İÇİNDEKİLER

Bilgi güvenliği politikası BGYS'nin en kritik öğesidir. Bir güvenlik politikası, verilerin ve kaynakların gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için bilgisayar kaynaklarına erişen herkesin uyması gereken asgari kuralları ve prosedürleri tanımlar. Ayrıca, kurumun bilgi güvenliği bakış açısını yansıtır, güvenlik sorumluluklarını tanımlar ve bilgi güvenliği olaylarına müdahale yaklaşımını ortaya koyar.

1-AMAÇ

Bu Bilgi Güvenliği Yönetim Sistemi Politikasının amacı, bilginin işlenmesi süreçlerinde bilgi güvenliğinin sağlanmasına yönelik tedbir almak; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden veya dışarıdan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak; yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesinde bilgi güvenliği açısından uyulması gereken usul ve esasları belirlemektir.

2- KAPSAM

Bu Politika, Hastanemizde görev yapan tüm personel ile kendilerine herhangi bir nedenle Bakanlık bilgi ve bilgi işleme tesislerine erişim yetkisi verilenleri, bilgi sistemlerini, insan kaynaklarını, fiziksel ve çevresel güvenlik sistemlerini, hizmet sağlayıcılarını, sistem, veri ve bilgi kullanıcılarını ve kurallarını kapsar.

3- TANIMLAR

Bilgi: Kurum için değeri olan, uygun bir şekilde korunması gereken, yazılı olarak veya bilgi sistemleri üzerinde işlenen tüm kaynakları,

Bilgi işleme: Veri ve bilgilerin manuel veya bir otomasyon sisteminin parçası olarak elde edilmesi, kaydedilmesi, depolanması, muhafazası, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veri ve bilgiler üzerinde gerçekleştirilen her türlü işlemi,

Bilgi işleme tesisi: Bilgi işlemede kullanılan her türlü sistem, servis, altyapı ve bunların konuşlandırıldığı fiziksel mekânları,

Bilgi güvenliği: Bilgi ve bilgi işleme tesislerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümünü,

Bilgi güvenliği yetkilisi: İlgili kurumdaki alt komisyon tarafından görevlendirilen ve komisyon adına bilgi güvenliği politikalarının uygulanması için yetki verilen kişiyi,

Bilgi güvenliği yönetim sistemi: Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, yazılı hale getirilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününü,

Bilgi sistemleri: Donanım, yazılım, veri, bilgisayar ağları ve insan unsurlarından oluşan, veri ve bilgileri toplayan, kaydeden, işleyen, dönüştüren ve yayan sistemler bütününü,

BGYS: Bilgi güvenliği yönetim sistemini,

Müdürlük: Kırklareli İl Sağlık Müdürlüğünü,

Hastane: Kırklareli Eğitim ve Araştırma Hastanesi

Kılavuz: Bilgi Güvenliği Politikaları Kılavuzunu,

Kullanıcı: Bakanlık merkez ve taşra teşkilatı ile bağlı kuruluşlarda yer alan bilgi ve bilgi işleme tesislerine erişen tüm kişileri,

Kurumsal SOME: Sektörel SOME tarafından belirlenen ve kritik altyapı işleten kurumlarda kurulan siber olaylara müdahale ekibini,

Rehber: Kurumsal SOME Kurulum ve Yönetim Rehberini,

Sızma testi: Bilişim sistemleri üzerinde, saldırgan bakış açısıyla güvenlik zafiyetlerinin tespit edilip bulunan zafiyetlerin kullanılarak sistemlere sızılmaya çalışılması ve raporlanması işlemlerini,

Siber güvenlik: Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini,

Siber ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,

Siber olay: Bilgi sistemleri ve endüstriyel kontrol sistemleri (ağa bağlanabilen diğer cihazlar, tıbbi cihazlar vb.) veya bu sistemlerde tutulan veya işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,

Siber olaya müdahale: Bilgi sistemleri ve endüstriyel kontrol sistemleri (ağa bağlanabilen diğer cihazlar, tıbbi cihazlar vb.) veya bu sistemlerde tutulan veya işlenen verilerin gizlilik, bütünlük veya erişilebilirliğinde meydana gelme riski bulunan veya meydana getirilen siber olayın kaynağını, nedenlerini ve sonuçlarını tespit ederek siber olayın devam etmesini, tekrarını veya zarar vermesini önleyen çalışmaları,

