# A. BİLGİ GÜVENLİĞİ

1. Bilgi Güvenliği Nedir?

Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir işletme ve kurum için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği ise "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır.

Bilgi güvenliğine duyulan ihtiyaçla birlikte, güvenliğin sağlanması için bilinçli personel barındırmak ve güvenlik sürecinin işletilmesi için yeterli doküman ve prosedürlerin oluşturulması da bir zorunluluk olmuştur. Bilgi güvenliği, bu politikada aşağıdakilerin korunması olarak tanımlanır:

- **Gizlilik:** Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etmek,
- **Bütünlük:** Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek,
- **Kullanılabilirlik:** Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

2. Bilgi Güvenliği Amaçları:

Bilgi Güvenliğinin hedefi her seviyede kullanıcıya Bilgi Sistemleri'ni kullanımları sırasında ne şekilde hareket etmeleri gerektiği konusunda yol göstermek, kullanıcıların bilinç ve farkındalık seviyelerini artırmak ve bu şekilde bilgi sistemlerinde oluşabilecek riskleri minimuma indirmek, kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamaktır.

3. Bilgi Güvenliği Kapsamı ve Temel İlkeler:

**3.1.** Tüm yöneticiler, yönetim alanları ve yerine getirmekle yükümlü oldukları tüm iş ve işlemlerin yürütülmesinde kullandıkları bilgi sistemleri ile ilgili olarak; bilgi güvenliği duyarlılığı çerçevesinde hareket etmekle, yönetim alanları ve işleri ile ilgili olarak bilgi güvenliği iş planı hazırlamakla ve yürürlüğe koymakla yükümlüdürler.

**3.2.** Her kullanıcı Kılavuzda yer alan kişisel veya çalışma alanı ile ilgili hususlara uymakla yükümlüdür.

**3.3.** Kullanıcı, bilgi sistemleri ve ağlarının güvenliğinin gerekliliği ve güvenliği artırmak için neler yapabileceği konularında bilinçli olmalıdır.

**3.4.** Tüm yöneticiler kendi sorumluluk alanlarındaki bilgi sistemleri ve ağlarının güvenliğinden sorumludurlar.

**3.5.** Kullanıcı, güvenlik tehditlerini önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmekten sorumludur.

**3.6.** Kullanıcılar, bilgi sistem ve ekipmanlarının kullanımında birbirlerinin haklarına saygı göstermekle yükümlüdürler.

**3.7.** Kullanıcı, idarece yapılmış olan risk değerlendirmelerinde kendileriyle ya da çalışma alanlarıyla ilgili öngörülen tedbirlere uymak zorundadır.

**3.8.** Kullanıcı, güvenliği; bilgi sistem ve ağlarının önemli bir unsuru olarak değerlendirmelidir.

**3.9.** Yönetim, bilgi güvenliği yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.

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

# B. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

1. Yönetimin Desteği

Yönetim kademeleri bilgi güvenliği konusunda ısrarcı olmalı, alt kademelerde bulunan personele sorumluluk verme ve örnek olma konusunda yardımcı olmalıdır. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, kurumun en alt kademe personeline kadar inilmesi zorunludur. Bu

yüzden kurumdaki yöneticilerin, gerek yazılı gerekse sözlü olarak güvenlik prosedürlerine uymaları, güvenlik konusundaki çalışmalara katılmaları ve güvenlik ile ilgili çalışmalarda bulunan personele destek olmaları gerekmektedir.

2. Bilgi Güvenliği Politikasının Oluşturulması, Güncellenmesi ve Gözden Geçirilmesi

*Tüm teşkilatımızda üretilen bilginin de en üst seviyelerde güvenlik anlayışı içerisinde korunması gerektiği bilinci ile hareket eden T.C. Sağlık Bakanlığı misyon ve vizyonuna bağlı kalarak Bilgi Güvenliği konseptinin esasını oluşturan basılı ve elektronik ortamdaki bilgilerin yasal mevzuat ışığında ve risk metotları kullanılarak "gizlilik, bütünlük ve erişilebilirlik" ilkelerine göre yönetilmesi amacıyla;*

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

*ana politikalar olarak öngörülmektedir.*

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yöneticisi sorumludur.

Bilgi Güvenliği Politikası Dokümanı, en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa kayıt altına alınıp değerlendirilerek Yönetime onaylatılmalıdır. Her değişiklik tüm kullanıcılara e-mail, sunucu üzerinden ya da yazılı olarak yayımlanmalıdır. Gözden geçirmelerde;

- Politikanın etkinliği, kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenmelidir.
- Politikanın güncelliği teknolojik değişimlerin etkisi vasıtasıyla gözlemlenmelidir.
- Politikanın güncelliği değişen personelle birlikte gözden geçirilmeli, yeni personelin katılımı sağlanmalıdır.
- Politika, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilmelidir.

3. Bilgi Güvenliği Altyapısı

Bilgi güvenliği ile ilgili tüm faaliyetlerden BGYS Yöneticisi sorumludur. Kurumlarda BGYS ile ilgili kapsamlı çalışmalar, Üst Yönetim tarafından oluşturulacak komisyon marifetiyle yürütülmektedir. Bu anlamda BGYS Yöneticisi Başkanlığında oluşan bir komisyon oluşturularak iletişim ile yürütme ve yönetim faaliyetleri gerçekleştirilmelidir.

İletişim faaliyetleri kapsamında BGYS komisyonu, BGYS Yöneticisi tarafından belirlenen periyotlarla toplanmalıdır. Bu koordinasyon toplantılarının amacı Sağlık Bakanlığı tarafından yayımlanan Bilgi Güvenliği Politikaları Kılavuzu doğrultusunda oluşturulan prosedürlerin birimlerde bulunan diğer personele aktarılması, birimlerin BGYS ile alakalı görüş ve önerilerinin çalışmalara ek bilgi olarak aktarılması amaçlanmaktadır. BGYS Komisyonu en az yılda bir kez toplanmalıdır.

Yürütme ve yönetim faaliyetleri kapsamında ise BGYS komisyonu, politikaları gözden geçirme, eylem planı oluşturma, karar alma ve uygulama faaliyetlerini yerine getirmeli ve komisyon toplantılarında toplantı gündemi aşağıdaki maddeleri içermelidir;

- Bilgi güvenliği politikalarının ve sorumlulukların gözden geçirilmesi,
- Büyük tehditlere karşı varlıklardaki önemli değişikliklerin değerlendirilmesi,
- Bilgi güvenliği olaylarının ve hatalarının gözden geçirilmesi,
- Bilgi güvenliği için önceliklerin gözden geçirilmesi.

