1. AMAÇ:

Bu güvenlik politikası, etkin ve yerleşmiş bilgi teknolojileri güvenlik süreçleri ve prosedürleri aracılığıyla sağlık hizmetlerinden faydalanan vatandaşa ait bilgilerin ya da kurumsal hizmetlerin icra edilmesi esnasında edinilen bilgi ve kaynakların güvenliğini, bütünlüğünü ve erişebilirliğini sağlamayı, ayrıca var olan bilginin kaybolmasını, zarara uğramasını, yok olmasını, yetkisiz ve kötü niyetli kişilerin eline geçmesini engellemeyi amaçlamaktadır.

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

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

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuyu da içinde barındırması sebebiyle İl Sağlık Müdürlüğü bilgi kaynaklarını kullanmakta olan tüm birimleri, bağlı kuruluşları, bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

3. TANIMLAR:

3.1.Bilgi Güvenliği: 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; bilgiyi, yetkisiz kişilerin görmesinden, değiştirmesinden, bilgilerin silinmesinden korumaktadır.
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, veritabanlarında, CD, Çıkarılabilir 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 yöntemlerin oluşturulması da bir zorunluluk olmuştur.
Bilgi güvenliği, bu politikada aşağıdakilerin korunması olarak tanımlanır:

- Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek;

- Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek;
- Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

3.2.İl Sağlık Müdürlüğü: Mersin İl Sağlık Müdürlüğü ve bağlı birimleri, Başkanlıklar ve bağlı birimleri

3.3.Bağlı Sağlık Tesisleri: İlçe Sağlık Müdürlükleri, Toplum Sağlığı Merkezleri, 112 Komuta Kontrol Merkezi ve Acil Sağlık Hizmetleri İstasyonları, Entegre Hastaneler ve Kamu Hastaneleri

3.4.Varlık: kurum içi değeri olan her türlü unsur (insan, donanım, yazılım, bilgi, vs.)

3.5.Gizlilik; Bilgiye sadece erişme izni olan yetkili kişiler ya da sistemlerin erişmesini sağlamaktır.

3.6.Bütünlük; Bilginin yetkisiz kişi ya da işlemler tarafından değiştirilmemesini sağlamaktır. Böylece bilginin tutarlılığı sağlanmış olur.

3.7.Erişilebilirlik; Bilgiye doğru zamanda erişimin ve erişim sürekliliğinin sağlanmasıdır.

3.8.Bilgi Güvenliği İhlal Olayı: Bilgi Güvenliği Politikalarının ve prosedürlerinin dışında işlem tesis edilmesi ile iş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen Bilgi Güvenliği olayıdır.

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

4. KISALTMALAR:

4.1.SBYS: Sağlık Bilgi Yönetim Sistemleri

4.2.BG: Bilgi Güvenliği

4.3.BGYS: Bilgi Güvenliği Yönetim Sistemi,

4.4.VTYS: Veri Tabanı Yönetim Sistemi

4.5.SBA: Sağlık Bilişim Ağı

5. BİLGİ GÜVENLİĞİ ORGANİZASYONU

İl genelindeki BGYS faaliyetlerinin faaliyetlerini yürütmek ve koordine etmek üzere "**Bilgi Güvenliği Komisyonu**" oluşturulur. Bu Bilgi Güvenliği Komisyonunun aldığı kararları ve yürüteceği faaliyetlerin il genelinde takibi, yürütülmesi ve koordinasyonu için **İl Bilgi Güvenliği Yetkilisi**, bağlı sağlık tesislerinde takibi ve yürütülmesi için **Sağlık Tesisi Bilgi Güvenliği Yetkilisi** görevlendirilir. Ayrıca Kamu Hastanelerinin her birinde hastane bünyesinde **"Bilgi Güvenliği Ekibi"** kurulur.

İl Sağlık Müdürlüğü ve bağlı sağlık tesisleri yönetimlerince BGYS'nin tüm süreçleri için gerekli yönetimsel destek ve kaynaklar sağlanır

5.1.BGYS Komisyonu: İl Sağlık Müdürlüğü bünyesinde oluşturulan BGYS Komisyonu Personel ve Destek Hizmetleri Başkanı başkanlığında yılda en az 2 (iki) kez toplanır.

5.2.BGYS Komisyon Görev, Yetki ve Sorumlulukları

- İl düzeyindeki Bilgi Güvenliği Politika ve stratejilerini belirler; Sağlık Bakanlığı BGYS yönergesi ve BG Politikaları Kılavuzu çerçevesinde, İl Sağlık Müdürlüğü ve bağlı sağlık tesisleri bünyesinde uygulanacak BGYS'ye yönelik çalışmaları koordine eder
- Bakanlık tarafından yayımlanan eylem planında yer alan hususların gerçekleştirilmesini sağlar.
- İl Bilgi güvenliği yetkilisinin belirler ve görevlendirmesini yapar.

- Bakanlık tarafından yayımlanan Kurumsal SOME Kurulum ve Yönetim Rehberi'nde belirtilen esaslar çerçevesinde Kurumsal SOME'sini kurar ve işletilmesini sağlar. Kurumsal SOME Ekip Lideri görevlendirmesini yapar.
- BG politikalarının uygulanmasını ve uygulanmadaki etkinliğini gözden geçirir.
- BG faaliyetlerinin yürütülmesini yönlendirir.
- BG eğitim ve farkındalığının sağlanması için plan ve program yapar.
- Yürütülen çalışmaların tabana yayılması hususunda planlanan çalışmalara katılır, bağlı oldukları birimlerde bu çalışmaların yayılmasına öncülük eder.

6. İNSAN KAYNAKLARI VE SON KULLANICI GÜVENLİĞİ

6.1.İşe Başlayış

6.1.1. Bilgi işleme tesislerine erişim izni verilecek tüm personel için (kamu personeli, tam zamanlı ya da yarı zamanlı olarak çalışan sözleşmeli personel, yüklenici firma çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli vb.) işe alma öncesinde/alım yapılırken aşağıdaki hususların dikkate alınması gerekir. İşe alma öncesinde yapılacak güvenlik kontrollerinin amacı, çalışanların kendilerinden beklenen sorumlulukları anlamalarını sağlamak ve düşünüldükleri roller için uygun olmalarını temin etmektir.

6.1.2. İşe alınacak 657 sayılı kanuna tabi personellerin eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilmesi Bakanlığımızca yapılıyor olup Müdürlüğümüze ve bağlı sağlık tesislerine atanan personelin İnsan Kaynaklarınca kimlik kontrolleri yapılır.

6.1.2.1. İşe alınacak Yüklenici personeli, destek personeli vb. statüde çalışacak personelin adli sicil kayıtları istenir ve incelenir.

6.1.3. 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.

6.1.4. 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.

6.1.5. Göreve başlayan personel, İnsan Kaynakları Biriminden alacağı Ek-7'deki "İşe Başlama Formunu" eksiksiz olarak doldurulması gerekmektedir.