SOME: Siber olaylara müdahale ekibini,

SOME ekip lideri: İlgili kurumun bilgi güvenliği yönetim komisyonu tarafından görevlendirilen, kurumsal SOME faaliyetlerini yürütmekle görevli kişiyi,

Sektörel SOME: Bakanlık bünyesinde kurulan siber olaylara müdahale ekibini,

Sosyal mühendislik testi: Kurum çalışanlarının kişisel hesaplarının güvenliği ve bilgi güvenliği politikaları ile ilgili farkındalık seviyelerini ölçmek için yapılan, senaryoları önceden paylaşılmış kontrolleri,

Veri: Bilginin işlenmemiş halini,
ifade eder.

4-BİLGİ GÜVENLİĞİ ORGANİZASYONU

4.1. Bilgi Güvenliği Alt Komisyonları

4.1.1. Bakanlık merkez, bağlı kuruluşlar ve il sağlık müdürlükleri bünyesinde, bilgi güvenliği ve siber olaylara müdahale faaliyetlerini yürütmek ve koordine etmek üzere, Bakanlık bünyesinde oluşturulan komisyona benzer şekilde "bilgi güvenliği alt komisyonları" oluşturulur.

4.1.2. Alt komisyonların çalışmaları, merkez teşkilat ve bağlı kuruluşlarda en az daire başkanı, taşra teşkilatında ise en az başkan seviyesinde bir yönetici tarafından koordine edilir. Bu kişiler aynı zamanda ilgili kurumların "bilgi sistemleri koordinatörü" olarak görev yapar.

4.1.3. Alt komisyon çalışmalarında bilgi güvenliği yetkilisi ve kurumsal SOME ekip liderine ilave olarak; kurumların bilgi işlem ve istatistik, insan kaynakları, kalite, hukuk ve fiziksel güvenlikten sorumlu birimlerinin yöneticileri de komisyon üyesi olarak yer alır. Ayrıca gerekli görülecek diğer personel de komisyon toplantılarına davet edilir.

4.1.4. Alt komisyonların görevleri şunlardır: A.2.3.4.1. Yönerge ve Kılavuzda belirtilen hususlar çerçevesinde, kendi kurumları bünyesinde uygulanacak BGYS'ye yönelik çalışmaları koordine eder.

4.1.5. Bakanlık tarafından yayımlanan eylem planında yer alan hususların gerçekleştirilmesini sağlar.

4.1.6. Bilgi güvenliği yetkili/yetkililerini belirler ve görevlendirmesini yapar.

4.1.7. 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.

5. İNSAN KAYNAKLARI VE SON KULLANICI GÜVENLİĞİ

5.1. İşe Alma Öncesinde Yapılacak Kontroller

5.1.1. 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.

5.1.2. İşe alma öncesinde yapılacak güvenlik kontrollerinin amacı, çalışanların kendilerinden beklenen sorumlulukları anlamalarını sağlamak ve düşünüldükleri roller için uygun olmalarını temin etmektir.
5.1.3. İşe alınacak adaylar iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol (tarama yapılır) edilir.

5.1.4. Tarama yapılırken yürürlükteki yasal mevzuata mutlak şekilde uyulur. Yasal ve etik olmayan tarama yöntemleri kullanılmaz. Tarama esnasında oluşturulan/elde edilen kayıtlar uygun şekilde saklanır. Saklanmasına ihtiyaç duyulmayan kayıtlar bekletilmeksizin imha edilir.

5.1.5. İşe alınacak kişilerin eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilmesi için aşağıdaki yöntemlerden biri ya da birkaçı birlikte kullanılabilir.

