T.C. Sağlık Bakanlığı
İzmir
İl Sağlık Müdürlüğü

BİLGİ GÜVENLİĞİ POLİTİKALARI KILAVUZU

İZMİR İL SAĞLIK MÜDÜRLÜĞÜ
DESTEK HİZMETLERİ BAŞKANLIĞI
BİLGİ İŞLEM BİRİMİ

Ekim 2018

İçindekiler

İZMİR İL SAĞLIK MÜDÜRLÜĞÜ
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI

BGYS (Bilgi Güvenliği Yönetim Sistemi) politikası, T.C. Sağlık Bakanlığı İzmir İl Sağlık Müdürlüğü ve Bağlı Birimler bünyesinde yürütülen BGYS çalışmalarının amaç, hedef ve kapsamını, içeriği ve yönetimini, sorumlularını, görev, yetki ve sorumluluklarını içeren bir dokümandır. Bu doküman İzmir İl Sağlık Müdürlüğü Destek Hizmetleri Başkanlığı Bilgi İşlem Birimi hedefleri doğrultusunda Sağlık Bakanlığı Bilgi Güvenliği Politikalar Kılavuzu esas alınarak hazırlanmıştır.

1. Amaç:

Bilgi Güvenliğinin gizlilik, bütünlük ve erişilebilirlik ilkelerine sadık kalmak koşuluyla üst yöneticilerin tam desteğiyle, tüm iç ve dış tehditlere yönelik Bilgi Güvenliği teknik, idari ve hukuki tedbirlerin alınmasını ve uygulanmasını sağlamak; ayrıca var olan bilginin kaybolmasını, zarara uğramasını, yok olmasını, yetkisiz ve kötü niyetli kişilerin eline geçmesini engellemektir.

2. Hedef:

Bilgi güvenliğinin teknik tedbirlerden ibaret olmaması sebebiyle; veri işleyen, veri sorumlusu, verilere ulaşabilen en uç kullanıcılar da dahil olmak üzere Bilgi Güvenliği farkındalığı oluşmasının sağlanması, kurumsal riskler kadar kullanıcıya dayalı risklerin de en aza indirgenmesini sağlamaktır.

3. Kapsam:

İzmir İl Sağlık Müdürlüğü tüm birimlerinin, hizmet alınan ve hizmet sunulan bireysel ve kurumsal tüm veri üreten ve veriye erişen tüm kullanıcılarının Bilgi Güvenliği Standartları gerekliliklerini yerine getirmesinin sağlanması ve risklerin bertaraf edilmesi için Sağlık Bakanlığı BGYS politikaları dokümanında yer alan adımlar kapsam dahilinde esas alınmıştır.

4. Tanımlar

- **İzmir İl Sağlık Müdürlüğü:** İzmir İl Sağlık Müdürlüğü, Başkanlıklar, Hukuk ve Muhakemat Birimi, İzleme-Değerlendirme-İstatistik-Raporlama ve Denetim Birimi, Sivil Savunma ve Seferberlik Hizmetleri Birimi, Basın Birimi, Özel Kalem, Tıbbi Cihaz/Tıbbi Hizmet Alımları Planlama Komisyonu Birimi, Başkanlıklara Bağlı İl Sağlık Müdürlüğü Birimleri
- **Bağlı Birimler:** İlçe Müdürlükleri ile 112 Komuta Kontrol Merkezi ve Acil Sağlık Hizmetleri İstasyonları
- **BGYS:** Bilgi Güvenliği Yönetim Sistemi.
- **Varlık:** kurum içi değeri olan her türlü unsur (insan, donanım, yazılım, bilgi, vs.)
- **Gizlilik;** Bilgiye sadece erişme izni olan yetkili kişiler ya da sistemlerin erişmesini sağlamaktır.
- **Bütünlük;** Bilginin yetkisiz kişi ya da işlemler tarafından değiştirilmemesini sağlamaktır. Böylece bilginin tutarlılığı sağlanmış olur.
- **Erişilebilirlik;** Bilgiye doğru zamanda erişimin ve erişim sürekliliğinin sağlanmasıdır.
- **Bilgi Güvenliği İhlal Olayı:** BG Politikalarının ve prosedürlerinin dışında işlem tesis edilmesi ile iş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen Bilgi Güvenliği olayıdır.

- **Bilgi Sistemleri:** Donanım, yazılım, bilgisayar ağları ve insan unsurlarından oluşan, veri ve bilgileri toplayan, kaydeden, işleyen, dönüştüren ve yayan sistemler bütününü ifade eder.

5. Bilgi Güvenliği Yapısı ve Organizasyonu

	Bilgi Sistemleri Koordinatörü	Bilgi Güvenliği Yetkilisi	Kurumsal SOME Ekip Lideri
	Asıl Personel		
Kadro Unvanı	Şube Müdürü	Bilgisayar Mühendisi	Bilgisayar Mühendisi
Görev Unvanı	Başkan Yardımcısı	Bilişim Uzmanı	Bilgisayar Mühendisi
Adı ve Soyadı	Erkan ERSOY	Abdullah Fatih AKGÜL	Ömer Öztekin
Kurumsal E-posta Adresi	erkan.ersoy@saglik.gov.tr	fatih.akgul@saglik.gov.tr	omer.oztekin@saglik.gov.tr
	Yedek Personel		
Kadro Unvanı		Tabip	Bilgisayar İşletmeni
Görev Unvanı		Tabip	Bilgisayar İşletmeni
Adı ve Soyadı		Nehire Tüten YÜKSEKOĞLU	Barış ÇAĞDAŞ
Kurumsal E-posta Adresi		nehire.yuksekoglu@saglik.gov.tr	baris.cagdas@saglik.gov.tr

Tablo 1 Bilgi Güvenliği Yapısı ve Organizasyonu

BGYS Komisyonu

İzmir İl Sağlık Müdürlüğü BGYS komisyonu İl Müdürü başkanlığında Personel Hizmetleri ve Destek Hizmetleri başkan ve başkan yardımcıları ve Bilgi İşlem Birim Sorumlusunun katılımı ile yılda bir kez toplanır.

BGYS Komisyon Görev, Yetki ve Sorumlulukları

1. İl düzeyindeki Bilgi Güvenliği Politika ve stratejilerini belirler; BGYS yönergesine bağlı revizyonları yapar.

2. BG politikalarının uygulanmasını ve uygulanmadaki etkinliğini gözden geçirir.

3. BG faaliyetlerinin yürütülmesini yönlendirir.

4. BG eğitim ve farkındalığının sağlanması için plan ve program yapar.

5. BG faaliyetleri ve kontrollerinin tüm kurum ve kuruluşlarda koordine edilmesini sağlar.

6. Yürütülen çalışmaların tabana yayılması hususunda planlanan çalışmalara katılır, bağlı oldukları birimlerde bu çalışmaların yayılmasına öncülük eder.

6. İnsan Kaynakları Zafiyeti Yönetimi

a. İşe başlama, görev değişikliği ve işten ayrılma süreçlerine yönelik prosedürün uygulanması sağlanır. Personel Gizlilik Sözleşmesi ve Bilgi Güvenliği Farkındalık Bildirgesi personele tebliğ edilerek söz konusu belgeler imzalatılarak özlük dosyasında saklanır.

b. Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.

c. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.

d. ÇKYS, İl Sağlık Bilgi Sistemi, vb. sistemler üzerinden kişiyle ilgili bir işlem yapıldığında ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.

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

f. İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt imha makinasında imha edilmelidir.

g. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

h. Personel giriş çıkışlarda kurum kimlik kartı okutmalıdır.

7. Sosyal Mühendislik Zafiyetleri

Sosyal Mühendislik, insan zafiyetlerinden faydalanarak çeşitli etkileme, ikna ve kandırma yöntemleriyle istenilen (normalde paylaşmamaları gereken) bilgileri elde etmeye çalışmaktır.

a. Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.

b. Kurum içi bilgiler, sosyal medyada paylaşılmamalıdır.

c. Kuruma ait hiçbir gizli bilgi ve yazı sosyal medyada paylaşılmamalıdır.

d. Arkadaşlarımızla paylaşılan bilgiler seçilirken dikkat edilmelidir.

e. Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararlar düşünülerek hareket edilmelidir.

f. E-Postalara gelen kaynağı belli olmayan, şüphe uyandıran e-postalar açılmamalı ve ilgili sorumlulara bilgi verilmelidir.

g. Kurum Web Sayfasında kurum ile ilgili paylaşılan bilgilere son derece dikkat edilmeli ve içerik sürekli olarak izlenmelidir.

h. Telefon veya sohbet yoluyla yapılan haberleşmelerde, resmi e-posta dışında, Kullanıcı adı ve özellikle şifre bilgileri paylaşılmamalıdır. Şifre kişiye özel bir bilgidir. Sistem yöneticileri dâhil

olmak üzere telefonda veya e-posta yazışmalarında şifre paylaşılmamalıdır. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.

i. eMule, torrent gibi dosya paylaşım ve indirme yazılımları kullanılmamalıdır.

8. Bilgi Varlıklarımız

Masaüstü bilgisayarlar, laptoplar, tabletler, telefonlar, CD, DVD ve USB Bellek ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-basılı ortamda bulunan veya iletişim ortamında (internet, e-mail, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

A. Varlık Sınıflandırması

BİLGİ SINIFLANDIRMA KILAVUZU		Saklanma Yeri Dolap
GİZLİ	En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır.	Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel bilgisayarlar
İÇ KULLANIM	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır.	Departmanın kilitli dolapları, kişisel bilgisayarlar
KİŞİSEL	Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, Laptop veya Dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır.	Çalışma masalarının kilitli çekmeceleri
KURUMA AÇIK	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın kilitli ortak dolapları
HALKA AÇIK	Bu bilgiler T.C. Sağlık Bakanlığına bağlı tüm teşkilatına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Her türlü fiziki ortam, erişime açık elektronik ortamı

Tablo 2 Bilgi Sınıflandırma Kılavuzu

Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan

ve işlem için üçüncü taraflara verilen kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

9. Erişim Kontrolü

1.Erişim Kontrol Politikası

1.1. Erişim kontrolünün amacı, bilgi ve bilgi işleme tesislerine yapılacak olan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin tesis edilmesidir.
1.2. Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı gizlilik dereceli) bilgiler için özel bir erişim kontrol tedbiri alınmasına gerek yoktur. Bu tür bilgiler, kurumların İnternet sitelerinin vatandaşlara açık bölümlerine konulabilir. Bina ve tesislerde duyuru panosu vb. ortamlarda yayımlanabilir.
1.3. Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan erişim kontrol politikalarının sıkılaştırılması (zorlaştırılması) gerekir.
1.4. Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.
1.5. Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.
1.6. "Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak, bir kişinin kendi başına tüm bilgi varlıklarına erişimi engellenir. Teknik nedenlerle görev ayrımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır.
1.7. "Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.
1.8. Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik sistemler için farklı kimlik doğrulama yöntemleri (akıllı kart, tek kullanımlık parola, elektronik imza, mobil imza vb.) kullanılabilir.
1.9. Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur.
1.10. Sağlık Bilişim Ağı dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.
1.11. Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. Veri tabanı yönetim sistemi sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.
1.12. Bilgi varlıklarına fiziksel olarak yapılacak erişimler için gerekli önlemler alınır.
1.13. Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için Kişisel Verileri Koruma Kurulu'nun 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.

2.Kullanıcı Erişimlerinin Yönetimi

2.1. Kullanıcı erişimlerinin yönetimi, sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek, sadece yetkili kullanıcıların erişimlerini temin etmek için yapılır.
2.2. Tüm sistem ve hizmetler için kullanıcı erişimi ile ilgili hususlar Erişim Kontrol Politikası içinde belirtilir. İlgili tüm kullanıcılara resmen duyurulur.
2.3. Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir. Bilmesi gereken prensibi uyarınca, gereksiz olarak verilmiş yetkilerin kaldırılması sağlanır.
2.4. İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en fazla altı aylık aralıklarla yapılır.
2.5. Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilir.
2.6. Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili incelemeler, üç ayı aşmayacak şekilde daha sık yapılır.
2.7. 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır.
2.8. Ayrıcalıklı erişim hakkı verilen kullanıcı sayısı (etki alanı yöneticisi, veri tabanı yöneticisi vb.) asgari düzeyde tutulur.

3.Parola Güvenliği

3.1. Parola politikaları belirlenirken, sistem ve uygulamaların, kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmaya zorlamaları sağlanır.
  3.1.1. Parolalar en az 6 (altı) karakterden oluşur. Root, administrator gibi sistem yönetim işlemlerinde kullanılan parolaların en az 12 karakterden oluşması tavsiye edilir.
  3.1.2. Parolalar karmaşıklık gereklerine uymalı, aşağıdaki dört kategorinin en az üçünü sağlamalıdır.
    3.1.2.1. İçerisinde en az 1 (bir) tane büyük harf bulunur.
    3.1.2.2. İçerisinde en az 1(bir) tane küçük harf bulunur.
    3.1.2.3. İçerisinde en az 1 (bir) tane rakam bulunur.
    3.1.2.4. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !, ?, +, $, €, #, &, %,], *, =, vb.)
  3.1.3. Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab...)
  3.1.4. Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf,1234,zxcvb...)
  3.1.5. Kişisel bilgiler veya klavye kombinasyonları ile basitçe üretilebilecek karakter dizilerinin kullanılması engellenir. (Örneğin 12345678, qwerty, doğum tarihi, çocuğun adı, soyadı gibi)
  3.1.6. Kullanıcının son 1 parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir.
3.2. Veri tabanı yönetim sistemi, aktif dizin sunucusu, uygulama sunucusu, ağ cihazları gibi sistem hesaplarına ait parolalar (root, administrator, vs.) en geç 3 (üç) ayda bir değiştirilir.
3.3. Kullanıcı hesaplarına ait parolalar (örnek: HBYS, İl Sağlık Bilgi Yönetim Sistemi, Masaüstü Bilgisayar vs.) en geç 6 (altı) ayda bir değiştirilmesi sağlanır.
3.4. Parolalar, e-posta iletilerine veya herhangi bir elektronik forma eklenmez.
3.5. Parolalar gizli bilgi olarak muhafaza edilir. Kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.
3.6. Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu bölümde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.
3.7. İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup, kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.

4.Uzaktan Çalışma ve Erişim

4.1. Uzaktan çalışma, 4857 sayılı İş Kanununun 14'üncü maddesine göre; "çalışanların, işveren tarafından oluşturulan iş organizasyonu kapsamında, iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisi" olarak tanımlanmaktadır.
4.2. Uzaktan çalışma; Müdürlüğümüz çalışanları ile yükleniciler, tedarikçiler, iş ortakları çalışanları gibi Müdürlüğümüz ile geçici olarak iş ilişkisi olan kişiler tarafından yapılabilir.
4.3. Uzaktan çalışma işlemi, yapısı itibarı ile güvensiz olarak kabul edilir ve bilgi güvenliğini sağlamak için ek önlemler alınması gerekir.
4.4. Uzaktan çalışma ile ilgili kontrol tedbirleri belirlenirken aşağıda sıralanan dört temel tehdit unsuru/modeli dikkate alınır.
  4.4.1. Uzak çalışma ortamlarının fiziki güvenliğindeki yetersizlikler,
  4.4.2. Uzak bağlantının güvenli olmayan ağ ortamları (çoğunlukla internet) üzerinden yapılması,
  4.4.3. Kurum güvenlik politikaları uygulanmamış güvenilir olmayan cihazların iç ağa bağlanması,
  4.4.4. İç ağdaki kaynaklara dışarıdan erişim.
    4.4.4.1. Farklı yöntemler kullanılarak uzak bağlantı yapılması mümkündür. Uzaktan erişim için ihtiyacın kendine özgü şartları ve riskleri değerlendirilerek en uygun yöntem belirlenir.
    4.4.4.2. Uzaktan erişim yöntemi olarak tünelleme, uzak masaüstü erişim veya doğrudan uygulama erişimi yöntemlerinin biri veya birkaçı birlikte kullanılabilir.
  4.4.5. Tünelleme yöntemi, uzaktan çalışmada kullanılan bilgisayar ile iç ağın kriptolojik yöntemler kullanılmak suretiyle oluşturulan güvenli bir tünel vasıtasıyla birbirine bağlanmasıdır. Tünelleme işlemi, ağırlıklı olarak sanal özel ağ (VPN: Virtual Private Network) teknolojileri vasıtasıyla yapılır. VPN işlemi IP güvenliği (IPsec: IP Security), taşıma katmanı güvenliği (TLS: Transport Layer Security) veya güvenli kabuk (SSH: Secure Shell) protokolleri kullanılmak suretiyle yapılabilir.

4.4.6. Uzak masaüstü erişim çözümleri, uzaktan çalışan kullanıcıların kurumun iç ağında yer alan bir sunucu veya istemci bilgisayarın karşısındaymış gibi kullanılmasını sağlar. Bu yöntemde, uzak kullanıcılar bağlanılan bilgisayarın klavye ve fare kontrollerini uzaktan yapar hale gelirler.

4.4.7. Doğrudan uygulama erişimlerinde, erişilecek uygulamalara ait sunucular kurumun halka açık sunucuların konumlandırıldığı arındırılmış bölgeye (DMZ:De-Militarized Zone) yerleştirilir. Bu mimaride kullanıcılar genellikle web arayüzleri üzerinden doğrudan ilgili uygulama sunucusuna bağlanarak işlemlerini gerçekleştirirler. Doğrudan uygulama erişimleri genellikle daha az kritik uygulamalar için kullanılır. Müdürlüğümüzün web sayfası, bu sayfa üzerinden erişilen uygulamalar ve hastanelerde laboratuvar tahlil sonuçlarının vatandaşlar tarafından doğrudan internet üzerinden sorgulanmasını sağlayan sistemler bu mimariye örnek olarak verilebilir.

4.5. Uzaktan erişim ile ilgili yöntem belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

4.5.1. Müdürlüğümüzde genel bir politika olarak uzak masaüstü işlemleri VPN bağlantısı üzerinden yapılır. VPN bağlantısı yapılmadan doğrudan uzak masaüstü bağlantısı yapılmasına hiçbir şekilde izin verilmez.

4.5.2. Özel nitelikli verilerin işlendiği, muhafaza edildiği elektronik ortamlara uzaktan erişim yapılırken, en az iki kademeli kimlik doğrulama sistemi kullanılması yasal bir zorunluluktur. Diğer sistemler için de çok faktörlü kimlik doğrulama yapılması tercih edilir.