6.1.6. Göreve başlayan personele Oryantasyon, Bilgi Güvenliği ve Sosyal Mühendislik zafiyetleri konularında eğitim verilmelidir.

6.1.7. Göreve başlayan personele, Ek-1 Personel Gizlilik Sözleşmesi ve Ek-2 Bilgi Güvenliği Farkındalık Bildirgesi imzalatılmalıdır.

6.1.8. Göreve başlayan personele kimlik ve yaka kartı düzenlenmelidir.

6.1.9. Göreve başlayan personele kullanacağı bilgi sistemlerine yönelik yetkili kullanıcılar tanımlanmalıdır.

6.1.10. Göreve başlayan personele EBYS tanımlanacak ise ilgili personele saglik.gov.tr uzantılı kurumsal posta adresi temin edilmelidir. İl içi kurum/birim değişikliklerinde kurum EBYS sorumlusu İl EBYS sorumluları ile iletişime geçerek gerekli olan değişiklikleri yaptırmalıdır.

6.2.Çalışma Esnasında Uyulacak Kurallar:

6.2.1. Çalışma esnasında uygulanacak güvenlik kontrollerinin amacı, çalışanların işlerini yaparken bilgi güvenliği ile ilgili sorumluluklarının farkında olmalarını ve beklenen şekilde yerine getirmelerini sağlamaktır.
6.2.2. Kurum Yönetimi, bilgi güvenliği politikalarını, prosedürlerini ve kontrollerini desteklediğini her fırsatta örnek teşkil edecek şekilde gösterir. Bu suretle, diğer çalışanların bilgi güvenliği ile ilgili motivasyonları üst düzeyde tutulur.
6.2.3. Bilgi güvenliği ile ilgili beklentiler ve sorumluluklar, çalışanların görev tanımlarına eklenir.
6.2.4. Çalışanların kuruluşun bilgi güvenliği politikasına uyumu izlenir.
6.2.5. Tüm çalışanlar için bilgi güvenliği farkındalık eğitimi programları hazırlanır ve uygulanır.
6.2.6. Bilgi güvenliği ihlali yapan personele uygulanan yaptırımlar (kişi kimlik bilgisi verilmeden) diğer çalışanlara duyurulur ve onlar için de örnek teşkil etmesi sağlanır.
6.2.7. Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
6.2.8. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
6.2.9. Bilgisayar ekranında kişisel bilgi içeren bir işlem yapıldığında(izin kâğıdı gibi) ekranda bulunan kişisel bilgilerin bilgi sahibi dışında diğer kişi veya kişilerce görülmesi engellenmelidir.
6.2.10. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
6.2.11. İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt kesme makinesinde imha edilmelidir.
6.2.12. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

6.3.Görev Değişikliği ve İşten Ayrılışta Yapılacak İşlemler:

6.3.1. Görev değişikliği veya işten ayrılma ile ilgili güvenlik kontrollerinin amacı, ayrılma işlemleri esnasında yapılması gereken bilgi güvenliği ile ilgili tedbirlerin ortaya konulması ve çalışanların görevleri sona erse dahi bilgi güvenliği ile ilgili devam eden sorumlulukları hakkında bilgilendirilmesidir
6.3.2. İşten ayrılan veya Görev değişikliği yapılan personel üzerindeki görev ve evrakları birim sorumlusunun belirlediği personele devrettiğine dair Ek-9'deki "Görev Devir-Teslim Formunu" doldurup birim sorumlusuna teslim etmelidir.
6.3.3. Görev değişikliği yapılan personel, esik görevi ile ilgi zimmetinde bulunan malzemeleri teslim etmelidir. Görev değişikliği yapılan personelin eski görev yeri ile ilgili bilgi sistemlerine yönelik kullanıcı ve/veya yetkileri iptal edilmeli ve yeni görev yerinde kullanacağı bilgi sistemlerine yönelik yetkili kullanıcılar tanımlanmalıdır.
6.3.4. Görev değişikliği yapılan personele, yeni görevi ile ilgili Oryantasyon eğitim verilmelidir.
6.3.5. İşten ayrılan veya Görev değişikliği yapılan personel, 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.
6.3.6. İşten ayrılan veya görev yeri değişen personelin eski görevi ile ilgili bilgisayar hesapları ve uzaktan erişim için kullandıkları hesaplar kapatılır veya erişim yetkileri yeni görev yerinin gereksinimlerine göre yeniden düzenlenir.
6.3.7. Personele teslim edilmiş tüm bilgi varlıkları (bilgisayarlar, yazılı ortamda saklanan bilgi ve belgeler, bilgisayar ortamında tutulan dosyalar, lisans belgeleri, CD'ler vb.) sayım yapılarak iade alınır.

6.3.8. Ayrılan veya görev yeri değişen personel tarafından yürütülen faaliyetlerin aksamaması için birim sorumlusu tarafından gerekli tedbirler alınır.
6.3.9. Mümkünse ayrılan personel ile yeni katılan personelin geçici bir süre birlikte görev yapması sağlanır.
6.3.10. Ayrılan kişiden teslim alınan bilgisayarlar güvenli silme işlemi yapılmadan bir başka kullanıcıya teslim edilemez.
6.3.11. Görevden ayrılan personel, Ek-8'deki "İşten Ayrılma Formunu" ilgili birimlerle ilişkisinin kalmadığına dair birim sorumlularına imzalatarak eksiksiz olarak doldurup bağlı bulunduğu İnsan Kaynakları Birimine teslim etmelidir.
6.3.12. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi ile insan kaynakları birimi müştereken sorumludur.
6.3.13. İnsan Kaynakları Birimi, görevden ayrılan personelin İşten Ayrılma Formundaki eksik bilgi ve imzaları tamamlatmadan kurum ile ilişiğini kesmemelidir.
6.3.14. Görevden ayrılan personelin, İşten Ayrılma Formunda da belirttiği üzere kullandığı bilgi sistemlerine yönelik kullanıcıları pasif hale getirilmelidir.
6.3.15. Görevden ayrılan personel, İşten Ayrılma Formunda da belirttiği üzere zimmetinde bulunan malzemeleri teslim etmelidir.
6.3.16. Görevden ayrılan personel, İşten Ayrılma Formunda da belirttiği üzere yaka kimlik kartı, giriş ve otopark kartlarını idareye teslim etmelidir.