5.1.5.1. Kişi özgeçmişinin doğrulanması (belgelerin tamlığı),

5.1.5.2. Kişinin atanacağı görevle ilgili eğitim ve tecrübe açısından gerekli yeterliliğe sahip olmasının sağlanması,

5.1.5.3. Beyan edilen akademik ve işle ilgili niteliklerin doğrulanması (diplomaların, referans mektuplarının, bonservis belgelerinin doğru ve geçerli olduğunun teyit edilmesi),

5.1.5.4. 657 sayılı Kanunun 48/8 maddesi gereği Yönetim Hizmetleri Genel Müdürlüğünce, devlet memurluğuna atanacak kişiler ile ilgili olarak 12 Nisan 2000 tarihli ve 24018 sayılı Resmi Gazetede yayımlanan "Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği" uyarınca "güvenlik soruşturması ve/veya arşiv araştırması" yaptırılması,

5.1.5.5. 657 sayılı Kanuna bağlı olmayan diğer personel için bağlı oldukları yasal mevzuatta yer alan hükümler uyarınca güvenlik incelemelerinin yaptırılması,

5.1.5.6. Yüklenici personeli, destek personeli vb. statüde çalışacak personelin adli sicil kayıtlarının istenmesi ve incelenmesi.

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

5.1.7. 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.

5.1.8. 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.

5.2. Çalışma Esnasında Uygulanacak Kontroller

5.2.1. Çalışma esnasında uygulanacak güvenlik kontrollerinin amacı, çalışanların işlerini yaparken bilgi güvenliği ile ilgili sorumluluklarının farkında olmalarını ve beklenen şekilde yerine getirmelerini sağlamaktır.
5.2.2. İşe yeni başlayan personelin başlayış işlemlerinin eksiksiz olarak yapılmasını sağlamak için "işe başlama formu" hazırlanır ve uygulanır.

5.2.3. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi sorumludur.

5.2.4. 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 mutlaka yer alır.

5.2.5. Üst yönetim, 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.

5.2.6. Bilgi güvenliği ile ilgili beklentiler ve sorumluluklar, çalışanların görev tanımlarına eklenir.

5.2.7. Çalışanların kuruluşun bilgi güvenliği politikasına uyumu izlenir.

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

5.2.9. Bilgi güvenliği ihlaline neden olan kişilere yapılacak işlemler (disiplin prosedürü) önceden belirlenir ve kişilere duyurulur. İhlal oluştuğunda, disiplin prosedüründe yazan hususlar uygulanır.

5.3. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri

5.3.1. Kurumların bilgi güvenliği yetkililerince, bilgi güvenliği teknik ve farkındalık eğitimleri için yıllık olarak uygulanmak üzere bir eğitim planı hazırlanır.

5.3.2. Hazırlanan plan, kurumun bilgi güvenliği alt komisyonu tarafından onaylanır.

5.3.3. Teknik eğitimler için Sağlık Bakanlığı merkez teşkilatı, üniversitelerin sürekli eğitim merkezleri, diğer kamu kurum ve kuruluşları (TSE, TÜBİTAK vb.) ve konusunda uzmanlaşmış eğitim firmaları tarafından sunulan eğitimler tercih edilir. Eğitimler için ihtiyaç duyulan kaynak önceden planlanır ve ilgili yılın bütçesine yeterli ödenek koyulması sağlanır.

5.3.4. Bilgi işleme faaliyetlerinde kullanılan cihaz ve sistemlerin tedarik şartnamelerine, garanti süresini de içerecek şekilde, eğitim verilmesi ile ilgili hükümler konulur. Aynı şekilde cihaz ve sistemler için işletme, bakım, idame hizmet alımlarına, ihtiyaç varsa personelin eğitimine yönelik hükümler eklenir.

5.3.5. 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.

5.3.6. Her yıl tüm personele en az bir kere, yüz yüze (sınıf ortamında veya konferans şeklinde) olacak şekilde bilgi güvenliği farkındalık eğitimi verilmesi tavsiye edilir.

5.3.7. Yüz yüze eğitimler haricinde özellikle bilgi teknolojilerinin sunmuş olduğu yetenekler/fırsatlar da kullanılmak suretiyle personelin farkındalık düzeylerinin artırılması sağlanır. Bu kapsamda;

5.3.7.1. Bilgi güvenliği afişleri,

5.3.7.2. Bilgi güvenliği broşür ve el kitapları, e-bültenler,

5.3.7.3. Bilgisayarların açılış ekranlarına merkezi olarak konulacak ara yüzler,

5.3.7.4. İnternet tabanlı eğitim,

5.3.7.5. Uzaktan eğitim gibi araçlar kullanılabilir.

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

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

5.4. Görev Değişikliği veya İşten Ayrılma İçin Uygulanacak Kontroller

5.4.1. 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.

