İÇİNDEKİLER

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. Şüphesiz kamu kurumlarında saklanan ve üretilen birçok bilgi yetkisiz kişiler tarafından görülmemesi gereken, silindiğinde ve yetkisiz kişilerin eline geçtiğinde kurumu sıkıntıya sokacak bilgilerdir.

Bilgi güvenliği, kurumlarda bilişim sistemlerinin kullanılmasıyla daha önemli hale gelmiştir. Bilgi saklama ortamları olarak çoğunlukla kâğıt kullanıldığı zamanlarda güvenlik önlemleri olarak fiziksel güvenlik önlemlerine ağırlık verilmiş, ancak gelişen teknolojiler kullanılarak bilgilerin dijital ortamlarda, veri tabanlarında, CD, disk gibi saklama ortamlarında kullanıcısının 24 saat erişebileceği şekilde saklanması gündeme geldiğinde fiziksel güvenlik önlemleri yetersiz kalmaya başlamıştır. Gerek bilişim sistemlerinin bağlantı ihtiyaçları sonucunda Internet erişimleri nedeniyle dünya üzerindeki birçok saldırganın tehdit oluşturması, gerekse iç kullanıcıların bilinçli veya bilinçsiz olarak bilgi güvenliğinde açıklıklara neden olması, kurumlarda bilgi güvenliğine olan ihtiyacı gün geçtikçe daha fazla artırmaktadır. 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.

Bilgi güvenliği politikası dokümanı, yukarıdaki korumaları ve gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır.

2. Bilgi Güvenliği Amaçları

Bilgi sistemleri henüz yeterli güvenlik seviyesinde tasarlanmamıştır. Teknik olanaklar aracılığıyla ulaşılabilen güvenlik sınırlıdır ve uygun yönetim ve yöntemlerle desteklenmelidir. OGM bünyesinde uygulanan Bilgi Güvenliğinin amacı uygun ve etkili prensip ile politikalar kullanarak bilgi sistemlerinin güvenlik seviyesini artırmaktır.

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. Kurumlar hedeflenmek sureti ile içerden ya da dışarıdan yapılacak siber saldırılara karşı kurumsal sorumluluk ve yetkiler çerçevesinde gerekli tedbirler alınmalıdır.

3.10. Yönetimler, bilgi güvenliği yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.

3.11. Yönetimler, 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 versiyon değişimi olarak kayıt altına alınmalı ve her versiyon İstatistik ve Bilgi İşlem Birim Sorumluları ile değerlendirilmeli ve Üst Yönetime onaylatılmalıdır. Her versiyon değişikliği 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.

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. Bilgi İşlem Biriminin Sorumlulukları

4.3.1. Güvenlik Politikasının sahibi olarak, politikaların güncelleştirilmesinden ve uygulanmasından sorumlu olmak,

4.3.2. Sorumlu oldukları Birimlerde Bilgi Güvenliği Politikasının işletilmesi, denetlenmesi ve testlerinin yapıldığını kontrol etmek,

4.3.3. Güvenlik zaafları ve olaylarının nedenlerini araştırmak; gerektiği zamanlarda delilleri saklamak ve raporlamak, önlemler ve iyileştirme önerilerinde bulunmaktan sorumludur.

4.3.4. Bilgi İşlem Birimi bünyesinde çalışan personel için hazırlanmış roller ve sorumluluklarla ilgili dokümanlarda belirtilen görevleri yerine getirmek.

4.3.5. Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak, herhangi bir hata/arıza/olay olduğunda ilgili kişilere haber vermek.

4.3.6. Bilgi Güvenliği Politikasına uygun hareket etmek,

4.3.7. **BGYS** Yöneticisi ile yakın olarak çalışmak ve bilgi alışverişinde bulunmak.

4.3.8. Bilgi güvenliği için kullanılan donanım ve yazılım kullanım talimatlarına uymak, alınan eğitimleri uygulamak ve yöntemler geliştirmek.

4.4. Kullanıcıların Sorumlulukları

4.4.1. Bilgi Güvenliği Politikasına uymak,

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

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

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

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

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

4.4.7. 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.

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

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

4.4.10. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmamak,

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

4.4.12. 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.