6.4.İnternet Kullanım Kuralları:

6.4.1. Müdürlüğümüz ve Bağlı Sağlık Tesislerinde görev yapan personel, İnternet hizmetini yalnızca iş faaliyetlerini destekleyecek şekilde kullanmalıdır. Bunun dışındaki kişisel kullanımda aşağıdaki hususlar çerçevesinde;

- Görev amaçlı kullanılabilecek kaynaklar az miktarda kullanılıyorsa,
- Çalışanların verimliliğini engellemiyorsa,
- Herhangi bir iş faaliyetini aksatmıyorsa,
- Kullanıcıların bazı kişisel işlerini daha hızlı yerine getirmesini sağlıyorsa

İzin verilebilir.
6.4.2. İnternet erişimi için kurum yönetiminin uygun gördüğü kullanıcı talebi ilgili kullanıcıların T.C. Kimlik no, ad, soyad, görev/unvan ve saglik.gov.tr uzantılı kurumsal e-posta adresleriyle beraber Müdürlüğümüz Bilgi işlem ve İstatistik birimine iletilir.
6.4.3. Bilgi işlem ve İstatistik birimince, internet erişimi için talep edilen kullanıcılara güvenlik duvarı üzerinden kullanıcı açılır. Kullanıcı adı ve geçici şifreleri kullanıcıların bildirilen e-posta adreslerine gönderilir.
6.4.4. İnternet erişim kullanıcısı, ilk girişinde geçici şifresini değiştirmesi gerekmektedir.
6.4.5. Kullanıcıların Internet kullanım yoğunluğu diğer kullanıcıların Internet'e ulaşımlarını engelleyecek şekilde olmamalıdır. Güvenlik yöneticileri, sistem yöneticileri ve bilgisayar operatörleri gibi sistem bakım-idame işlerini yürüten personele ayrıcalıklar tanınabilir.
6.4.6. Internet kullanımı, Güvenlik Duvarı kullanılarak sınırlandırılmaktadır. Kullanıcılar, bu kontrollerin yapıldığını bilerek Internet'i kullanmalı, güvenlik amacıyla konulan önlemleri devre dışı bırakmaya çalışmamalıdır.

6.5.E-Posta Kullanım Kuralları:

6.5.1. Müdürlüğümüz ve Bağlı Sağlık Tesislerinde görev yapan personel tarafından görevleri gereği yürütülen kurumsal iş ve işlemlerde, *@saglik.gov.tr uzantılı kurumsal veya tüzel e-Posta hesabı kullanılır. Kurumsal iş ve işlemler, kişilerin özel işleri için (Gmail, Hotmail gibi) internet hizmet sağlayıcılarından alınan hesaplar üzerinden yürütülmez.

6.5.2. KVKK tarafından 6698 sayılı Kanunda yer alan bazı hususların açıklanması amacıyla alınan 2018/10 sayılı karar gereği, e-Posta ile aktarılacak verilerin özel nitelikli kişisel veri statüsünde olması durumunda aktarma işlemlerinin kurumsal e-Posta veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak yapılması kanuni zorunluluktur.

6.5.3. Müdürlüğümüz ve Bağlı Sağlık Tesislerinde görev yapan 657 sayılı Kanuna bağlı tüm kamu personeli, talep etmeleri halinde https://eposta.saglik.gov.tr adresinden kurumsal e-Posta hesabı açabilir.

6.5.4. Çeşitli sözleşmeler kapsamında Müdürlüğümüz ve Bağlı Sağlık Tesislerinde görev yapan ve yaptıkları iş gereği e-Posta hesabı olması gereken personele, sıralı yöneticileri tarafından onay verilmesi halinde resmi yazıyla Sağlık Bilgi Sistemleri Genel Müdürlüğü'nden kurumsal e-Posta hesabı talebi yapılabilir.

6.5.5. Müdürlüğümüz ve Bağlı Sağlık Tesislerinde yer alan birimler için ihtiyaç olması halinde, tüzel e-Posta hesapları resmi yazıyla Sağlık Bilgi Sistemleri Genel Müdürlüğü'nden talep edilir. Tüzel e-Posta hesapları, Kurumun adı + "." + ilgili birimin adı veya yürüttüğü işlev ile alakalı olarak belirlenir. (mersin.kalite@saglik.gov.tr, mersindh.personel@saglik.gov.tr gibi).

6.5.6. Kurumsal ve tüzel e-Posta kullanım kayıtları Bakanlıkça tutulur. Bu kayıtlar 6698 sayılı kanunun 28 inci maddesinin birinci ve ikinci fıkralarında yer alan şartlar kapsamında; yalnızca yetkili kişi, kurum ve kuruluşlar tarafından, yine aynı Kanun'un 4'üncü maddesinde yer alan genel ilkelere uymak kaydıyla incelenebilir.

6.5.7. Kurumsal ve tüzel hesapların kullanımında dikkat edilmesi gereken hususlar şu şekildedir;

6.5.7.1. Kullanıcılar, kendilerine tahsis edilen e-Posta hesabını bir başka kişiye kullandıramaz veya devredemez.

6.5.7.2. Kullanıcılar, parolalarını Kurum Parola Politikasında uyarınca oluşturur ve kullanır.

6.5.7.3. Kullanıcılar, kendilerine ait parolanın güvenliğinden ve söz konusu parola kullanılarak gönderilen e-Postalardan doğacak hukuki işlemlerden sorumludur.

6.5.7.4. Kurumsal e-Posta hesabı yalnızca kurumsal süreçlere ilişkin iş ve işlemlerde kullanılabilir. Kurumsal e-Posta hesaplarının, idari ve hukuki düzenlemelere aykırı ya da şahsi iş ve işlemlere ilişkin kullanımından kaynaklanan her türlü adli, idari, mali ve cezai sorumluluk ilgili hesap kullanıcısına aittir.

6.5.7.5. Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-Posta hesapları kullanılamaz. Aksine durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.

6.5.7.6. Konusu suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden ve sahip olduğu görev kapsamı içindeki iş ve işlemler dışındaki e-Posta hesabının kullanımından kullanıcı sorumludur.

6.5.7.7. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-Posta gönderilemez.

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

6.5.7.9. İnternet haber gruplarına üyelik için kurumun sağladığı e-Posta hesapları kullanılmaz. Ancak iş gereği üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak kurumun sağladığı resmi e-Posta adresi kullanılabilir.
6.5.7.10. Kullanıcılar, e-Posta hesaplarında hukuki açıdan suç teşkil edecek materyal ve belgeleri bulunduramaz. Kullanıcılar, kendi kullanıcı hesaplarında barındırdıkları içeriklerden ve gerçekleştirilen tüm elektronik posta işlemlerinden sorumludur.
6.5.7.11.e-Posta gönderimlerinde, mesajın en alt kısmına gönderen kişinin kimlik ve iletişim bilgileri yazılır.
6.5.7.12.E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir.
6.5.7.13. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.
6.5.7.14. Kullanıcılar, gelen veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemek için her türlü tedbiri alır.
6.5.7.15. Tanınmayan elektronik postaların açılması, eklentilerinde bulunan dosya veya programların indirilip çalıştırılmasından kaynaklanabilecek güvenlik sorunlarının sorumluluğu kullanıcıya aittir.
6.5.7.16. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-Postalara yanıt verilmez.
6.5.7.17. Kurumsal E-posta adresi, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.
6.5.7.18. Kaynağı bilinmeyen e-Posta ekinde gelen dosyalar kesinlikle açılmaz.
6.5.7.19. Kullanıcılar, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.
6.5.7.20.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.
6.5.7.21. 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.
6.5.7.22. Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir.
6.5.7.23. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren epostalar alındığında başkalarına iletilmemelidir.
6.5.7.24. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
6.5.7.25. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.

