkış yerlerine sükunetle gidiniz ve gereksiz acelecilikten sakınınız.

5.Merdiven ve çıkış kapılarını düzenli olarak kullanınız ve sıkışıklığa sebep olmayınız.

6.İşletme sahasındaki valflere yetkili şahısların dışında müdahale etmeyiniz.

7.Bina ve sahayı tahliye ettikten sonra, belirlenen toplanma yerlerinde yeniden görev almak üzere **“AMİRİNİZİ”** bekleyiniz.

İHBAR VERMEK:

1.Soğukkanlılık muhafaza edilmeli;paniğe kapılmadan **"YANGININ YERİ İLE BİRLİKTE","YANGIN VAR"** diye bağırılmalıdır.

2.Mevcut yangın ikaz sistemi kullanılarak (yangın zili veya çanı) alarm verilmelidir.

3.Yetkili görevlilere derhal haber verilmelidir.

4.Yangına ilk müdahale yapılmalıdır.

5.Kapalı alanlarda hava cereyanını azaltmak için kapılar kapalı tutulmalı ancak kilitlenmemelidir.

6.Yangının havayla teması mümkünse kesilmelidir.

7.Organize Sanayi itfaiyesine acilen haber verin.

8.İtfaiyeye verilecek ihbar aşağıdaki formata göre alınacağından ihbar verilirken formdaki sorulara cevap teşkil edecek şekilde bilgi aktarılması doğru ve hızlı ihbar verilip alınmasını sağlayacaktır.

9.Yangın ihbarı Jandarma,Yerel İtfaiyesi ve gerekirse civar itfaiyelere bildirilecektir.Böylece Adli ve Mülki makamlara bilgi verilmesi sağlanacaktır.

D-DOĞAL AFETLERDEN KORUNMA

KISIM I - AMAÇ :

İzmir Karabağlar Belediyesi'nde deprem ve yer hareketine maruz kalacak bina ve bina türü yapılarının tamamının veya bölümlerinin depreme dayanıklı tasarımı ve yapımı için gerekli minimum koşulları tanımlamaktır.

KISIM II - DOĞAL AFETLERİN SINIFLANDIRILMASI :

DOĞAL AFETLER : Nerede,ne zaman,ne ölçüde,nasıl ve ne türde olacağı bilinmeyen doğal afetler varolduğu günden beri insanların can ve malına yönelik en büyük tehlikedir.

Doğal Afet: Yerleşim,Üretim,alt yapı,ulaşım,haberleşme gibi,genel hayatın zorunlu vasıtalarını ve akışını bozacak ölçüde aniden ve belirli bir süreç içerisinde meydana gelen doğal yer ve hava hareketleridir.

Doğal Afetin Çeşitleri :

- Deprem, (Yer Sarsıntısı)
- Su Baskını, (Sel)
- Kaya Düşmesi,
- Toprak Kayması,
- Çığ,
- Kuraklık,
- Fırtına-Kasırga-Tayfun-Tornada,
- Volkan Patlaması,
- Yangın,
- Baraj Patlaması,
- Hava, Su, Çevre Kirlenmesi,
- Sınai Kazalar,
- Ulaşım (Karayolu- Demiryolu- Hava- Deniz) Kazaları

Doğal Afetin Özellikleri- Sonuçları :

- Çeşitli güç ve genişlikte olurlar,
- Alt yapıyı bozarlar,
- Şok tesiri yaratırlar,
- Ölüm, sakatlık ve öksüz kalma gibi sonuçlar doğururlar,
- Bulaşıcı ve salgın hastalıkların (Tifo, tifüs, sarılık, veba vb.) çıkmasına neden olurlar,
- Yörenin ekonomik yapısını bozarlar,
- Devletin planladığı yatırımları geciktirirler,
- Depremin başka zararları da vardır.Örneğin;salgın hastalıklara,şok, işsizlik,ulaşım ve haberleşmede aksaklık,insanlar üzerinde psikolojik bozukluklar,sakatlık,öksüz kalma v.s. gibi.

2.1.DEPREM:

Yer kabuğu içindeki kırılmalar nedeniyle ani olarak ortaya çıkan titreşimlerin dalgalar halinde yayılarak geçtikleri ortamları ve yer yüzeyini sarsma olayına **DEPREM** denir. Başka bir deyişle arzın içindeki bir noktada meydana gelen kırılmanın doğurduğu sismik dalgaların arz yüzeyine kadar ulaşarak onu sarsmasıdır.

Ülkemizde de depremi önceden haber alma tekniği henüz araştırma safhasında ise de,afet bölgelerinde yapılacak yapılar ile ilgili yönetmelik çıkarılmıştır. (02.09.1997 gün ve 23098 sayılı R.G. yayınlanmıştır.)

Deprem sadece can ve mal kaybına neden olmakla kalmaz,ayrıca;baraj patlamalarına,taşkın sulara,yangınlara,kaya düşmelerine,çığ ve yer kaymalarına neden olur ki,bu etkisi bazen doğrudan meydana getirdiği zarardan da daha büyük olabilir.Depremin başka zararları da vardır.Örneğin;salgın hastalıklara,şok,işsizlik, ulaşım ve haberleşmede aksaklık,insanlar üzerinde psikolojik bozukluklar,sakatlık, öksüz kalma vs. gibi.