4.5.3. VPN işlemi İl SBA Bulutu girişinde bulunan Müdürlüğümüze ait güvenlik duvarı üzerinden yapılır.

4.5.4. Erişim kontrollerinin uygulanabilmesi maksadıyla, hedef bilgisayarlara sabit IP adresi verilir. Yapılacak erişim; erişim yapacak kişi, hedef bilgisayar IP adresi ve kullanılacak port/uygulama bazında sınırlandırılır.

4.5.5. VPN bağlantılarına ilişkin iz kayıtları tutulur ve söz konusu iz kayıtları en az iki yıl süre ile saklanır.

4.5.6. Uzak bağlantı yapılacak uygulamalara/kaynaklara erişimin daha kontrollü olarak yapılması gerekiyorsa, bağlantılar bu amaçla ayrılan bir terminal/vekil sunucu üzerinden de yapılabilir.

4.5.7. Uzak bağlantı yapacak istemci bilgisayarların IP adresleri/blokları biliniyorsa, hedef bilgisayara sadece belirtilen IP adreslerinden erişim yapılması için gerekli ayarlar yapılır.

4.5.8. Uzak erişim için yapılan bağlantıda boşta kalma süresi (herhangi bir işlem yapılmadığı takdirde connection time out süresi) 10 dakikadır.

4.5.9. Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

4.5.9.1. Bağlantı VPN üzerinden yapılır.

4.5.9.2. Bağlantı yapan kişinin, hedef bilgisayarda oturum açma iznine sahip bir kullanıcı olması gerekir.

4.5.9.3. Hedef bilgisayara kullanıcı adı ve parola girilerek oturum açılır. Anonim girişlere izin verilmez.

4.5.9.4. Hedef bilgisayarda uzak bağlantı için kullanılan servis/ara yüz vasıtasıyla, bilgisayara erişecek kullanıcılar “kullanıcı adı ve/veya IP adresi” bazında sınırlandırılır. Bu yöntemle sadece yetki verilen kullanıcıların/bilgisayarların uzaktan erişim yapması sağlanır.

4.5.9.5. Bağlantı yapan kullanıcının hedef bilgisayardaki oturum açma, oturum kapatma gibi kullanıcı hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az 2 (iki) yıl süre ile saklanır.

4.5.9.6. Hedef bilgisayar üzerinden bir başka sunucuya bağlantı yapılacak ise ilgili kullanıcının söz konusu sunucuda yaptığı işlemlere ait iz kayıtları da kayıt altına alınır.

4.5.9.7. Uzak bağlantı yazılımı olarak mümkün ise “Microsoft Uzak Bağlantı Programı” kullanılır.

4.5.9.8. Microsoft işletim sistemi dışında bir başka bilgisayara erişim yapılıyorsa aynı güvenlik özelliklerini sağlayan, lisanslı ve/veya açık kaynak kodlu, güvenilir bir erişim programının kullanılması tercih edilir.

10. Ağ İşletim Güvenliği

1. Yeni teknolojileri, uygulamaları tehdit veya açıklıkları takip etmek için dernek, forum siteleri, e-Posta grupları ilgili personel tarafından takip edilir.

2. Ulusal Siber Olaylara Müdahale ekibi (USOM) tarafından sağlanan ürünler ile ilgili güvenlik güncelleştirmeleri ile zararlı bağlantılar takip edilir. Ayrıca https://some.saglik.gov.tr/ ve https://bilgiguvenligi.saglik.gov.tr adreslerinde yayınlanan güvenlik haberleri takip edilir.

3. Güvenlik cihazları ve ağ yönetiminde ayrıcalıklı erişim hakkı verilen kullanıcıların sisteme erişimi onay mekanizmasından geçerek tamamlanır. Erişim talepleri, resmi yazı veya kurumsal e-Posta ile bildirilir. Ayrıcalıklı erişim hakkı elde eden personelin yer ve görev değişikliği olması durumunda erişimleri düzenleyen birime bilgi verilmesi sağlanır.

4. Güvenlik ve ağ cihazlarında yönetici olarak erişim yetkisine sahip olan kullanıcı hesaplarındaki değişiklikler kontrol edilir. Sistemler üzerinde ortak erişim yetkisi olan hesaplar açılmaz.

5. Sahibi bilinmeyen hesaplar kaldırılır.

6. Güvenlik ve ağ cihazlarına yapılacak uzaktan erişim yetkisi verilen kullanıcılara bağlantı zamanı ve süresi ile ilgili kısıtlamalar getirilir. Kurumdaki görevi gereği kullanıcıların bağlantı süreleri farklı olabilir.

7. Güvenlik duvarları, ana omurga cihazları gibi kritik sistemlere yapılacak erişimler için yerel kullanıcılar yerine ikincil bir kimlik doğrulamasının kullanılması tavsiye edilir.

8. Güvenlik ve ağ cihazlarının gösterildiği “ağ mimarisi krokisi” hazırlanır. Hazırlanan kroki, sadece ilgili personelin görebileceği bir şekilde saklanır. Güvenlik ve ağ mimarisinde değişiklik yapıldığı zaman kroki de güncellenir.

9. Güvenlik ve ağ cihazlarının kurulumunu, yapılandırmasını ve sistemde karşılaşılan hataları gidermek için izlenilen yöntemleri anlatan kılavuz dokümanları hazırlanır. Bu kılavuzlardan bilgi havuzu oluşturulur.

10. Yedekleme politikası uyarınca güvenlik ve ağ cihazlarının konfigürasyon yedekleri düzenli aralıklarla alınır. Yedekler 2 (iki) farklı lokasyonda saklanır.

11. Sistemi etkileyecek bir çalışma yapılması gerekiyorsa mesai saati dışında yapılır. Bu çalışmadan etkilenecek kurum/firma ya da kişilere bilgi verilir.

12. Kablosuz ağlara giriş yapan tüm kullanıcılar kaydedilir ve bu bilgiler belirlenen süreler boyunca saklanır.

13. Telnet gibi güvensiz bağlantılara izin verilmez. SSH protokolünü kullanan bağlantılarda SSH Ver2 kullanılır.

14. İhtiyaç olmayan tüm portlar kapatılır. Dışarıdan tarama yapıldığında portların durumunun açık olarak görülmemesi için gerekli tedbirler alınır. Kurum web sayfaları, laboratuvar sonuç sorgulama sayfası gibi uygulamalarca kullanılan 80 ve 443 dışındaki portlar kullanıma kapatılır.

15. Güvenlik duvarı ve ağ cihazları için kontrol listeleri (ACL, güvenlik ürünleri erişim kısıtlaması vb.) tanımlanır.

16. Güvenlik ve ağ cihazlarının fiziksel güvenliğini sağlamak için gerekli tedbirler alınır.

17. Güvenlik ve ağ cihazlarının yazılım güvenliğini sağlamaya yönelik tedbirler alınır. Cihazlar ilk kurulduğunda varsayılan olarak atanmış olan kullanıcı adı ve parolalar değiştirilir. Parolalar güçlü parola ilkeleri esaslarına göre oluşturur.

18. Güvenlik ve ağ cihazları üzerindeki gereksiz ve kullanılmayan tüm servisler kaldırılır.

19. Cihazlara, saldırılara karşı korumak için 5 (beş) yanlış deneme sonrasında oturum belirli bir süre kilitlenecek şekilde ayarlama yapılır.

20. Doğru yapılandırılmış zaman damgası için cihazlar NTP sunucu ile senkronize olarak çalıştırılır.

21. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Kanunu uyarınca tutulması gereken trafik bilgileri (iz kayıtları) kayıt altına alınır.

22. Dış ağdan sunucular üzerindeki servislere, sunucu yönetim protokolleri (RDP, SSH) ile erişim engellenir. Sunucular, sadece belirli portlardan erişim sağlanacak şekilde yapılandırılır.

23. Kurum bünyesinde barındırılan ve hizmet veren uygulamalara HTTPS üzerinden bağlanılır.

24. Güncel atak metotlarından korunmak için saldırı tespit ve önleme sistemleri, ağ hizmetlerine erişim ilkelerinin belirlenmesi için Güvenlik Duvarı kullanılır.

25. Kurumsal kaynakların etkin olarak kullanılması, 5651 sayılı kanundan kaynaklanan uyum zorunlulukları, veri güvenliğinin sağlanması, zararlı içerik ve yazılımlardan korunma vb. maksatlarla internet erişimi kısıtlamaları yapılabilir. Kısıtlama ile ilgili politikalar belirlenirken aşağıdaki hususlar dikkate alınır:

25.1 . Ulusal Siber Olaylara Müdahale ekibi (USOM) ve Siber Olaylara Müdahale Birimi (SOME) tarafından yayınlanan zararlı içerik barındıran URL adresleri erişime kapatılır.

25.2 . Virüs, Spyware, Malware, Trojen, Spam, Solucan, Hacking (korsan), Fishing (oltalama) saldırıları içerdiği tespit edilen güvenlik seviyesi düşük internet sitelerine erişimler kapatılır.

25.3 . Alkol, sigara, uyuşturucu, silah vb. sağlığa zararlı ürünlerin reklam ve satış sitelerinin erişimleri engellenir.

25.4 . Erotik içerikli siteler, çocuk istismarı, bahis ve kumar siteleri, oyun siteleri erişime kapatılır.

25.5 . Kurumun internet bant genişliğini olumsuz etkileyen uygulama ve sitelerin (Torrent, P2P, Streaming Media, Download vb.) erişimleri engellenir.

25.6 .Basın yayın organlarını takip ederek idareye raporlamakla sorumlu personel haricindeki tüm personelin dizi, film, radyo ve televizyon erişimleri kapatılır.

25.7 . Kuruma ait sosyal medya hesaplarını yönetmekle sorumlu personel dışındaki tüm personelin Facebook, Twitter, Instagram vb. uygulamalara erişimleri engellenir veya bant genişliği sınırlaması yapılır.

25.8 .Youtube, Vimeo, Dailymotion gibi platformlarda erişimlerle ilgili olarak sadece ihtiyaç duyan personele izin verilir veya bu platformlara erişimlere bant genişliği sınırlaması yapılır.

11. Antivirüs Yönetimi

1. Tüm bilgisayarlar lisanslı antivirüs yazılımı ile korunur. Antivirüs yazılımının virüs veritabanı güncel tutulur.

2. Antivirüs veritabanı güncelleme işlemi antivirüs sunucusu üzerinden haftanın yedi günü yapılır.

3. Antivirüs yazılımının (100 bilgisayar ve üzeri için) antivirüs sunucusu üzerinden yönetilmesi gerekir.

4. Sunucu üzerinden periyodik güncellemeler, virüs taraması, zayıf noktalar (farklı programların açıkları) antivirüs yazılımının sürümü, durum bilgisi ve birçok yararlı bilgi sunucu üzerinden raporlanır.

5. Antivirüs yazılımının yönetilmesi ve doğru politikayla çalışmasını bağlı olduğu antivirüs sunucusu uygular. Bunun için yönetilen bilgisayara antivirüs yazılımı haricinde agent (ajan) yazılımının da yüklenmesi gerekmektedir.

6. Güncelleme sırasında kapalı olan bilgisayarlar sunucu üzerinde listelenir ve açıldığı anda güncelleme gönderilip doğrulanır.

7. Antivirüs sunucusunu yöneten personel ağda yönetilen tüm bilgisayarların antivirüs yazılımının ne durumda olduğunu görür ve ona göre müdahalelerde bulunur.

8. Antivirüs Sunucusu üzerinde sunucular, bilgisayarlar ve diğer cihazlar için gruplar oluşturulur ve her bir gruba ayrı politika uygulanır.

9. Antivirüs yazılımları herhangi bir ağ saldırısı durumunda sunucuya bu durumu raporlar ve kaynağını 60 saniye boyunca keser. Kaynağın hangi ip ve port üzerinden geldiği sunucu üzerinden izlenir ve müdahalede bulunur.

10. Antivirüs yazılımları sunucu üzerinden yönetiliyorsa lisans anahtarları sunucu üzerinden tüm bilgisayarlara gönderilir.

11. Antivirüs yazılımları bazı otomasyonların (hbys, pacs, tıbbi cihaz yazılımları vs) yoğun ağ trafiğini saldırı olarak görüp engelleyebilir. Bu durumda antivirüs yazılımına sunucu üzerinden ilgili yazılımın güvenli olduğunu gösteren "güvenilir uygulama" tanımlaması yapılır.

12. Antivirüs yazılımları her zaman güncel ve sunucuyla haberleşebilir durumda olmalıdır.

13. Yüklü olan antivirüs programının kullanıcı tarafından devre dışı bırakılması veya sistemden kaldırılmasını engellemek amacıyla parola koruması uygulanır.

12. Etki Alanı Kurulum ve Yönetimi

1. Yönetilebilirlik, ölçeklenebilirlik, genişletilebilirlik, güvenlik entegrasyonu, diğer etki alanları ile birlikte çalışabilme, güvenli kimlik doğrulama ve yetkilendirme, grup politikaları ile yönetim, DNS ve DHCP gibi servislerle birlikte çalışabilme gibi avantajları nedeniyle etki alanları kurulur ve işletilir.

2. Tüm Başkanlık ve Birimlerin etki alanı hizmetleri İzmir İl Sağlık Müdürlüğü (izmirsm.gov.tr) merkezi etki alanı vasıtasıyla sağlanır.

3. Ek Hizmet Binaları, İlçe Sağlık Müdürlükleri, Toplum Sağlığı Merkezleri vb. İl Sağlık Müdürlüğü'ne bağlı tüm birimlerin merkezi etki alanı ile yönetilmesi hedeflenir.

13. İz Kayıtları (Log) Yönetimi

1.Kurum bünyesindeki kullanıcı faaliyetleri, bilişim sistemlerine yönelik saldırı ya da hatalar, saldırının tespit edildiği anda saldırıya ait detayları gösteren iz kayıtları oluşturulur ve belirli kurallar dâhilinde toplanır.

2.İz kayıtlarının tutulması ve yönetilmesi (iz kayıtlarının üretilmesi, aktarılması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi gibi süreçler) sadece erişim yetkisi verilen bir birim/kişiler tarafından yapılır. Bu yetkilerin tercihen kurumsal SOME yetkililerine verilmesi uygundur.

3.Farklı sistemler tarafından üretilen iz kayıtları; güvenlik denetimi sağlamak, iz kayıtlarını daha etkin ve verimli olarak saklamak, yedeklemek ve raporlayabilmek amacıyla merkezi bir sunucuda toplanır.

4.İz kaydı (log) alınması gereken fiziksel ortam kayıtları; kritik bilişim sistemleri odaları giriş-çıkış kayıtları ve kamera kayıtları, çalışma ortamları giriş-çıkış kayıtları ve kamera kayıtlarından oluşur. Kamera kayıtları 2 (iki) ay, kritik sistem odaları ve çalışma ortamları giriş-çıkış kayıtları 2 (iki) yıl süreyle tutulur.

5.İz kayıtlarının saklanma süresi belirlenirken; yasal zorunluluklar, iz kayıtlarından sağlanacak fayda, saklama maliyeti ve ilgili iz kaydının kritikliği göz önünde bulundurulur. Başka bir yasal zorunluluk yoksa elektronik olarak üretilen tüm iz kayıtları en az 2 (iki) yıl süre ile saklanacak şekilde önlem alınır.

6.Kritik sistemlerde oluşan iz kayıtları eş zamanlı olarak merkezi iz kayıtları sunucusuna aktarılır. Merkezi sunucuya aktarılan kayıtların silinmesi ve değiştirilmesinin engellenmesi için gerekli teknik ve idari tedbirler alınır.

7.Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemleri hayata geçirilir.

8.Teknik olarak mümkün olması durumunda, iz kayıtları gizlilik ve hassasiyet seviyelerine göre sınıflandırılarak, ilgili kullanıcıların sadece verilen yetkiler çerçevesinde iz kayıtlarına bakmaları sağlanır.

9.Bütün sistemlerin zamanlarının aynı olması için Ağ Zaman Protokolü (NTP-Network Time Protocol) sunucusu kurularak kayıt üreten farklı sistemlerin zamanları bu sunucu ile senkronize edilir.

10.İz kayıtları periyodik olarak yedeklenir ve yedeklerin uygun şekilde muhafaza edilmesi sağlanır.

11.Merkezi iz kaydı sunucusu sadece yeni iz kayıtlarının saklanması için fonksiyonlar içerir. Bu sunucuda iz kayıtlarının silinmesi/değiştirilmesi amaçlı erişimlere izin verilmez.