6.6.Sosyal Mühendislik Ve Sosyal Medya Güvenliği

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.
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.

6.6.1. Sosyal mühendislik saldırılarından korunmak için kişisel olarak dikkat edilmesi gereken hususlar şu şekildedir:

6.6.1.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunuz.

6.6.1.2. Bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket ediniz.

6.6.1.3. Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.

6.6.1.4. Özellikle telefonda, e-Posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi kesinlikle paylaşmayınız.

6.6.1.5. Parola kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-Posta ile parolanızı hiç kimseyle kesinlikle paylaşmayınız.

6.6.1.6. Oluşturulan dosyaya erişecek kişiler ve haklarını, "bilmesi gereken" prensibine göre belirleyiniz ve erişim kontrol tedbirleri uygulayınız.

6.6.1.7. Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.

6.6.1.8. Çöpe atılan kâğıtlara dikkat ediniz. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtları, kâğıt kırpma makinesinde imha ediniz.

6.6.1.9. Çok acele bilgi istendiği zaman istenen bilginin niteliğine göre teyit mekanizması kullanınız.

6.6.1.10. Bilgisayarınızı yabancı bir kişiye kullandırmayınız. Bu kişiler tarafından bilgisayarınıza takılacak olan USB depolama aygıtları ya da harici disklerden bilgisayarınıza zararlı yazılım bulaştırabilir.

6.6.1.11. Hediye olarak verilen USB depolama aygıtlarını kullanmadan önce mutlaka virüs taramasından geçiriniz.

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

6.6.2.1. 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.

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

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

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

6.6.3. Kişisel Sosyal Medya Güvenliği

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

6.6.3.2. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.

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

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

7. VARLIK YÖNETİMİ

7.1. Taşınabilir Ortam Yönetimi:

7.1.1. Personellerin Taşınabilir Ortamların kullanımında dikkat edeceği hususları açıklamak için hazırlanmıştır.

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

7.1.3. Taşınabilir cihazlardaki bilgileri üçüncü taraflarla paylaşımında da gerektiği kadar bilgi verme prensibi göz önünde bulundurulmalıdır.

7.1.4. Personelin kullanımı için tahsis edilmiş olan taşınabilir ortamlar sadeci yetkilendirilmiş personel tarafından ve veriliş amaçları doğrultusunda kullanılmalıdır.

7.1.5. Elektronik medya kullanımı ile ilgili olarak aşağıdaki hususlar göz önünde bulundurulmalıdır.

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

7.1.5.2. Kuruma ait medyalar varlık envanteri içinde listelenir ve kimler tarafından kullanıldığı kayıt altına alınır. Görev devir teslimlerinde veya işten ayrılışlarda, kişilere teslim edilmiş olan medyaların iade edilmesi istenir veya ne şekilde sarf edildiği bilgisi sorgulanır.

7.1.5.3. Özellikle eski SBYS verileri ve SBYS yedeklerinin saklandığı medya ortamlarının mutlak surette envanter listesi oluşturulur, 6 (altı) aydan az olmayacak şekilde belirlenecek sürelerde sayım işlemleri yapılır ve sayım sonuçları kayıt altına alınır.

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

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

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

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

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

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

7.1.7. Taşınabilir ortamların bir yerden başka yere taşınması esnasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı gerekli önlemler alınmalıdır. Bu çerçevede;

7.1.7.1. Güvenilir kargo/taşıma şirketleri ya da kuryeler kullanılır,

7.1.7.2. Yönetim tarafından yetkili kurye listeleri oluşturulur.

7.1.7.3. Paketleme ve taşıma sırasında ortaya çıkabilecek herhangi bir fiziksel hasardan korumak için üreticinin belirlediği teknik özelliklere uygun önlemler (ısı, nem ya da elektromanyetik alanlara maruz kalma gibi çevresel faktörlere karşı koruma vb.) alınır.

7.2.Bilgi Saklama Ortamları Yok Etme Kuralları:

7.2.1. Basılı Ortamlar ve bilgi işlem cihazları da dahil her türlü ortamda saklanan bilgilerin silinmesi, anonim hale getirilmesi ve imha edilmesi ile ilgili hususları açıklamak için hazırlanmıştır.

7.2.2. Kullanılan bilgi kaynaklarının 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

7.2.3. Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik veya fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dışı bırakılmasına karar verilen bilgi sistem cihazları ile ilgili kayıt silme işlemleri 2006/11545 sayılı Taşınır Mal Yönetmeliğinde belirtilen usul ve esaslar çerçevesince, ilgili birimler ve komisyonlar tarafında yapılır.

7.2.4. Kaydı silinen bilgi sistem cihazlarına ait veri depolama üniteleri, içerisinde gizlilik dereceli bilgi bulundurma ihtimali nedeniyle usulüne uygun olarak imha edilir veya güvenli silme işlemi yapılır.

7.2.5. Kaydı silinen bilgisayarların sabit diskleri, ilgili teknik birimlerden destek alınmak suretiyle sökülür.

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

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

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

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

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

7.2.11. Tamamen tahrip edilememiş disk parçalarının delme, kesme makineleri ile kullanılamaz hale getirilmelidir.

7.2.12. Hacimsel küçültme işlemi için parçalanmalıdır.

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

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

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

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

7.2.17. Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

7.2.17.1.İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan veriler güvenli olarak silinmelidir,

7.2.17.2.Güvenli silmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
7.2.17.3.Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, hassas verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

8. ERİŞİM KONTROLÜ

8.1.Erişim Kontrol Politikası

8.1.1. 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.
8.1.2. Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı gizlilik dereceli) bilgiler için özel bir erişim kontrol tedbiri alınmasına gerek yoktur. Bu tür bilgiler, kurumların İnternet sitelerinin vatandaşlara açık bölümlerine konulabilir. Bina ve tesislerde duyuru panosu vb. ortamlarda yayımlanabilir.
8.1.3. Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan erişim kontrol politikalarının sıkılaştırılması (zorlaştırılması) gerekir.
8.1.4. Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.
8.1.5. Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.
8.1.6. "Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak, bir kişinin kendi başına tüm bilgi varlıklarına erişimi engellenir. Teknik nedenlerle görev ayrımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır.
8.1.7. "Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.
8.1.8. Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik sistemler için farklı kimlik doğrulama yöntemleri (akıllı kart, tek kullanımlık parola, elektronik imza, mobil imza vb.) kullanılabilir.
8.1.9. Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur.
8.1.10. Sağlık Bilişim Ağı dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.
8.1.11. Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. Veri tabanı yönetim sistemi sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.
8.1.12. Bilgi varlıklarına fiziksel olarak yapılacak erişimler için gerekli önlemler alınır.
8.1.13. Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için Kişisel Verileri Koruma Kurulu'nun 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.
8.1.14. Bakanlığımız ortak uygulamalarına erişim, SBSGM Bilgi Güvenliği Politikaları Kılavuzuna uygun şekilde yapılır.