2.1.1.Depremden Önce Yapılması Gerekenler:

1. Yaşadığınız/bulunduğunuz mekan incelenerek,korunma için bulunacağınız yer ve muhtemel kaçış yolları belirlenmelidir.Eğer bulunduğunuz noktadan kendinizi 10-15 saniye içinde bina dışına çıkartacak ve güvenli bir açık alana ulaştıracak pozisyonunuz varsa,bu yolu saptayın.(Bu yöntem sadece giriş altı,giriş ve 1.katta olanlar için geçerlidir.)
2. Deprem sırasında ilk 10-15 saniye binayı terk edebilmek açısından çok önemlidir.Daha önce yaşanan depremlerden elde edilen istatistik verilere göre,binalarda yıkıma yol açan unsur,hissettiğiniz ilk sarsıntı değil,binanın rezonansa girmesidir.Bu da size anılan süreyi kazandırmaktadır.Bu süre içinde kaçma eylemini gerçekleştirebilecek bir yöntem bulduğunuz takdirde, tatbik ederek zamanı saptayın.Böylelikle hem kesin kaçış sürenizi öğrenebilir,hem bu süreyi daha da kısaltacak yöntemler geliştirebilir.

DİKKAT: Kişisel kaçış zamanı ile,birilerine yardım ederek (eşiniz,çocuğunuz,iş arkadaşınız yada özürlü,sakat vb.) kaybedeceğiniz zaman çok farklıdır.Bu farklı senaryoları denemenizde yarar vardır.

1. Kapı veya cam kenarında yada bulunduğunuz yeri 10-15 saniye içinde terk edebilecek bir mesafede iseniz,herhangi bir acil çıkış anında kullanacağınız güzergah üzerinde size engel olabilecek saksı,masa,sandalye,koltuk, sandık ve benzeri unsurlar ortadan kaldırılmalıdır.
2. Bazı durumlarda ani bir acil çıkış olanağı yaratılabilir.(giriş katındaki camı kırarak dışarı çıkmak gibi).Bu cam kalın yada sağlamlaştırılmış olabilir. Bunu kırmak için bir seyyar yangın söndürme cihazını kaçış yolu üzerinde bulundurulabilir.Bina terk edilirken kendinizi yüksekten veya tavandan düşen nesnelerden (tuğla, kiremit, avize vb.) korumalısınız.Bu aşamada yastık bir işe yaramayacak,aksine çevrenizi görmenize ve sesleri duymanıza engel olacaktır.Bir kask veya baret,bulamazsanız bir sandalye, bir tahta parçası,büyük ve kalın bir kitap işinize yarayabilir.

3. Eğer bina 10-15 saniye içinde terk edilemiyorsa,kesinlikle merdivenlerden, merdiven boşluklarından uzak durulmalıdır.Asansör bir tuzaktır, kullanılmamalıdır.Yıkılan binalarda en yüksek oranda ölüm bu noktalarda meydana gelmektedir.Birinci kattan daha yüksektekiler atlamayı denememelidir.
4. Yaşanan depremlerde ölümle ve ciddi yaralanmalarla sonuçlanan olayların büyük bir bölümü yüksekten atlamayla ilişkilidir.Bunun yerine yüksek binalarda yapılması zorunlu olan harici yangın merdivenler kullanılmalıdır. Demir konstrüksiyondan inşa edilen bu merdivenler,binadan bağımsız olduğu için yıkım darbesinden daha zor etkilenecek ve bağlı olduğu yerden kopması halinde,çeperlerindeki kuşaklar nedeniyle düşme anında bir koruma alanı oluşturacaktır.

2.1.2.Deprem Anında Yapılması Gerekenler:

1. Deprem anında 10-15 saniye içinde bulunduğunuz binayı terk edebiliyorsanız derhal kaçılır,yoksa güvenli bir yer bulunur.İlk sarsıntıyı hissettiğiniz anda paniğe kapılmadan hareket ettirilir.Panik,sağlıklı düşünmenizi engelleyecek,hatalı,bilinç dışı hareket etmenize yol açacaktır. Bilinçli düşünebilmek,hazırlıklarınızı felaket anında değil,daha önce yapmanıza ve planlamanıza bağlıdır.10-15 saniye içinde bulunduğunuz yerden bina dışına güvenli bir açık alana çıkma olanağınız ve planınız varsa,bu derhal önceki bölümde anılan önlemleri alarak uygulamaya koyulur.Eğer bina terk edilemiyorsa,daha önce belirlenen yaşam üçgeni alanına gidilerek cenin pozisyonunu alınır.Kesinlikle oradan oraya koşularak ayakta durulmamalıdır.

DİKKAT: Enkaz altında öncelikle böbreklerin iflas ettiği bilinmelidir.Depremzedelerin kurtarılması halinde bile vücudunda büyük hasarların oluştuğu ve bu nedenle ölüm olaylarının yaşandığı saptanmıştır.Cenin pozisyonunun bir diğer özelliği ise,kurtarma ekiplerinin kazazedenin bulunduğu bölüme en küçük bir gedikten de olsa ulaşması halinde,onu bulunduğu yerden çıkartmasa bile elini tutmasına izin vermesidir.Bu durumda kazazedenin beyni adrenalin pompalamaya başlayacak onu yeniden hayata bağlayacak çok önemli bir köprü kurmuş olacaktır.