4. Roller ve Sorumluluklar

### 4.1. Birim Sorumlularının Sorumlulukları

**4.1.1.** BGYS Politikasını uygulamak.

**4.1.2.** Kendisine bağlı çalışan personelin kurumsal uygulama ve özel erişim yetkilerini onaylamak.

**4.1.3.** Kendisine bağlı kısımda çalışacak üçüncü taraf bilgi sistemleri kullanıcılarının politikalardan haberdar olmasını sağlamak.

**4.1.4.** Fark ettiği veya kendisine çalışanları aracılığıyla iletilen bilgi sistemleri ile ilgili güvenlik problemlerini BGYS Yöneticisine bildirmek.

**4.1.5.** Sahibi olduğu bilgi varlığını korumak, varlıkları gözden geçirmek ve gerektiğinde BGYS Yöneticisine güncelleme talebinde bulunmak.

### 4.2. BGYS Yöneticisinin Sorumlulukları

**4.2.1.** BGYS Komisyonun gündemini belirlemek, alınan kararların uygulanmasını takip etmek.

**4.2.2.** Eğitimleri planlamak ve gerçekleştirmek.

**4.2.3.** BGYS Komisyonunun hazırlamış olduğu dokümanları onaylamak ve uygulanmasını sağlamak.

**4.2.4.** BGYS Komisyonunun yapmış olduğu faaliyetleri kontrol etmek ve onaylamak.

**4.2.5.** Gereken iyileştirmeler ve geliştirmeler konusunda üst yetkililere brifingler vermek.

**4.2.6.** Bilgi güvenliği ile ilgili konularda bölümler ve dış servis sağlayıcıları arasında koordinasyonu sağlamak.

**4.2.7.** BGYS Komisyonu tarafından hazırlanan Güvenlik Politikasını gözden geçirerek üst yönetimin onayına sunmak.

### 4.3. Kullanıcıların Sorumlulukları

**4.3.1.** Bilgi Güvenliği Politikasına uymak.

**4.3.2.** Herhangi bir bilgi güvenliği olayını fark ettiğinde, zaman geçirmeden Teknik Servis Uygulamasına kayıt girmek ve acil durumlarda telefon ile bilgi vermek.

**4.3.3.** Kendisine ait olan hesapların şifrelerinin (varsa e-anahtarının) güvenliğini sağlamak.

**4.3.4.** Taşınabilir cihazların güvenliğini sağlamak, yetkilendirme olmadan kurum dışına varlık çıkarmamak.

**4.3.5.** Bütün PC ve dizüstü bilgisayarları otomatik olarak 10 dakika içerisinde şifreli ekran korunmasına geçecek şekilde ayarlamak.

**4.3.6.** Dizüstü bilgisayarları güvenlik açıklarına karşı daha dikkatli kullanmak ve işletim sistemi şifrelerini aktif hale getirmek.

**4.3.7.** Kurumda domain (çalışma alanı) yapısı varsa mutlaka login olmak, domain'e bağlı olmayan bilgisayarları yerel ağdan çıkarılmak ve yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapmamak.

**4.3.8.** Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Birimi 'ne haber vermek.

**4.3.9.** Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan (örnek, elektronik bankacılık vs.) bilgisayarın sahibi sorumludur.

**4.3.10.** Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmamak.

**4.3.11.** Kurumun e-posta sistemini, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kullanmamak.

**4.3.12.** Ağ güvenliğini (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket sniffing, paket spoofing, denial of service vs. ) gibi eylemlerden kaçınmak.

**4.3.13.** Port veya ağ taraması yapmamak ve Ağ güvenliğini tehdit edici faaliyetlerde bulunmamak. DoS saldırısı, port-network taraması vb. yapmamak.

**4.3.14.** Kurum bilgilerini kurum dışından üçüncü şahıslara iletmemek.

**4.3.15.** Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapmamak.

**4.3.16.** Cihaz, yazılım ve veriyi izinsiz olarak kurum dışına çıkarmamak.

**4.3.17.** Şifreleri başkası ile paylaşmamak, kağıtlara ya da elektronik ortamlara yazmamak.

**4.3.18.** Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD'leri veya internetten indirilen programlar vs) kurmamak ve kullanmamak.

**4.3.19.** Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem göstermek. Bu verileri, Bakanlığımızın bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kâğıt ortamında üçüncü kişi ve kurumlara vermemek.

**4.3.20.** Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarında kurumsal bilgilerin düzenli olarak farklı ortamlara (cd, dvd, usb, external harddisk vs.) yedeklenmesinden sorumludur.

**4.3.21.** Bilgisayarlarda oyun ve eğlence amaçlı programları çalıştırmamak/ kopyalamamak.

**4.3.22.** Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunmamak.

**4.3.23.** İlgili BGYS Sorumlusu ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri v.b. üzerinde mevcut yapılan düzenlemeleri hiçbir surette değiştirmemek.

**4.3.24.** Bilgisayarlara herhangi bir şekilde lisanssız program yüklemek.

**4.3.25.** Gerekmedikçe bilgisayar kaynaklarını paylaşıma açmamak, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket etmek.

**4.3.26.** Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde mesajlaşma ve sohbet programları gibi chat programlarını kullanmamak. Bu chat programları üzerinden dosya alışverişinde bulunmamak.

**4.3.27.** Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmemek.

**4.3.28.** İş ile ilgili olmayan (müzik, video dosyaları ) yüksek hacimli dosyalar göndermemek (upload) ve indirmemek (download).

**4.3.29.** İnternet üzerinden kurum tarafından onaylanmamış yazılımları indirmemek ve Kurum sistemleri üzerine bu yazılımları kurmamak.

**4.3.30.** Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girmemek ve dosya indirimi yapmamak.

5. Risk Yönetimi

**5.1. Varlıkların Belirlenmesi, Sınıflandırılması ve Denetimi**

**Varlık:** Bir kurum için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır.

- Bilgi,
- Donanım (kişisel bilgisayarlar, yazıcılar, sunucular),
- Yazılım (işletim sistemleri, geliştirilen uygulamalar, ofis programları),
- Haberleşme cihazları (telefonlar, hatlar, kablolar, modemler, anahtarlama cihazları),
- Dokümanlar(stratejik toplantıların tutanakları, sözleşmeler vb.),
- Üretilen mallar,
- Servisler,
- Personel,
- Kurumun itibarı / imajı.

**5.1.1.** Kurum bünyesinde kullanılmakta olan her bir varlık envanter kayıtlarına geçirilmelidir. Envanter kayıtları sürekli olarak güncel tutulmalı ve yeni varlıklar envanter kayıtlarına hemen girilmelidir.