8.2.Kullanıcı Erişimlerinin Yönetimi:

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

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

8.2.3. İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en fazla altı aylık aralıklarla yapılır.

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

8.2.5. Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili incelemeler, üç ayı aşmayacak şekilde daha sık yapılır.

8.2.6. 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır.

8.2.7. Ayrıcalıklı erişim hakkı verilen kullanıcı sayısı (etki alanı yöneticisi, veri tabanı yöneticisi vb.) asgari düzeyde tutulur.

8.3.Uzaktan Erişim Kuralları:

8.3.1. Müdürlüğümüz ve Bağlı Sağlık Tesislerine bünyesindeki bilgi kaynaklarına(sunucu ve hizmetlere) uzaktan erişim için alınması gereken tedbirler ve uyulması gereken kuralları açıklamaktır.

8.3.2. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahiptir.

8.3.3. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar SSL VPN teknolojisini kullanmalıdırlar. SSL VPN Kullanıcısı Müdürlüğümüz Bilgi İşlem Biriminden talep edilecektir.

8.3.4. SSL VPN bağlantılarına ilişkin kayıtlar müdürlüğümüz loglama sisteminde loglanmaktadır.

8.3.5. SSL VPN Kullanıcı şifresi Kurum Parola Politikası ile uyumlu olmalıdır.

8.3.6. SSL VPN Kullanıcısı bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

8.3.7. SSL VPN bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) 10 dakika olarak belirlenmiş olup herhangi bir işlem yapılmadığı takdirde ilgili oturum kapanacaktır.

8.3.8. Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

8.3.8.1. Bağlantı SSL VPN üzerinden yapılır.

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

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

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

8.3.8.5. Bağlantı yapan kullanıcının hedef bilgisayardaki oturum açma, oturum kapatma gibi kullanıcı hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az 1 (bir) yıl süre ile saklanır.

8.3.8.6. Hedef bilgisayar üzerinden bir başka sunucuya bağlantı yapılacak ise (örneğin SBYS yazılımı kullanılacak ise) ilgili kullanıcının söz konusu sunucuda yaptığı işlemlere ait iz kayıtları da kayıt altına alınır.
8.3.8.7. Uzak bağlantı yazılımı olarak mümkün ise "Microsoft Uzak Bağlantı Programı" kullanılır.
8.3.8.8. Microsoft işletim sistemi dışında bir başka bilgisayara erişim yapılıyorsa aynı güvenlik özelliklerini sağlayan, lisanslı ve/veya açık kaynak kodlu, güvenilir bir erişim programının kullanılması tercih edilir.
8.3.9. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların bilgileri Müdürlüğümüz Bilgi İşlem birimine mümkün olan en kısa zamanda bildirilmeli ve Yetkili personelce ilgili kullanıcının yetki ve hesap özellikleri buna göre güncellenmelidir.
8.3.10. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantıyı herkese açık güvenli olmayan alanlarda(kafeler, lokantalar, oteller vb.) yapmamalıdır.
8.3.11. Uzaktan erişim yaparken sahibi bilinmeyen/herkes tarafından erişilebilen cihazlar(internet kafe, otel bilgisayarları, kiosklar vb.) kullanılamaz
8.3.12. Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmış olması gerekir:
8.3.12.1. Cihazlara kişisel güvenlik duvarı kurulur ve aktif halde olmalıdır.
8.3.12.2.İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanmalıdır.
8.3.12.3. Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir koruma yazılımı olmalıdır. Yazılımın kendisi ve imza dosyaları güncel halde tutulur.
8.3.12.4. Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.
8.3.12.5. Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.
8.3.12.6. Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise dizüstü bilgisayar kilidi kullanılmak suretiyle çalınmaya karşı cihaz emniyete alınır.
8.3.12.7. Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (WİFİ, bluetooth, RS232 vb.) pasif hale getirilir.
8.3.12.8. Disk şifreleme vb. araçlarla bilgisayarlarda tutulan verilerin şifreli olarak saklanması sağlanır. Disk şifreleme işlemleri için https://bilgiguvenligi.saglik.gov.tr/ adresinde yayımlanan sürücü şifreleme el kitaplarından yararlanılır.
8.3.12.9. Uzaktan çalışma için kullanılan bilgisayarların yerel disklerinde yer alan kurumsal verilerin yedeklenmesi için gerekli tedbirler alınır. Alınacak bu yedekler sadece şifreli ortamlarda ve/veya şifreli yedeklenmiş olarak tutulabilir.
8.3.12.10. Uzaktan çalışma ve uzaktan erişim için kullanılacak cihazlara çok faktörlü kimlik doğrulama yapılarak giriş yapılması tercih edilir.
8.3.12.11. Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.
8.3.12.12. Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.
8.3.12.13. Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.

8.3.12.14. Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için "jailbreak" veya "rootlama" işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.
8.3.12.15. Tüm mobil cihazlara (telefon/tablet) mutlaka lisanslı anti-virüs yazılımı kurulması gerekir.
8.3.12.16. Kullanılan her türlü mobil cihaz için üreticinin sağladığı işletim sistemi güncelleştirmeleri ve yazılım güncelleştirmeleri mutlaka periyodik olarak kontrol edilir ve uygulanır.

8.4.Kurum Parola Politikası

8.4.1. Müdürlüğümüz ve bağlı Sağlık Tesislerinde kullanılan sistem ve uygulamaların, kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmaya zorlamaları sağlanmalıdır.
8.4.1.1. Parolalar en az 8 (sekiz) karakterden oluşur. Sistem yönetim işlemlerinde kullanılan parolaların (root, administrator, sysadmin vb.) en az 12 karakterden oluşması tavsiye edilir.
8.4.1.2. İçerisinde en az 1 (bir) tane büyük ve en az 1(bir) tane küçük harf bulunur.
8.4.1.3. İçerisinde en az 1 (bir) tane rakam bulunur.
8.4.1.4. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !,?,A,+,$,#,&,/,{,*,-,],=,...)
8.4.1.5. Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab...)
8.4.1.6. Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf,1234,zxcvb...)
8.4.1.7. Kişisel bilgiler veya klavye kombinasyonları ile basitçe üretilebilecek karakter dizilerinin kullanılması engellenir. (Örneğin 12345678, qwerty, doğum tarihi, çocuğun adı, soyadı gibi)
8.4.1.8. Sözlükte bulunabilen kelimelerin kullanılması engellenir.
8.4.1.9. Kullanıcının son 3 (üç) parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir.
8.4.1.10. Sistem ve uygulamalarda oturum kontrolü yapılarak bir kullanıcı adı ve parolasının aynı anda birden çok bilgisayarda kullanılması engellenir.
8.4.2. VTYS, aktif dizin sunucusu, uygulama sunucusu, ağ cihazları gibi sistem hesaplarına ait parolalar (root, administrator, sysadmin vb.) en geç 3 (üç) ayda bir değiştirilir.
8.4.3. Kullanıcı hesaplarına ait parolalar (örnek: SBYS, e-Posta, web, masaüstü bilgisayar vb.) en geç 6 (altı) ayda bir değiştirilmesi sağlanır.
8.4.4. Sistem yöneticileri ayrıcalıklı işlemleri normal kullanıcı adı ve parola ile yapmaz. Bu maksatla farklı kullanıcı adı ve parola kullanılır.
8.4.5. Parolalar, e-Posta iletilerine veya herhangi bir elektronik forma eklenmez.
8.4.6. Parolalar gizli bilgi olarak muhafaza edilir. Kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.
8.4.7. Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu bölümde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.
8.4.8. İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.