2.Deprem sırasında eğer dışarıda bulunuluyorsa;bina,direk,reklam panosu, duvar gibi devrilebilecek materyallerin uzağında durmak gereklidir.Herhangi bir nesnenin (araba, balkon..) altına girmek çok sakıncalıdır.Deprem bitene kadar açık alanda beklenmelidir.Eğer bina içinde bulunuluyorsa,en güvenli yerler,ev yıkıldığında bizim yaşamamız için gerekli yer kalmasını sağlayacak sağlam ve büyük eşyaların yanıdır.

3.Deprem sırasında araçta bulunanlar;tünelde yada kapalı bir otoparkta hissedildiği anda paniğe kapılmadan,aracı yol kenarından çekip binalardan, elektrik direklerinden veya uzakta durdurmalıdır.Tünel içinde iseniz ve çıkışa yakın değilseniz,aracınızı durdurup aşağıya inerek cenin pozisyonu alınır. Aracın içinde durulmamalıdır.

2.1.3.Depremden Sonra Yapılması Gerekenler:

1. Psikolojik hasarın büyümesinin engellenmesi gerekir.Bu sebeple paniğe girilmemesi, fısıltılara kulak asılmaması,kurtarma çalışmalarına katılmak suretiyle,yaralılara gerekli yardımın koordine şeklinde sağlanması vs. işlemler yapılır.
2. Elektrik ve suyun kısa zamanda afet bölgesine yeniden kontrollü şekilde verilmesi, gerekli sığınak,ısınma,beslenme olanaklarının acilen sağlanması, yağmaya yönelik güvenlik tedbirlerinin sıkı bir şekilde alınması,depremin tekrarlanma olasılığının jeolojik takibi, önlemlerinin alınması gerekir.
3. Hasarın bölgelenmesi,ileride tetkiki,hataların ve eksiklerin belirlenmesi, şehirden göç ve dışarıdan olumsuz etkilerin azalması,hizmetlerin afet önleme eylem planına uygun yapımının sağlanması gerekir.
4. Enkaz kaldırmada görev alanlar mutlaka koruyucu aşılarını yaptırmalı, koruyucu teçhizat kullanmadan cesetlere temas edilmemelidir.
5. Enkaz altında çakmak,kibrit gibi aydınlatma yerine pilli fenerler tercih edilmelidir.

6. Güvenli gıda yönünden;son kullanma tarihi geçmemiş,ayrı bir tabak kullanılmadan kendi ambalajında yiyecekler yenilmeli,ısıtma maksatlı tabak kullanılması gerekirse kullanıldıktan sonra atılması gerekir.

2.2.SU BASKINI (Sel):

Deprem felaketinin aksine su baskınlarını gerek meteorolojik bulgular ve gerekse baskın bölgelerinden bugüne kadar elde edilen istatistikler ve gözlemler sayesinde önceden saptamak mümkün olabilmektedir.Kısaca,bir dizi teknik önlemler ve gözlemler değerlendirilerek su baskınlarından önceden haberdar olunabilmekte ve can-mal kaybı önlenebilmektedir.Günümüzde baskın sahalarında etütler yapılmakta ve afete maruz yerleşim yerleri daha emin bölgelere kaldırılmaktadır.Ancak;Devlet Su İşleri Genel Müdürlüğü'nce,yapılan etütler sonucu taşkınları teknik önlemlerle kontrol altına alma işlemi daha ekonomik görülürse,yer değiştirme yapılmamakta sadece bent ve kanal yapılarak gerekli önlemler alınmaktadır.Ayrıca;nehir ve barajların su seviyeleri düzenli olarak izlenmelidir.Bölgemizde muhtemel su baskınları işletmelerin bodrum tabir edilebilen sıfır kot altında kalan kısımlarında yağmur,su borularında kırılma veya drenaj sisteminde tıkanma sonucu meydana gelen kazlar ile oluşabilir. Acil durum eylem planları kapsamında bu tip kazalar faraziye olarak değerlendirilmeli ve önlemleri alınmalıdır.

KISIM III - DOĞAL AFETLERE KORUNMA TEDBİRLERİ :

A-DEPREM AFETİNDEN KORUNMA

1. İşletme kaçış güzergahı incelenerek acil aydınlatma için yeterli önlem alınmalıdır.
2. Deprem sırasında ilk 10-15 saniye binayı terk edebilmek açısından çok önemlidir.Bunun için işletmece periyodik olarak deprem tatbikatları yapılmalı,farklı senaryolar geliştirilmeli ve süre tutularak denenmelidir.
3. Deprem sonrası gerekli olabilecek mekanik yardımcıların tedariki yapılmalı merkezi bir yerde kullanıma hazır bulundurulmalıdır.