5.4.2. 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.

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

5.4.4. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi ile insan kaynakları birimi müştereken sorumludur.

5.4.5. 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.

5.4.6. Kişiye 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.

5.4.7. Ayrılan veya görev yeri değişen personel tarafından yürütülen faaliyetlerin aksamaması için birim sorumlusu tarafından gerekli tedbirler alınır.

5.4.8. Mümkünse ayrılan personel ile yeni katılan personelin geçici bir süre birlikte görev yapması sağlanır.

5.4.9. Ayrılan kişiden teslim alınan bilgisayarlar güvenli silme işlemi yapılmadan bir başka kullanıcıya teslim edilemez.

5.5. Kullanıcıların Bilgi Güvenliği Sorumluluğu

5.5.1. Personel, T.C. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzu'nda yer alan koşullara uygun hareket eder. Burada yer alan hükümleri kişisel olarak ihlal etmesi halinde Bakanlığa, görev yaptığı kuruma ve üçüncü kişilere vereceği her türlü zarardan sorumludur.

5.5.2. Personel, görev yaptığı kurum tarafından kendisine teslim edilmiş veya erişim yetkisi verilmiş olan bilgileri, sadece görevi ile ilgili işler için kullanır. Bu bilgileri kendi gizli bilgisi gibi korur ve bilmesi gereken yetkili kişiler haricinde hiçbir kimse ile paylaşmaz. Personel, bilgi paylaşabileceği kişiler konusunda şüpheye düşerse, bilginin sahibi olan veya süreci yöneten birim ile irtibata geçerek veriyi kimlerle paylaşabileceğini teyit eder.

5.5.3. Personel, özel olarak yetkilendirildiği durumlar dışında, hizmet verilen tarafların yetkilileri de dâhil olmak üzere yetkisi olmayan hiçbir kişi ile bilgi paylaşımı yapmaz. Yetkisi olmadığı halde bulunduğu görev ve makamı kullanarak kendisinden ısrarla bilgi talep eden kişileri en yakın amirine bildirir.

5.5.4. Personel, görevi kapsamında kendisine teslim edilmiş olan bilgileri ilgili mevzuata uygun olarak korur, işler ve aktarır. Görev yaptığı kuruma ait bilgileri, yetkisi olmayan üçüncü kişilerin yanında konuşmaz.

5.5.5. Personel, edindiği bilgileri hiçbir kişi, grup, kurum veya kuruluşun menfaati için kullanamaz.

5.5.6. Bakanlığımızda kullanılan bilgi sınıflandırması ile ilgili hususlar Kılavuzun A.4.3 (Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi) numaralı maddesinde açıklanmıştır. Bu kapsamda usulüne uygun olarak sınıflandırılmamış ve etiketlenmemiş olsa dahi; Bakanlığa veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar ve telekomünikasyon sistemleri içerisinde saklanan veriler, donanım-yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu tüm işler gizlidir. Bunların, görevin gerektirdiği durumlar haricinde kullanılması kesinlikle yasaktır.

5.5.7. Personel, görevi ile ilgili olsun veya olmasın edindiği ve gizlilik arz eden her türlü bilgiyi sır olarak saklamak ve bunları üçüncü kişilere hiçbir şekilde iletmemekle yükümlüdür.

5.5.8. Bu yükümlülük, personelin görev yaptığı kurum ile ilişkisinin sona ermesi halinde de devam eder.
5.5.9. Personel, görevi nedeniyle edindiği gizli bilgiler hakkında, hiçbir sebeple yazılı veya sözlü açıklama yapamaz.