**5.1.2.** Belli başlı bilgi, yazılım, donanım ve hizmet varlıkları için sahipler atanmalı ve varlıkların sahipleri envanter kayıtlarında bulunmalıdır. Herhangi bir bilgi teknolojisi varlığının sahibi olarak belirlenmiş personel, bu varlığın korunmasından sorumludur.

**5.1.3.** Tüm bilgi, veri ve dokümanlar anlaşılır bir biçimde etiketlenmelidir. Bilgi varlıklarının sınıflandırılmasından ve bu sınıflandırmanın belirli zamanlarda gözden geçirilmesinden BGYS Yöneticisi sorumludur. Gerektiğinde BGYS yöneticisi sınıflandırmayı belirleyebilir veya belirlemek üzere komisyonun tamamını ya da komisyon üyelerinden birini görevlendirebilir.

**5.1.4.** Varlık envanterinde kaydı bulunan her türlü varlık performans ve yeterlilik kapsamında yardımcı programlar vasıtasıyla, sürekli gözden geçirilmelidir. Yetersizlik veya ihtiyaç durumlarında değişim planlaması yapılarak satın alma süreci başlatılmalıdır.

**5.1.5.** Erişim kontrol prosedürü ve risk analizi tedavi planı hazırlanırken varlık envanteri listesi göz önünde bulundurulmalıdır.

### 5.2. İşletim, Tehdit ve Olay Yönetimi Prosedürleri

Kurum içi donanım ve uygulamaların işletim prosedürleri hazırlanmalı ve aşağıdaki hususlara uyulmalıdır:

**5.2.1.** Yazılı prosedürler ihtiyaç duyulduğunda BGYS Yöneticisi veya onun görevlendireceği komisyon dahili üyesi yada üyeler tarafından hazırlanır ve üst yönetim tarafından onaylanarak güncellenir.

**5.2.2.** Onaylı olmayan işletim prosedürleri geçersizdir. Geçerlilik onayı için üst yönetim ve BGYS yöneticisinin imzalaması gereklidir.

**5.2.3.** Kurum genelinde tüm işletim prosedürleri yazılı olarak bulunur ve ihtiyaç duyulduğunda sürekli erişilebilen ortamlarda yayınlanır (web, basılı doküman, vs.).

**5.2.4.** Prosedürlerin süreklilikleri atanmış sahipleri tarafından kontrol edilmeli, değişen işletim talimatları prosedürlere yansıtılmalıdır.

**5.2.5.** Bilgi güvenliği ihlal olayı olarak değerlendirilen her durum için düzeltici önleyici faaliyet ve sonuç raporu oluşturulmalıdır.

**5.2.6.** Belirlenen eksiklikler tamamlanarak olayların tekrar gerçekleşmesinin önüne geçilmelidir.

## C. POLİTİKALAR

1. İnsan Kaynakları ve Zafiyetleri Yönetimi

**1.1.** Tüm çalışanlar, kurumun bilgi güvenliği politikalarına uymakla yükümlüdürler. Kullanıcılar, politikalara uygun olmayan davranışları sonucu meydana gelebilecek bilişim olaylarından sorumlu olacaklardır.

**1.2.** Kurum çalışanları, kurum personeli olduğu sürece ve kurumdan ayrılmaları (emeklilik, istifa, vs.) durumlarında kurum bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur. Bu nedenle güvenlik politikaları ve prosedürleri konusunda gerekli taahhütnameler hazırlanmalı ve ilgili personele imzalatılmalıdır.

**1.3.** Tüm kurum personeline Bilgi güvenliği farkındalık eğitimi verilmelidir. Bu eğitimler, her yeni personel alımı sonrasında yeni personel için de tekrarlanmalıdır.

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

**1.5.** Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.

**1.6.** ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.

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

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

**1.9.** Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

**1.10.** Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.

**1.11.** Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

**1.12.** Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

2. Fiziksel ve Çevresel Güvenlik

**2.1. Fiziksel Güvenlik Sınırı**

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

**2.1.2.** Bilgi işlem servisini korumak amacıyla herhangi bir fiziksel sınır güvenliği tesisi kurulmuş olmalıdır.

**2.2. Fiziksel Giriş Kontrolleri**

**2.2.1.** Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmalıdır.

**2.2.2.** Kapsam ve prosedürü idarelerce belirlenmek suretiyle ziyaretçilerin giriş ve çıkış zamanları kaydedilmelidir

**2.2.3.** Kapsam ve prosedürü idarelerce belirlenmek suretiyle tüm personel ve ziyaretçiler güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartlarını devamlı takmalıdır

**2.2.4.** Güvenli alanlara erişim hakları düzenli olarak gözden geçiriliyor olmalıdır.

**2.2.5.** Personel, önemli varlıkların bulunduğu güvenli alanlarda sigara içmemeli, yiyecek ve içecekle güvenli alana girmemelidir.

**2.3. Ofislerin ve Odaların Güvenliğinin Sağlanması**

**2.3.1.** Ofisler ve odalarla ilgili fiziksel güvenlik önlemleri alınmalıdır.

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

**2.3.3.** Binada bilgi işlem faaliyetlerinin yürütüldüğüne dair işaret tabela vb bulunmamasına dikkat edilmelidir.

**2.4. Harici ve Çevresel Tehditlerden Korunma**

**2.4.1.** Yangın sel deprem patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.

**2.5. Güvenli Alanlarda Çalışma**

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

**2.5.2.** Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor olmalıdır.

**2.5.3.** Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir

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

3. Ekipman Güvenliği

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 tehditleri yok edebilmek için aşağıda yer alan belli başlı temiz masa kurallarına ilişkin politikalar geliştirilmeli ve bu politikalardan çalışanların haberdar olması sağlanmalıdır.