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

4.4.14. Kurum bilgilerini kurum dışından üçüncü şahıslara iletmemek.

4.4.15. Kullanıcıların kişisel bilgisayarları üzerine İstatistik ve Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapmamak,

4.4.16. Cihaz, yazılım ve veriyi izinsiz olarak kurum dışına çıkarmamak.

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

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

4.4.19. 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,

4.4.20. 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.

4.4.21. Bilgisayarlarda oyun ve eğlence amaçlı programları çalıştırmamak/ kopyalamamak.

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

4.4.23. Birimlerde ilgili BGYS Sorumlusu ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeleri hiçbir surette değiştirmemek.

4.4.24. Bilgisayarlara herhangi bir şekilde lisanssız program yüklememek,

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

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

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

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

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

4.4.30. 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 Son Kullanıcı Güvenliği

1.1. İşe Alma Öncesinde Yapılacak Kontroller

1.1.1. İşe alınacak adaylar iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol (tarama yapılır) edilir.

1.1.2. Yükleniciler ile yapılan sözleşmelerde, idare tarafından yüklenici personeli için tarama yürütüleceği ve tarama sonuçlarının menfi olması durumunda alınacak önlemler (örneğin personelin değiştirilmesi vb.) belirtilir.

1.1.3. İşe başlamadan önce tüm personel ve yükleniciler ile kişisel ve/veya kurumsal gizlilik sözleşmesi imzalanacağı ilgili taraflara bildirilir. İmzalatılacak sözleşmelerin içeriği ve ilgililerin yükümlülükleri detaylı olarak açıklanır. Sözleşmelerde kişilerin ve idarenin bilgi güvenliği sorumlulukları açıkça belirtilir.

1.1.4. Kuruluşun güvenlik gereksinimleri dikkate alınmadığında, çalışanlar ve yükleniciler için yürütülecek işlemler (disiplin kurallarının uygulanması, gerekiyorsa iş akitlerinin sonlandırılması, tedarik sözleşmesinin feshi vb.) önceden belirlenir ve taraflara duyurulur.

1.2. Çalışma Esnasında Uygulanacak Kontroller

1.2.1. İşe yeni başlayan personelin başlayış işlemlerinin eksiksiz olarak yapılmasını sağlamak için "işe başlama formu" hazırlanır ve uygulanır.

1.2.2. İşe başlama formunda bilgi güvenliği ile ilgili olarak personel giriş kartı çıkarılması ve bina/tesislere erişim için verilecek yetkiler, bilgi sistemlerine erişim için hesap açılması ve verilecek yetkiler (e-Posta, elektronik belge yönetim sistemi, hastane bilgi yönetim sistemi, insan kaynakları sistemi gibi), bilgi güvenliği farkındalık eğitimi, oryantasyon eğitimi, gizlilik sözleşmesi imzalatılması gibi hususlar yer almaktadır.

1.2.3. Tüm çalışanlar ve yükleniciler için bilgi güvenliği farkındalık eğitimi programları hazırlanır ve uygulanır.

1.3. Bilgi Güvenliği Farkındalık Eğitimleri

1.3.1. Bilgi güvenliği yetkililerince, bilgi güvenliği farkındalık eğitimleri için yıllık olarak uygulanmak üzere bir eğitim planı hazırlanır.

1.3.2. İşe yeni başlayan her personele, hassas bilgilere erişim izni verilmeden önce bilgi güvenliği farkındalığı eğitimi verilir. Farkındalık eğitiminde, genel bilgi güvenliği hususlarına ilave olarak anılan göreve yönelik özel bilgi güvenliği gereksinimleri de mutlaka yer alır.

1.3.3. Sunulan bilgi güvenliği teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülür ve eğitim etkililiği hususunda değerlendirme yapılır.

1.3.4. Eğitim katılım formları hazırlanır, katılımcılara imzalatılır ve bilgi güvenliği alt komisyonu tarafından belirlenecek süre boyunca muhafaza edilir.

1.4. Görev Değişikliği veya İşten Ayrılma İçin Uygulanacak Kontroller

1.4.1. Kişi, görevi esnasında edinmiş olduğu bilgileri, görev yeri değişmesi veya ayrılması durumunda dahi sır olarak saklamaktan ve hiçbir şekilde yetkisiz olarak ifşa etmemekten sorumludur. Sır saklama yükümlülüğü süresizdir.

1.4.2. İşten ayrılan veya görev değişikliği yapan personelin ayrılma işlemlerinin eksiksiz olarak yapılmasını sağlamak için "işten ayrılma formu" hazırlanır ve uygulanır.