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

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

5.5.12. Personel, başkasına zarar vermek ya da kendisine veya başkasına haksız yarar sağlamak maksadıyla yahut herhangi bir maksat gütmeksizin, kullandığı bilgi işleme ortamlarını ve bu ortamlarda saklanan verileri kısmen veya tamamen tahrip etmek, değiştirmek, silmek, sistemin işlemesine engel olmak veya yanlış biçimde işlemesini sağlamak gibi davranışlarda bulunamaz.

5.5.13. Personel, hangi amaçla olursa olsun görevi kapsamında edindiği bilgileri, bilgi işleme ortamlarında çeşitli şekillerde (basılı, manyetik vb.) bulunabilecek olan verileri, yetkisiz ve izinsiz olarak kullanamaz, kopyalayamaz, taşıyamaz ve aktaramaz.

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

5.5.15. Personel, görev yaptığı kuruma ait sunucular üzerinden kendisine tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP adresini kullanarak gerçekleştirdiği her türlü etkinlikten, Kurum bilişim kaynakları kullanılarak oluşturduğu ve/veya kendisine tahsis edilen Kurum bilişim kaynağı üzerinde bulundurduğu her türlü içerikten (kayıt, doküman, yazılım vb.) sorumludur.

5.5.16. Personel, 5651 sayılı kanun gereği tutulması gereken kayıtlara ilave olarak; görev yaptığı kurum tarafından uygun görülen diğer sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtlarının hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla toplanabileceğini kabul eder.

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

5.6. Elektronik Posta Güvenliği

5.6.1. Hastanemizde 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.

5.6.2. Kişisel Verilerin Korunması Kanunu (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.

5.6.3. Hastanemizde görev yapan 657 sayılı Kanuna bağlı tüm kamu personeline, talep etmeleri halinde kurumsal e-Posta hesabı açılır.

5.6.4. Çeşitli sözleşmeler kapsamında hastanemizde görev yapan ve yaptıkları iş gereği e-Posta hesabı olması gereken personele, sıralı yöneticileri tarafından onay verilmesi halinde kurumsal e-Posta hesabı açılır.

5.6.5. Kurumsal e-Posta adresi isimlendirme politikası, istisnai durumlar dışında "ad.soyad@saglik.gov.tr" şeklindedir. Yeni bir kullanıcı oluşturulurken o kullanıcının adı ve soyadı ile daha önce bir hesap açılmış ise "ad.soyad" kombinasyonunun ardına her seferinde bir artacak şekilde sıradaki sayı eklenir. (yilmaz.demir2, yilmaz.demir3 gibi).

5.6.6. Hastanemizde yer alan birimler için ihtiyaç olması halinde, tüzel e-Posta hesapları açılır. Tüzel e-Posta hesapları, ilgili birimin adı veya yürüttüğü işlev ile alakalı olarak belirlenir. (bilgiguvenligi@saglik.gov.tr, some@saglik.gov.tr gibi).

6.7. Kurumsal ve tüzel e-Posta hesabı açılması için başvuru usulleri ve ilgililerince yapılacak işlemler Kılavuzun A.6.5 (Merkezi Aktif Dizin ve E-Posta Sistemine Erişim) maddesinde belirtilmiştir.

5.6.8. 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.

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

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

5.6.12. Kullanıcılar, parolalarını Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen parola politikaları uyarınca oluşturur ve kullanır.

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

5.6.14. 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.

5.6.15. 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.

5.6.16. 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.

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

5.6.18. 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.

5.6.19. 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.

5.6.20. Kurumsal e-Posta vasıtasıyla gizlilik dereceli veri aktarımı için Kılavuzun A.10.4.17 (e-Posta ile Veri Aktarımı) maddesinde belirtilen hususlara riayet edilir. e-Postaların, gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilir.

5.6.21. e-Posta gönderimlerinde, mesajın en alt kısmına gönderen kişinin kimlik ve iletişim bilgileri yazılır.

5.6.21. Kullanıcılar, gelen veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemek için her türlü tedbiri alır.

5.6.22. Tanınmayan elektronik postaların açılması, eklentilerinde bulunan dosya veya programların indirilip çalıştırılmasından kaynaklanabilecek güvenlik sorunlarının sorumluluğu kullanıcıya aittir.

5.6.23. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-Postalara yanıt verilmez.