**3.1. Belli Başlı Temiz Masa Kuralları;**

**3.1.1.** Hassas bilgiler içeren evraklar bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir. Bu bilgi ve belgelerin kilitli yerlerde muhafaza edilmesi gerekmektedir

**3.1.2.** Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir Bu işlem Windows + L tuşuna basılarak yapılabilir

**3.1.3.** Sistemlerde kullanılan şifre telefon numarası ve TC kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır

**3.1.4.** Kullanım ömrü sona eren ve artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.

**3.1.5.** Faks makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır.

**3.1.6.** Her türlü bilgiler şifreler anahtarlar ve bilginin sunulduğu sistemler ana makineler (sunucu) PC'ler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

**3.2. Ekipman Yerleşimi ve Koruması;**

**3.2.1.** Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır.

**3.2.2.** Ekipman gereksiz erişim asgari düzeye indirilecek şekilde yerleştirilmelidir

**3.2.3.** Nem ve sıcaklık gibi parametreler izlenmelidir.

**3.2.4.** Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme konularını düzenleyen kurallar olmalıdır.

**3.3. Destek Hizmetleri;**

**3.3.1.** Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem merkezi için yeterli düzeyde olmalıdır.

**3.3.2.** Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.

**3.3.3.** Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.

**3.3.4.** Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

**3.4. Kablolama Güvenliği;**

**3.4.1.** Hatalı bağlantıların olmaması için ekipman ve kablolar açıkça etiketlenmiş ve işaretlenmiş olmalıdır.

**3.4.2.** Alternatif yol ve iletişim kanalları mevcut olmalıdır.

**3.4.3.** Fiber optik altyapı yapılandırılmalıdır.

**3.4.4.** Bağlantı panelleri ve odalara kontrollü erişim altyapısı kurulmuş olmalıdır.

**3.5. Ekipman Bakımı;**

**3.5.1.** Ekipmanın bakımı doğru şekilde yapılmalıdır.

**3.5.2.** Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılmalıdır.

**3.5.3.** Bakım sadece yetkili personel tarafından yapılıyor olmalıdır.

**3.5.4.** Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutulmalıdır.

**3.5.5.** Ekipman bakım için kurum dışına çıkarılırken kontrolden geçirilmeli, ekipmanın teslimi sırasında marka, demirbaş, seri numara gibi bilgilerin yer aldığı bir tutanak tutulmalıdır.

**3.5.6.** İçindeki hassas bilgiler yedeklenmesi gerekiyorsa yedeklenip silinmelidir.

**3.6. Kurum Dışındaki Ekipmanın Güvenliği;**

**3.6.1.** Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir.

**3.6.2.** Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulmalıdır

**3.6.3.** Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenmelidir.

**3.6.4.** Ekipmanın Güvenli İmhası ya da Tekrar Kullanımı;

**3.6.5.** Ekipman imha edilmeden önce gizli bilginin bulunduğu depolama cihazı fiziksel olarak imha edilmelidir.

**3.6.6.** Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format işlemlerinin ötesinde yeterli düzeyde işlem yapılmalıdır.

4. İşletim Sistemleri ve Son Kullanıcı Güvenliği

**4.1. İşletim Sistemleri Güvenliği**

**4.1.1.** Kurum son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar verir ve bu işletim sistemine uygun yazılım donanım sistemlerinin kurulumunu temin eder.

**4.1.2.** Kurum, işletim sistemlerinin güncel ve güvenli olması için yama ve güncelleme yönetimi yapmalıdır.

**4.1.3.** Kurum, mevcut envanteri haricindeki işletim sistemlerinin kurum bilgisayarlarında kullanımını engellemelidir.

**4.2. Son Kullanıcı Güvenliği**

**4.2.1.** Son kullanıcılar yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir.

**4.2.2.** Son kullanıcıların yetkileri içinde bulundukları grup politikasına göre belirlenmelidir.

**4.2.3.** Son kullanıcıların aktiviteleri güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı loglanarak kayıt altına alınmalıdır.

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

**4.2.5.** Son kullanıcılar bilgisayarlarındaki ve sorumlusu oldukları cihazlardaki işle ilgili bilgilerin gerekiyorsa düzenli olarak yedeklerini almalıdır.

**4.2.6.** Son kullanıcılar güvenlik zafiyetlerine sebep olmamak için bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.

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

**4.2.8.** Son kullanıcılar mesai bitiminde bilgisayarlarını kapatmalıdır.

**4.2.9.** Kullanıcı bilgisayarlarında güncel anti virüs bulunmalı ve otomatik olarak internet üzerinden güncellenmelidir.

5. Parola Güvenliği Politikası

Güvenliğin oluşturulacağı birim için kullanılan programlarda uygulanan parola standardı belirlenmeli, bu parola sistemi aşağıdaki unsurları içerecek standarda getirilmelidir.

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

**5.2.** Parola en az 8 karakterden oluşmalıdır.

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

**5.4.** Büyük ve küçük harfler bir arada kullanılmalıdır.

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

**5.6.** Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi)

**5.7.** Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.

**5.8.** Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

**5.9.** Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.

**5.10.** Parola Yönetim Prosedüründe ayrıca güvenli parola oluşturulması ayrıntılı olarak açıklanmıştır.

6. İnternet ve Elektronik Posta Güvenliği

**6.1.** İnternet sistemi yalnızca iş faaliyetlerini destekleyecek şekilde kullanılmalıdır. Internet kullanımı;

- Kişisel kullanımda, görev amaçlı kullanılabilecek kaynaklar az miktarda kullanılıyorsa,
- Çalışanların verimliliğini engellemiyorsa,
- Herhangi bir iş faaliyetini aksatmıyorsa,
- Kullanıcıların bazı kişisel işlerini daha hızlı yerine getirmesini sağlıyorsa bu tip kişisel kullanıma izin verilebilir.

**6.2.** Kullanıcıların Internet kullanım yoğunluğu diğer kullanıcıların Internet'e ulaşımlarını engelleyecek şekilde olmamalıdır. Dış merkezlerle irtibatlı çalışan Radyoloji, Laboratuvar birimleri, güvenlik yöneticileri, sistem yöneticileri ve bilgisayar operatörleri gibi sistem bakım-idame işlerini yürüten personele ayrıcalıklar tanınabilir.

**6.3.** İnternet kullanımı, içerik kontrolcüleri ve virüs tespit sistemleri kullanılarak sınırlandırılmaktadır. Kullanıcılar, bu kontrollerin yapıldığını bilerek interneti kullanmalı, güvenlik amacıyla konulan önlemleri devre dışı bırakmaya çalışmamalıdır. (Ultrasurf programı gibi)

**6.4.** Çalışanlar işle ilgili olarak kurum tarafından belirlenen e-posta/iletişim ağı hizmetleri (saglik.gov.tr uzantılı) haricinde e-posta hizmeti kullanamazlar.

**6.5.** Hastane ayniyatına kayıtlı ve hastane ağına dahil olmuş bilgisayar ve diğer ekipmanlarda suç veya kanunsuz olması muhtemel olarak görülen her türlü malzemeyi kendi bilgi sistemlerinden çıkarma hakkını ve bununla ilgili resmi işlem başlatma hakkını saklı tutar.