12.İz kayıtları tutulan belli başlı sistemler:

13.Çalışma ortamları ve sistem/sunucu odalarına yapılan giriş-çıkışlara ait kamera kayıtları, varsa bunlarla ilgili diğer kayıtlar (kartlı geçiş sistemi, parmak izi okuyucuları vb. sistemler tarafından üretilen iz kayıtları),

14.Sanal ortam kayıtları,

15.Bilişim sistemleri tarafından üretilen kayıtlar, SBYS'ler,

16.Güvenlik duvarları iz kayıtları,

17.Antivirüs yazılımları,

18.Saldırı tespit/önleme sistemleri,

19.Yönlendiriciler ve anahtarlama cihazları,

20.Sunucular,

21.Diğer iş uygulamaları (kritik kurumsal projeler),

22.Veri tabanları,

23.VPN iz kayıtları

24.Tutulması gereken asgari iz kayıtları;

25.1. Kaydı oluşturan sistem,

25.2. Kaydın oluşturulma zamanı (tarih, saat, zaman dilimi),

25.3. Kaydı oluşturan olay,

25.4. Kaydın ilişkili olduğu kişi (IP/Port bilgisi, MAC adresi, işlemi yapan tekil kullanıcı adı veya sistemin adı).

14. Sunucu ve Sistem Odası Güvenliği

1. Hizmet sunumunun sürekliliğinin sağlanması için kesintisiz ve sürekli çalışan elektronik ve donanımsal altyapı ihtiyacı bulunmaktadır. Donanım, elektronik altyapı ya da çevresel faktörlerden kaynaklanabilecek sorunlar hizmetlerin sunumuna birçok açıdan zarar verebilir ve olumsuz etkilerin giderilmesi gerek maliyet gerek zaman açısından çok zor olabilir. Bu nedenle, hizmet sunumunda yer alan tüm aktif ve pasif donanımın; sadece sunuculara tahsis edilmiş, yetkisiz personelin girişinin engellendiği, sıcaklık ve nemin kontrol edildiği, elektrik kaynağının stabilize edildiği, özel şekilde iklimlendirilmiş ve güvenliği sağlanmış sunucu/sistem odasında konumlandırılması gerekir. Sistem odalarındaki donanımların hizmet sürekliliğinin sağlanması için yedekli bir güç kaynağı sistemi, yedekli haberleşme bağlantıları, sıcaklık, nem gibi çevre değişkenlerinin kontrolü için iklimlendirme cihazları ve güvenlik cihazları yer alır.
2. Bir sistem odasının en temel özellikleri;
    a. 7×24 kesintisiz çalışabilirlik,
    b. Güç yönetimi ve ağ bağlantılarında farklı kanallardan yedeklilik,
    c. Ağ güvenliği, fiziksel erişimlerde yetkilendirme ve görüntülü gözetleme,
    d. Çevre şartlarının kontrol altında tutulması,
    e. Yangına karşı duman algılama gibi erken uyarı sistemleridir.
3. Sistem odasının kesintisiz çalışmasına; sıcaklığın normal aralığın dışına çıkması, yangın, su baskını, deprem, yetkisiz kişilerin sistem odasına girmesi, odadaki herhangi bir cihazın arızalanması engel olabilir. Tüm bu olumsuz durumların yaşanmasının önlenmesi ve hizmetlerin sağlıklı çalışabilmesi için standartlara uygun bir sistem odası oluşturulması ve ana bilgisayar, sunucu ve diğer hizmet sürecindeki bileşenlerin güvenli olarak bu alanlarda konumlandırılması gerekir.
4. Sistem odası ile ilgili aşağıdaki ölçütlere dikkat edilmesi gerekir;
    a. Sistem Odasının Yeri: Çevresel faktörlerden en az etkilenecek bir yer tercih edilmelidir. Binanın nem ve sıcaklık oluşturabilecek kalorifer ve su tesisatlarından uzak, eğer mümkünse orta katlarda ya da 2. katında konumlandırılmalıdır. Sistem odasının yeri iklimlendirme açısından da değerlendirilerek, sistem odasından bina çıkışındaki klimanın dış ünitesine giden borunun mesafesi düşünülerek seçilmelidir. Mümkün olduğunca sistem odasında cam pencere ve duvarlar olmamalıdır. Sistem odasının bulunduğu binada yıldırımlara karşı paratoner kurulmalı ve kablolaması sistem odasından uzakta olmalıdır. Manyetik alan oluşturabilecek enerji ve elektrik hatlarından izole olmalı, telefon santrali ve benzeri dış unsurlar kesinlikle sistem odasına alınmamalıdır, kullanılması gerekiyorsa kafes yapmak gibi ek güvenlik önlemi alınmalıdır.
    b. Sistem Odasının İnşaat Özellikleri: Kesintisiz güç kaynakları ve elektrik dağıtım panoları; aktif cihazlar ve sunucuların yerleştirildiği alandan ayrı bir bölüm olarak tasarlanabilir. Odanın dış duvarları, mümkünse yangına ve sızdırmazlığa karşı gaz beton tuğla veya iki tarafı alçı ile kaplanmış –50º ile +650º arasındaki sıcaklıklara dayanıklı bir malzeme olan taş yünü ile örülmelidir. İç duvarlar pasif yangın koruması sağlayacak epoksi boya ile kaplanmalıdır. Sistem odalarındaki kablo yoğunluğu ve diğer iletim hatları yükseltilmiş taban, asma tavan ve/veya asma kablo tavalarının içinden geçirilerek sistem odası içerisinde oluşabilecek karmaşa önlenmelidir.
    c. Giriş – Çıkış Kontrolü: Sistem odasına giriş ve çıkışlar kart okuyucu, avuç içi damar okuyucu veya şifreli giriş ile kontrol altına alınmalı ve giriş/çıkışlara ait iz kayıtları tutulmalıdır. IP kamera ile izleme sistemi kurulmalı, odanın durumu, giriş çıkışları ve yapılan işlemler kameralarla kayıt altına alınmalıdır.
    d. Sıcaklık Kontrolü: Birçok işlemci için üreticisi tarafından belirtilen en yüksek sıcaklık derecesi ortalama 70 °C'dir. Bu ısıya ulaşan sunucular, üzerlerindeki sensörler aracılığıyla kendilerini kapatırlar. Hizmet sürekliliği için ortam sıcaklığının 18 °C ile 22 °C arası olması kabul edilir. Sistem odasına e-Posta, SMS ya da telefon çağrısı aracılığıyla bilgilendirme yapan sıcaklık sensörleri konumlandırılmalıdır.
    e. Nem Kontrolü: Nem sadece sunucular ve bilgisayar sistemleri için değil üzerinde elektronik devre elemanları bulunduran tüm cihazlar için bir risk oluşturur. Ortamdaki nem oranının eşik değerlerinin altına düşmesi elektronik devre elemanlarının statik elektrikle yüklenmesine, üstüne çıkması ise sıvı oluşumlarına neden olur ki bu da cihazlarınızın kullanabileceğinden fazla

elektrik taşıması ya da kısa devre nedeniyle bozulmasına sebep olacaktır. Bu nedenle sistem odasının e-Posta, SMS ya da telefon çağrısı aracılığıyla bilgilendirme yapan nem sensörleri ile izlenmesi ve uygun koşullarda tutulması gerekmektedir. Bunun için en uygun nem aralığı %45 ile %70 arasıdır.

f. Toz Kontrolü – Temizlik: Tozlu ortamlar elektronik sistemlerin aşırı ısınmasına yol açabilmektedir. Bundan dolayı sistem odasının tozdan arındırılmış olması, kabinetler ve sistemlerde filtreler kullanılması gerekmektedir. Tozların temizliği dışa üflemeli ve içe emmeli kompresör ile yapılmalı, böcek ilaç ve tabletleri ile sistem odasında örümcek, sinek gibi böceklerin varlığı engellenmelidir.

g. Yangın Kontrolü: Sistem odasının dışında çıkabilecek yangınlara karşı, odanın dış kısımları su püskürtmeli yangın sistemi ile koruma altına alınmalıdır. Sistem odasının kapısı yangına dayanıklı, ısıyı ve dumanı diğer tarafa geçirmeyen, standartlara uygun özel üretim bir kapı olmalıdır. Duman algılama detektörü ile yangın söndürme sistemi konumlandırılmalıdır. Elektrik yangınlarına müdahalede, bilgisayar kabinlerinin zarar görmesini engellemek için karbondioksitli veya halon gazlı (FM200 vb.) ve basınç kontrollü yangın söndürme sistemi kullanılmalıdır. Herhangi bir yangın tehlikesi durumunda sistem odasının elektriği kesilerek yangına müdahale edilmelidir.

h. Su Baskını Kontrolü: Su basmasına karşı kabinler yerden 15-20 cm yükseltilmiş olmalı ve su dedektörü konumlandırılmalıdır.

i. Enerji Kontrolü: Enerjinin sürekliliği ve yedekliliği, iletimi, izlenmesi ve topraklama hassasiyetle üzerinde durulması gereken konulardır. Sistem odasındaki cihazların çektiği enerjinin kapasitesine uygun olarak ve büyüme kapasitesi de göz önüne alınarak, elektrik kesintisi ya da şebekedeki dalgalanmaları önleyecek regülatörlü bir UPS ve sistemlerin kritiklik durumuna göre jeneratör kurulumu yapılmalıdır. Enerjinin iletimi için doğru kablo tipi ve kalınlığı seçilmeli, enerji kabloları kablo kanalı ile korunmalıdır. Kablo ısınması ya da sigorta atması ve benzeri sonuçların engellenmesi için tüm cihazların kullandığı enerji miktarı sayısal değer olarak izlenmelidir. Sistem odası kuruluş aşamasında topraklama yapılmalıdır.

j. Deprem Kontrolü: Kabinler yere veya duvara sabitlenmeli, kabinler arası yerleşim deprem ve havalandırma şartlarına uygun tasarlanmış olmalı, deprem yönetmeliği şartları sağlanmalıdır.

k. Kablolama Kontrolü: Data ve elektrik kablolama için TSE standartlarına uygun malzemeden imal edilmiş kablo kanalları kullanılmalıdır. Tüm kanallar bölmeli olmalıdır. Kuvvetli akım ve zayıf akım kabloları ayrı ayrı bölmelerden geçirilmelidir. Kablolar kablo kanalı ile (haşereler de düşünülerek) korunmalıdır. Kabin içi kablolarda kablo toplayıcı aparatlar kullanılması ve ağ kablolarının etiketlenmesi gerektiğinde kolay müdahale için zaman kazandıracaktır.

l. Kabin Düzeni: Kabinlere cihazlar yerleştirilirken yerel ağ ve DMZ bölgesine hizmet eden sunucuları ve anahtarlama cihazlarını (switchleri) ayrı konumlandırmak, veri depolama, yedekleme, ağ bağlantısı ve güvenlik cihazlarını kolay erişilebilir bir kabine yerleştirmek planlı büyüme için kolaylık sağlayacaktır.

m. İzleme: Cihazların hata ya da alarmlarını manuel olarak kontrol etmek yerine Basit Ağ Yönetim Protokolü (SNMP) destekli cihazları bir izleme yazılımı üzerinden kontrol etmek için arıza durumunda e-Posta ve/veya SMS yoluyla bilgilendirme yapacak bir sistem oluşturulmalıdır. Bu iş için mevcut sunucuların üreticisinin izleme için özel ürünlerini kullanmak bir yöntem olabilir ya da bakım anlaşması ve garanti kapsamındaki cihazlar için donanım arızası durumunda otomatik çağrı açılması ve arızalı parçanın değişim sürecinin otomatik olarak başlatılması sağlanabilir.

15. Yedekleme Yönetimi

1. Kurum Yedekleme Politikası

a. Verilerin yedeklenmesi iş sürekliliğinin en temel prensipleri arasında yer alır. Donanım arızaları, yazılım hataları, kullanıcıdan kaynaklanan sorunlar ya da doğal tehditler gibi nedenlerle veri kayıpları yaşanabilir. Başarılı bir yedekleme işlemi ve yedeklenen verinin ihtiyaç anında veri kaybı olmadan kurtarılabilmesi veri yedekleme sistemlerinin en temel iki bileşenidir.

b. Yedeklerin kurumun gereksinimleri dikkate alınarak hazırlanmış olması, yönetimin konuya bakış açısını yansıtan bir yedekleme politikası doğrultusunda alınıp güvenliğinin sağlanması,

saklanması ve belirli sıklıkta geri dönüş testlerinin yapılması veri kaybı riskini minimum seviyeye indirecektir. Yedekleme sisteminin kurulumu; yedeklenecek veri miktarı, yedekleme sıklığı, yedeklenen verinin zaman içerisinde değişme oranı, kabul edilebilir maksimum veri kaybı gibi parametrelere bağlıdır.

c. Her kurumun kendine özgü yasal veya sözleşmeden doğan gereksinimleri ile verinin saklanma ve korunma gerekliliklerini karşılayacak şekilde bir politika oluşturması gerekir.

d. Yedekleme politikası; olası bir felaket durumu ya da sistem hatası sonrası gerekli tüm verilerin geri getirilebilmesini sağlayacak şekilde yedekleme kuralları tanımlanmış, etkin, yönetilebilir ve izlenebilir bir yedekleme sistemi kurulması ve işletilmesine imkân verecek şekilde hazırlanmalıdır.

e. Yedekleme politikasının yerine getirilmesi için bir yedekleme planı ortaya koyulmalıdır. Yedekleme planı; Yedekleme sıklığı, hangi saklama ortamında ne kadar süre tutulacağı, hangi yedekleme türü ile yedekleneceği, kabul edilebilir geri dönüş süresi ve kabul edilebilir veri kaybı süresi bilgilerini içermelidir.

2. Yedekleme Planlarının Oluşturulması

a. Kurumun sistem gereklilikleri göz önüne alınarak; Sunucular, Sanal Sunucular, Veri Tabanları, Etki Alanı Denetleyicisi, Güvenlik ve Ağ Cihazları gibi veri içeren platformların yedeklenmesi planlanmalıdır.

b. Yedeklenecek veriler bilgi işleme süreci içerisinde değişiklik gösterebileceğinden yedekleme listesi oluşturularak en az yılda 2 (iki) kez gözden geçirilmeli ve güncellenmelidir.

c. Başarılı bir yedekleme sistemi için kategorize edilmiş ve önceliklendirilmiş verilerin yedekleme planları oluşturulur.

d. Yedekleme planları asgari olarak; yedeklenecek bileşenin adı (host name), ulaşım yolu (ip adresi), yedekleme tipi ve sıklığı, yedek geri dönüş testi raporları gibi bilgileri içerir.

e. Yedekleme planına göre yedeklerin düzenli aralıklarla alınması ve sürekli olarak gözden geçirilmesi gerekir.

3. Yedekleme Çalışmaları

a. Kritik veriler yedeklenirken iki farklı şekilde yedeklenmek üzere bir yedekleme sistemi oluşturulmalıdır. Bunlardan ilki; canlı çalışma ortamında eş zamanlı olarak kümelenmiş disk sisteminin farklı disk bölümlerine; ikincisi ise, çevrimdışı olarak varsa yedekleme sunucusu yoksa şifrelenmiş olarak harici depolama ortamlarında yedeklenmesidir.

b. Kritik olmayan veriler yedeklenirken, verilerin bir kopyası mevcut sunucular üzerinde, diğer bir kopyası çevrimdışı olarak yedekleme sunucusu veya harici depolama ortamlarında tutulur.

c. Yedekleme politikası ve planları doğrultusunda yapılan yedekleme işlemleri düzenli olarak kontrol edilmelidir.

d. Özel nitelikli kişisel veri kategorisinde bulunan sağlık kayıtlarının yer aldığı yedekleme ortamları şifrelenir.

e. Yedekleme medyalarının acil durumlarda kullanılması gerekebileceğinden güvenilir ürünlerden seçilmeli ve düzenli periyotlarda test edilmelidir.

f. Yedekleme medyalarının bulundurulduğu ortamların fiziksel uygunluğu ve güvenliği sağlanmalı ve herhangi bir felaket anında etkilenmeyecek şekilde bilgi işlem odalarından farklı odalarda veya binalarda saklanmalıdır.

4. Geri Dönüş Testleri

a. Yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için yılda en az 2 (iki) kez geri dönüş testlerinin yapılması gerekir.

b. Yedekten geri yükleme testlerinin, başarısız olması nedeniyle veri kaybı olabileceği durumu göz önüne alınarak, canlı ortamda değil gerçek ortamın aynısı olan test ortamında yapılması gerekmektedir.

5. Yedekleme Süreci Görev ve Sorumlulukları

a. Yedekleme politikasının işletilmesi ve zaman içerisinde günün ihtiyaçlarına göre güncellenmesi veri kaybı durumunda kurumun göreceği zararı en aza indirecektir.

b. Yedekleme sistemlerinin yönetimi, yedekleme politikasının ve yedekleme planının hazırlanması, uygulanması ve güncellenmesinden sorumlu personelin görevlendirilmesi gerekmektedir.

c. Yedekleme işleminin gerekli eğitimi almış personel tarafından yapılması sağlanmalıdır.

16. Taşınabilir Ortam Yönetimi ve Ortamın Yok Edilmesi

1.**Taşınabilir Ortam Yönetimi**

1.1. Kaybolma, kolayca çoğaltma vb. nedenlerden dolayı özellikle elektronik medya (CD/DVD, USB girişli hafif taşınabilir bellekler, taşınabilir diskler, hafıza kartları, teyp kartuşları vb.) ve basılı evraklar (yazılar, dosya klasörleri, etüdler, çizimler, krokiler, proje evrakları vb.) olmak üzere taşınabilir ortamlarda saklanan her türlü bilginin korunması ve yetkisiz kişilerin eline geçmemesi için özel önlemler alınır.

1.2. Elektronik medya kullanımı ile ilgili olarak aşağıdaki hususlar göz önünde bulundurulur:

1.2.1. Kuruma ait veriler, kişilere ait medyalar üzerinde saklanamaz. Verilerin bir taşınabilir ortama aktarılması ihtiyacı kaçınılmaz ise bu maksatla kuruma ait medyalar kullanılır.

1.2.2. Görev devir teslimlerinde veya işten ayrılışlarda, kişilere teslim edilmiş olan medyaların iade edilmesi istenir veya ne şekilde sarf edildiği bilgisi sorgulanır.

1.2.3. ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL veriler, taşınabilir ortamda saklanamaz. Özellikle bu tür ortamlarda saklama zorunluluğu var ise şifreli olarak saklanır.

1.2.4. Bir bilgi sadece taşınabilir medya ortamında saklanıyorsa, bozulma/kaybolma gibi ihtimallere karşı bir başka medya ortamında da yedeklenmesi tavsiye edilir. Veriler çok kıymetli ise yedeklenen medya ortamı, doğal afet vb. tehditlere karşı önlem olmak üzere fiziksel olarak farklı bir yerde muhafaza edilir.

1.2.5. Yeni medya teknolojilerinin ortaya çıkması nedeniyle üç yıldan uzun süredir eski teknolojilerin kullanıldığı bir medya ortamında saklanan verilerin daha yeni bir medya ortamına taşınması tavsiye edilir.

1.2.6. Gizlilik derecesi taşıyan kurumsal verilerin saklandığı medya ortamları, kişisel (şahsın kendisine ait) bilgisayarlarda kullanılamaz. Bu tip veriler kişisel bilgisayarlarda işlenemez.

1.2.7. Tüm ortamlar üretici talimatında belirtildiği şekilde toz, nem vb. çevresel şartlardan etkilenmeyecek şekilde güvenli bir ortamda saklanır.

1.3. Elektronik medya da dâhil tüm taşınabilir ortamlar, kullanılmadığı zamanlarda içinde bulunan verilerin gizlilik derecesi dikkate alınarak fiziki güvenlik tedbirleri alınmış kasa, dolap, çekmece gibi ortamlarda saklanır.

2.**Ortamın Yok Edilmesi**

2.1. Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik veya fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dışı bırakılmasına karar verilen ve kayıt silme işlemleri tamamlanan bilgi sistem cihazlarına ait veri depolama üniteleri, içerisinde gizlilik dereceli bilgi bulundurma ihtimali nedeniyle usulüne uygun olarak imha edilir veya güvenli silme işlemi yapılır.