B-SU BASKINI AFETİNDEN KORUNMA: (7269 sayılı kanunun 1051 sayılı kanunla değiştirilen on dördüncü maddesini kapsar)

1. Binaların su ile temas etme olasılığı bulunan kısımlarında,suya dayanıklı olmayan yapay ve doğal yapı malzemeleri (kerpiç,ahşap,tüf,alçı taşı,çamur vs.) kullanılmamalıdır.
2. Binaların en yüksek su düzeyinden en az 0.30 metre yüksekliğe kadar olan kısımları,250 doz çimento harçlı taş duvar, ya da daha dayanıklı malzeme ile yapılmalıdır.
3. Temel zeminin su altında kalma olasılığı varsa,bu durum göz önünde tutularak gerekli teknik önlemler alınmalıdır.
4. En yüksek su düzeyinin altında kalacak depo, çamaşırlık, sığınak ve benzeri yapı bölümleri yapılmamalıdır.

KISIM IV DOĞAL AFET VUKUUNDA YAPILACAK İŞLER :

DOĞAL AFET ÇALIŞMA SAATLERİ İÇİNDE OLURSA :

1. Herhangi bir doğal afet meydana geldiğinde işletme personeli toplanma yerinde bölümlere ayrılarak kısa sürede mevcut alınmalı,göçük altında kalan personel mevcudu çıkarılmalıdır.(Kurtarma operasyonu itfaiyeye ile müşterek olarak öncelikli işletmelere göre yapılacaktır.)
2. Eğer haberleşme telefon ile yapılıyorsa,İtfaiyeye telefonla irtibat kurulamıyorsa,ulaşım ve pasaparola ekiplerinden birer kişi bir araçla İtfaiyeye haber vermelidir.
3. Doğal afetler için kurulan ekipler daha önceden (kurtarma,ilkyardım vs.) konularında eğitilmelidir.
4. Özellikle ilkyardım ve kurtarma ekip personeli için bulaşıcı hastalıklara karşı koruyucu teçhizat temin edilmelidir.

5. Gerekli olan aydınlatma,su,yemek ihtiyaçları elektrik-su ekibi koordinesinde emre intizar personelce karşılanmalıdır.

DOĞAL AFET ÇALIŞMA SAATLERİ DIŞINDA OLURSA :

1. Yine aynı işlemler takip edilecek farklılık gerektiren durumlar göz önünde tutulacaktır.(İşletme yetkilisinin bulunmaması, elektrik sorunu vs.)Herhangi bir doğal afet meydana geldiğinde işletme personeli toplanma yerinde bölümlere ayrılarak kısa sürede mevcut alınmalı,göçük altında kalan personel mevcudu çıkarılmalıdır.

D. ACİL TELEFONLAR

Yangın (İtfaiye)	:110
Acil servis (Ambulans)	:112
Zehir Danışma	:114
Alo Trafik	:154
Polis İmdat	:155
Jandarma İmdat	:156
Sağlık Danışma	:184
Su Arıza	:185
Elektrik Arıza	:186
Doğalgaz Acil	:187
Telefon Arıza	:121
Alo Valilik	:179

C.32. Bilgi Güvenliği Ulaştırma Güvenliği Yönetimi

Evrak kelimesi Türkçe'de "yazılı kâğıt" anlamına gelen Arapça varak kelimesinin çoğul halidir. Yani evrak kelimesinin anlamı kâğıt yaprakları, kitap sayfaları, yazılmış mektuplar, yazılardır. Kurumumuzda evrak diye tanımladığımız resmi nitelikteki yazı, kamu kurum ve kuruluşlarının aralarında veya gerçek ve tüzel kişilerle iletişimlerini sağlamak amacıyla yazılan yazı, resmi belge, resmi bilgi ve elektronik belgeyi tanımlar. Bu yazılar bilgi verme, talep ya da arz belirtme amacı taşırlar.

"Gizlilik" uygulamasının amacı, kamu kurum ve kuruluşlarının güvenliğini sağlamak, yürütülen işlemlerin ve muhafaza edilen her türlü gizlilik dereceli, bilgi, belge, evrak, doküman ve malzemelerin, düşman veya yetkili ve ilgili olmayan kimseler tarafından öğrenilmesine veya elde edilmesine engel olmaktır. Bu amaca ulaşmak için yapılan bütün düzenlemelere ve alınan bütün önlemlere" güvenlik tedbirleri" denir.

C.32.1. Taşınılabilir materyaller üzerine iletilen verinin içeriği ile ilgili herhangi bir şey yazmamalıdır. Genel başlıklar kullanmalıdır.(Örneğin gizli evrakların bulunduğu bir cd üzerine "gizli evraklar"

yazılmamalıdır.)

C.32.2. İçinde veri bulunan taşınır materyal başka bir yere gönderiyorsa tutanak ile yetkili bir kişiye teslim edilmelidir.

C.32.3. Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Örneğin özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.

C.32.4. Çok gizli evraklar, torba veya çanta gibi kilitli muhafaza içinde ve "Çok Gizli" gizlilik dereceli güvenlik belgesi olan özel kurye ile gönderilirler. Eğer normal kargo ile gönderilmesi zorunlu ise, içerik uygun bir şekilde kripto edilir (şifrelenir). Dışarıdan kargonun takip edilmemesi için kargo takip numarasının maskelenmesi yapılmalıdır.