1.4.3.. İşten ayrılan veya görev yeri değişen kişinin eski görevi ile ilgili bilgisayar hesapları ve uzaktan erişim için kullandıkları hesaplar kapatılır veya erişim yetkileri yeni görev yerinin gereksinimlerine göre yeniden düzenlenir.

1.5. Elektronik Posta Güvenliği

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

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

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

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

1.5.5. 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.

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

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

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

1.5.9. 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.

1.5.10. 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.

1.5.11. Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.

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

1.5.13. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yönetimine haber verilmelidir.

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

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

1.5.16. 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.

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

1.5.18. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.

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

1.5.20. . Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Sistem Yönetimine haber verilmelidir.

1.5.21. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.

1.6. Sosyal Mühendislik ve Sosyal Medya Güvenliği

1.6.1. Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanır. Başka bir tanım ise insanoğlunun zaaflarını kullanarak istenilen bilgiyi, veriyi elde etme sanatıdır.

1.6.2. Sosyal mühendislik yapan kötü niyetli kişiler, sosyal medya ve analiz yöntemlerini kullanarak hedef kişiler hakkında bilgi toplarlar. Sonrasında sosyal mühendislik tekniklerini kullanarak insanların zaaflarından faydalanıp istedikleri bilgilere ulaşmak için çalışma yaparlar.

1.6.3. Hastanelerde sosyal mühendislik alanında alınacak bazı önlemler şu şekilde sıralanabilir:

1.6.3.1. Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınır.

1.6.3.2. Telefon ile hasta hakkında bilgi almak isteyen kişilere, hastanın kişisel bilgileri ile ilgili açıklama yapılmaz.

1.6.3.3. Hasta dosyaları ilgili doktor ve hemşire dışında kimseyle paylaşılmaz. Kolay ulaşılır yerlere konulmaz.

1.6.3.4. Sağlık Bilgi Yönetim Sistemi (SBYS) programlarında kullanılan parolalar kimseyle paylaşılmaz.

1.6.4. Kişisel Sosyal Medya Güvenliği

1.6.4.1. Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalar farklı seçilir.

1.6.4.2. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.

1.6.4.3. Kuruma ait gizli bilgiler, resmi yazılar, çeşitli gelişmeler sosyal medya ortamında yayımlanamaz.

1.6.4.4. Eğitimlerde sosyal medya güvenliği ile ilgili hususlara yer verilir.

2. Bilgi Kaynakları Atık ve İmha Yönetimi

2.1. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.

2.2. 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.

2.3. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.

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

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

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

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

2.8. Hacimsel küçültme işlemi için parçalanmalıdır.

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

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

3. Erişim Kontrol Politikası

3.1. 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.

3.2. Erişim kontrolü ile ilgili hususları açıklamak üzere, kurumun BGYS politikası ile uyumlu olacak şekilde "Erişim Kontrol Politikası" dokümanı hazırlanır. 6698 sayılı kanun kapsamında çıkarılan ikincil mevzuat uyarınca, kişisel verilere erişim için yapılan düzenlemeler söz konusu doküman içinde ayrı bir başlık/bölüm olarak ayrıntılı bir şekilde açıklanır.

3.3. Erişim kontrol politikası, kurumun bilgi güvenliği yetkilisi tarafından hazırlanır ve bilgi güvenliği alt komisyonu tarafından onaylanarak yayımlanır.

3.4. 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.

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

4. Kullanıcı Erişimlerinin Yönetimi

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

4.2. 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.

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

4.4. 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır. Bu süre kurumların bilgi güvenliği alt komisyonları tarafından değiştirilebilir. Her bir sistem için belirlenecek süreler, kurumların erişim kontrol politikası içinde yazılı olarak kayıt altına alınır.

5. Parola Güvenliği

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

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. Basit bir cümle ya da ifade içerisindeki belirli kelimeler özel karakter veya rakamlarla değiştirilerek güçlü bir parola elde edilebilir.

6. Sunucu/Sistem Odası Güvenliği

6.1. Bir sistem odasının en temel özellikleri;
6.1.1. 7×24 kesintisiz çalışabilirlik,
6.1.2. Güç yönetimi ve ağ bağlantılarında farklı kanallardan yedeklilik,
6.1.3. Ağ güvenliği, fiziksel erişimlerde yetkilendirme ve görüntülü gözetleme,
6.1.4. Çevre şartlarının kontrol altında tutulması,

6.1.5. Yangına karşı duman algılama gibi erken uyarı sistemleridir.

6.2. 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.