2.2. Sökülen sabit disklerden daha önce ilgili teknik birimler tarafından “onarımı mümkün değil” şeklinde rapor verilenler ile sağlam olmakla birlikte “yeniden kullanımı düşünülmeyen” cihazlar fiziksel yok etme yöntemi ile imha edilir.

2.3. Fiziksel yok etme; optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.

2.4. Disk imha işlemleri, bizzat disklerin sahipleri veya taşınır mal sorumlularının nezaretinde yapılır.

2.5. Kâğıt ve mikrofiş ortamlarındaki veriler, kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünerek imha edilir.

2.6. Yeniden kullanılması planlanan disklere, içlerinde yer alan bilgilerin yetkisiz kişilerin eline geçmesini engellemek maksadıyla 'güvenli sil' (üzerine yazma) işlemi yapılır.

2.7. Güvenli silme işlemi, manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu iş için uygun bir yazılım (DBAN, Kill Disk, Eraser, Disk Wipe, HDShredder gibi) veya donanım kullanılır.

2.8. Arızalanan ya da bakıma gönderilen cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce veri saklama ortamının sökülerek saklanması sağlanır.

17. Lisanslama ve Fikri Mülkiyet Hakları

1. Fikri mülkiyet insan zekâsının, entellektüel birikiminin, zihinsel yaratıcılığının ortaya çıkarmış olduğu müzikten, edebiyata, endüstriyel tasarımlardan bilimsel buluşlara kadar uzanan geniş bir yelpaze içinde yer alan ürünleri kapsar. Bu ürünler düşünce safhasında kaldığı ve üreticisi dışındakilerle paylaşılmadığı sürece korumaya konu olmazlar. Ancak bu düşüncelerin ve ürünlerin, uygun şekilde kayıt altına alınmalarını takiben diğer kişilerle paylaşılmaları ve özellikle bu ürünlerin kazanç amacıyla ticarete konu olmaları söz konusu olduğu zaman korunmaları gerekir.

2. Fikri mülkiyet, sınai mülkiyet hakları ve telif hakları olmak üzere iki ana başlık altında incelenir.

3. Sınai mülkiyet hakları; teknolojik buluşlar, patentler, mal ve hizmetlerin ticari markaları, modeller, endüstriyel tasarımları ve coğrafi işaretleri kapsar. Bu haklar 6769 Sayılı Sınai Mülkiyet Kanunu ile korunur. Tescil işlemleri, Türk Patent ve Marka Kurumu tarafından koordine edilir.

4. Telif hakları; edebiyat, müzik, sanat ürünleri ve görsel-işitsel ürünler, filmler, bilgisayar program ve yazılımlarını ortaya çıkaran kişilerin bu ürünler üzerindeki haklarını içerir. Bu haklar 5846 sayılı Fikir ve Sanat Eserleri Kanunu ile korunur. Konu ile ilgili faaliyetler, T.C. Kültür ve Turizm Bakanlığı Telif Hakları Genel Müdürlüğü tarafından yürütülür.

5. Müdürlüğümüz ve bağlı birimlerince yapılan her türlü iş ve işlemlerde, fikri mülkiyet haklarına saygılı davranılır. Bu hakların korunması için gerekli tedbirler alınır.

6. Lisanslı yazılım kullanımı ile ilgili hususlarda Başbakanlık'ın 2008/17 sayılı Genelgesinde belirtilen esaslara dikkat edilir. Genelge ile lisanslı yazılım kullanımı ile ilgili işlerde "birinci derecede" sorumluluğun "ilgili kamu kurum ve kuruluşunda bilgi işlem ünitesi veya bu işten sorumlu birimde çalışanlara" verilmiş olduğu dikkate alınır.

7. Çeşitli maksatlar için tedarik edilen yazılımlar, kurumların taşınır kayıt birimleri tarafından envantere alınmak suretiyle kayıt altına alınır.

8. Yazılımlara ait lisans belgeleri, yazılımın üreticisi firma tarafından sağlanan lisans takip/indirme sayfasına erişim şifresi, varsa CD/DVD ve benzeri materyal, USB dongle vb. anahtarlar, ilgili projenin yürütüldüğü birimde muhafaza edilir.

9. Herhangi bir proje veya faaliyet kapsamında yeni bir yazılım tedarik edilmesi ihtiyacı olduğunda, tedarik faaliyetine başlanmadan Bilgi İşlem Birimi ve Taşınır Kayıt Birimi ile koordinasyon kurulur.

10. Müdürlüğümüze ait hiçbir cihazda, üreticisi tarafından açıklanmış lisanslama politikasına aykırı bir şekilde (lisanslama/kullanım anahtarının kırılması, yazılımın izinsiz olarak kopyalanması vb.) yazılım kullanılamaz.

11. Lisans çerçevesinde izin verilen kullanıcı sayısının aşılmaması için gerekli tedbirler alınır.

12. Çeşitli isimler altında (open source, freeware, shareware) ücretsiz olarak dağıtılan yazılımlar, zararlı öğeler barındırma ihtimaline karşı test edilmeden kuruma ait bilgisayarlara kurulmaz.

13. Müdürlüğümüz çalışanlarınca, görev tanımlarının bir parçası olarak resmi bir hizmetin ifası için kurum kaynakları kullanılmak suretiyle üretilen (her türlü bilgi, belge, rapor, doküman, grafik, kitapçık, sunum, tasarım, proje, yazılım vb.) fikri mülkiyete konu olabilecek varlıkların mülkiyeti, Müdürlüğümüze aittir. Müdürlük söz konusu varlıkları, ilgili mevzuat uyarınca kendi adına tescil ettirebilir. Kişiler, söz konusu varlıklar üzerine kişisel bir hak iddia edemezler.

14. Aksi kararlaştırılmadıkça, tedarik sözleşmeleri kapsamında yüklenici firmalar tarafından yapılan/yaptırılan tasarım, geliştirme ve/veya eklemelere ilişkin ortaya çıkan fikri mülkiyet hakları Müdürlüğümüze aittir. Bu kapsamda, yükleniciler tarafından geliştirilen (tasarım, yazılım, yazılım kodu, algoritma vb.) fikri mülkiyete konu olabilecek varlıklar, sözleşme süresi sonunda idare tarafından teslim alınır. Yükleniciler ve/veya çalışanları, söz konusu varlıklar üzerinde kişisel/kurumsal bir hak iddia edemezler.

15. Yüklenici firmalar, sözleşmeler kapsamında Müdürlüğümüz için yaptıkları iş ve işlemlerde üçüncü taraflara ait herhangi bir fikri mülkiyet hakkını ihlal edemezler. Bu husus sözleşmelere konulmak suretiyle garanti altına alınır.

16. Telif hakları kapsamında korunan kitaplar, makaleler, raporlar ve diğer belgeler hiçbir şekilde kopyalanamaz, çoğaltılmaz ve dağıtılamaz.

18. Fiziksel Ve Çevresel Güvenlik

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

Günümüzde bilgiler, büyük oranda bilgi sistemleri vasıtasıyla işlenmekte ve sayısal ortamlarda saklanmaktadır. Bu nedenle bilgi güvenliği ile ilgili tedbirlerin önemli bir kısmını, bilgi sistemleri ve ağlarının korunmasına yönelik siber güvenlik önlemleri oluşturmaktadır. Bununla birlikte, fiziksel ortamda saklanan bilgiler ile elektronik ortamda saklanan verilerin muhafaza edildiği bilişim sistemleri ve ağlarının güvenliği için, fiziksel ve çevresel önlemlerin alınması kaçınılmazdır.

2. Güvenli Alanlar

2.1 Fiziksel ve çevresel güvenlik tedbirlerinin belirlenmesi ve uygulamaya alınmasının ön koşulu, hassas veya kritik bilgi ve bilgi işleme tesislerini barındıran güvenli alanların tespit edilmesi ve bu alanların güvenlik sınırlarının tanımlanmasıdır.

2.2 Güvenlik sınırları belirlenirken kademeli bir yaklaşım kullanılır. Gerekiyorsa iç içe güvenli alanlar oluşturularak, daha hassas ve kritik bilgilerin işlendiği alanlara erişim için birden fazla fiziksel sınırdan geçilmesi zorunlu hale getirilir.

2.3 Güvenlik sınırları belirlenirken kişilerin kontrolsüz olarak giriş çıkış yapabilecekleri herhangi bir boşluk bulunmamasına dikkat edilir. Bu tür boşlukların kapatılması/korunması için ilave tedbir alınır.

2.4 Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunur.

2.5 Göreceli olarak daha az hassas varlıkların yer aldığı dış güvenlik sınırında alınan güvenlik tedbirleri ile kritik varlıkların yer aldığı iç güvenlik sınırlarındaki tedbirler farklılaştırılır.

2.6 Güvenli alanlar, fiziksel güvenlik engelleri ile çevrili, kilitlenebilir bir ofis ya da birkaç oda olabilir. Birden fazla kuruluşun aynı bina içerisinde olduğu durumlarda fiziksel erişim güvenliğine özel dikkat gösterilir.

2.7 Fiziksel koruma, bir ya da daha fazla fiziksel engel konularak gerçekleştirilir. Birden fazla fiziksel engel kullanımı (kartlı geçiş sistemleri, turnikeler, kayar kapılar, kilitli odalar vb.) ilave koruma sağlayarak tek bir engelin başarısızlığı durumunda güvenliğin tehlikeye girmesini önler.

2.8 Giriş kontrolleri, korunacak tesis veya varlığa göre değişir.

2.9 Sağlık hizmet sunumu yapan tesislerde en dışta yer alan güvenlik sınırlarının geçiş noktaları, sadece gözle veya elektronik tarama araçları ile korunur. Burada amaç, vatandaşların gereksiz giriş kontrolleri ile uğraşmadan en kısa yoldan sağlık hizmetine eriştirilmesidir. Bununla birlikte sürekli gözetim yapılarak şüpheli durumlarda, güvenlik personeli vasıtası ile gerekli müdahalelerde bulunulur. Bölgesel koşullar dikkate alınarak ilave güvenlik tedbirleri alınabilir.

2.10 İl Sağlık Müdürlüğü, İlçe Sağlık Müdürlükleri, Toplum Sağlığı Merkezleri gibi sağlık hizmeti sunumu yapılmayan ancak sağlık hizmetinin sunumu için destek hizmetlerinin verildiği bina ve yerleşkelerde, en dış güvenlik sınırında yer alan geçiş noktalarında, sadece yetkili personele erişim izni verilmesini temin edecek giriş kontrolleri yapılır.

2.11 Kapsamı ve yöntemi idareler tarafından belirlenecek şekilde ziyaretçilerin giriş ve çıkışlarının tarih ve saatleri kayıt altına alınır. Daha önce erişimi onaylanmadığı sürece tüm ziyaretçiler denetlenir. Ziyaretçilere sadece belirli, yetkilendirildikleri amaçlar için erişim verilir. Ziyaretçilerin kimliği uygun bir yöntem ile doğrulanır.

2.12 Sunucu odaları, güvenlik kontrol merkezleri, arşiv odaları vb. hassas bilgilerin işlendiği veya saklandığı alanlar kolayca ulaşılamayacak yerlere kurulur. Bu gibi yerlere giriş için iki faktörlü kimlik doğrulama mekanizmaları kullanılır.

2.13 Kapsam ve yöntemi idarelerce belirlenmek suretiyle tüm personel ve ziyaretçilerin güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartları hazırlanır ve kullanılır.

2.14 Personel kartı veya ziyaretçi kartı takmayan bir kişi görüldüğüne güvenlik personeline bilgi verilir.

2.15 Dış taraf destek personeline güvenli alanlara veya gizli bilgi işleme tesislerine erişim izni, sadece gerekli olduğu durumlar için geçici süre ile verilir. Bu tür erişimlerde, mümkün olduğu kadar erişim kısıtlaması yapılır ve takip edilir.

2.16 Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilir.

2.17 Güvenli alanlara erişim hakları düzenli olarak gözden geçirilir. Gereksiz erişim izinleri iptal edilir veya yetki kısıtlaması yapılır.

2.18 Sahipsiz güvenli alanlar fiziksel olarak kilitlenir ve periyodik olarak gözden geçirilir.

2.19 Yetki verilmediği sürece, güvenli alanlarda fotoğraf, video, ses ve diğer kayıt cihazları ve mobil cihazlardaki kameralara izin verilmez.

2.20 Yetkisiz kişilerin teslimat ve yükleme işlemleri için güvenli alanlara giriş yapmasını engellemek üzere, güvenli alan dışında olacak şekilde teslimat ve yükleme alanları oluşturulur.

2.21 Postacı, kurye personeli, dağıtıcı gibi kişilerin tesis içlerine kontrolsüz olarak girmesi engellenir. Teslimat ile ilgili kurallar oluşturulur. Teslimat işlemlerinin kurum içinde belirlenecek noktalarda yapılması için tedbir alınır.

2.22 Personel güvenliği ve sağlığı için ilgili yönetmelikler uygulanır.

2.23 Yangın, sel, deprem, patlama ve diğer doğal afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınır ve uygulanır.

2.24 Giriş/çıkış yapılan yerler ve ortak kullanım alanları güvenlik kameraları ile kayıt altına alınır.

3. Ekipman Güvenliği

3.1 Belli Başlı Temiz Masa Kuralları

3.1.1 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 belli başlı temiz masa kurallarına çalışanlar tarafından uyulması sağlanır.

3.1.2 Hassas bilgiler içeren bilgi, belge ve evraklar masa üzerlerinde ya da kolayca ulaşılabilir yerlerde açıkta bulundurulmaz. Bu gibi bilgi ve belgeler kilitli dolap, çelik kasa ya da arşiv odası gibi fiziki koruması olan güvenli alanlarda muhafaza edilir.

3.1.3 Yetkisiz kişilerin erişiminin engellenmesi için bilgisayar başından ayrılma durumunda ekran kilitlemesi yapılır. Otomatik ekran kilitlemesi devreye alınır.

3.1.4 Sistemlerde kullanılan parola, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulundurulmaz.

3.1.5 Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler imha edilir.

3.1.6 Faks makinelerine gelen yazılar sürekli kontrol edilir ve makinede yazı bırakılmaması için tedbir alınır.

3.1.7 Her türlü bilgiler, parolalar, anahtarlar ve bilginin sunulduğu sistemler, sunucular, kişisel bilgisayarlar ve benzeri cihazlar yetkisiz kişilerin erişebileceği bir şekilde parola korumasız ve fiziki olarak güvensiz bir şekilde gözetimsiz bırakılmaz.

3.1.8 Fotokopi ve diğer çoğaltma teknolojilerinin (tarayıcı, sayısal kamera vb.) yetkisiz kullanımını önlemek için uygun idari ve teknik tedbirler alınır.

3.2 Ekipman Yerleşimi ve Koruması

3.2.1 Yüksek maliyetli, özel koruma gerektiren, elektronik cihazların (tıbbi cihazlar dahil) yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine dikkat edilir.

3.2.2 Ekipmanlar, gereksiz erişimleri asgari düzeye indirecek şekilde yerleştirilir.

3.2.3 Kritik veri içeren araçlar, yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilir.

3.2.4 Özel koruma gerektiren ekipmanlar izole edilmiş şekilde kullanılır.

3.2.5 Nem ve sıcaklık gibi parametreler izlenir.

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

3.2.7 Paratoner kullanılır.

3.2.8 Bilgi işlem araçlarının yakınında yeme, içme ve sigara kullanımı konularını düzenleyen kurallar oluşturulur ve uygulanır.

4. Destek Hizmetleri

4.1 Elektrik, su, kanalizasyon ve iklimlendirme sistemlerinin, desteklediklerı bilgi işlem birimi için yeterli düzeyde olmasına dikkat edilir.

4.2 Ekipmanların elektrik arızalarından korunması için ana besleme noktalarında elektrik şebekesine yedekli bağlantı yapılır.

4.3 Kritik sistemlerde hizmet kesintisi yaşanmaması için kesintisiz güç kaynağı ve jeneratör kullanılır.

4.4 Jeneratör kullanımı için yeterli düzeyde yakıt bulundurulur.

4.5 Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

5. Kablolama Güvenliği

5.1 Güç ve iletişim kablolarının (ağ kabloları, güç kaynağı kabloları, telefon kabloları, vb.) fiziksel etkilere ve dinleme faaliyetlerine karşı korunması için önlemler alınır.

5.2 Kablolar binalar arası geçişte yeraltında, bina içlerinde kablo kanalları veya tavalar içerisinden geçirilir.

5.3 Karışmanın (interference) olmaması için güç ve iletişim kabloları fiziksel olarak ayrılır.

5.4 Hatalı bağlantıların olmaması için ekipman, kablolar ve prizler görülebilecek bir şekilde etiketlenir ya da işaretlenir.

5.5 Kablolama yapılırken gelecekteki ihtiyaçlar dikkate alınarak yedekli olarak kablo çekilir.

5.6 Bina içindeki yerel alan ağı ana omurgası fiziksel olarak yedekli bir şekilde çalıştırılır.

5.7 Dağıtım panelleri ve kenar anahtarların konulduğu kabinler yetkisiz erişime karşı kilitli olarak bulundurulur.

5.8 Bahse konu kabinlerin de kesintisiz güç kaynağı ve jeneratör altyapısından faydalanması sağlanır.

6. Ekipman Bakımı

6.1 Kurumda kullanılmakta olan ekipmanların yıllık bakım planları oluşturulur. Planda yer alan ekipman listesinin envanter ile uyumlu olması kontrol edilir.

6.2 Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılır.

6.3 Bakım işlemleri sadece yetkili personel tarafından yerine getirilir. Son kullanıcıların ya da yetkisiz kişilerin donanım yapılandırmalarında değişiklik yapmasını engellemek için (kasa kilidi, kasa açma/ kapama etiketi gibi) gerekli tedbirler alınır.

6.4 Bakım kayıtları düzenli olarak tutulur.

6.5 Ekipmanlar bakım için kurum dışına çıkarılırken sabit disklerinde yer alan bilgilerin yetkisiz kişilerin eline geçmemesi için tedbir alınır. Bu kapsamda diskler sökülür ya da diskte yer alan bilgiler kalıcı olarak silinir.

6.6 Ekipmanlar sigortalıysa, sigorta şartlarının sağlanması için gerekli özen gösterilir.

6.7 Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınır ve takip edilir.

7. Kurum Dışındaki Ekipmanın Güvenliği

7.1 Kuruma ait bilgisayarların kurum dışına çıkarılması ya da kişisel/yüklenici firmalara ait bilgisayarların işyerlerine getirilerek kurumsal amaçlarla kullanımı için yetkilendirme yapılması gerekir.