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

**6.7.** İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.

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

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

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

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

**6.12.** E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir.

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

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

**6.15.** Bakanlık 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.

**6.16.** Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir.

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

**6.18.** Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmemelidir.

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

**6.20.** 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.

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

**6.22.** Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

**6.23.** Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalıdır.

**6.24.** Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda saglik.gov.tr uzantılı e-posta hesapları için Bakanlığa acilen başvurulması amacıyla BGYS Yöneticisi ile irtibata geçilmelidir.

7. Sunucu ve Sistem Güvenliği

### 7.1. Sunucu Güvenlik Politikaları

**7.1.1.** Sunucu üzerindeki servislere erişimler kaydedilmeli ve servis erişimleri erişim kontrol yöntemleri ile sağlanmalıdır.

**7.1.2.** Sunucu üzerinde çalışan işletim sistemleri hizmet sunucu yazılımları anti virüs vb koruma amaçlı yazılımlar sürekli güncellenmelidir

**7.1.3.** Güncellemelerde değişiklik yapılacak ise bu değişiklikler önce değişiklik yönetimi kuralları çerçevesinde uygulama sahipleri tarafından test mekanizmasından geçirilmeli onaylanmalı sonra uygulanmalıdır.

**7.1.4.** Kurumda bulunan sunucuların yönetiminden ilgili sunucu yönetimi için yetkilendirilmiş personel sorumludur. Yetkilendirme BGYS Yöneticisi tasarrufunda yapılmalıdır. Görevinden ayrılan personelin tüm erişim yetkileri anında iptal edilmelidir.

**7.1.5.** Sunucu kurulumları, konfigürasyonları, işletim sistemi yedeklemeleri, yamaları, güncellemeleri Uzman Bilgi İşlem Personeli tarafından yapılmalıdır

**7.1.6.** Sunuculara ait bilgilerin yer aldığı envanter veri tabanı oluşturulmalıdır. Bu veri tabanında sunucuların isimleri, IP adresleri, yeri, ana görevi, üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi, işlemlerinden sorumlu personelin isimleri yer almalıdır.

### 7.2. Sahip Olma ve Sorumluluklar İle İlgili Kurallar

**7.2.1.** Kurumda bulunan sunucuların yönetiminden ilgili sunucuyla yetkilendirilmiş personel sorumludur.

**7.2.2.** Sunucu kurulumları konfigürasyonları, işletim sistemi yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılmalıdır

**7.2.3.** Tüm bilgiler sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.

**7.2.4.** Sunucular ile ilgili üçüncü parti firmalar ile yapılacak çalışmalarda ilgili sunucuyla yetkilendirilmiş personel eşlik etmelidir.

8. Ağ Cihazları Güvenliği

### 8.1. Ağ Cihazları Güvenlik Politikası

**8.1.1.** Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.

**8.1.2.** Cihazlar üzerinde yerel kullanıcı hesapları açılmamalıdır.

**8.1.3.** Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması kurumun içerisinden yapılmalıdır.

**8.1.4.** İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.

**8.1.5.** Yönlendirici ve anahtarları Ağ Yönetimi kontrolünde olmalıdır.

**8.1.6.** Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli sonra çalışma günlerinin dışında üretim ortamına taşınmalıdır.

**8.1.7.** Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.

**8.1.8.** Cihazlar Sistem odası gibi yerlerde şifreli kabinlerde konumlandırılmalıdır Sistem odası dışında kalan cihazlar yine uygun kabinlerde kapalı dolap ya da şifreli kabinlerde muhafaza edilmelidir.

### 8.2. Kablosuz Ağlar Güvenliği

**8.2.1.** Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802 lx erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.

**8.2.2.** Kablosuz ağa bağlanacak cihazlar, ilgili kablosuz yayın yapan cihazda MAC filtrelemeyle ağa bağlanmalıdır.

**8.2.3.** Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir. Bu donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.

**8.2.4.** Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

**8.2.5.** Varsayılan SSID isimleri kullanılmamalıdır. SSID ayar bilgisi içerisinde kurumla ilgili bilgi olmamalıdır. (Kurum ismi ilgili bölüm çalışanın ismi vb.)

**8.2.6.** Erişim cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.

**8.2.7.** Kullanıcı bilgisayarlarında kişisel anti-virüs ve güvenlik duvarı yazılımları yüklü olmalıdır.

**8.2.8.** Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

**8.2.9.** Kablosuz erişim noktalarının aktif cihazlara giden kablolamasında fiziksel güvenliğe dikkat edilmelidir.

**8.2.10.** Kablosuz ağa dâhil olan kurum çalışanları için bile erişimler sınırlandırılmalıdır.

9. Mal ve Hizmet Alımları Güvenliği

**9.1.** Mal ve hizmet alımlarında ilgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnamelerde belirtilmelidir.

**9.2.** Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

- Bilgi güvenliği politikası,
- Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,
- Gerekli fiziki koruma için kontrol ve mekanizmalar,
- Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,
- Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,
- Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,
- Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,
- Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,
- Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,
- Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,
- Uygun olduğu yerde personel transferi için hüküm,
- Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,
- Açık bir raporlama yapısı ve anlaşılan raporlama formatı,
- Değişim yönetimi sürecinin açıkça belirlenmesi,
- Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,
- İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,
- Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,
- Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,
- Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,
- Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,
- Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,
- Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,
- Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,
- Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,
- Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,
- Sorun çözümü için bir yükseltme sürecinin kurulması,
- Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dâhil olmak üzere hizmet sürekliliği gerekleri,
- Anlaşmayla ilgili tarafların yükümlülükleri,
- Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak)
- Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,
- Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,
- Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,
- Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.
- Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi,
- Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

**9.3.** Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde

yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.

### 9.4. Gizlilik Sözleşmeleri

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

- Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),
- Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dahil olmak üzere anlaşma süresi,
- Anlaşma sona erdiğinde yapılması gereken eylemler,
- Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi ('bilmesi gereken' gibi),
- Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,
- Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları,
- Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,
- Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesinin bildirimi ve raporlama süreci,
- İade veya imha anlaşmasına bırakılacak bilgi için terimler,
- Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.

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

**9.4.3.** Gizlilik ve ifşa etmeme anlaşmaları uygulandığı yerin geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.

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

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

**9.4.6.** Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçları doğrultusunda farklı şekillerde kullanılmalıdır.

## 10. Uygulama Yazılımları Güvenlik Yönetimi

### 10.1. Yazılım Geliştirme Politikası

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

**10.1.2.** Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

**10.1.3.** Uygulama yazılımlarının kurum içerisindemi hazırlanacağı yoksa satınmı alınacağının belirlenmesi, uygun bir şekilde tanımlanmalıdır.