6.3. Sistem odası ile ilgili aşağıdaki ölçütlere dikkat edilmesi gerekir;

6.3.1. Sistem Odasının Yeri: Çevresel faktörlerden en az etkilenecek bir yer tercih edilmelidir. Binanın nem ve ısı 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.

6.3.2. 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, 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 ve asma tavanların içinden geçirilerek sistem odası içerisinde oluşabilecek karmaşa önlenmelidir. Yangın ve su baskını durumunda cihazların etkilenme riskini azaltma, gerektiğinde hızlı ve kolay müdahale edebilme, soğuk hava koridoru oluşturma gibi amaçlarla taban yerden 40-100 cm kadar yükseltilmiş olmalıdır. Yükseltilmiş zemin anti-statik (epoksi boya ya da epoksi kaplama) malzeme ile kaplanmalıdır. Uygulanacak döşemenin üzerine yerleştirilecek malzemeyi emniyetle taşıyabilecek noktasal ve yayılı yük mukavemetine sahip taşıyıcı ayaklar tesis edilmelidir. Yangın söndürme tertibatına ait gaz tahliye boruları ile iklimlendirme sistemlerinin dış ünite bağlantıları ve sistem odasına yerleştirilen algılayıcılara ait iletim kablolarının yerleştirilebilmesi için asma tavan uygulanmalıdır. Asma tavan, neme ve yangına dayanım standartlara sahip özellikte plakalardan oluşmalıdır.

6.3.3. 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.

6.3.4. Isı 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 odasının birkaç noktasına, e-Posta, SMS ya da telefon çağrısı aracılığıyla bilgilendirme yapan ısı sensörleri konumlandırılabilir. Ayrıca, hava dolaşımının uygun bir şekilde sağlanması için sunucuların ön yüzleri birbirine bakacak şekilde konumlandırılmalı, yükseltilmiş zemin yardımıyla soğuk havanın sunuculara ön yüzden ulaşması sağlanmalı, dışarıya verilen sıcak havanın ise soğutma tesisatının girişine ulaşacak şekilde olması sağlanmalıdır.

6.3.5. 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.

6.3.6. 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.

6.3.7. 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 (TS EN 1634-1:2014+A1) uygun özel üretim bir kapı olmalıdır. Yükseltilmiş tabanın altına ve asma tavan arasına 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. Havalandırma ünitesi olası bir yangında devreye girerek otomatik olarak kapanmalı ve kilitlenmelidir. Herhangi bir yangın tehlikesi durumunda sistem odasının elektriği kesilerek yangına müdahale edilmelidir.

6.3.8. Su Baskını Kontrolü: Su basmasına karşın su tahliye yolları planlanmalı, zemini yerden 15-20 cm yükseltilmiş olmalı ve su dedektörü konumlandırılmalıdır. Dedektör – alarm düzeneği iki basamaklı olup birinci düzeyde (daha alçakta) suyu fark edip alarmı çalıştıracak bir dedektör, ikinci düzeyde (daha yüksekte) ise elektriği kesecek ve bilgisayar sistemlerinin elektrik bağlantısını sonlandıracak bir dedektör kullanılmalıdır.

6.3.9. 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 yapılmalı, ölçümleri düzenli olarak izlenmeli ve ölçüm sonuçlarına göre önlemlerin yeterliliği değerlendirilmelidir. Topraklama sistemleri 'Elektrik Tesislerinde Topraklama Yönetmeliği'ne uygun olarak yapılmalıdır.

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

6.3.11. 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.

6.3.12. 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.

6.3.13. 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 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.

7. Yedekleme Yönetimi

7.1. 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.

7.2. Yedekleme politikasının yerine getirilmesi için detaylı bir yedekleme analiz çalışması yapılmalı ve politikayı sağlayacak bir yedekleme planı ortaya koyulmalıdır. Yedekleme planının asgari aşağıdaki bilgileri içermesi gerekmektedir;

7.2.1. Yedekleme sıklığı,
7.2.2. Hangi saklama ortamında ne kadar süre tutulacağı,
7.2.3. Hangi yedekleme türü ile yedekleneceği,
7.2.4. Kabul edilebilir geri dönüş süresi,
7.2.5. Kabul edilebilir veri kaybı süresi.