5.6.24. Kaynağı bilinmeyen e-Posta ekinde gelen dosyalar kesinlikle açılmaz.

5.6.25. Kullanıcılar, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

5.6.26. e-Posta güvenliği ile ilgili şüpheli bir durum oluşması halinde ivedilikle sistem yöneticisine (eposta@saglik.gov.tr) haber verilir. Ayrıca https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir adresinde yer alan olay bildirim formu doldurulur.

5.7. Sosyal Mühendislik ve Sosyal Medya Güvenliği

5.7.1. 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.

5.7.2. 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.

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

5.7.3.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunuz.

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

5.7.3.3. Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.

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

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

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

5.7.3.7. Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.

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

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

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

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

5.7.4. Kişisel Sosyal Medya Güvenliği

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

5.7.4.2. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.

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

6. ERİŞİM KONTROLÜ

6.1. Erişim Kontrol Politikası

6.1.1. 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.

6.2. Parola Güvenliği

6.2.1. Parola politikaları belirlenirken, sistem ve uygulamaların, kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmaya zorlamaları sağlanır.

6.2.2. Parolalar en az 8 (sekiz) karakterden oluşur. Sistem yönetim işlemlerinde kullanılan parolaların (root, administrator, sysadmin vb.) en az 12 karakterden oluşması tavsiye edilir.

6.2.3. İçerisinde en az 1 (bir) tane büyük ve en az 1(bir) tane küçük harf bulunur.

6.2.4. İçerisinde en az 1 (bir) tane rakam bulunur.

6.2.5. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !,?,A,+,$,#,&,/,{,*,-,],=,...)

6.2.6. Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab...)

6.2.7. Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf,1234,zxcvb...)

6.2.8. Kişisel bilgiler veya klavye kombinasyonları ile basitçe üretilebilecek karakter dizilerinin kullanılması engellenir. (Örneğin 12345678, qwerty, doğum tarihi, çocuğun adı, soyadı gibi)

6.2.9. Sözlükte bulunabilen kelimelerin kullanılması engellenir.

6.2.10. Kullanıcının son 3 (üç) parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir.

6.2.11. Sistem ve uygulamalarda oturum kontrolü yapılarak bir kullanıcı adı ve parolasının aynı anda birden çok bilgisayarda kullanılması engellenir.

6.2.13. VTYS, aktif dizin sunucusu, uygulama sunucusu, ağ cihazları gibi sistem hesaplarına ait parolalar (root, administrator, sysadmin vb.) en geç 3 (üç) ayda bir değiştirilir.

6.2.14. Kullanıcı hesaplarına ait parolalar (örnek: HBYS, e-Posta, web, masaüstü bilgisayar vb.) en geç 6 (altı) ayda bir değiştirilmesi sağlanır.

6.2.15. Sistem yöneticileri ayrıcalıklı işlemleri normal kullanıcı adı ve parola ile yapmaz. Bu maksatla farklı kullanıcı adı ve parola kullanılır.

6.2.16. Parolalar, e-Posta iletilerine veya herhangi bir elektronik forma eklenmez.

6.2.17. Parolalar gizli bilgi olarak muhafaza edilir. Kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.

6.3. Uzaktan Çalışma Ve Erişim

6.3.1. Uzaktan çalışma, 4857 sayılı İş Kanununun 14'üncü maddesine göre; "çalışanların, işveren tarafından oluşturulan iş organizasyonu kapsamında, iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisi" olarak tanımlanmaktadır.

6.3.2. Uzaktan çalışma; ağırlıklı olarak yükleniciler, tedarikçiler, iş ortakları çalışanları gibi Bakanlığımız ile geçici olarak iş ilişkisi olan kişiler tarafından yapılır. Ancak acil durumlarda Bakanlığımız çalışanları için de söz konusu olabilir.

6.3.3. Uzaktan çalışma ile ilgili esaslar belirlenirken, uzaktan çalışmanın ne tür fiziki ortamlarda yapılacağı göz önüne alınır. Muhtemel uzak çalışma ortamları aşağıda sıralanmıştır.