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

**10.1.5.** Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

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

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

**10.1.8.** Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

**10.1.9.** Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalı ve tutanak altına alınmalıdır.

**10.1.10.** Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

**10.1.11.** Yazılımlar sınıflandırılmalı/etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

**10.1.12.** Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması engellenmelidir.

### 10.2. Güvenlik Donanım ve Yazılımları Yönetimi

**10.2.1.** Bu sunuculara Bilgi İşlem Biriminin admin/root yetkisi bulunmalıdır. Yapılacak tüm işlemler Bilgi İşlem Biriminin nezaretinde yürütülmelidir. Kuruma ait sunucularda, sadece yetkili kişilerin erişebileceği administrator/root yetkisi bulunmalıdır.

**10.2.2.** Kuruma ait sunucular üzerinde bulunan, tüm kullanıcı hesapları (administrator ve root hesapları da dâhil olmak üzere) güçlü şifreler ile korunmalıdır.

**10.2.3.** Yapılacak tüm işlemler düzgün bir şekilde dokümante edilmeli ve ilgili birim sorumlularına iletilmelidir.

**10.2.4.** Güvenlik yazılım ve donanımlarının erişim logları, merkezi log sisteminde tutulmalı ve izlenmelidir.

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

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

**10.2.7.** Güvenlik donanımlarının konfigürasyon yedekleri düzenli olarak alınmalı ve bir back-up sunucusunda tutulmalıdır.

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

**10.2.9.** Kurumda kullanılan güvenlik donanımları, harici izleme yazılım ya da donanımları ile izlenmeli ve cihazlarda oluşan sorunlar sms ve/veya eposta aracılığı ile ilgili sorumlulara iletilmelidir.

**10.2.10.** Kurumun tüm istemcileri ve sunucuları anti-virüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak anti-virüs yazılımı yüklenmeyebilir.

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

**10.2.12.** Kullanıcı hiç bir sebepten dolayı anti-virüs yazılımını bilgisayarından kaldırmamalıdır.

**10.2.13.** Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.

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

**10.2.15.** Optik Media ve harici veri depolama cihazları anti-virüs kontrolünden geçirilmelidir.

11. Bilgi Güvenliği Teknolojileri Güvenliği

### 11.1.Yazılım Güvenliği

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

**11.1.2.** Bilgisayarlarda kullanılan anti virüs yazılımları düzenli olarak güncellenmelidir.

**11.1.3.** Bilgisayarların üzerinde kullanılan işletim sistemleri düzenli olarak güncelleştirilmelidir.

**11.1.4.** Bilgisayarlar üzerinde korsan yazılımlar bulundurulmamalıdır.

**11.1.5.** Geliştirilen yazılımlar gizlilik, bütünlük ve erişebilirlik şartlarına uygun olmalıdır.

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

**11.1.7.** Yazılım geliştirme süreci boyunca, gerekli bütün testler eksiksiz şekilde yapılmalıdır.

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

**11.1.9.** Uygulamalar geliştirilme süreçlerinde gerçek ortamda uygulanmadan önce test sunucularında test edilmelidir.

**11.1.10.** Web sitesi, çevresel bilgi sistemi ve diğer yollarla İnternet üzerinde bulunan halka açık kurum bilgilerinin izinsiz olarak değiştirilmesine, eklenmesine veya silinmesine karşı gerekli koruma önlemleri alınmalı ve yetkilendirmeler yapılmalıdır.

**11.1.11.** Ftp sunucusuna yapılan bağlantılar kullanıcı adı ve şifre korumalı olmalı ftp üzerindeki her türlü hareket kayıt altına alınmalıdır.

**11.2.**Donanım Güvenliği

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

**11.2.2.** Kurumda kullanılan güvenlik cihazlarının loglarının düzenli olarak alınması ve saklanması gerekmektedir.

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

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

**11.2.5.** Taşınabilir ortamdaki bilgi artık kullanılmayacaksa, silinmelidir.

12. Mobil Cihazlar Güvenliği

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

**12.1.**Mobil cihazlara erişimde mutlaka parola kullanılmalıdır.

**12.2.**Mobil cihazda ne tür bilgiler saklandığının farkında olunmalı, hassas ve gizli bilgiler mümkün olduğunca mobil cihazlarda bulundurulmamalıdır.

**12.3.**Verilerinin yedekleri alınmalı ve güncel bir kopyası farklı bir yerde saklanmalıdır.

**12.4.**Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

13. İletişim ve İşletim Güvenliği

**13.1.Uygulama geliştirme, test ve operasyonel sistemlerinin ayrılması;**

**13.1.1.** Geliştirme ve uygulama yazılımları ayrı işlemcilerde veya ayrı sistemlerde çalıştırılmalıdır.

**13.1.2.** İhtiyaç olmadığı durumlarda operasyonel sistemlerde derleyici, editör, ve diğer geliştirme araçları bulundurulmaz.

**13.1.3.** Test sistemi operasyonel sistemle mümkün olduğunca aynı sistem olmamalıdır.

**13.2.Ağ Güvenliği;**

**13.2.1.** Mümkün olduğu takdirde ağdan sorumlu personel bilgisayar işletiminden sorumlu personelden ayrı görevlendirilmelidir.

**13.2.2.** Uzak cihazların yönetimiyle ilgili sorumluluklar belirlenmelidir.

**13.2.3.** Güvenlikle ilgili olayların kaydedilmesini sağlayıcı uygun izleme yöntemleri kullanılmalıdır.

**13.2.4.** Ağ hizmetlerinin güvenli bir şekilde verildiği düzenli olarak izlenmelidir.

**13.2.5.** Gerekli görüldüğünde ağ kullanımına sınırlar getirilmelidir.

**13.2.6.** Özellikle sağlık bilgisinin iletildiği ağların kesintiye uğraması durumundaki riskler ayrıca değerlendirilmelidir.

**13.3.Taşınabilir Ortamların Güvenliği;**

**13.3.1.** İhtiyaç kalmadığında tekrar kullanılabilir ortamların içeriği tekrar düzeltilemeyecek hale getirilmelidir.

**13.3.2.** Tüm ortamlar üretici talimatında belirtildiği şekilde emniyetli ve güvenli ortamda saklanmalıdır.

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

**13.4.Ortamın İmha Edilmesi**

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

**13.4.2.** Mümkün olduğu takdirde imha işlemi kayıt altına alınmalıdır.

**13.5.Bilgi işleme süreci aşağıda belirtilen hususları kapsar;**

**13.5.1.** Yetkisiz personelin erişimini önlemek için erişim kısıtlamaları konulmalıdır.

**13.5.2.** Veriyi alan yetkililer kayıt altına alınmalıdır.

**13.5.3.** Özellikle sağlık bilgisi fiziksel olarak çok iyi korunmalı ya da şifrelenmelidir.

**13.6.Sistem dokümantasyonunun güvenliği;**

**13.6.1.** Sistem dokümantasyonu güvenli bir ortamda saklanmalıdır.

**13.7.Bilgi Değişim Esasları;**

**13.7.1.** Kritik ve hassas bilgi, yazıcılar, kopyalayıcı cihazlar, faks makineleri vb. cihazlar üzerinde bırakılarak yetkisiz kişilerin erişmelerine imkân verilmemelidir.