7.2 Bu şekilde kullanılan ekipmanların ve kullanıcıların listesi oluşturulur ve takip edilir.

7.3 Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenir.

7.4 Bu şekilde kullanılan ekipmanlar, Taşınabilir Ortam Yönetimi tedbirleri alınmak suretiyle kullanılır.

7.5 Tesis dışına çıkarılan ekipmanın gözetimsiz bırakılmamasına ve seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilir.

7.6 Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulur.

8. Ekipmanın Güvenli İmhası

Üzerlerinde kalıcı olarak veri barındıran ekipmanlar (sunucu, masaüstü veya dizüstü bilgisayarın, merkezi veri depolama birimlerinin ve benzeri bilgi sistem cihazlarının sabit diskleri ile USB flaş sürücüsü, USB hafıza ünitesi, flash disk ya da USB hafıza olarak bilinen taşınabilir veri depolama ortamları) usulüne uygun yöntemler kullanılarak imha edilir veya güvenli silme işlemi yapılır.

19. Haberleşme Güvenliği

1. Ağ Güvenliği

a. Bilgisayar ağları; küçük bir alan içerisindeki veya uzak mesafelerdeki bilgisayar ve/veya iletişim cihazlarının iletişim hatları aracılığıyla birbirine bağlandığı, dolayısıyla bilgi ve sistem kaynaklarının farklı kullanıcılar tarafından paylaşıldığı, bir yerden başka bir yere veri aktarımını mümkün kılan iletişim sistemleridir.

b. Ağ güvenliği, bir kuruluşun bilgisayar ağına bağlı olarak çalışan varlıklarının ve ağ trafiğinin güvenliğini sağlamak üzere, uygulamakta olduğu politikalar ve kontrol önlemleridir. Ağ güvenliği, bilgi güvenliğinin sağlanması için en önemli bileşenlerden biridir.

c. Ağ güvenliği, kurum bilgi güvenliği politikaları kapsamında alınacak idari ve teknik tedbirler ile sağlanır. Bu maksatla çeşitli yazılım ve donanımlar kullanılır.

d. Daha güvenli bir iletişim ortamı sağlamak maksadıyla (Aile Sağlığı Merkezleri, Acil Sağlık Hizmetleri İstasyonları, müstakil bir binada çalışan ve ağa bağlı aktif cihaz sayısı 5'den az olan birimler hariç) Müdürlüğümüze bağlı tüm birimlerin geniş alan ağı bağlantıları ve internet erişimleri SBA (Sağlık Bilişim Ağı) üzerinden sağlanır.

e. Aile Sağlığı Merkezleri, Acil Sağlık Hizmetleri İstasyonları, müstakil bir binada çalışan ve ağa bağlı aktif cihaz sayısı 5'den az olan birimlerin internet erişimleri doğrudan ADSL aboneliği vb. yöntemlerle sağlanır.

f. SBA mimarisi uyarınca illere bağlı uç noktalar "toplama noktaları" olarak adlandırılan yapılar üzerinden, SBA Merkez Bulutuna ve internete bağlanır.

g. Buluta bağlı kullanıcıların internet erişimleri toplama noktalarında bulunan internet bağlantısı üzerinden gerçekleştirilir. Bu noktada sınır güvenliği için tesis edilmiş olan güvenlik duvarının yönetimi Bilgi İşlem Birimi tarafından yapılır.

h. İnternet üzerinden vatandaşlar tarafından erişilen uygulamalara ait sunucular (kurumların herkese açık web sayfaları, hastanelerin laboratuvar sonuçlarının sorgulandığı uygulamalar vb.), SBA'ya bağlı kullanıcılar tarafından erişilen sunucular (muhtelif SBYS uygulama sunucuları, etki alanı sunucuları, dosya sunucuları vb.) ve VTYS sunucuları bu noktada yer alan güvenlik duvarı vasıtası ile tesis edilen DMZ bölgesine konulur.

2. Uç Nokta (Yerel Alan Ağı) Ağ Güvenliği

a. SBA'ya bağlı olsun veya olmasın tüm yerel alan ağlarında ağ güvenliği ile ilgili tedbirler uygulanır.

b. Yerel alan ağının fiziki güvenliği sağlanmalıdır.

c. Kablosuz sistemler kullanılarak tesis edilen yerel alan ağları için ilave tedbirler alınır.

d. Yerel alan ağları performans, güvenlik ve ölçeklenebilirlik avantajlarını kullanmak üzere VLAN'lara bölünerek yönetilir.

e. Ağa bağlanan tıbbi cihazlar, sunucular ve istemci bilgisayarlar farklı VLAN'lara konulur.

f. SBA altyapısında çalışan ürün veya cihazların ikincil bağlantı yöntemleri üzerinden internete dâhil edilmesi (örneğin ağa bağlı bir tıbbi cihaza 4G kablosuz modem takılarak doğrudan internet erişimi sağlanıp güncelleme yapılması, ağa bağlı bilgisayarın cep telefonu ile oluşturulan bir kablosuz erişim noktası üzerinden internete bağlanması vb.) kesinlikle yasaktır.

g. Herhangi bir nedenle böyle bir bağlantı ihtiyacı olması halinde, söz konusu bağlantı için yazılı onay alınması ve yazılı onayda belirtilen ilave güvenlik tedbirlerinin uygulanması gerekir.

h. Yazılı onay alınmaksızın yukarıda belirtilen şekilde internet bağlantılarının yapıldığının tespit edilmesi halinde, ilgililer hakkında idari ve yasal işlemler yapılır.

i. Yerel alan ağlarının SBA'ya bağlandığı noktalarda sınır güvenliğinin sağlanması için asgari tedbir olarak bir adet güvenlik duvarı kurulur.

j. Bu noktalarda tesis edilen güvenlik duvarlarının yönetimi, uç noktalardaki bilgi işlem yöneticileri tarafından yapılır.

k. Hastanelerin misafir ağları ile SBA'ya bağlanan yerel alan ağları fiziksel olarak ayrı ağlar olarak tesis edilir. Misafir ağlarına bağlı kullanıcıların SBA ağına erişimine izin verilmez.

3. Kablosuz Ağ Güvenliği Kablosuz erişim noktası olarak kullanılan cihazların yönetimi için kullanılan parolalar değiştirilir. Kurum parola politikasına uygun olarak karmaşık parola verilir.

b. Cihazların varsayılan yayın adı (SSID değeri) değiştirilir.

c. Bağlantı ayarları için şifreleme etkinleştirilir. Şifreleme seçeneği etkinleştirilirken ağa erişim için kullanılmak üzere üçüncü taraflar tarafından tahmin edilemeyecek karmaşık bir parola belirlenir. Şifreleme yöntemi olarak öncelikle WPA3 Güvenlik protokolü kullanılır. WPA3 desteklemeyen cihazlarda üretici firmaların yayımlamış olduğu güncel yazılım sürüme yükseltilir.

d. Uyumluluk, güvenilirlik, performans ve güvenlik ile ilgili nedenlerle WEP ve WPA1 kullanımı uygun değildir.

e. Kablosuz ağa bağlanacak kullanıcı sayısı kısıtlı ise ilave güvenlik önlemi olarak ağa bağlanacak cihazların MAC adresleri, kablosuz erişim cihazı üzerinde tanımlanır.

f. Erişim noktasının sinyal gücü kapsama alanı, ihtiyaca cevap verecek şekilde en aza indirilir.

20. Kişisel Verilerin Korunması

1. Anayasa'nın 20'ci maddesinin, 6698 sayılı kanunun ve Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin, kişisel verilerin korunmasına ilişkin hükümlerine azami düzeyde hassasiyet gösterilir.

2. Kişisel verilerin ve kişisel sağlık verilerinin işlenmesinde, 6698 sayılı kanunun 4'üncü maddesinde yer alan genel ilkelere; ayrıca kişisel verilerin işlenmesinde Kanun'un 5'inci maddesinde, kişisel sağlık verilerinin işlenmesinde ise Kanun'un 6'ncı maddesinde yer alan hükümlere riayet edilir.

3. Kişisel verilerin ve kişisel sağlık verilerinin aktarılmasında, 6698 sayılı kanunun 8'inci ve 9'uncu maddesinde yer alan hükümlere riayet edilir.

4. 6698 sayılı kanunun 12'nci maddesinin birinci fıkrası uyarınca veri sorumlusu; verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek, verilerin muhafazasını sağlamak amaçlarıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

5. 6698 sayılı kanunun 12'nci maddesinin ikinci fıkrası uyarınca veri sorumlusu (İdare), kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişiler (sağlık hizmet sunucularında SBYS işletimi hizmeti veren yüklenici) ile birlikte müştereken sorumludur.

6. 6698 sayılı kanunun 12'nci maddesinin üçüncü fıkrası uyarınca veri sorumlusu, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Dolayısı ile Kanun hükümlerine uyumluluğun sağlanıp sağlanmadığı hususunda veri sorumlusu, veri işleyeni (SBYS işletimi hizmeti veren yüklenici) denetleyebilir.

7. 6698 sayılı kanunun 12'nci maddesinin dördüncü fıkrası uyarınca veri sorumlusu ile veri işleyen (SBYS işletimi hizmeti veren yüklenici), öğrendiği kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

8. Kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ile 140'ıncı madde hükümleri uygulanır.

9. 6698 sayılı kanun hükümlerine uygunsuzluk nedeniyle Kişisel Verileri Koruma Kurumu tarafından verilecek idari para cezaları ile ilgili kişiler tarafından açılacak davalarda hükmedilecek maddi ve manevi tazminat davaları, kusurlu olması hâlinde veri işleyen (SBYS işletimi hizmeti veren yüklenici) tarafından ödenir.

21. 5651 Sayılı Kanun ile Uyum

1.Türkiye'de internet ile ilgili en kapsamlı düzenleme 2007 yılında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile sağlanmıştır.

2.5651 sayılı kanun ile temel olarak aşağıdaki hususlarda düzenlemeler yapılmıştır:

2.1. İnternet aktörlerinin (içerik sağlayıcı, yer ve erişim sağlayıcı, toplu kullanım sağlayıcı) tanımı yapılmış ve bu aktörlerin hak ve sorumlulukları belirlenmiştir.

2.2. Yasada suçlar bakımından erişimin engellenmesi usul ve esasları düzenlenmiştir.

2.3. İnternet ortamında yayımlanan içerik nedeniyle haklarının ihlal edildiğini iddia eden kişilere ilişkin; içeriğin yayından çıkarılmasını sağlama ve cevap hakkı uygulamalarına ilişkin usul ve esaslara yer verilmiştir.

2.4. Konusu suç teşkil eden (ve/veya küçükler için zararlı olan) içerik kapsamında filtreleme usulü öngörülmüştür.

2.5. Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen katalog suçlara ilişkin şikâyetlerin yapılabileceği internet bilgi ihbar merkezi (ihbarweb.org.tr) kurulmuştur.

3.Kurumlarımızda tesis edilmiş olan ağların hemen hemen tamamına yakını bir şekilde internet ortamına bağlı olarak çalışmakta ve Kanunda belirtilen internet aktörlerinden "içerik sağlayıcı, yer sağlayıcı veya toplu kullanım sağlayıcı" rollerinden bir veya birkaçına girebilmektedir.

4."Erişim sağlayıcı" kuruluşlar, abonelerine ticari olarak internet erişimi sağlayan telekomünikasyon firmaları olup Müdürlüğümüze bağlı hiçbir kurum bu kategoriye girmemektedir.

5.İçerik Sağlayıcı, İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir. Müdürlüğümüz ve bağlı birimleri web sayfaları vasıtası ile kullanıcılara içerik sundukları için "İçerik Sağlayıcı" konumundadır.

6.İçerik Sağlayıcı;

6.1. İnternet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

6.2. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur.

7.Bu nedenlerle web sayfalarımızda yer alan her türlü içeriğin mutlaka bir sahibi olmalı ve kayıt altına alınmalı, kurumun web sayfasında içerik yayımlama ile ilgili usul ve esaslar belirlenmelidir.

8.Sistemi işleten Müdürlüğümüz değil ilgili web sitesine içeriği koyan kişi veya kurumlar sorumludur.

9.Yer Sağlayıcı, internet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.

10. Yer sağlayıcı;

10.1. Yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, Kanun ve ilgili mevzuat hükümlerine göre BTK, adli makamlar veya hakları ihlal edilen kişiler tarafından haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde, hukuka aykırı içeriği yayından kaldırmakla,

10.2. Yer sağlayıcı trafik bilgisini ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri iki yıl süre ile saklamakla sorumludur.

10.3. Yer sağlayıcı trafik bilgisi, internet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgilerdir.

11.Müdürlüğümüz ve bağlı birimlerine ait web sayfalarının ve uygulamaların sunumunda kullanılan yazılım ve donanımları işleten birimler "Yer Sağlayıcısı" konumundadır. Bu kapsamda;

11.1. Web siteleri ve uygulamaları, kuruma ait sunucu/sistemler vasıtası ile sunuluyorsa yer sağlayıcısı ilgili kurumun kendisi,

11.2. Web siteleri barındırma hizmeti, hizmet alımı ile SBYS firmaları veya diğer üçüncü kişilerden alınıyorsa yer sağlayıcısı ilgili SBYS firması veya üçüncü kişiler olmaktadır.

12. Web siteleri barındırma hizmeti, hizmet alımı ile SBYS firmaları veya diğer üçüncü kişilerden alınıyorsa, hizmet sözleşmelerine 5651 kanunu ile ilgili maddelerin koyulması ve yapılacak firma denetimleri ile bu verilerin alındığının kontrol edilmesi gerekir.

13.İnternet Toplu Kullanım Sağlayıcılar, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişilerdir. Müdürlüğümüz ve bağlı birimleri, tesis edilen bilişim altyapısı kullanılmak suretiyle, son kullanıcılara internet ortamına erişim sağlıyorsa "İnternet Toplu Kullanım Sağlayıcı" konumundadırlar.

14.İnternet Toplu Kullanım Sağlayıcıları;

14.1. Erişim kayıtlarını ve bu kayıtların doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri 2 (iki) yıl süre ile saklamakla,

14.2. Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme (İnternet ortamında web adresi, alan adı, IP adresi, kelime ve benzeri ölçütlere göre erişimi engelleyen yazılımları ve donanımları) sistemini kullanmakla,

14.3. Kamuya açık alanlarda internet erişimi sağlayan toplu kullanım sağlayıcılar, kullanıcıları tanımlayacak sistemleri kurmakla sorumludur.

14.4. Erişim kaydı olarak kullanıcılara iç ağda dağıtılan IP adres bilgilerinin, IP adreslerinin kullanıma başlama ve bitiş zamanlarının ve bu IP adreslerini kullanan bilgisayarların MAC adreslerinin, hedef IP adreslerinin kayıt altına alınması gerekir.

15.İnternet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sisteminin yanı sıra, ilave tedbir olarak güvenli internet hizmeti de alabilirler.

22. Mal ve Hizmet Alımı Güvenliği

1. Kurum olarak mal ve hizmet alımlarında ilgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak rekabeti engellemeyecek şekilde gerekli güvenlik düzenlemeleri İdari veya Teknik şartnamelerde belirtilmelidir.

2. 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.

23. Yazılım Güvenliği Politikası

1. Kullanıcı hesabı incelemeleri tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en fazla 6 (altı) aylık aralıklarla yapılır.

2. Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilir.

3. 60 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır.

4. Parolalar kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.

5. Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da parola oluşturma özelliklerine uygun olmak zorundadır.

6. İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.

7. İl Sağlık Bilgi Sistemi parolasını hatırlamayan kullanıcıların;

7.1. Sağlık Bakanlığı personeli ise saglik.gov.tr uzantılı elektronik posta adresi üzerinden,

7.2. Sağlık Bakanlığı dışı kullanıcılar için kurumsal veya kişisel elektronik posta hesabı üzerinden, elektronik posta hesabı yoksa SMS üzerinden, SMS gönderilecek telefon yoksa dilekçe ile şahsen müracaat ederek, parola sıfırlama işlemi gerçekleştirilir.

24. Bilgi Güvenliği İhlal Olay Yönetimi

1.İhlal Bildirimi ve Olay Yönetimi

1.1. Müdürlük çalışanları ve vatandaşlar tarafından tespit edilen Sağlık Müdürlüğü ile ilgili her türlü bilgi güvenliği ihlal olayı https://www.ism.gov.tr/BGIhlalBildirimi.aspx adresinde yer alan ihlal bildirim sistemine girilir.
1.2. İhlal birim sistemi dışında, Müdürlüğün diğer birimlerince bilgi güvenliği ihlal olaylarının bildirimi için ayrı bir sistem/yazılım kurulmasına gerek yoktur.
1.3. İhlal bildirim sistemine girilen olaylar, Sağlık Müdürlüğü ekipleri tarafından ön değerlendirmeye tabi tutulur. Bildirim yapan kişiyle irtibat kurulur.
1.4. Küçük çaplı, yalnızca kendi kurumunu ilgilendiren konu ise bilgi işlem birimi personeli tarafından gerekli müdahale yapılır
1.5. Hizmet verdiği kurumla birlikte diğer kurum ya da kişileri etkileyecek şekilde iş sürekliliğine zarar veren veya durduran, acil müdahale gereken, kurum imajına zarar verebilecek ihlal olaylarında Sağlık Bakanlığı SOME' den görüş/destek alınır.
1.6. İhlal bildirimi sistemine girilen tüm ihlal olaylarının süreç ve sonuçları Bilgi İşlem Birimi tarafından takip edilir.