7.3. Geri Dönüş Testleri

7.3.1. Yılda en az 2 (iki) kez geri dönüş testi yapılarak tutanakla kayıt altına alınır. Tutanakta; sunucu adı, test tarihi, önceki test tarihi, yedek türü ve yedek durumu, geri yükleme testlerinin kimler tarafından ne zaman yapıldığı, başarılı olup olmadığı gibi asgari bilgiler yer almalıdır.

7.3.2. 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.

8. Veri Aktarımı Güvenliği

8.1. Veri aktarımı, verilerin ilgili kişiler ya da sistemler arasında otomatik, yarı otomatik ya da manuel bir yöntemlerle aktarılması işlemidir. Bir bilginin e-Posta ile bir başka kişiye gönderilmesi, arayan bir kişiye telefonla bilgi verilmesi, bir bilgi sisteminden bir başka bilgi sistemine çeşitli araçlarla veri gönderilmesi işlemleri, verinin üçüncü kişilerin erişimine açılması "veri aktarma" olarak adlandırılabilir.

8.2. Veri aktarımı, yanlış veya yetkisiz yapılması durumunda hukuki sonuçlar doğurabilecek ve tarafları için idari veya cezai yaptırımlara neden olabilecek çok önemli bir işlemdir. Bu nedenle veri aktarım taleplerinde aşağıda sıralanan önlemlerin alınması gerekir.

8.3. Veri aktarımı talepleri karşılanırken, başta kişisel veriler olmak üzere hassas verilerin aktarımı için çeşitli kısıtlamalar ve yasal yaptırımlar olduğu dikkate alınır.

8.4. Kurum içi veya dışından bir bilgi talep edildiğinde, ilgili kişinin bu bilgilere gerçekten ihtiyacı ve erişim izni olup olmadığı dikkatlice değerlendirilir. Her talebe otomatik olarak yanıt verilmez.

8.5. Üçüncü taraflarla ilişki kurulurken, verilerin aktarılmasını kapsayan herhangi bir veri paylaşım anlaşması veya gizlilik sözleşmesi olup olmadığı kontrol edilir. Ayrıca üçüncü kişiler ile yapılacak veri aktarım yöntemleri ile ilgili özel bir şart olup olmadığı dikkate alınır.

8.6. Veri aktarımını yapacak kişi, aktarımla ilgili risklerin değerlendirilmesinden ve aktarım için en uygun yöntemin seçilmesinden sorumludur.

8.7. Gizli kalması gereken bilgilerin aktarımı öncesinde, alıcının kimliği ve aktarılacak veriyi işleme yetkisi olup olmadığı kontrol edilir.

8.8. Aktarılacak veri, kişisel veri kategorisinde ise aktarım kararı konusunda daha fazla hassasiyet gösterilir. Gerekiyorsa veriyle ilgili hizmet biriminden veya bağlı bulunulan sıralı yöneticilerden yetki alınır.

8.9. Aktarılacak bilgiler Hizmete Özel, Özel, Gizli, Çok Gizli gizlilik derecesinde bilgiler ise dinlemeye, kopyalamaya, bütünlüğünün bozulmasına, hedef alıcısı dışında başka kişilere yönlendirmeye ve yok edilmeye karşı korunur. Bunu sağlamak için veri/bilgiler şifrelenir, şifreli/güvenli aktarım araçları kullanılır ya da ikisinin bir arada kullanıldığı yöntemler uygulanır.

8.10. Aktarım için öncelikle Bakanlığımız kontrolünde olan araçlar/sistemler (Kurumsal e-Posta, Kurum Dosya Sunucusu, Kurum tarafından sağlanan taşınabilir depolama ortamları) kullanılır.

9. Gizlilik Sözleşmeleri

9.1. Hastanemize ait gizli kalması gereken bilgilerin korunması maksadıyla, hastanemizde görev yapan 657 sayılı Kanuna bağlı personel de dâhil kendilerine herhangi bir nedenle kurumun bilgi ve bilgi işleme tesislerine erişim yetkisi verilen tüm çalışanlar ve tedarikçiler ile gizlilik sözleşmeleri yapılır.

9.2. Gerçek kişiler ile personel gizlilik sözleşmesi, tüzel kişiler ile kurumsal gizlilik sözleşmesi imzalanır. Staj vb. nedenlerle geçici olarak çalışanlar da dâhil tüm personel ile gizlilik sözleşmesi yapılması esastır.