**13.7.2.** Telefonla görüşürken hassas bilginin ifşa edilmemesi, bilginin dinlenmemesi için tedbir alınmasına dikkat edilmelidir.

**13.7.3.** Personel faks makinelerinin dikkatsiz kullanımının bilgi güvenliği açısından verebileceği zararlar konusunda bilinçli olmalıdır.

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

**13.8.Elektronik Mesajlaşma;**

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

14. Erişim Kontrol Politikası ve Erişim Kaydı Tutulması

**14.1. Erişim Kontrol Politikası**

**14.1.1.** 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.

**14.1.2.** Erişim kontrol politikasının ayrılmaz bir parçası olarak "erişim yetki ve kontrol matrisi" oluşturulur. Erişim yetki ve kontrol matrisinde kimin, hangi bilgiye, hangi yetkilerle erişeceği ve erişimin kontrolü için kullanılacak yöntemler yer alır.

**14.1.3.** Erişim yetki ve kontrol matrisi gerekiyorsa "daha genel hususlardan daha özele olacak şekilde" birden fazla kademe şeklinde de hazırlanabilir.

**14.1.4.** Erişim kontrol politikası/erişim yetki ve kontrol matrisleri hazırlanırken aşağıda sıralanan prensipler dikkate alınır:

**14.1.4.1.** 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.

**14.1.4.2.** Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan erişim kontrol politikalarının sıkılaştırılması (zorlaştırılması) gerekir.

**14.1.4.3.** Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.

**14.1.4.4.** Bilgiye erişim talepleri ve ilgili makamlarca bu taleplere yapılan işlemlerin takip edilebilirliğini sağlamak üzere yazılı kurallar oluşturulur.

**14.1.4.5.** Erişim izinleri ile ilgili kayıtlar, varsa ilgili mevzuatta belirtilen sürelerce, yoksa varlığın sahibi tarafından belirlenecek süre boyunca saklanır.

**14.1.4.6.** Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.

**14.1.4.7.** "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. Gerekiyorsa idari kontrol mekanizmaları oluşturulur.

**14.1.4.8.** "Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.

**14.1.4.9.** Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik sistemler için farklı kimlik doğrulama yöntemleri (token, akıllı kart, tek kullanımlık parola, parmak izi/retina/avuç içi tarama vb.) kullanılabilir.

**14.1.4.10.** Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur. Erişim ile ilgili hangi kullanıcı hareketlerinin izleneceği hususu varlık sahipleri tarafından belirlenir.

**14.1.4.11.** Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. VTYS sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.

### 14.2. Kullanıcı Erişimlerinin Yönetimi

**14.2.1.** Kullanıcı erişimlerinin yönetimi, sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek ve sadece yetkili kullanıcıların erişimlerini temin etmek için yapılır.

**14.2.2.** Başta kişisel sağlık verilerinin işlendiği bilgi sistemleri olmak üzere erişim kontrolüne tabi tutulacak tüm sistem ve hizmetler için "kullanıcı erişim yönetimi esasları" belirlenir. Belirlenen

esaslar, ilgili tüm taraflara (muhtemel kullanıcılara) resmen duyurulur. Kullanıcı erişimi ile ilgili hususlar Kurumun "Erişim Kontrol Politikası" ve/veya her bir sistem/hizmet için ayrı ayrı hazırlanacak "kullanıcı/işletim el kitapları/kılavuzları" içinde yer alır.

**14.2.3.** Kullanıcı erişimleri ile ilgili yönetim esasları belirlenirken aşağıdaki hususlar dikkate alınır:

**14.2.3.1.** Hizmet veya sisteme erişim için nasıl müracaat edileceği,

**14.2.3.2.** Müracaat esnasında hangi bilgilerin isteneceği,

**14.2.3.3.** Kullanıcıların yetkilendirilmesinde kullanılan roller ve haklarının neler olduğu,

**14.2.3.4.** Yetki değişiklik taleplerinin hangi koşullarda ve nasıl yapılacağı,

**14.2.3.5.** Ayrıcalıklı erişim taleplerinin nasıl değerlendirileceği,

**14.2.3.6.** Kullanıcı erişimlerinin izlenmesi için alınmış olan tedbirler,

**14.2.3.7.** Kullanıcı hesaplarının kapatılması/silinmesi için yapılacak işlemler.

**14.2.4.** Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir. Bilmesi gereken prensibi uyarınca gereksiz olarak verilmiş yetkilerin kaldırılması sağlanır.

**14.2.5.** İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en az 6 (altı) aylık aralıklarla yapılır.

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

**14.2.7.** Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili incelemeler, 3 (üç) ayı aşmayacak şekilde daha sık yapılır.

**14.2.8.** 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır. Bu süre bilgi güvenliği alt komisyonu tarafından değiştirilebilir. Her bir sistem için belirlenecek süreler, erişim kontrol politikası içinde yazılı olarak kayıt altına alınır.

**14.2.9.** Ayrıcalıklı erişim hakkı verilen kullanıcı sayısı (etki alanı yöneticisi, veri tabanı yöneticisi vb.) asgari düzeyde tutulur. Mümkün olduğu yerlerde, rutin ve düzenli sistem yönetim işlevlerinin otomatik araçlarla (batch/otomatik kod yazılması, sistem yeteneklerinin kullanılması vb.) yapılması sağlanır.

**14.2.10.** Ayrıcalıklı erişim hakları, düzenli iş faaliyetleri için kullanılan kullanıcı kimliğinden farklı bir kullanıcı kimliğine tahsis edilir. Düzenli iş faaliyetleri, ayrıcalıklı kullanıcı kimliği ile yapılmaz.

**14.2.11.** Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanır ve sıkı bir şekilde kontrol edilir.

**14.2.12.** Programların kaynak kodları ve ilgili öğelere (tasarımlar, özellikler, doğrulama planları ve geçerleme planları gibi) erişim (yetkisiz işlevsellik girişini ve istenmeyen değişiklikleri önlemenin yanı sıra değerli fikri mülkiyet haklarının gizliliğini sağlamak için) sıkı bir şekilde kontrol edilir.