2.İhlal bildirim sisteminde yer alan olay türleri ve açıklamaları şu şekildedir:

2.1. Servis Dışı Bırakma Saldırısı (DoS/DDoS): Saldırının amacı hedef alınan sistemi hizmet veremeyecek hale getirecek yöntemlerle, ilgili servisi hizmet dışı bırakmaktır. Kullanılan temel yöntem, ilgili hizmet servisine olağan dışı miktarda (çok sayıda) paket gönderip, engellemektir.
2.2. Bilgi Sızdırma (Data Leakage): Kurumun ürettiği, kullandığı ya da işlediği verilerin bilinçli veya bilinçsiz olarak yanlış hedefe gönderilmesi, çalınması ve/veya sızdırılmasıdır.
2.3. Zararlı Yazılım (Malware): Her türlü bilgi işleme yapabilen sistemlere zarar vermek, veri çalmak ve/veya yok etmek için üretilen yazılımlardır.
2.4. Sahtecilik (Fraud): Daha çok finansal sistemlerde karşılaşılan, aldatma amacı ile yapılan kasıtlı eylemlerdir.
2.5. Port Tarama: Ağa bağlı olarak çalışan aktif cihazlarda çalışan servislerin varlığını tespit etmek, bilgi toplamak ve tespit edilecek zafiyetler ile zararlı bir işlem yapma amacı ile gerçekleştirilen eylemlerdir.
2.6. Veri Tabanı Saldırısı: VTYS yazılımları, VTYS'nin çalıştığı donanımlar veya VTYS ile ilişkili uygulama yazılımlarında bulunan açıklıkların kullanılması suretiyle yetkisiz bir şekilde verilerin ele geçirilmesini hedefleyen saldırılardır. SQL Injection saldırısı buna örnek verilebilir.
2.7. Web Uygulamaları Güvenlik İhlalleri: Siteler arası betik çalıştırma (XSS: Cross-Site Scripting) saldırıları, kötü amaçlı dosya çalıştırılması, güvenli olmayan direk nesne referanslama, sunucu taraflı çapraz kod çalıştırma (CSRF: Cross Site Request Forgery), bilgi sızdırma ve uygun olmayan hata kontrolü, İhlal edilmiş kimlik doğrulama ve oturum yönetimi, güvensiz iletişimler gibi ihlaller bu madde altında değerlendirilir.
2.8. Sosyal Mühendislik: Kişilerin zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye yönelik teknikler içerir.
2.9. Veri Kaybı/İfşası: Gizli bilgilerin e-Posta aracılığı ile iletimi, ağ üzerinden iletilen bilgilerin yetkisiz ya da yanlış alıcıya iletimi, internet üzerinden güvenli olmayan kanallar aracılığıyla veri iletimi, ortak kullanım yazıcılarından alınan çıktıların sahiplenilmemesi ya da güvenliğine önem verilmemesi, masaüstü ya da ortak alanlarda basılı kopyaların denetimsiz bırakılması vb. durumları ifade eder. Zararlı Elektronik Posta (SPAM): Kişinin bilgisi ve talebi dışında, ticari içerikli veya politik bir görüşün propagandasını yapmak ya da bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-Posta iletileridir.
2.10. Parola Ele Geçirme: Depolanmaması gereken bir yerde depolanan parolaların herhangi bir saldırı yöntemi ile ele geçirilmesidir.

2.11. Taşınır Cihaz Kaybı: CD/DVD, DAT (manyetik ses bandı), veri depolamak için kullanılan USB taşınabilir bellekler, Harici Sabit Disk sürücüleri gibi taşınabilir cihazlar ve her türlü bilgi işleme yapabilen cihazlar (bilgisayar, akıllı telefon, tablet v.s)'ın kaybedilmesi veya çalınması durumunu ifade eder.

2.12. Kimlik Taklidi: Kişilerin fiziksel, telefon ya da dijital ortamda olmadığı bir kişi gibi davranıp, onun yetkilerini bilgisi dışında kullanmasıdır.

2.13. Oltalama: Saldırgan kişilerin, kurumsal/bireysel kişilere e-Posta göndererek, kritik bilgilerini ele geçirme ve/veya bu bilgileri paylaşmaları konusunda kandırmaya yönelik olan saldırı türüdür.

2.14. Kişisel Bilgilerin Kötüye Kullanımı: Kişisel verilerin işlenmesine ilişkin süreçlerde 6698 sayılı kanunda yer alan usul ve esaslara uygunluk sağlanmalıdır. Kişisel verilerin işlenmesinde, 6698 sayılı kanunda yer alan genel ilkeler göz önünde bulundurulmalıdır. Kişisel verilerin hukuka aykırı işlenmesi ve aktarılması hâlinde; hukuki, idari ve cezai yaptırımlarla karşı karşıya kalınabilir.

3.Kanıt Toplama

3.1. Delillerin değişmesini, bozulmasını önlemek ve delilleri korumak amacıyla olay yerinin güvenliği sağlanır. Olay yerine girişler kontrol altına alınır. Yetkisiz girişlere izin verilmez. Olay yerinden çıkış yapan kişilerin üzerinde adli delil oluşturabilecek materyal olup olmadığı kontrol edilir.

3.2. Olay yerinde işleme başlamadan önce, farklı açılardan olay yerinin görüntüleri çekilir. Çekilen fotoğraflarda tarih ve zaman bilgisinin doğru olduğuna dikkat edilir.

3.3. Delil niteliği taşıyan tüm materyaller açıklayıcı bilgi içerecek şekilde etiketlenir. Bilgisayara bağlı tüm bağlantılar, bağlantı noktasını gösterecek şekilde etiketlenir ve sistem bağlı olduğu ağdan ayrılmaz.

3.4. Bilgisayara bağlı olan cihazlar tespit edilerek, sökülmeden önce etiketlenir.

3.5. Olay yerindeki bilgisayar kapalı ise kesinlikle açılmaz.

3.6. Bilgisayar açık ise ekranının fotoğrafı çekilir ve üzerinde çalışan programlar kayıt altına alınır. Bilgisayarın sistem tarih ve zaman bilgileri ve inceleme esnasındaki gerçek tarih ve zaman bilgisi kaydedilir. Yapılan işlemlerde, her aşamada ayrı ayrı kayıt tutulur. İşlemlerin kimin tarafından yapıldığı ve kullanılan yazılım ve donanım bilgileri kayıt altına alınır.

3.7. Değişme olasılığı yüksek olan dijital deliller, öncelikli olarak ele alınır. Bilgisayarın kapatılması veya yeniden başlatılması uçucu delillerin kaybolmasına sebep olacaktır. Bu nedenle veri kayıt işlemlerine, bellek ve ön bellekte bulunan uçucu verilerin kopyalanması ile başlanır. Bu işlem yapılmadan hiçbir şekilde bilgisayarın kapatılmaması gerekir.

3.8. Bilgisayar kapatıldığında, sistem yapılandırma dosyaları ve geçici dosya sistemleri değişebilir. Bilgisayarın kapatılması delil bütünlüğünü bozar ve delili değiştirebilir. Olay yerindeki kapalı bir bilgisayarı açmak da yine aynı şekilde delillere zarar verebilir. Delillerin zarar görmemesi için veri toplama ve kayıt işlemlerinin ilgili teknik uzmanlar tarafından "canlı analiz" şeklinde yapılması gerekir.

3.9. Bilgisayarın dijital imza (hash) değeri alınır. İmajların gizliliği, erişilebilirliği ve bütünlüğü sağlanır. Kopya alma (imaj) işlemi dışında kesinlikle orijinal delile dokunulmaması gerekir. Deliller toplanıp, birebir kopyası (imajı) alınmadan, delil analiz işlemlerine başlanmaz. İmaj alma işlemi de bir tutanak ile kayıt altına alınır. İmajın hangi yazılım veya araç ile alındığı mutlaka tutanağa yazılır.

3.10. Yedeklenecek diskin hafızası şüpheli bilgisayar diskinden büyük olur.

3.11. Silinmiş verilerin yeniden kurtarılması ve şifrelenmiş verilerin şifrelerinin çözülmesi için tüm dosyalar analiz edilir. Elde edilen deliller, programlar vasıtası ile incelenir. Gerekiyorsa şifre çözme yöntemleri kullanılır.

3.12. Olay yerindeki dijital delillerin bütünlüğünün bozulmaması için uygun koşullarda muhafaza edilmesi gerekir. Hassas veri depolama birimlerinin taşınmasına özen gösterilir. Taşınma esnasındaki fiziksel darbelere karşı korunur. Toplanan delillerin taşınma öncesi taşınacağı ünitelerde, mutlaka etiketlenmesi ve kayıt altına alınması gerekir. Birden fazla dijital delile müdahale edildiğinde, her birim dâhil olduğu sistem ile paketlenir. (Bilgisayar-Klavye-Fare gibi)

3.13. Dijital delil mutlaka tutanak ile teslim edilir. Tutanağa yazılan hash değeri kontrol edilir. Dijital delil raporu kolluk kuvvetlerine teslim edilirken raporda, delilleri kimlerin topladığı, deliller üzerinde hangi işlemlerin yapıldığı, hangi yazılım veya donanımların kullanıldığı, işlemin yapıldığı zaman, delilin üzerindeki zaman bilgisi gibi bilgiler de kayıt altına alınarak raporda açık bir şekilde belirtilir.

3.14. Doğruluğu ve güvenilirliği kabul edilmiş yazılım ve donanımlar kullanılır.

25. e-Posta Kullanım Politikası

1.Amaç: Bu politikanın amacı, T.C. Sağlık Bakanlığı İzmir İl Sağlık Müdürlüğü "@saglik.gov.tr" uzantılı e-posta mesajlarında alma, gönderme, yönlendirme ve otomatik gönderme kurallarına genel kuralları tanımlamaktır.

2.Kapsam: Bu politika, T.C. Sağlık Bakanlığı İzmir İl Sağlık Müdürlüğü bünyesinde kurumun sağladığı resmi e-posta hesabı olan tüm kullanıcılar içindir.

3.Politika Metni:

3.1. İzmir İl Sağlık Müdürlüğü hizmet veren ve İzmir İl Sağlık Müdürlüğü fiziki alanlarında çalışan tüm personel (memur, danışman ve firma) için kurumsal e-posta (@saglik.gov.tr) hesabı tahsis edilir ve tüm iş amaçlı e-postaların kurumsal e-posta hesabı ile gerçekleştirilmesi zorunludur.

3.2. Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.

3.3. İş dışı konulardaki haber grupları kurumsal e-posta adres defterine eklenemez.

3.4. E-Posta hesapları, kurum içi ve dışı başka kullanıcılara Spam (istenmeyen e-posta), Phishing (kimlik avı) mesajlar göndermek için kullanılamaz.

3.5. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.

3.6. Hiçbir kullanıcı, gönderdiği e-posta adresinin Kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.

3.7. Personel konu alanı boş bir e-posta mesajı göndermemelidir.

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

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

3.10. Kurum 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.

3.11. Kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajlar gönderilemez. Bu tür özelliklere sahip bir mesaj alındığında İl Sağlık Müdürlüğü Bilgi İşlem Birimine haber verilmelidir.

3.12. Kullanıcı hesapları, doğrudan ya da dolaylı, ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-posta gönderilmesi yasaktır.

3.13. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-posta alındığında, e- posta başka kullanıcılara iletilmeden İl Sağlık Müdürlüğü Bilgi İşlem Birimine haber verilmelidir.

3.14. Zararlı e-posta, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt verilmemelidir.

3.15. Kullanıcı hiçbir suretle kurumsal e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) gönderemez.

3.16. 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.

3.17. Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.

3.18. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın İl Sağlık Müdürlüğü Bilgi İşlem Birimine haber vermelidir.

3.19. Kullanıcı, posta hesabını sürekli kontrol etmeli; kurumsal e-postalara, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

3.20. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar İl Sağlık Müdürlüğü Bilgi İşlem Birimine haber verilmelidir.

3.21. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının çalındığını fark ettiği anda İl Sağlık Müdürlüğü Bilgi İşlem Birimine haber vermelidir.

26. İşe Başlayış ve İşten Ayrılma

İşe Başlayış ve İşten Ayrılma Prosedürü

1.a. <u>İşe Başlayış Prosedürü:</u> İlk işe başlayan, görev ve yer değişikliği olan tüm personel için geçerlidir.

1.a.1. İşe başlayan her personele bilgi güvenliği ve sosyal mühendislik zafiyetleri konularıyla ilgili yılda en az 1 kez eğitim verilmelidir.

1.a.2. İşe başlayış ve görev değişikliği kurumda kullanılan personel bilgi sistemine işlenmelidir.

1.a.3. Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış Personel Gizlilik Sözleşmesi ve Bilgi Güvenliği Farkındalık Bildirgesi imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Her çalışan personel "Bilgi Güvenliği Kullanıcı Sözleşmesini (Bilgisayar kullansın kullanmasın, kadrolu, sözleşmeli, sürekli işçi, alınan hizmet kapsamında çalışan tüm personel) imzalamakla yükümlüdür.

1.a.4. Var ise kullanacağı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri tanımlanmalıdır.

1.a.5. EBYS üzerinden yazışma yapabilmesi veya yazışmaları takip edebilmesi için ilgili personele saglik.gov.tr uzantılı e-mail adresi tanımlanmalıdır. İl içi yer değişikliklerinde ise sistem üzerinden kurum/birim değişikliği tanımlaması yapılmalıdır.

1.a.6. Tüm personele kurum kimlik kartı çıkartılmalıdır.

1.b. <u>İşten Ayrılma Prosedürü</u> Görev ve yer değişikliği olan, istifa eden ve emekli olan personeller için geçerlidir.

1.b.1. Görevden ayrılan personelin kurum kimlik kartı ve yaka kartı teslim alınmalıdır.

1.b.2. Görevden ayrılan personel kurumda kullanılan personel bilgi sistemine işlenmelidir.

1.b.3. Kullandığı bilgi sistemlerine yönelik (ÇKYS/TSIM, EBYS vb.) kullanıcı adı ve şifreleri ilgili sistem yöneticileri tarafından iptal edilmeli ya da pasif hale getirilmelidir.

1.b.4. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.

1.b.5. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

1.b.6. Görevden ayrılan personel "İŞTEN AYRILMA ONAY FORMU" nu doldurarak bağlı bulunduğu kurumun insan kaynaklan birimine teslim etmelidir.

1.b.7. İlgili form doldurulmadan personelin kurum ile ilişiği kesilmez.

27. Sözleşmeler

27.a. İzmir İl Sağlık Müdürlüğü Bilgi Güvenliği Farkındalık Bildirgesi

27.b. İzmir İl Sağlık Müdürlüğü Kurumsal Gizlilik Taahütnamesi

27.c. İzmir İl Sağlık Müdürlüğü Personel Gizlilik Sözleşmesi

T.C. SAĞLIK BAKANLIĞI
İZMİR İL SAĞLIK MÜDÜRLÜĞÜ
BİLGİ GÜVENLİĞİ FARKINDALIK BİLDİRGESİ

Bilgi Güvenliği Farkındalık Bildirgesi

1.Amaç:

Bu bildirge; T.C. Sağlık Bakanlığı İzmir İl Sağlık Müdürlüğü bünyesinde görev yapan tüm personelin, hizmetin ifası esnasında veya herhangi bir gerekçeyle vâkıf oldukları, kuruma ait gizli kalması gereken bilgilerin, gizliliğinin sağlanması ve ifşa edilmemesi için uyulması gereken kuralları tanımlar.

2.Kapsam:

Bu bildirge, Kurum bünyesinde görev yapan tüm personel için hazırlanmıştır. Kuruma ait gizli bilgilere erişim ihtiyacı olan diğer personel (danışman, firma personeli vb.) için Personel Gizlilik Sözleşmesi hükümleri uygulanır.

3.Yasal Dayanak:

Sağlık Bakanlığı Bilgi Güvenliği Yönergesine istinaden hazırlanmıştır.

4.Tanımlar: Bu bildirgede geçen;

4.1. Kurum: İzmir İl Sağlık Müdürlüğü

4.2. Kuruma Ait Gizli Kalması Gereken Bilgiler:

4.2.1. 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar" ile tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belgeyi,

4.2.2. Kurum tarafından işlenen (24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan) kişisel veriler ile (20/10/2016 tarihli ve 29863 sayılı Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik ile tanımlanan) kişisel sağlık verilerini,

4.2.3. Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belgeyi,

4.2.4. Bakanlığa veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar sistemleri içerisinde saklanan veriler, donanım/yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu işleri ifade eder.

5.Personelin Yükümlülükleri:

5.1. Kuruma ait gizli kalması gereken bilgileri, yasal zorunluluklar ve Kurum tarafından resmi olarak izin verilmesi halleri dışında süresiz olarak koruyacağımı; Kurum tarafından aksi belirtilmedikçe, hiç bir şekilde söz konusu bilgileri doğrudan veya dolaylı olarak kullanmayacağımı; başka bir yere aktarmayacağımı, yayınlamayacağımı, açıklamayacağımı, kişisel kopyalarını almayacağımı,

5.2. Kuruma ait gizli kalması gereken her türlü bilgiyi sır olarak saklamak, bunları üçüncü kişilere inceletmemek, söylememek, iletmemek ve açıklamamakla yükümlü olduğumu; öğrendiğim sırları veya bilgileri ve bunlara ilişkin belgeleri yetkileri olmayan kişilere ve makamlara açıklamayacağımı; bu yükümlülüğümün Kurum ile ilişkimin sona ermesi halinde de devam ettiğinin bilincinde olduğumu,

5.3. Sosyal medya hesaplarımı kullanırken görevimin gerektirdiği dikkat ve özeni göstereceğimi, kuruma ait gizli kalması gereken bilgileri, hastalara ilişkin kişisel bilgileri (hasta görüntüleri vb.) sosyal medya platformlarında paylaşmayacağımı,

5.4. Kurum tarafından uygun görülen sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtlarının; hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla toplanabileceğini,

5.5. Kurum tarafından verilen bilgisayar, tablet, telefon, taşınabilir medya gibi cihazları sadece göreve yönelik, kurumsal faaliyetler için kullanacağımı, özel işlemlerimde kullanmayacağımı,

5.6. Tarafıma verilen "kullanıcı adı" ve "parola"yı bir başkası ile paylaşmayacağımı ve bir başkasına kullandırmayacağımı, Kurumdan ayrılmam halinde şahsıma tahsis edilen kullanıcı adı ve parolayı iptal ettireceğimi; kullandığım bilgisayar ve/veya diğer elektronik veri depolama cihazlarında oluşturduğum veri, bilgi ve belgeler dâhil tüm dosyaları, cihazları ve ofis malzemelerini eksiksiz olarak kurum yetkilisine teslim edeceğimi ve hiçbir kopyasını almayacağımı,

5.7. Bilgisayarımda tarafıma tahsis edilen "kullanıcı adı" ve "parola" ile oturum açacağımı; çalışmam bitince, oturumu veya bilgisayarımı kapatarak kendi kullanıcı adı şifremle başka personelin işlem yapmasına fırsat vermeyeceğimi, bilgisayarımın başından kısa süreli ayrılmalarımda bilgisayar oturumunu kilitleyeceğimi,

5.8. Kurum tarafından sağlanan İnternet üzerinden girilen ve girilemeyen tüm siteler ve adreslerin, sistem tarafından gerekli olduğunda kullanılmak üzere kayıt altına alındığını; bu kapsamda 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" gereği bana tahsis edilen kullanıcı adı ve parola kullanılmak suretiyle usulüne uygun olarak kayıt altına alınan işlemlerden yasal olarak sorumlu tutulacağımı bildiğimi,

5.9. Kurum sunucuları üzerinde bana tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP/MAC adresini kullanarak gerçekleştirdiğim her türlü etkinlikten, Kurum bilişim kaynaklarını kullanarak oluşturduğum ve/veya bana tahsis edilen Kurum bilişim kaynağı üzerinde bulunduğum her türlü kaynağın (belge, doküman, yazılım vb.) içeriğinden sorumlu olduğumu,

5.10. Şahsıma teslim edilen kullanıcı adı ve parolanın gizli kalmasını sağlamakla yükümlü olduğumu, şahsi kusurum nedeniyle kullanıcı adı ve parolamın başkaları tarafından öğrenilmesi halinde, bu bilgiler kullanılarak yapılan iş ve işlemlerden şahsen sorumlu tutulabileceğimi bildiğimi,

5.11. İşin gerektirdiği haller dışında kurumsal e-Posta hesabımı kullanmayacağımı, Kurum içindeki diğer kullanıcılara iş ile ilgili olmayan toplu ve/veya kişisel e-Posta göndermeyeceğimi; Kurum içine veya Kurum dışına göndermiş olduğum tüm e-Postalardan kişisel olarak sorumlu olduğumu ve ilgili tüm yasal sorumlulukların tarafıma ait olduğunu,

5.12. Tarafıma teslim edilmiş elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gereç üzerinde kurum bilgisi dışında hiçbir mekanik ya da yazılımsal yapılandırma değişikliği yapmayacağımı,

5.13. Bilgisayarıma Kurum tarafından yüklenmiş işletim sistemi ve uygulama yazılımları dışında herhangi bir işletim sistemi veya lisanssız yazılım yüklemeyeceğimi, Kurum tarafından yüklenmemiş yazılımlardan doğacak her türlü hukuki sorumluluğun tarafıma ait olduğunu,

taahhüt eder, bu taahhütlerimi yerine getirmemem veya kasıtlı olarak taahhütlerimi ihlal etmem hâlinde; Kurum açısından oluşacak zararı karşılayacağımı, mali, cezai ve hukuki tüm sorumlulukların bana ait olduğunu beyan ve kabul ederim.