9. İŞLETİM GÜVENLİĞİ

9.1.Kurum Yedekleme Politikası

Bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerine ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi için standartları belirlemek amacıyla hazırlanmıştır.

9.1.1. Bilgi sistemlerinde oluşabilecek hatalar karşısında, sistemlerin kesinti sürelerine ve olası bilgi kayıplarını en az düzeye indirmek için sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekmektedir.
9.1.2. Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk bölümlerinde ve offline olarak Backup Server, Harici Disk, Nas Cihazları, DVD veya CD ortamına yedekleri alınmalıdır.
9.1.3. Yedekleme ortamları (Backup Server, Harici Disk, Nas Cihazları, DVD veya CD vb.) fiziksel olarak bilgi işlem odalarından farklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır, veriler offline ortamlarda sınırsız süreyle saklanmalıdır.
9.1.4. Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintilerin kritik olduğu sistemlerin bir varlık envanteri çıkarılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak kayıt altına alınmalıdır.
9.1.5. Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya, bilgi sistemlerinde değişiklik yapma yetkili personel ve yetki seviyeleri kayıt altına alınmalıdır.
9.1.6. Kurumun gereklilikleri doğrultusunda bir Kurum Yedekleme Planı hazırlanmalı(Örneği Ek-5 Kurum Yedekleme Planı) ve bu plana göre yedeklerin düzenli aralıklarla alınması ve sürekli olarak gözden geçirilmesi gerekir.
9.1.7. Bu Yedekleme planları doğrultusunda yapılan yedekleme işlemleri düzenli olarak kontrol edilmeli ve Yedekleme Kontrol Listesi(Örneği Ek-6 Yedekleme Kontrol Listesi) ile kayıt altına alınmalıdır.
9.1.8. Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır bu konu ile ilgili sorumluluklar tamamlanmalı ve atamalar yapılmalıdır.
9.1.9. Yedeklerin alınacağı sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak konu ile ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
9.1.10. Yedek ünite, gereksiz yer tutmamak üzere kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dâhil edilmemelidir.
9.1.11. Yedeklenecek bilgiler değişik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
9.1.12. Yeni sistem ve uygulamalar devreye alındığında yedekleme sistemleri güncellenmelidir.
9.1.13. Yedekleme işlemi için gerekli sayı ve kapasiteye uygun yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.
9.1.14. Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
9.1.15. Geri yükleme prosedürlerinin düzenli olarak ve test edilecek etkinlerinin doğrulanması ve operasyonel prosedürlerin ön gördüğü süreler dâhilinde tamamlanabileceğinden emin olunması gerekir.
9.1.16. Yedek ünitelerin saklandığı ortamların fiziksel uygunluğunun güvenliği sağlanmalıdır.
9.1.17. Yedekleme standartı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması gerekmektedir.
9.1.18. Veri yedekleme standartının, yedekleme sıklığı kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasındaki sorunlardan nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanması ve işlerliği periyodik olarak gözden geçirilmelidir.

9.1.19. Mümkünse yedeklerin bir felaket anında kısa sürede devreye alınabilmesi için Kurum dışında bir yerde Felaket Kurtarma Merkezi (FKM)'nde tutulmalı ve bu veriler sürekli güncellenmelidir.

9.1.20. Geri Dönüş Testleri

9.1.20.1. Yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için belirli aralıklarla geri dönüş testlerinin yapılması gerekir.

9.1.20.2. 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.

9.1.20.3. 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.

9.2. Antivirüs Yönetimi

9.2.1. İl Sağlık Müdürlüğümüz ve bağlı sağlık tesisleri ağına bağlı olarak çalışan bilgisayarlara lisanslı antivirüs yazılımının yüklenmesi zorunludur. Eğer kullaıncının bilgisayarında antivirüs yazılımı yok ise bunu bilgi işlem birimine bildirmekle yükümlüdür.

9.2.2. Tüm bilgisayarlar lisanslı antivirüs yazılımı ile korunur. Antivirüs yazılımının virüs veritabanı güncel tutulur. Kullanıcı, antivirüs yazılımının güncelleme yapmadığını fark ederse derhal bilgi işlem birimine bildirir.

9.2.3. Kullanıcı, bilgisayarındaki antivirüs yazılımını kapatmamalı yada devre dışı bırakmamalıdır.

9.2.4. Kullanıcı, bilgisayarına taktığı CD/DVD, USB, Taşınabilir Disk vb. ortamları mutlaka güncel antivirüs yazılımıyla taratmalı ve tarama tamamladıktan sonra kullanmalıdır.

9.2.5. Kullanıcıların, bilgi sistemlerine zarar verebilecek herhangi bir bilgisayar kodunun kasıtlı olarak yazmaları, çoğaltmaları, kopyalamaları, üretmeleri ve çalıştırmaları yada tanıtmaları yasaktır.

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

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

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

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

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

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

10. BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

10.1. İhlal Bildirimi ve Olay Yönetimi

10.1.1. İl Sağlık Müdürlüğü ve bağlı sağlık tesisleri çalışanları ve vatandaşlar tarafından tespit edilen Sağlık Bakanlığı uygulamaları ile ilgili her türlü bilgi güvenliği ihlal olayı **https://bilgiguvenligi.saglik.gov.tr/** adresinde yer alan merkezi ihlal bildirim sistemine girilir.