### 14.3. İz Kayıtları (Log) Yönetimi

**14.3.1.** 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.

**14.3.2.** 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.

**14.3.3.** 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.

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

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

**14.3.6.** 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.

**14.3.7.** Olay sonrası incelenmek üzere güvenilir delillerin elde edilmesi için tutulacak kayıtların asgari niteliklerinin aşağıdaki gibi olması gerekir:

**14.3.7.1.** Fiziksel ortam kayıtları: 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),

**14.3.7.2.** Sanal ortam kayıtları,

**14.3.7.3.** Bilişim sistemleri tarafından üretilen kayıtlar, SBYS'ler,

**14.3.7.4.** Güvenlik duvarları,

**14.3.7.5.** Antivirüs yazılımları,

**14.3.7.6.** Saldırı tespit/önleme sistemleri,

**14.3.7.7.** Yönlendiriciler ve anahtarlama cihazları,

**14.3.7.8.** Sunucular,

**14.3.7.9.** Diğer iş uygulamaları (kritik kurumsal projeler),

**14.3.7.10.** Veri tabanları,

**14.3.7.11.** VPN iz kayıtları.

**14.3.7.12.** Tutulması gereken asgari iz kayıtları;

**14.3.7.13.** Kaydı oluşturan sistem,

**14.3.7.14.** Kaydın oluşturulma zamanı (tarih, saat, zaman dilimi),

**14.3.7.15.** Kaydı oluşturan olay,

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

15. Uzaktan Erişim Yönetimi

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

**15.2.** Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir.

**15.3.** Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

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

**15.5.** Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri, üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

**15.6.** Uzak erişimde yapılan tüm network hareketleri loglanmalıdır.

**15.7.** Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.

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

16. Veri Tabanı Güvenliği

**16.1.** Veri tabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.

**16.2.** Veri tabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.

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

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

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

**16.6.** Veri tabanı erişim politikaları kimlik doğrulama ve yetkilendirme usulleri çerçevesinde oluşturulmalıdır. Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil Durum Yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.

**16.7.** Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

**16.8.** Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.

**16.9.** Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

**16.10.** Bilgi saklama medyaları kurum dışına çıkartılmamalıdır.

**16.11.** Sistem dokümantasyonu güvenli şekilde saklanmalıdır.

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

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

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

**16.15.** Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.

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

**16.17.** Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.

**16.18.** En üst düzey veri tabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.

**16.19.** Veri tabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.

**16.20.** Veri tabanı sunucularına ancak yetkili kullanıcılar erişmelidir.

**16.21.** Veri tabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler ara yüzden sağlanmalıdır. (örnek; Kullanıcılar tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmamalıdır.

**16.22.** Bütün şifreler düzenli aralıklarla değiştirilmelidir. Şifre belirleme konusunda "Parola Güvenliği Politikası" esas alınmalıdır.

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

17. Kaydedilebilir Taşınır Materyaller Güvenliği

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

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

**17.3.** Taşınacak verinin de tehdit unsuru içeren herhangi bir yazılım içermediğine emin olunmalıdır.

**17.4.** Veriyi usb disk ile taşıyorsak; bunların bilgisayara takılırken usb lerin sağlıklı çalıştığından emin olunmalı. Aksi takdirde aygıtın bozulmasına neden olabilir.

**17.5.** Usb diskler bilgisayardan çıkartılırken; "aygıtı düzenli şekilde çıkart" denildikten sonra bilgisayardan çıkartılmalı aksi takdirde aygıt bozulabilir.

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

**17.7.** Cd ve dvd lerde veri saklamak için ise kaliteli medyalar kullanmalı, düşük hızla yazdırmalı, alt yüzeye mümkün olduğunca temas etmemeli, nemli, ışık almayan ortamlarda cd leri çok fazla sıkıştırmadan saklamalıdır.

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

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

18. Bilgi Kaynakları Atık ve İmha Yönetimi
    - **18.1.** Bakanlık ve Bağlı Kuruluşlar kendi bünyelerinde oluşturacakları arşivden sorumludur. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.
    - **18.2.** Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.
    - **18.3.** Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir.
    - **18.4.** İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
    - **18.5.** Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
    - **18.6.** Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
    - **18.7.** Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
    - **18.8.** Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.
    - **18.9.** Hacimsel küçültme işlemi için parçalanmalıdır.
    - **18.10.** Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.
19. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri
    - **19.1.** Kurum içerisinde bilgi güvenliği teknik ve farkındalık eğitimleri için yıllık bir plan yapılmalıdır.
    - **19.2.** Yıllık planlar çerçevesinde bilgi güvenliği teknik ve farkındalık eğitimleri gerçekleştirilmelidir.
    - **19.3.** Sunulan bilgi güvenliği teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülmeli ve eğitim etkililiği hususunda değerlendirme yapılmalıdır.
    - **19.4.** Kurumların teknik işlerinde (Bilişim faaliyetleri), uygulama geliştirme, sistem güvenliği kapsamında hizmet veren personellerin kişisel gelişimlerinin devamlılığı konusunda eğitimler düzenlenmelidir.
    - **19.5.** Eğitime katılım formları muhafaza edilmelidir.
20. Bilgi Güvenliği Ulaştırma Güvenliği Yönetimi

"Gizlilik" uygulamasının amacı, kamu kurum ve kuruluşlarının güvenliğini sağlamak, yürütülen işlemlerin ve muhafaza edilen her türlü gizlilik dereceli, bilgi, belge, evrak, doküman ve malzemelerin, düşman veya yetkili ve ilgili olmayan kimseler tarafından öğrenilmesine veya elde edilmesine engel olmaktır. Bu amaca ulaşmak için yapılan bütün düzenlemelere ve alınan bütün önlemlere" güvenlik tedbirleri" denir.

- **20.1.** Taşınılabilir materyaller üzerine iletilen verinin içeriği ile ilgili herhangi bir şey yazmamalıdır. Genel başlıklar kullanmalıdır. Örneğin gizli evrakların bulunduğu bir cd üzerine "gizli evraklar" yazılmamalıdır.
- **20.2.** İçinde veri bulunan taşınır materyal başka bir yere gönderiyorsa tutanak ile yetkili bir kişiye teslim edilmelidir.
- **20.3.** Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Örneğin özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.
- **20.4.** Gizli evraklar veya cd, dvd, usb bellekler gönderilirken, iki adet zarf kullanmalıdır. Birinci zarfın üzerine içeriğin niteliğine göre sınıflandırılmalı ve zarfın kapağı mühürlenmelidir. İkinci zarf ise normal adres yazılan zarf olmalıdır. "GİZLİ" yazılı olan zarf diğer normal zarfın içine koyulmalıdır.