9.3. Aynı şekilde resmi bir sözleşme veya protokol olmasa bile yasal bir gerekçeye istinaden geçici olarak kendilerine hassas bilgiler verilen/hassas bilgilere erişim izni verilen tüzel kişiler ile gizlilik sözleşmesi yapılması gerekir.

10. Mal ve Hizmet Alımları Güvenliği

10.1. Satın alma faaliyetine konu olan iş kapsamında; yüklenicinin yükümlülüklerini gerçekleştirmesi için yükleniciye özel koruma ihtiyacı olan veri/bilgi teslim edilmesi, ilgili kurumun fiziki alanlarında

personel çalıştırılması veya kurum bilgi sistemlerine (uzaktan erişimler dâhil) erişim yapılması ihtiyacı olması halinde; satın alma için hazırlanan teknik ya da idari şartnamelere "Bilgi Güvenliği Gereksinimleri" başlığı altında asgari olarak aşağıdaki hususlar eklenir.

10.1.1. İdareye ait bilgilerin korunması maksadıyla, yükleniciler ile "Kurumsal Gizlilik Sözleşmesi" ve söz konusu iş kapsamında çalışacak olan yüklenici personeli ile "Personel Gizlilik Sözleşmesi" imzalanır. Bahse konu dokümanların boş halleri, hazırlanan teknik veya idari şartnameye eklenir.

10.1.2. İhaleyi kazanan firma ile sözleşmenin imzalanmasını takiben kurumdaki yetkili makam (Satın Alma Birimi ve/veya Kurum Bilgi Güvenliği Yetkilisi) huzurunda "Kurumsal Gizlilik Sözleşmesi" imzalanır

10.1.3. "Kurumsal Gizlilik Sözleşmesi" ve ihaleye konu iş kapsamında çalıştırılacak personelin "Personel Gizlilik Sözleşmeleri" imzalanmadan ve idareye teslim edilmeden, yüklenici tarafından işe başlanamaz.

10.1.4. Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, "Personel Gizlilik Sözleşmeleri" idareye teslim edildikten sonra tanımlanır.

10.1.5. Yapılacak iş kapsamında alt yüklenici kullanılacaksa, alt yükleniciler de yukarıda belirtilen hükümlere aynen uymak zorundadır. Yüklenici, alt yüklenicileri ve çalışanlarının gizlilik sözleşmeleri ile ilgili yükümlüklere uymasından birinci derecede sorumludur.

10.2. Yüklenicinin fikri mülkiyet hakları ve telif hakları dâhil, yasal ve düzenleyici gereksinimlere uyması ile ilgili hususlar satın alma dokümanlarına konulur.

10.3. Alınacak mal veya hizmetin tahmini bedelleri bağlamında idare tarafından yapılan yaklaşık maliyet çalışması, ihale aşamasına kadar gizli tutulur.

10.4. Söz konusu alım için gerekli iş tanımı ölçütleri, personel istihdam edilecekse ilgili personel özellikleri açıkça belirtilir.

10.5. Ürünlerin satın alınmadan önce kurumsal olarak belirlenen güvenlik gereksinimleri için risk oluşturmadığından emin olunması için test edilmesi gerekir.

11. İhlal Bildirimi ve Olay Yönetimi

11.1. Tüm sağlık çalışanları ve vatandaşlar tarafından tespit edilen Sağlık Bakanlığı ile ilgili her türlü bilgi güvenliği ihlal olayı https://bilgiguvenligi.saglik.gov.tr/ adresinde yer alan merkezi ihlal bildirim sistemine girilir.

11.2. Olay bildirim sistemini kullanamayacak durumda olanlar hastanemizdeki bilgi güvenliği yetkililerine bildirim yapabilir. Bilgi güvenliği yetkilisine yapılan bildirimler, bilgi güvenliği yetkilisince merkezi sisteme girilir.

11.3. Kanıt Toplama:

11.3.1. 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.

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

11.3.3. 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.

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

11.3.5. Olay yerindeki bilgisayar kapalı ise kesinlikle açılmaz.

11.3.6. 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.

11.3.7. 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.

11.3.8. 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.

11.3.9. 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.

11.3.10. 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.

11.3.11. 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)

11.3.12. 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.

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