C.32.5. Gizli evraklar veya cd, dvd, usb bellekler gönderilirken, iki adet zarf kullanmalıdır. Birinci zarfın üzerine içeriğin niteliğine göre sınıflandırılmalı ve zarfın kapağı mühürlenmelidir. İkinci zarf ise normal adres yazılan zarf olmalıdır. "GİZLİ" yazılı olan zarf diğer normal zarfın içine koyulmalıdır.

C.32.6. Genel kayıt birimine gelen evrak/zarf kayıt biriminde görevli memur personel tarafından kontrol edilerek alınmalıdır.

C.32.7. Gizli ibaresi ile gelen zarflar personel tarafından açılmadan Yazı İşleri Müdürüne teslim edilmelidir. Yazı İşleri Müdürünün ilgili birimine havalesinden sonra sisteme kayıt edilerek zimmet defteri ile havale edilen birime teslimi sağlanmalıdır.

C.32.8. Kullanılan MIS yazılımlarında evrak kayıt edilirken GİZLİ olarak işaretlenmeli ve diğer kullanıcılar evrak içeriğini görmemelidir.

C.33. Sosyal Mühendislik Zafiyetleri

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaaflarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanırlar.

C.33.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.

C.33.2. Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.

C.33.3. Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.

C.33.4. Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.

C.33.5. Şifre kişiye özel bilgidir. Sistem yöneticiniz dahil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.

C.33.6. Oluşturulan dosyaya erişecek kişiler ve hakları "bilmesi gereken" prensibine göre belirlenmelidir.

C.33.7. Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.

C.33.8. Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.

C.33.9. Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.

C.33.10. Kazaa, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.

C.34. Sosyal Medya Güvenliği

C.34.1. Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar paylaştıkları her verinin içeriğinden sorumludurlar.

C.34.2. Sosyal medya hesaplarına gönderilen mesajlar, kuruma ait bilgiler sözlü ya da yazılı olarak hiçbir platformda kullanılmamalıdır.
C.34.3. Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar, hesapların şifrelerini kurum içi şifrelendirme sisteminden farklı düzenlemelidir.
C.34.4. Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar, hesapların şifrelerini kimseyle paylaşmamalıdır.
C.34.5. Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar, şifreleri belirli aralıklarla güncellemeli ve şifrelerin en az 8 karakterden oluşmasına dikkat etmelidir.
C.34.6. İnternet sitesi (web) Basın Yayın ve Halkla İlişkiler Müdürlüğü sorumluluğunda olmakla birlikte, Bilgi İşlem Müdürlüğü tarafından görevlendirilecek 1 (bir) personel de teknik destek vermelidir.
C.34.7. Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcıların, bilgisayarlarını kullanmadıkları zamanlarda kapatmaları veya kilitlemeleri gerekmektedir.
C.34.8. Sosyal medya hesaplarına ve internet sitesine (web) veri girişi için yetkilendirilen kullanıcılar, içerik paylaşılmadan önce Basın Yayın ve Halkla İlişkiler Müdüründen onay almalıdırlar.
C.34.9. Sosyal medya hesaplarında ve internet sitesinde (web) paylaşılması istenen tüm verilerin ilgili müdürlükler tarafından en az 1 (bir) gün önce Basın Yayın Halkla İlişkiler Müdürlüğü'ne yazıyla bildirilmelidir.

D. KISALTMALAR

T.C. : Türkiye Cumhuriyeti

BG: Bilgi Güvenliği

BGYS: Bilgi Güvenliği Yönetim Sistemi

BT: Bilgi Teknolojileri

BSI: British Standarts Institute, İngiliz Standartları Enstitüsü

ÇKYS: Çekirdek Kaynak Yönetimi Sistemi

DTVT: Devlet Teşkilatı Veri Tabanı

IEC: International Electrotechnical Commission, Uluslararası Elektroteknik Komisyonu

ISO: International Organization for Standardization, Uluslararası Standartlar Teşkilâtı

Coso Modeli

E. SÖZLÜK

Açılır Pencere Engelleyicisi (Popup Blocker): Açılır Pencere Engelleyicisi, istenmeyen çoğu açılan pencerenin görüntülenmesini engeller.

ADSL: Asimetrik Sayısal Abone Hattı anlamına gelen hızlı internet erişim teknolojisidir.

Ağ (Network): Ağ birbirine kablolarla veya kablosuz bağlanmış sunucu, yazıcı, bilgisayar, modem gibi birçok haberleşme cihazlarının en ekonomik ve verimli yoldan kullanılmasıdır.

Aldatmaca e-posta (Hoax): Elektronik posta adresi toplamak veya markaları karalamak için oluşturulan yalan haber (asparagas) içeren e-postalardır.

Anti virüs (Virüsten Korunma): Bilgisayarınızı ya da sisteminizi bilgisayar virüslerinden korumaya ve bilgisayar virüslerini temizlemeye yarayan yazılımdır.

Bağlantı Noktası (Port): Bir elektronik devreye, şebekeye veya sisteme giriş ve bağlantı noktasıdır.