10.1.2. Olay bildirim sistemini kullanamayacak durumda olanlar kendi kurumlarındaki bilgi güvenliği yetkililerine bildirim yapabilir. Bilgi güvenliği yetkilisine yapılan bildirimler, bilgi güvenliği yetkilisince merkezi ihlal bildirim sistemine girilir.
10.1.3. Merkezi ihlal bildirim sistemine girilen olaylar; SBSGM Bilgi Güvenliği Politikaları Kılavuzunda belirtildiği şekilde Sağlık Bilgi Sistemleri Genel Müdürlüğünce işlem tesis edilir.
10.1.4. Küçük çaplı, yalnızca kendi kurumunu ilgilendiren ve Sağlık Tesisi Bilgi Güvenliği Yetkilisi kendi imkânları ile yerel olarak çözülebilecek olaylarda Ek-4 OLAY BİLDİRİM VE MÜDAHALE FORMU doldurulur. Bu tür olaylarda Sağlık Tesisi Bilgi Güvenliği Yetkilisince veya bilgi işlem personeli tarafından gerekli müdahale yapılır. Müdahale sonrası Ek-4 OLAY BİLDİRİM VE MÜDAHALE FORMU'nun 2'nci Bölümünü (Olay Müdahale) doldurulur ve İl Bilgi Güvenliği Yetkilisine bilgi verilir.
10.1.5. Hizmet verdiği kurumla birlikte diğer kurum ya da kişileri etkileyecek şekilde iş sürekliliğine zarar veren veya durduran, acil müdahale gereken, kurum imajına zarar verebilecek ihlal olaylarında olay müdahale ekibi kurulur. İlgili ekip, gerekli müdahaleyi yapar. Destek istediği durumlarda sırasıyla İl Sağlık Müdürlüğümüz SOME ekibinden, Sektörel SOME'den görüş/destek alır. Olayın çözümünde Ek-4 OLAY BİLDİRİM VE MÜDAHALE FORMU'nun 2'nci Bölümünü (Olay Müdahale) doldurarak bilgiguvenligi@saglik.gov.tr adresine gönderir.

11. TEDARİKÇİ İLİŞKİLERİ

11.1. Mal ve Hizmet Alımları Güvenliği

11.1.1. Satın alma faaliyetleri; 4734 sayılı Kamu İhale Kanunu, 4735 sayılı Sözleşmeler Kanunu, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, Kamu İhale Kurumu Tebliğleri ve yönetmeliklerinin tanımlamış olduğu usul ve esaslara göre yapılır.
11.1.2. 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:
11.1.2.1.Yüklenici sözleşmeye konu yükümlülüklerini ifa ederken, Bakanlık Bilgi Güvenliği politikalarına uymak zorundadır. Bakanlığın Bilgi Güvenliği Politikaları, "Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi" ve "Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu"nda açıklanmıştır. Bahse konu dokümanlara, Bakanlığın resmi web sitesinden erişilebilir.
11.1.2.2. Bakanlık/Kurum BGYS Politikaları uyarınca, idareye 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.
11.1.2.3.İhaleyi kazanan firma ile sözleşmenin imzalanmasını takiben kurumdaki yetkili makam (Satın Alma Birimi vb.) huzurunda "Kurumsal Gizlilik Sözleşmesi" imzalanır.
11.1.2.4."Kurumsal Gizlilik Sözleşmesi" ve ihaleye konu iş kapsamında çalıştırılacak personelin "Personel Gizlilik Sözleşmeleri" imzalanmadan ve idareye teslim edilmeden, yüklenici tarafından işe başlanamaz.
11.1.2.5.Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, "Personel Gizlilik Sözleşmeleri" idareye teslim edildikten sonra tanımlanır.

11.1.2.6. 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.

11.1.3. Yukarıda belirtilen gereksinimlere ek olarak, aşağıdaki konular teknik/idari şartnamelere veya tedarikçiler ile imzalanacak gizlilik sözleşmelerine eklenerek, garanti altına alınır:

11.1.3.1. Alınan hizmetle ilgili olarak güvenlik kontrol gereksinimleri, hizmet seviyeleri ve yönetim gereksinimleri,

11.1.3.2.Yükleniciye verilecek veya erişilecek bilgilerin tanımları ile bu bilgilerin sağlanma veya erişim metodları,

11.1.3.3.Yüklenici ile paylaşılacak olan bilgilerin kabul edilebilir kullanım kuralları ve gerekiyorsa kabul edilemez kullanım durumları,

11.1.3.4.Yüklenici personeli için erişim yetkilendirme ve yetki kaldırma prosedürleri,

11.1.3.5. Bilgi güvenliği olay müdahale prosedürleri (özellikle olay bildirimi ve olay müdahalesinde işbirliği kuralları).

11.1.4. "Kurumsal Gizlilik Sözleşmesi" ve "Personel Gizlilik Sözleşmesi" olarak Ek'te yer alan sözleşmeler kullanılabilir. Bahse konu sözleşmelerin içeriği, satın almaya konu mal veya hizmetin türüne ve kurumun kendine özgü ihtiyaçlarına bağlı olarak revize edilip kullanılabilir.

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

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

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

11.1.8. Tedarikçinin çalıştırılacağı personelin adli sicil kayıtlarını sorgulatıp, bunları idareye bildirmesi istenir. Projelerde çalışacak personelin; TCK'nın 53'ncü maddesinde belirtilen süreler geçmiş olsa bile devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan mal varlığı değerlerini aklama ve kaçakçılık suçlarından mahkûm olmamış olması gerekir.

11.1.9. Satın alma faaliyetine konu iş uygulama/yazılım geliştirme ise; uygulama ile ilgili gerekli dokümantasyonun hazırlanması, ilgili projeye ait kaynak kodların teslim edilmesi gibi hususlar, idare tarafından açıkça tanımlanır. Ayrıca geliştirilen yazılım/uygulamada özel nitelikli kişisel veriler işlenecek ise KVKK'nın 2018/10 sayılı kararında belirtilen ilave güvenlik tedbirleri ile ilgili hususlar da teknik şartnamelere eklenir.

11.1.10. Anlaşmalar gereği, tedarikçilerce üretilen hizmet raporları düzenli olarak gözden geçirilir ve proje ilerleme toplantıları yapılır.

11.1.11. Tedarikçilere verilen fiziksel ve mantıksal erişimler, İl Bilgi Güvenliği Alt komisyonlarında gözden geçirilir. Hassasiyet arz eden erişimler için yönetim onayı alınır. Olası güvenlik zafiyetlerinin engellenmesi için yüklenici personeline verilen yetkiler periyodik olarak kontrol edilir. İhtiyacın bitmesi durumunda, verilen yetkiler kaldırılır. Personelin kurumla ilişiği kesilir kesilmez, erişim yetkileri de kapatılır.

11.1.12. Yazılım tedarikçilerinin destek faaliyetleri (ör: tedarikçi personelinin sistem üzerinde çalıştırdığı komutların iz kayıtlarının tutulması ve incelenmesi gibi) izlenir.

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

11.2. SBYS Firmaları ile İlişkilerde Dikkat Edilecek Hususlar

11.2.1. Sağlık tesisleri tarafından klinik, idari ya da yönetimsel amaçlarla kullanılan, gerektiğinde diğer bilgi yönetim sistemleri ile veri alış verişi yapabilen yazılım, sistem ya da alt sistemler Sağlık Bilgi Yönetim Sistemi (SBYS) olarak adlandırılır.

11.2.2. Hastane Bilgi Yönetim Sistemi (HBYS), Aile Hekimliği Bilgi Sistemi (AHBS), Laboratuvar Bilgi Yönetim Sistemi (LBYS), Görüntü Saklama ve Arşivleme Sistemleri/Radyoloji Bilgi Sistemi (PACS/RIS) vb. yazılımların tamamı SBYS yazılımıdır.