Adı Soyadı / Tarih / İmza

T.C. SAĞLIK BAKANLIĞI
İZMİR İL SAĞLIK MÜDÜRLÜĞÜ
KURUMSAL GİZLİLİK TAAHÜTNAMESİ

Kurumsal Gizlilik Taahhütnamesi

1.Taraflar, Amaç ve İşin Tanımı

1.1. T.C. Sağlık Bakanlığı İzmir İl Sağlık Müdürlüğü .... adresinde faaliyet göstermekte olup bundan sonra "**Kurum**" olarak anılacaktır.

1.2. Kurum ile aramızda 1.3. maddede yazılı iş/faaliyet kapsamında, Sözleşme, Protokol veya benzeri adlar altında imzalanmış ve/veya imzalanması planlanan akdi ilişkinin amaçlarını gerçekleştirmek üzere Kuruma ait ve "gizli bilgi" niteliği taşıyan yazılı ve/veya sözlü bilgilere ulaşacak olmamız sebebiyle, aşağıdaki hususlara riayet etmeyi peşinen kabul ve taahhüt ederiz.

1.3. İş/Faaliyet Tanımı[1]

.....

.....

2.Gizli Bilginin Tanımı

2.1. Aşağıdaki bilgileri kesinlikle "**GİZLİ BİLGİ**" olarak kabul ederiz:

2.1.1. 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar" ile tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belge.

2.1.2. 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan kişisel veriler ile 20/10/2016 tarihli ve 29863 sayılı Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik ile tanımlanan kişisel sağlık verileri.

2.1.3. Bakanlığa veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar sistemleri içerisinde saklanan veriler, donanım/yazılım ve tüm diğer düzenleme ve uygulamalar ile yüklenici ve çalışanlarının çalışma süresi içerisinde yapmış olduğu işler.

2.1.4. Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belge.

3.Gizli Bilginin Korunması

3.1. Bu gizli bilgiyi;

3.1.1. T.C. Sağlık Bakanlığı tarafından yayımlanmış yürürlükteki Bilgi Güvenliği Politikası Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzunda belirtilen tedbirleri almak suretiyle korumayı,

3.1.2. Herhangi bir üçüncü kişiye hangi suretle olursa olsun vermemeyi, açıklamamayı, değiştirmemeyi, çoğaltmamayı ve/veya kamuya duyurmamayı,

3.1.3. İşin yürütülmesi haricinde doğrudan ya da dolaylı olarak hiçbir şekilde ve sebeple kullanmamayı,

3.1.4. Üçüncü kişiler tarafından doğrudan ya da dolaylı olarak ulaşılmaması için gerekli tüm tedbirleri almak suretiyle saklamayı,

3.1.5. Gizli bilgilerin tutulduğu ortamlar ile ilgili işlemlerin kayıtlarının olması açısından erişimleri ve yapılan işlemleri loglamayı, bu logların erişimine, değiştirilmesine ve silinmesine izin vermemeyi ve yukarıda sayılan surette sonuçlanacak sair davranışlardan kaçınmayı taahhüt ederiz.

Kendi gizli bilgilerimizi korumakta gösterdiğimiz özenin aynısını, Kurumun gizli bilgisini korumakta da göstereceğimizi, sadece zorunlu hallerde ve işin gereği bu bilgiyi öğrenmesi gereken çalışanlarımıza işin yürütülmesi için gereken nispette ve bilginin korunması için her türlü azami önlemi alarak verebileceğimizi; Kurumun gizli bilgilerine erişecek personelimize Kurum tarafından kullanılan "Personel Gizlilik Sözleşmesini imzalatacağımızı; çalışanlarımızın bilginin gizliliği hususunda bu Taahhütname ve Personel Gizlilik Sözleşmesi yükümlülüklerine aykırı davranmayacaklarını ve böyle davranmaları halinde doğrudan tarafımızın sorumlu olacağını peşinen kabul ve taahhüt ederiz.

Kurumdan temin etmiş olduğumuz gizli bilgilerin bu Taahhütnameye aykırı biçimde açıklandığından haberdar olduğumuzda, derhal ve yazılı olarak Kuruma durumu bildirmekle yükümlü olduğumuzu da kabul, beyan ve taahhüt ederiz.

4.Gizli Bilgi Tanımına Girmeyen Durumlar

4.1. Aşağıdaki bilgilerin gizli bilgi olarak nitelendirilmeyeceğini kabul ve beyan ederiz.

4.1.1. Bakanlığın veya Kurumun bizzat kendisi tarafından alenileştirilmiş bilgiler,

4.1.2. Açıklanmasına Bakanlık veya kurum tarafından yazılı olarak onay verilmiş bilgiler,

4.1.3. Yürürlükte olan bir kanuna ya da verilmiş olan bir mahkeme kararına istinaden açıklanması gereken bilgiler.

Bu Taahhütnamenin 4.1.3 maddesi gereğince gizli bilgiyi açıklamaya mecbur kalmamız halinde, gizli bilgiyi açıklamadan önce Kuruma derhal yazılı bir bildirimde bulunacağımızı, gizli bilgiyi sadece hukuken gerektiği kadar açıklayacağımızı ve bu açıklamanın kapsamına ilişkin olarak Kuruma yazılı olarak bildirimde bulunacağımızı, 4.1.3 maddesi kapsamında bilgi paylaşımında bulunmuş olmamızın bu Taahhütnamedeki yükümlülüklerimizin sona erdiği anlamına gelmediğini beyan, kabul ve taahhüt ederiz.

5.Denetim ve Referans

5.1. Kurumun gerekli gördüğü hallerde, önceden haber vermek kaydıyla tesis ve sistemlerimizde, bu taahhütnamenin konusu ve kapsamı ile sınırlı kalmak şartıyla, bilgi güvenliği denetimleri yapma hakkına sahip olduğunu kabul ve beyan ederiz.

5.2. Kurumun resmi kurumlarca denetlenmesi halinde bu denetim kapsamında tarafımızdan bilgi ve belge talep edilmesi halinde, tarafımızdan talep edilen bilgi ve belgeleri derhal sağlamakla yükümlü olduğumuzu beyan, kabul ve taahhüt ederiz.

5.3. Kurumun bu konuda açık yazılı izni olmadıkça görsel ya da yazılı medya aracılığıyla T.C. Sağlık Bakanlığı ve kurumu referans olarak gösteremeyeceğimizi ya da reklam aracı olarak ve/veya reklam amacıyla kullanmayacağımızı beyan, kabul ve taahhüt ederiz.

6.Gizli Bilgilerin İadesi

6.1. Bu Taahhütnamenin sona ermesi veya feshedilmesi veya Kurum tarafından daha önce talep edilmesi durumunda, masrafları tarafımıza ait olmak üzere zilyetliğimizde bulunan gizli bilgi içeren her türlü dokümanı ve bunların kopyalarını derhal Kuruma iade edeceğimizi beyan, kabul ve taahhüt ederiz.

6.2. Bilgisayar dâhil herhangi bir elektronik cihaz veya mecraya yaptığımız kayıtları geri alınamaz şekilde yok edeceğimizi, Kurum tarafından talep edilmesi durumunda söz konusu gizli bilgileri barındıran diskleri bedelsiz olarak Kuruma teslim edeceğimizi; kayıtların yok edilmesi ve/veya gizli bilgi barındıran disklerin tespiti faaliyetine Kurum tarafından görevlendirilecek bir uzman personelin refakat etmesine izin vereceğimizi kabul ve taahhüt ederiz.

---

[1] Yapılacak işe ait KİK ihale kayıt numarası, sözleşme imza tarihi ve konusu veya ilgili protokolün adı (veya konusu) ve tarihi yazılır.

6.3. **6.3**. 6.2 maddesinde belirtilen kayıtların geri alınamaz bir şekilde yok edildiğini, bir şirket yetkilisinin imza edeceği tutanakla belgeleyeceğimizi beyan, kabul ve taahhüt ederiz.

7.Tazminat ve Cezai Şart

7.1. Bu Taahhütnameden doğan yükümlülüklerimizi tamamen veya kısmen ihlal etmemiz halinde, doğrudan ve dolaylı tüm zarar ve ziyanı karşılayacağımızı şimdiden kabul, beyan ve taahhüt ederiz.

7.2. Bu maddede yer alan tazminat ödeme yükümlülüğüne ek olarak, bu Taahhütnameden doğan yükümlülüklerimizi tamamen veya kısmen ihlal etmemiz nedeniyle idari veya adli makamlarca Kuruma kesilecek her türlü cezayı ilk talep halinde tazmin edeceğimizi, ayrıca bu cezaların doğmasına neden olan aykırılıklar nedeniyle ortaya çıkan her türlü zararı karşılayacağımızı kabul, beyan ve taahhüt ederiz.

8.Kısmi Geçersizlik

Bu Taahhütname maddelerinden herhangi biri geçersiz sayılır ya da iptal edilirse, bu halin Taahhütnamenin diğer maddelerinin geçerliliğine etki etmeyeceğini kabul ederiz.

9.Taahhütname Geçerliliği ve Değişikliği

Kurumun yeni bir Gizlilik Taahhütnamesi yayımlaması ve yayımlanan yeni Gizlilik Taahhütnamesinin tarafımızca imza altına alınması durumunda, bu taahhütname hükümlerinin ortadan kalkacağını ve yeni Gizlilik Taahhütnamesi hükümlerinin geçerli olacağını beyan, kabul ve taahhüt ederiz.

10.Devir ve Süre

10.1. Bu Taahhütnamenin, imza tarihinden itibaren yürürlüğe gireceğini ve yazılı olarak Kurum tarafından sona erdirilmedikçe yürürlükte kalacağını, Kurum ile aramızdaki akdi ilişki sona erse veya bu taahhütname herhangi bir şekilde sona erdirilse dahi bu Taahhütnamedeki gizlilik yükümlülüklerinin geçerli olmaya devam edeceğini beyan, kabul ve taahhüt ederiz.

10.2. Bu Taahhütnamede yer alan hak ve/veya yükümlülüklerin tarafımızca tamamen ya da kısmen bir başkasına devredilemeyeceğini beyan, kabul ve taahhüt ederiz.

11.Yetkili ve Görevli Mahkeme

Bu Taahhütnamenin yorumunda ve bu Taahhütnamede yer alan hükümlere ilişkin ortaya çıkacak olan tüm uyuşmazlıklarda, İzmir Mahkemeleri ve İcra Dairelerinin yetkili ve görevli olduğunu beyan, kabul ve taahhüt ederiz.

<table>
<tr><th>İZMİR İL SAĞLIK MÜDÜRLÜĞÜ TEMSİLCİLERİ</th><th>FİRMA /KURUM/ KURULUŞ YETKİLİ TEMSİLCİSİ</th></tr>
<tr><td>Bu Taahhütnamenin, madde 1.3’te belirtilen iş/faaliyet kapsamında, Ek’te yer alan imza sirküleri ile “Firma/Kurum/Kuruluş[2]” adına imza atmaya yetkili kılınmış kişi tarafından imzalandığına şahitlik ederiz.</td><td>Bu Taahhütnameyi, madde 1.3’te belirtilen iş/faaliyet kapsamında, yetkili temsilcisi olduğum “Firma/Kurum/Kuruluş[3]” adına imzaladığımı beyan ederim.</td></tr>
<tr><td>İzmir İl Sağlık Müdürlüğünde Madde 1.3 kapsamında yapılacak iş/faaliyeti takip eden;
<u>Birim Sorumlusunun</u>
Adı Soyadı Tarih
….. /….. /…….
Unvanı
İmza
Birimi</td><td rowspan="2"><u>Yetkili Temsilcinin</u>
Adı Soyadı Tarih
….. /….. /…….
Unvanı
Kaşesi İmza</td></tr>
<tr><td>İzmir İl Sağlık Müdürlüğünde Madde 1.3 kapsamında yapılacak iş/faaliyeti takip eden;
<u>Birimin bağlı olduğu Başkanının</u>
Adı Soyadı Tarih
. ./. . / . . . .
Unvanı
İmza
Başkanlığı</td></tr>
</table>

12.EKLER

Firma, Kurum veya Kuruluş temsilcisinin bu ve/veya benzeri sözleşme/taahhütnameleri imzalamaya yetkili olduğunu gösterir imza sirküleri.

[2] İlgili Firma/Kurum veya Kuruluşun açık adı yazılacaktır.

[3] İlgili Firma/Kurum veya Kuruluşun açık adı yazılacaktır.

T.C. SAĞLIK BAKANLIĞI
İZMİR İL SAĞLIK MÜDÜRLÜĞÜ
PERSONEL GİZLİLİK SÖZLEŞMESİ

Personel Gizlilik Sözleşmesi

Bu sözleşme ……. / …… / 20….. tarihinde, aşağıda yer alan hükümler çerçevesinde, İzmir İl Sağlık Müdürlüğü[4] (Kurum) ile aşağıda kimlik bilgileri yazılı kişi (Personel) arasında akdedilmiştir.

1.**Tanımlar:**

Kuruma Ait Gizli Kalması Gereken Bilgiler:

1.1. 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar" ile tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belge.

1.2. Kurum tarafından işlenen (24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan) kişisel veriler ile (20/10/2016 tarihli ve 29863 sayılı Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik ile tanımlanan) kişisel sağlık verileri.

1.3. Kuruma veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar sistemleri içerisinde saklanan veriler, donanım/yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu işler.

1.4. Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belge.

2.**Yükümlülükler:**

2.1. Personel, kuruma ait gizli bilgilerin korunması için aşağıdaki kurallara uyacağının beyanı olarak bu sözleşmeyi imzalar.

2.2. Personel, Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzunda yer alan koşullara uygun hareket eder.

2.3. Personel, bu sözleşme hükümlerine uygun davranmaktan, ihlali halinde ise Bakanlığa, Kuruma ve üçüncü kişilere vereceği her türlü zarardan sorumludur. Sözleşmenin ihlal edilmesi sonucu doğacak tüm hukuki ve cezai sorumlukları peşinen kabul eder.

2.4. Personel, Kurumda uygulanmakta olan BGYS kapsamında yayımlanmış politika, prosedür, süreç ve sözleşmelere uygun davranır. Bahse konu dokümanlarda belirtilen hususları eksiksiz olarak yerine getirir.

2.5. Personel, Kurum tarafından kendisine teslim edilmiş veya erişim yetkisi verilmiş olan gizli kalması gereken bilgileri, sadece görevi ile ilgili işler için kullanır. Bu bilgileri kendi gizli bilgisi gibi korur ve bilmesi gereken yetkili kişiler haricinde hiç kimse ile paylaşmaz. Personel, bilgi paylaşabileceği kişiler konusunda tereddütte kalırsa, bilginin sahibi olan veya süreci yöneten birim ile irtibata geçerek bu bilgileri kimlerle paylaşabileceğini teyit eder.

2.6. Personel, özel olarak yetkilendirildiği durumlar dışında, hizmet verilen tarafların yetkilileri de dâhil olmak üzere yetkisi olmayan hiç kimse ile gizli kalması gereken bilgileri paylaşmaz. Yetkisi olmadığı halde, bulunduğu görev ve makamı kullanarak kendisinden bu bilgileri talep eden kişileri yöneticisine bildirir.

2.7. Personel, görevi kapsamında kendisine teslim edilmiş olan gizli kalması gereken bilgileri, ilgili mevzuata uygun olarak korur, işler ve aktarır. Bu bilgileri, yetkisi olmayan üçüncü kişilerin yanında konuşmaz.

2.8. Personel, gizli kalması gereken bilgileri hiçbir kişi, grup, kurum veya kuruluşun menfaati için kullanmaz.

2.9. Personel, görevi ile ilgili olsun veya olmasın, edindiği ve gizlilik arz eden her türlü bilgiyi sır olarak saklamak ve bunları üçüncü kişilere hiçbir şekilde iletmemekle yükümlüdür. Bu yükümlülük, personelin Kurum ile ilişkisinin sona ermesi halinde de süresiz olarak devam eder.

2.10. Personel, görevi nedeniyle edindiği gizli bilgiler hakkında, yasal zorunluluklar ve kurum tarafından resmi olarak izin verilmesi halleri dışında, yazılı veya sözlü açıklama yapamaz.