Bilgisayar Korsanı (Hacker): Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren ve onları kullanabilen kişidir. Amaçlarına göre farklı adlandırılırlar:

Siyah Şapkalılar: Her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabilen bu en bilindik hackerlar, sistemleri kullanılmaz hale getirir veya gizli bilgileri çalar. En zararlı hackerlar siyah şapkalılardır.
Beyaz Şapkalılar: Beyaz şapkalılar da her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabiliyor ancak kırdığı sistemin açıklarını sistem yöneticisine bildirerek, o açıkların kapatılması ve zararlı kişilerden korunmasını sağlıyorlar.

Bilgisayar Solucanı (Computer Worm): Bilgisayar solucanı kendi kendini çoğaltabilen ve kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmış kötücül (malware) yazılımdır. Bilgisayar virüsünden farkı bunu otomatik olarak yapmasıdır.

Bilgisayar Virüsü (Computer Virus): Veri girişi yoluyla bilgisayarlara yüklenen, sistemin veya programların bozulmasına, veri kaybına veya olağandışı çalışmasına neden olan yazılım.

Bilişim (Informatics): İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi.

Bilmesi Gereken Prensibi (Need to Know Principle): Gizlilik dereceli bir ilgiyi, belgeyi, projeyi veya malzemeyi ancak görevi gereği öğrenme ve kullanma sorumluluğu olma ve uygun gizlilik dereceli Şahıs Güvenlik Derecesine sahip olma durumudur.

BIOS (Basic Input/Output System): Temel Giriş/Çıkış Sistemi, bilgisayarın ilk açılma işlevini yerine getiren yazılımdır.

Casus Yazılım (Spyware): Casus yazılım, en başta gelen bir kötücül yazılım (malware) türüdür. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır.

Disk Biçimlendirme (Disc Partitions): Diskinizi biçimlendirmek demek diskinizi farklı mantıksal disk bölümlerine ayırmak anlamına gelir.

EFS: Veri Şifreleme Sistemi anlamına gelen bir bilgisayar terimi kısaltmasıdır.

Ekran Koruyucusu (Screen Saver): Bilgisayarda monitörün uzun süre kullanılmadan açık kalması durumunda devreye giren, monitörün ömrünün azalmasını ve parola ile korunduğunda yetkisiz erişimi engelleyen yazılımdır.

Elektronik Sertifika (Electronic Certificate): Elektronik Sertifika, yani elektronik kimlik, sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşıyan ve taşıdığı açık anahtar bilgisinin, belirtilen kişi veya kuruma ait olduğunu garanti eden belgedir. Elektronik kimlik belgesi kişilere ait olabildiği gibi kurumlara veya web sunucularına ait olabilir.

Exe: Çalıştırılabilir dosya tiplerinin dosya uzantısıdır.

FTP: Dosya aktarım iletişim kuralı, (File Transfer Protocol; FTP), bir dosyayı ağ üzerindeki başka kullanıcıya o ağdaki bilgisayarda geçerli bir kullanıcı ismi ve şifresi ile yollamak için kullanılmaktadır.

Güvenlik Duvarı (Firewall): Güvenlik duvarı kurulduğu sisteme gelen ve giden ağ trafiğini kontrol ederek yetkisiz veya istenmeyen yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.

Hata (Bug): Bir yazılım ya da donanımda var olan, meydana gelen hata, kod hatasıdır.

Hizmet Paketi (Service Pack): Piyasaya sürülen bilgisayar yazılımlarının, ortaya çıkan hata ve

açıklıklarını giderecek, varsa yeni özelliklerini ortaya çıkaracak yama tabir edilen programcıkların tek bir paket halinde toplandığı yazılımdır.

HDD: Sabit disk ya da Hard disk kısaca HDD ya da Türkçesi ile sabit disk sürücüsü veri depolanması amacı ile kullanılan manyetik kayıt ortamlarıdır. Önceleri büyük boyutları ve yüksek fiyatları nedeni ile sadece bilgisayar merkezlerinde kullanılan sabit diskler, cep telefonları ve sayısal fotoğraf makineleri içine sığabilecek kadar küçülen boyutları ile günlük hayatımıza girmişlerdir. Sabit disklerin en yoğun kullanım yeri bilgisayarlardır. Ses, görüntü, yazılımlar, veri tabanları gibi büyük miktarlarda bilgi, gerektiğinde kullanılmak üzere sabit disklerde saklanır.

HTTP : HTTP (Hypertext Transfer Protocol, Türkçe Hipermetin Aktarma İletişim Kuralı) bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiper ortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır.

HTTPs : HTTPS (Secure Hypertext Transfer Protocol, güvenli hipermetin aktarım iletişim kuralı) hipermetin aktarım iletişim kuralının (HTTP) güvenli ağ protokolü ile birleştirilmiş olanıdır. Klasik HTTP protokolüne SSL protokolünün eklenmesi ile elde edilir.

ICMP: Internet Kontrol Mesaj İletişim Kuralı, ICMP(Internet Control Message Protocol), hata mesajları ve TCP/IP yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır. Kontrol amaçlı bir protokoldür.

IEEE: (Institute of Electrical and Electronics Engineers, Elektrik ve Elektronik Mühendisleri Enstitüsü) elektrik, elektronik, bilgisayar, otomasyon, telekomünikasyon ve diğer birçok alanda, mühendislik teori ve uygulamalarının gelişimi için çalışan, kar amacı olmayan, dünyanın önde gelen teknik organizasyonudur.