11.2.3. Sağlık kuruluşlarında kullanılacak tüm SBYS yazılımlarının Bakanlık tarafından yayımlanan sağlık bilişimi standartlarına ve veri gönderim servislerine uyumlu olmaları gerekmektedir. SBYS üreticisi firmalar, Bakanlık ve İl Sağlık Müdürlüğümüz tarafından talep edilen geliştirmeleri ve güncellemeleri belirtilen süreler içerisinde sistemlerine yansıtmakla mükelleftir.

11.2.4. SBYS yazılımları, sağlık kuruluşları içerisindeki entegre edilebilir cihazlar, sistemler ve Bakanlığın tanımladığı ve yürüttüğü uygulamalarla uyum sağlamak zorundadır.

11.2.5. SBYS yazılım üreticileri, Bakanlık Kayıt Tescil Sistemine (KTS) kayıt olarak aktif listede yer alması gerekmektedir.

11.2.6. Kullanılmasına karar verilen sağlık bilişimi standartları ve veri gönderiminde dikkat edilecek hususlar SBSGM web sayfasında yayımlanır ve güncellenir. SBYS yazılımı üreticilerinden bu güncellemeleri takip etmesi ve sisteminde gerekli güncellemeleri yapması beklenir.

11.2.7. Sağlık hizmeti sunucularınca SBYS yazılım üreticilerinden, ürettiği SBYS yazılımının minimum şartlara uyum sağladığını gösteren "KTS Kayıt Belgesi" istenir. KTS kayıt belgesinin geçerliliği KTS web sayfası üzerinden sorgulanır.

11.2.8. KTS yetki belgesi olmayan, geçersiz yetki belgesi ibraz eden ya da KTS web sayfasında pasif listede yer alan SBYS yazılım üreticileri ile sözleşme imzalanmaz.

11.2.9. Sağlık kuruluşları ile SBYS yazılım üreticisi arasında yaşanabilecek uyuşmazlıklarda uygulanacak cezai şartların SBYS yazılım üreticisi ile yapılacak sözleşmelerde yer alması sağlanır.

11.2.10. Sağlık kuruluşları ve aile hekimleri, SBYS yazılım üreticisi ve bayileriyle ayrıca gizlilik sözleşmesi imzalamalıdır. Sağlık tesisleri ve aile hekimleri bu maksatla Ek'teki Kurumsal Gizlilik Sözleşmesini kullanabilecekleri gibi kendileri de sözleşme metinlerini oluşturabilirler.

11.2.11. SBYS'lerin ilk kurulumu esnasında uzaktan destek ile kurulum talepleri kabul edilmez.

11.2.12. SBYS yazılım üreticisi, ilk kurulum esnasında çalıştıracağı personel ile ilgili planlamayı kurulum ve proje planında detaylı olarak açıklamak zorundadır.

11.2.13. Kurulum ve proje planının işletmeye alınacağı tarihe, sağlık kuruluşları tarafından karar verilir.

11.2.14. Sağlık kuruluşları, HBYS tedarikçilerinden en az altı ayda bir kez olacak şekilde son alınan yedek üzerinden veri kurtarma testi yapmasını istemeli ve gerekli kontrolleri yapmalıdır.

11.2.15. Herhangi bir sebeple mevcut SBYS yazılımının kullanımına son verilirse, verilerin tamamı orijinal veri tabanı formatında, kolay ve sorunsuz okunabilir bir medya ortamında, 3 (üç) kopya halinde sağlık kuruluşuna teslim edilmek zorundadır.

11.2.16. Kritik alanlardaki değiştirme ve silme işlemlerinin, ancak yetki ölçüsünde yapılması gerekir. Değişikliklere sonradan erişim ve geri düzeltme için mutlaka iz kaydı dosyaları detayları olarak tutulmalı veya VTYS katmanındaki denetleme (audit) uygulama yazılımından da desteklenir olmalıdır.

11.2.17. Kişisel sağlık verileri özel nitelikli kişisel veriler kapsamında olması sebebiyle; sözleşme süresince veya sonrasında kayıtlı tüm veriler hiçbir surette, hiçbir zaman SBYS üreticisinde kalmak üzere kopyalanamaz, çıktı alınamaz, firma sunucularına aktarılamaz, ifşa edilemez.
11.2.18. SBYS yazılımları tüm sistem genelindeki kullanıcı, işlem ve bilgi düzeylerinde bilgi gizliliğini ve güvenliğini sağlamak zorundadır. Her kullanıcının gerektiğinde değiştirilebilir kişisel bir parolası olmalıdır. Bu parola ile farklı bir lokasyonda oturum açıldığında ilk oturum otomatik olarak kapatılmalıdır. Bir kişiye ait parolanın birden çok kişi tarafından kullanılmasına izin verilmemelidir.
11.2.19. Çeşitli yetki düzeyleri ve grupları tanımlanabilmeli, yetki değişimi SBYS Yöneticisi tarafından yapılabilmelidir. Verilere erişim bu tanımlamalar çerçevesinde yapılmalıdır.
11.2.20. SBYS'de kullanıcılar için saat bazında sisteme giriş sınırlandırması yapılabilmelidir.
11.2.21. SBYS'de kullanıcıların otomasyona giriş-çıkış zamanları ve geçersiz giriş denemeleri istenildiğinde raporlanabilmelidir.
11.2.22. Poliklinik, Klinik, Laboratuvar bazında yetkilendirmeler yapılabilmelidir. Kullanıcının yetki verilmeyen bir polikliniktekı hasta listesine erişimi engellenmelidir.
11.2.23. SBYS yazılımlarında Kurum Parola Politikası maddesinde belirtilen parola özellikleri tanımlanabilmeli ve bu kurala uymayan parolalar kabul edilmemelidir.
11.2.24. Sağlık kuruluşu ile ilişiği kalıcı olarak kesilen tüm personelin SBYS erişim yetkisi tamamen ve otomatik olarak iptal edilmelidir.
11.2.25. Geçici olarak sağlık kuruluşunda bulunmayan (izin, rapor, geçici görev kurs, eğitim vb.) personelin SBYS'ye girişi otomatik olarak engellenmelidir.
11.2.26. Sunucu işletim sistemi, sunucu yazılımları, veri tabanında yapılacak yapısal değişiklikler gibi tüm sistemi etkileyen güncellemeler mesai saatleri dışında veya hasta yoğunluğunun en az olduğu saatlerde yapılmalıdır. Acil müdahale edilmesi gereken bir arıza durumunda ise mesai saatleri içinde güncelleme yapılabilir.

EKLER:

1. Personel Gizlilik Sözleşmesi
2. Bilgi Güvenliği Farkındalık Bildirgesi
3. Kurumsal Gizlilik Sözleşmesi
4. Olay Bildirim ve Müdahale Formu
5. Kurum Yedekleme Planı
6. Kurum Yedekleme Kontrol Listesi
7. İşe Başlama Formu
8. İşten Ayrılma Formu
9. Görev Devir-Teslim Formu