2.11. Personel, görevi kapsamında erişim hakkının bulunduğu sistemleri ve bilgileri, yetkisi içinde ya da yetkisini aşarak kendisine veya bir başkasına çıkar sağlamak amacıyla kullanamaz.

2.12. Personel, bilgi sistemlerinde kullanılan/yer alan programları, verileri veya diğer unsurları hukuka aykırı olarak ele geçirme, değiştirme, silme girişiminde bulunamaz ve bunları nakledemez veya çoğaltamaz.

2.13. Personel, Kurumun bilgisi veya onayı dışında, proje ve faaliyetlerde kullanılan veriler ve sistemler üzerinde, görevin gerektirdiği iş ve işlemler dışında değişiklik yapamaz.

2.14. Personel, hangi amaçla olursa olsun görevi kapsamında Kurumda edindiği bilgileri, proje ve faaliyetlerde kullanılan çeşitli şekillerde (basılı, dijital, manyetik vb.) bulunabilecek olan verileri yetkisiz ve izinsiz olarak kullanamaz, kopyalayamaz, taşıyamaz ve aktaramaz.

2.15. Personel, Kurum tarafından kendisine emanet edilen bilgisayar, tablet, telefon, taşınabilir medya gibi cihazları sadece göreve yönelik, kurumsal faaliyetler için kullanır. Bu cihazlarda kurumun bilgisi dışında hiçbir mekanik ya da yazılımsal yapılandırma değişikliği yapamaz.

2.16. Personel, Kurum tarafından kendisine verilen ya da tanımlanan kullanıcı adı/parolayı hiç kimseyle paylaşmaz. Parolasının gizli kalması için gereken tüm tedbirleri alır. Kurumdan ayrılması halinde kullanıcı adı/parolayı iptal ettirir. Kullandığı bilgisayar ve/veya diğer veri depolama ortamlarına oluşturduğu veri, bilgi ve belgeler dâhil tüm belgeleri, cihazları ve ofis malzemelerini eksiksiz olarak ilgilisine teslim eder ve bunların hiçbir kopyasını alamaz.

2.17. Personel, Bakanlık ve/veya Kurum sunucuları üzerinden kendisine tahsis edilen e-İmza/mobil imza, kullanıcı adı/parola ve/veya IP/MAC adresini kullanarak gerçekleştirdiği her türlü etkinlikten, kurum bilişim kaynakları kullanılarak oluşturduğu ve/veya kendisine tahsis edilen kurum bilişim kaynağı üzerinde bulundurduğu her türlü içerikten (belge, doküman, yazılım vb.) sorumludur.

2.18. Personel, 5651 sayılı kanun gereği tutulması gereken kayıtlara ilave olarak; Kurum tarafından uygun görülen diğer sistemlerin, uygulamaların, kullanıcı işlemlerinin, bilgi sistem ağındaki verilerin ve veri akışının iz kayıtlarının hukuki ve idari süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla tutulabileceğini peşinen kabul eder.

2.19. Bakanlık/Kurum tarafından kişilere tahsis edilen e-Posta hesabı sadece işle ilgili kurumsal faaliyetler için kullanılır. Personel, kendi hesabı kullanılarak gönderilen tüm e-Postalardan kişisel olarak sorumludur.

2.20. Personel, sosyal medya hesaplarını kullanırken görevinin gerektirdiği dikkat ve özeni gösterir. Kuruma ait gizli kalması gereken bilgiler, sosyal medya ortamlarında paylaşılmaz.

2.21. Kişinin kendi kusuru nedeniyle parolasının ifşa olması durumunda, başkası tarafından yapılmış olsa dahi, personele teslim edilen kullanıcı adı ve parolalar ile yapılan iş ve işlemlerden, ilgili personel şahsen sorumludur.

2.22. İşbu sözleşme iki nüsha olarak imzalanır, bir nüshası Kurumun Personel biriminde saklanır. Diğer nüshası ise personelin kendisine verilir.

2.23. Kurumda görev yapan Personel, çalışma süresi sona erdiğinde ya da kurumdan ilişiği herhangi bir gerekçeyle kesildiğinde, İşten Ayrılma Formunu doldurur ve ilgili birim sorumlusuna teslim eder.

---

[4] Uygun olanı yazılır. Diğerleri silinir.

3.**Yaptırımlar:**

3.1. Yukarıda sayılan kurallardan biri ya da birkaçının ihlâlinin tespit edilmesi halinde, güvenlik ihlâline yol açan personel hakkında işlem başlatılır.

3.2. Yapılan ihlalin ilgili kanunlar gereği suç ve ceza öngören bir fiil olması halinde, ilgili personel hakkında suç duyurusunda bulunulur.

3.3. Ayrıca idari bir tedbir olarak, yapılan ihlalin 3.2 maddesinde belirtildiği şekilde suç olup olmadığına bakılmaksızın, Kurum tarafından ihtiyaç duyulması halinde; 657 Sayılı Devlet Memurları Kanununa tabi olanlar için aynı kanunun 125. maddesinde sayılan hükümlere göre, 657 Sayılı Devlet Memurları Kanununun dışında kalan çalışanlar ile ilgili olarak (danışmanlar, firma personeli vb.) sözleşmelerinde belirtilen özel hükümlere göre, yoksa genel hükümlere göre idari işlem tesis edilir.

3.4. Kişisel veriler ile gizli bilgilerin hukuka aykırı olarak üçüncü kişilere aktarılması ve/veya onların erişimine açılması ya da kullanımına sunulması hâlinde;

3.4.1. Cezaî bakımdan 5237 sayılı Türk Ceza Kanunu'nun madde 135. vd. hükümlerine,

3.4.2. İdarî bakımdan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 18'inci madde hükmüne,

3.4.3. Hukukî bakımdan 4721 sayılı Türk Medeni Kanunu'nun Madde 23. vd. hükümlerine,

3.4.4. Sözleşme hukuku kapsamında muhtelif konulara ilişkin süreçler bakımından 6098 sayılı Türk Borçlar Kanunu'nun madde 112. vd. hükümlerine göre, söz konusu hükümlerin ilgili durum bakımından yasal uygulama alanlarının bulunduğu ölçüde, yetkili merci ve kişilerce işlem tesis edilir.

Yukarıda sıralanan yükümlülüklere uygun davranacağımı, bu yükümlülüklerden bir veya birkaçına herhangi bir şekilde uygun davranmamam halinde, doğabilecek her türlü idari, mali, hukuki ve cezai yaptırımların uygulanabileceğini kabul ve beyan ederim.

İLGİLİ PERSONELİN	
T.C. Kimlik No	
Adı Soyadı	
Cep Telefonu	
İkametgâh Adresi	
e-Posta Adresi	
Çalıştığı Firma & Kurum	
Çalıştığı Proje & Birim	
Proje & Sözleşme Bitiş Tarihi	
İmza	

28. Formlar

Ayrıcalıklı Erişim Talep Formu

BİLGİ İŞLEM BİRİMİ **AYRICALIKLI ERİŞİM TALEP FORMU**	
ADI SOYADI	
TC KİMLİK NUMARASI	
ACTIVE DIRECTORY KULLANICI ADI	
BİRİM ADI	
E-POSTA ADRESİ	
KULLANILACAK CİHAZA AİT IP/MAC ADRESİ	
AYRICALIKLI ERİŞİM TÜRÜ **(WEB SAYFASI, PORT, UYGULAMA vb.)**	
AYRICALIKLI ERİŞİM ZAMAN ARALIĞI	
AYRICALIKLI ERİŞİM NEDENİ	

AÇIKLAMA: Bu formun eksiksiz olarak doldurularak, ıslak imzalı olarak BİLGİ İŞLEM BİRİMİ'ne teslim edilmesi gerekmektedir. Formdaki bilgiler kişiye özeldir ve gizlilik değeri bulunmaktadır. Bu sebepten ötürü talep formunun doldurulduktan sonra zarf içerisinde ilgili Bilgi İşlem Personeline teslim edilmesi gerekmektedir. Ayrıcalıklı erişim talebi ile ilgili geri bildirim, formda girilmiş olan e-posta adresine gönderilecektir.

SÖZLEŞME

1. Bilgi İşlem Birimi tarafından; kurumsal kaynakların etkin olarak kullanılması, 5651 sayılı kanundan kaynaklanan uyum zorunlulukları, veri güvenliğinin sağlanması, zararlı içerik ve yazılımlardan korunma vb. maksatlarla internet, port ve uygulama erişimleri kısıtlaması yapılmaktadır. Bu kısıtlama ile ilgili politikalar belirlenirken aşağıdaki hususlar dikkate alınır:
   1.1. Ulusal Siber Olaylara Müdahale ekibi (USOM) ve Siber Olaylara Müdahale Birimi (SOME) tarafından yayınlanan zararlı içerik barındıran URL adresleri erişime kapatılır.
   1.2. Virüs, Spyware, Malware, Trojen, Spam, Solucan, Hacking (korsan), Fishing (oltalama) saldırıları içerdiği tespit edilen güvenlik seviyesi düşük internet sitelerine erişimler kapatılır.
   1.3. Alkol, sigara, uyuşturucu, silah vb. sağlığa zararlı ürünlerin reklam ve satış sitelerinin erişimleri engellenir.
   1.4. Erotik içerikli siteler, çocuk istismarı, bahis ve kumar siteleri, oyun siteleri erişime kapatılır.
   1.5. Kurumun internet bant genişliğini olumsuz etkileyen uygulama ve sitelerin (Torrent, P2P, Streaming Media, Download vb.) erişimleri engellenir.
   1.6. Basın yayın organlarını takip ederek raporlamakla sorumlu personel haricindeki tüm personelin dizi, film ve TV erişimleri kapatılır.
   1.7. Kuruma ait sosyal medya hesaplarını yönetmekle sorumlu personel dışındaki tüm personelin Facebook, Twitter, Instagram vb. uygulamalara erişimleri engellenir veya bant genişliği sınırlaması yapılır.
   1.8. Youtube, Vimeo, Dailymotion gibi platformlarda erişimlerle ilgili olarak sadece ihtiyaç duyan personele izin verilir veya bu platformlara erişimlere bant genişliği sınırlaması yapılır.
2. Ayrıcalıklı erişim sağlanan personel, bu erişim ile ilgili oluşabilecek her türlü problemden birinci dereceden sorumlu olarak kabul edilir.
3. Ayrıcalıklı erişim sağlanan personelin işinden ayrılması, görev değişikliği, bu erişim hizmetinin kullanılmasının gerekli olmadığına karar verilmesi, herhangi bir sebepten dolayı erişimin güvenlik riski içerdiğinin tespit edilmesi vb. durumlarda erişimin kapatılması için Bilgi İşlem Birimine bilgi verme sorumluluğu hizmet alan personele aittir.
4. Ayrıcalıklı erişim hizmeti kurumun bilgi güvenliği politikaları dışında kullanılamaz.
5. Bu form ile verilen ayrıcalıklı erişim hizmeti, sadece erişim talebi yapan ilgili personelin kullanımı içindir, üçüncü şahıslarla paylaşılamaz, amacı dışında kullanılamaz.
6. Personele verilmiş olan ayrıcalıklı erişim hizmetinin bu sözleşmeye aykırı bir biçimde kullanıldığının tespit edilmesi durumunda ayrıcalıklı erişim hakkı iptal edilip, ilgili personel hakkında yasal işlem başlatılır.
7. Personele verilen ayrıcalıklı erişim, güvenlik vb. gerekçelerle Bilgi İşlem Birimi tarafından ilgili personele e-posta yoluyla haber verilmek sureti ile kapatılabilir.

Sözleşmede bulunan tüm maddeleri okudum ve kabul ediyorum.

TALEP EDEN KİŞİNİN İMZASI	**YÖNETİCİ ONAYI**
…./…./2018	**…./…./2018**

Uzak Bağlantı Talep Formu

BİLGİ İŞLEM BİRİMİ
BİLGİ SİSTEMLERİ UZAK BAĞLANTI
TALEP FORMU

ADI SOYADI:	
TC KİMLİK NUMARASI:	
ACTIVE DIRECTORY KULLANICI ADI	
BİRİM ADI/FİRMA ADI:	
CEP TELEFONU:	
E-POSTA ADRESİ:	
UZAK BAĞLANTI YAPILACAK SİSTEM (SUNUCU, UYGULAMA, KLASÖR vb.)	

AÇIKLAMA: Bu formun eksiksiz olarak doldurularak, ıslak imzalı olarak BİLGİ İŞLEM BİRİMİ 'ne teslim edilmesi gerekmektedir. Formdaki bilgiler kişiye/firmaya özeldir ve gizlilik değeri bulunmaktadır, bu sebepten ötürü talep formunun doldurulduktan sonra zarf içerisinde ilgili personele teslim edilmesi gerekmektedir. Uzak bağlantı talebine ait erişim bilgileri bu formda girilmiş olan e-posta adresine gönderilecektir.

SÖZLEŞME

1. Bilgi Sistemlerine uzak bağlantı ile erişim sağlayan personel / firma, bu bağlantı ile oluşabilecek her türlü problemden ötürü, birinci dereceden sorumlu olarak kabul edilir.
2. Uzak bağlantı hizmetini kullanan personelin işinden ayrılması, firmanın sözleşmesinin bitmesi, uzak bağlantı hizmetinin kullanılmasının gerekli olmadığına karar verilmesi, herhangi bir sebepten dolayı bağlantının güvenlik riski içerdiğinin tespit edilmesi vb. durumlarda bağlantının kapatılması için bilgi işlem birimine bilgi verme sorumluluğu uzak bağlantı hizmetini kullanan personel / firma'ya aittir. Bu sebepten ötürü oluşabilecek her türlü problemden personel / firma birinci dereceden sorumlu olarak kabul edilir.
3. Bağlantı kurulan bilgi sistemi, kurumun bilgi güvenliği politikaları dışında kullanılamaz.
4. Bu form ile erişim talebi yapan personele / firmaya verilmiş olan erişim bilgileri sadece ilgili personelin / firmanın kullanımı içindir, üçüncü şahıslarla paylaşılamaz, amacı dışında kullanılamaz.
5. Bağlantı ve erişim bilgileri güvenli olmayan bilgisayar, internet (mail, ftp, filesharing) veya yazılı bastırılmış doküman vb. üzerinde saklanamaz.
6. Erişim bilgilerinin sorumluluğu, talebi yapan personelin / firmanın kendisine aittir. İlgili personel /firma erişim bilgilerinin illegal olarak üçüncü şahısların eline geçmemesi için gerekli önlemleri almakla yükümlüdür. (Örnek: Kullandığı bilgisayarın virüs, casus veya zararlı yazılım barındırmaması, internet kafelerden erişim yapılmaması vb.)
7. Personel / firma uzak bağlantı ile erişim yaptığı bilgi ve belgeleri amacı dışında kullanamaz, dağıtımını yapamaz.
8. Personele / firmaya verilmiş olan erişim bilgilerinin bu sözleşmeye aykırı bir biçimde kullanıldığının tespit edilmesi durumunda erişim hakkı tekrar verilmemek üzere iptal edilip, ilgili personel / firma hakkında yasal işlem başlatılacaktır.
9. Personele / firmaya verilen erişim bilgileri güvenlik vb. gerekçelerle Bilgi İşlem Birimi tarafından ilgili personele / firmaya e-posta yoluyla haber verilmek sureti ile değiştirilebilecektir.

Sözleşmede bulunan tüm maddeleri okudum ve kabul ediyorum.

TALEP EDEN KİŞİNİN İMZASI	**YÖNETİCİ ONAYI**
…./…./2018	**…./…./2018**

İşe Başlayış Formu

İZMİR İL SAĞLIK MÜDÜRLÜĞÜ

İŞE BAŞLAYIŞ FORMU

ADI SOYADI	
UNVAN	
SİCİL NO	
BAŞKANLIK / BİRİM	
GÖREVE BAŞLAMA/GÖREV DEĞİŞİKLİĞİ TARİHİ	

TAMAMLANMASI GEREKEN İŞLEMLER	**İLGİLİ BİRİM / KİŞİ**	**İŞLEMİ YAPAN AD SOYAD İMZA**
Kurum Kimlik Kartı çıkarılması	Personel Hizmetleri Başkanlığı	
Oryantasyon eğitimi	Eğitim Birimi	
Birime görevlendirme	Personel Hizmetleri Başkanlığı	
Birimde başlayış yazısı	İlgili Birim Sorumlusu	
Bilgi Güvenliği eğitimi	Bilgi İşlem Birimi	
Personel Gizlilik Sözleşmesi imzalatılması	Birim Sorumlusu	
Kullanıcı hesabı, parola ve yetki tanımlanmaları	Bilgi İşlem Birimi	
Zimmet oluşturulması	Ambar Birimi	

İŞE BAŞLAYAN AD-SOYAD-İMZA	**BİRİM SORUMLUSU AD-SOYAD-İMZA**
Form Doldurulma Tarihi: …. / …. / 20…..	

İşten Ayrılış Formu

İZMİR İL SAĞLIK MÜDÜRLÜĞÜ

İŞTEN AYRILIŞ FORMU

ADI SOYADI	
UNVAN	
SİCİL NO	
BAŞKANLIK / BİRİM	
GÖREVDEN / İŞTEN AYRILMA TARİHİ	

TAMAMLANMASI GEREKEN İŞLEMLER	**İLGİLİ BİRİM / KİŞİ**	**İŞLEMİ YAPAN AD SOYAD İMZA**
Yapılan iş ve işlemlerle ilgili doküman ve bilgi devri yapılması	Birim Sorumlusu	
Bilgi ve gereği klasörleri boşaltılarak, EBYS hesabı pasife alınması	Bilgi İşlem Birimi	
Birim ile ilgili e-posta gruplarından çıkartılması	Bilgi İşlem Birimi	
Bilişim sistemleri uygulamalarında kullanıcı ve yetki iptali	Bilgi İşlem Birimi	
Bilişim malzemelerinin Bilgi İşlem Birimine teslimi	Bilgi İşlem Birimi	
Zimmet devri	Ambar Birimi	
Kurum Kimlik Kartının teslimi	Personel Hizmetleri Başkanlığı	
Birimden ayrılış yazısı	Birim Sorumlusu	

AYRILIŞ YAPAN PERSONEL AD-SOYAD-İMZA	**BİRİM SORUMLUSU AD-SOYAD-İMZA**
Form Doldurulma Tarihi: …. / …. / 20…..	