IEEE 802.1x: Bağlantı noktası tabanlı ağ erişim kontrolü için bir IEEE standartıdır. Bu, ağ protokolleri IEEE 802.1 grubunun bir parçasıdır. Bir LAN veya WLAN eklemek isteyen cihazlara kimlik doğrulama mekanizmasını sağlar.

İç Ağ (Intranet): Kuruluşların, kurumun veya herhangi bir grubun, bilgisayarları arasında güvenli bir şekilde bilgi paylaşması için oluşturulmuş büyük çaplı yerel ağ yapısıdır.

IP adresi: IP (Internet Protokol) adresi, interneti protokolünü kullanan diğer ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adrestir.

İstenmeyen e-posta (Spam): Talep edilmeyen veya istenmeyen e-posta mesajıdır.

İşletim Sistemi (Operating System): İşletim sistemi, bilgisayar donanımının doğrudan denetimi ve yönetiminden, temel sistem işlemlerinden ve uygulama yazılımlarını çalıştırmaktan sorumlu olan sistem yazılımıdır.

Kırılmış (Crack): Ücretli yazılımları ücretsiz kullanmayı sağlayan, program kırıcıları (cracker) tarafından yazılmış programcıkları ve korsan yazılımları ifade eder.

Kriptoloji: Şifre bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda alıcıya iletilmesi ve iletilmiş mesajın deşifresiyle uğraşır. Kriptoloji=Kriptografi + Kriptoanaliz Kriptoloji bilmi kendi içerisinde iki farklı branşa ayrılır. Kriptografi ; şifreleri yazmak ve Kriptoanaliz ;şifreleri çözmek ya da analiz etmekle ilgilenir.

Kriptografi: Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi -dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da- koruma amacı güderler. Bir başka deyişle kriptografi, okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerin tümü olarak da gösterilir.

Korsan (Warez): Telif yasaları çiğnenerek ticareti yapılan telif hakkı saklı materyallere denir. Telifli ürünlerin kopyalanmasını, çoğaltılmasını ve dağıtımını yapan kişilere korsan, yapılan işe korsancılık denmektedir.

Kötücül Yazılım (Malware): Kötücül yazılım (malware: İngilizce "malicious software"in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır.

Linux: Unix'e fikirsel ve teknik anlamda atıfta bulunarak geliştirilmiş; açık kaynak kodlu, özgür ve ücretsiz bir işletim sistemi çekirdeğidir. Çekirdeğin kaynak kodları GNU Genel Kamu Lisansı çerçevesinde özgürce dağıtılabilir, değiştirilebilir ve kullanılabilir. Linux'un Unix ile herhangi bir kod ortaklığı bulunmamaktadır yani Linux'un kodları sıfırdan başlanılarak yazılmıştır.

MAC Adresi: MAC adresi (Media Access Control, yani Ortam Erişim Yönetimi) bir cihazın ağ donanımını tanımaya yarar, bir anlamda fiziksel adresidir.

Modem: Bilgisayarınızın telefon ya da internet hattına bağlanarak diğer bilgisayarla bağlantı kurmasına yarayan cihazdır.

NTFS: (New Technology File System; Yeni Teknoloji Dosya Sistemi), Windows NT'nin standart dosya sistemidir ve Windows 2000, Windows XP, Windows Server 2003 ve Windows Vista'da da standart olarak kullanılmıştır. Microsoft'un önceki FAT dosya sisteminin yeniden yapılandırılmasıyla oluşmuştur.

Olay Kayıtları (Event Logs): Bir işletim sisteminin tuttuğu kayıtları ifade eder. Olay günlüğü kayıtları, sorunları incelerken ve çözerken size önemli bilgiler sağlar.

Oltalama (Phishing): Yasal bir e-posta gibi görünen ve kişisel bilgilerinizi talep eden bir e-posta mesajıdır. İkna yöntemiyle gizli bilgilerin elde edilmesini amaçlayan bir sosyal mühendislik metodudur.

Otomatik Çalıştır (Autorun): Autorun, taşınabilir disklerin bilgisayara takıldığında istenilen programı veya programları otomatik olarak çalıştırması için kullanılan bir uygulamadır.

Paylaştırılmış Klasör (Shared Folder): Paylaştırılmış klasörler başkasının erişimine izin verdiğiniz ve çoğu zaman dosya paylaşmak amacıyla kullandığımız klasörlerdir.

Privilege: Ayrıcalık, imtiyaz, özel hak.

Rar: Bir dosya sıkıştırma ve arşivleme formatıdır. Eugene Roshal tarafından oluşturulmuş ve oluşturucusunun soyadını almıştır. RAR uzantılı dosyalar .rar şeklinde gözükür.

Robot (Bot): Bot, bilişim dünyasında "robot" anlamında kullanılan yaygın bir terimdir.
Pek çok bilgisayar işlemini yarı-otomatik olarak yapabilen robotlar anlamında kullanılır.

TCP/IP: İnternet protokol takımı, İnternet'in çalışmasını sağlayan bir iletişim protokolleri bütünüdür. Bazen TCP/IP protokol takımı olarak da adlandırılır. TCP (Transmission Control Protocol) ve IP (Internet Protocol) ün kısaltmalarıdır.

Truva Atı (Trojan): Bilgisayar yazılımı bağlamında Truva atı zararlı program barındıran veya yükleyen programdır. Terim klasik Truva Atı mitinden türemiştir. Truva atları masum kullanıcıya kullanışlı veya ilginç programlar gibi görünebilir ancak çalıştırıldıklarında zararlıdırlar.

Tuş Kaydedici (Keylogger): Bilgisayarda yazılanları siz farkında olmadan kaydedebilen yazılım veya donanımlardır.

Sabit disk (Hard Disk): Sabit Disk ya da Hard disk kısaca HDD, veri depolanması amacı ile kullanılan manyetik kayıt ortamlarıdır.

SMS: (İngilizce Short Message Service; Kısa Mesaj Hizmeti), cep telefonu aracılığı ile yazılan mesajın bir cep telefonundan diğer bir cep telefonuna gönderilmesi, mesajlaşması hizmetidir.

SNMP: "Simple Network Management Protocol"'ün kısaltması. "Basit Ağ Yönetimi Protokolü" adı verilen bu teknoloji, bilgisayar ağları büyüdükçe bu ağlar üzerindeki birimleri denetlemek amacıyla tasarlanmıştır.

SSH: (Secure Shell) güvenli veri iletimi için kriptografik ağ protokolüdür. Ssh ile ağa bağlı olan iki bilgisayar arasında veri aktarımı güvenlik kanalı üzerinden güvensiz bir ağda yapılır. Bu durumda ağda Ssh ile haberleşen makinelerden biri ssh sunucusu diğeri ssh istemcisi olur. Ssh kabuk hesabına erişim için Unix ve benzeri işletim sistemlerinde protokolün en iyi uygulaması olarak bilinir, ama aynı zamanda Windows üzerindeki hesaplara erişim için de kullanılabilir. SSH uzaktaki makineye bağlanıp kimlik kanıtlaması yapmak için açık anahtarlı şifrelemeyi kullanır ve bu sayede kullanıcıya sistemi kullanmasına izin vermiş olur.

SSL: Secure Socket Layer (Türkçe'ye Güvenli Yuva Katmanı olarak çevrilebilir) protokolü, internet üzerinden şifrelenmiş güvenli veri iletişimi sağlar.

Sunucu: (İngilizce: Server), bilgisayar ağlarında, diğer ağ bileşenlerinin (kullanıcıların) erişebileceği, kullanımına ve/veya paylaşımına açık kaynakları barındıran bilgisayar birimi. Bir ağda birden fazla sunucu birim bulunabilir. Karşıtı istemci (İngilizce: Client) dir.

USB Bellek (USB Flash): Kapasiteleri 256 GB'a kadar ulaşabilen, küçük, hafif, çalışma esnasında sökülüp takılabilir ve taşınabilir veri depolama aygıtlarıdır.

Virüs Tespit Ajanı (Antivirus Agent): Bilgisayarınızı zararlı programlardan korumak için virüsten korunma yazılımının virüsleri tespit eden yazılım parçasıdır.

WEP: WEP (Wired Equivalent Privacy), kablosuz ağ bağlantılarında veri bağ tabakasında çalışan şifreleme yöntemidir. Kabloya Eşdeğer Mahremiyet (KEM) olarak Türkçe'ye çevrilebilir.

Wi-fi: Wi-fi: "Wireles Fidelity" kelimelerinin kısaltması olup kablosuz bağlılık veya kablosuz bağlantı anlamına gelir.

WPA: WPA (Wi-Fi Protected Access)Wi-Fi korumalı Erişim olarak adlandırılır. WEP şifreleme sisteminden daha güvenli olduğu söylenen ve WEP şifrelemeden daha yeni bir teknolojidir.

Yazılım Yaması (Software Patch): Yazılımlarda oluşan bir hatayı ya da programın içeriğindeki hatalı bir fonksiyonu düzelten bir programcıktır.

Zip: (dosya formatı), bir popüler veri sıkıştırma ve arşivleme formatıdır. ZIP uzantılı dosyalar ".zip" şeklinde gözükür.

Zombi Bilgisayar (Zombie): Zombi bilgisayar, (genelde yalnızca zombi olarak kısaltılır) genel ağa (internet) bağlı, bir kırıcı (hacker) tarafından bilgisayar virüsü veya truva atı ile tehlikeye atılmış bilgisayardır.

F. KAYNAK

1. Sağlık Bilgi Sistemleri Genel Müdürlüğü
2. TUBİTAK-BİLGEM
3. http://www.bilgiguvenligi.gov.tr/kilavuz-dokumanlar/index.php
4. www.bilgimikoruyorum.org.tr
5.http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/veri-merkezlerinin-sahipolmasi-gereken-ozellikler.html
6. Ömer Faruk Acar, TÜBİTAK BİLGEM
7. Neşe SAYARI, Türkiye Bilişim Derneği, Bilgi Güvenliği ve Yönetimi
8. TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, BGYS Risk Yönetim Süreci,2007

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.

Muhittin SELVİTOPU
Harita ve Kadastro Mühendisi
Belediye Başkanı