6.3.3.1. Bakanlığımıza ait ancak SBA bağlantısı olmayan yerler (aktif cihaz sayısı 10'dan az olan müstakil bina ve tesisler),

6.3.3.2. Çalışanların evleri veya (tedarikçiler, iş ortakları için) ofisleri,

6.3.3.3. Herkese açık alanlar (kafeler, lokantalar, oteller vb.),

6.3.3.4. Bakanlığımıza bağlı birimlerin fiziki ortamını kullanan ancak kurum ağına (SBA'ya) doğrudan bağlanma izni verilmeyen durumlar (örneğin; kurum tesislerinde çalışan yüklenici personeli, kendi cihazları ile kurumun misafir ağına bağlanan çalışanlar).

6.3.4. Uzaktan çalışma işlemi, yapısı itibarı ile güvensiz olarak kabul edilir ve bilgi güvenliğini sağlamak için ek önlemler alınması gerekir.

6.3.5. Uzaktan çalışma ile ilgili kontrol tedbirleri belirlenirken aşağıda sıralanan dört temel tehdit unsuru/modeli dikkate alınır.

6.3.5.1. Uzak çalışma ortamlarının fiziki güvenliğindeki yetersizlikler,

6.3.5.2. Uzak bağlantının güvenli olmayan ağ ortamları (çoğunlukla internet) üzerinden yapılması,

6.3.5.3. Kurum güvenlik politikaları uygulanmamış güvenilir olmayan cihazların iç ağa bağlanması,

6.3.5.4. İç ağdaki kaynaklara dışarıdan erişim.

6.3.6. Günümüzde teknolojinin bizlere sağlamış olduğu yetenekler kullanılmak suretiyle, farklı yöntemler kullanılarak uzak bağlantı yapılması mümkündür.

6.3.7. Uzaktan erişim için en uygun yöntemin belirlenmesi amacıyla, her ihtiyacın kendine özgü şartları ve risklerinin ayrıntılı olarak değerlendirilmesi gerekir.

6.3.8. Uzaktan erişim yöntemi olarak aşağıda açıklamaları verilen tünelleme, uygulama portalleri, uzak masaüstü erişim veya doğrudan uygulama erişimi yöntemlerinin biri veya birkaçı birlikte kullanılabilir.

6.3.8.1. Tünelleme yöntemi, uzaktan çalışmada kullanılan bilgisayar ile iç ağın kriptolojik yöntemler kullanılmak suretiyle oluşturulan güvenli bir tünel vasıtasıyla birbirine bağlanmasıdır. Tünelleme işlemi, ağırlıklı olarak sanal özel ağ (VPN: Virtual Private Network) teknolojileri vasıtasıyla yapılır. VPN işlemi IP güvenliği (IPsec: IP Security), taşıma katmanı güvenliği (TLS: Transport Layer Security) veya güvenli kabuk (SSH: Secure Shell) protokolleri kullanılmak suretiyle yapılabilir.

6.3.8.2. Uzak masaüstü erişim çözümleri, uzaktan çalışan kullanıcıların kurumun iç ağında yer alan bir sunucu veya istemci bilgisayarın karşısındaymış gibi kullanılmasını sağlar. Bu yöntemde, uzak kullanıcılar bağlanılan bilgisayarın klavye ve fare kontrollerini uzaktan yapar hale gelirler. Uzak masaüstü erişim yöntemleri kendi içlerinde birçok kısma ayrılır. Bazı erişim modellerinde vekil/terminal sunucu vasıtasıyla işlem yapılırken, bazı erişim modellerinde arada bir vekil/terminal sunucu olmadan da bağlantı kurulur.

6.3.8.3. Doğrudan uygulama erişimlerinde, erişilecek uygulamalara ait sunucular kurumun halka açık sunucuların konumlandırıldığı "arındırılmış bölgeye (DMZ:De-Militarized Zone) yerleştirilir. Bu mimaride kullanıcılar genellikle web arayüzleri üzerinden doğrudan ilgili uygulama sunucusuna bağlanarak işlemlerini gerçekleştirirler. Doğrudan uygulama erişimleri genellikle daha az kritik uygulamalar için kullanılır. Bakanlığımızın güvenli metin aktarma iletişim protokolü (HTTPS: Secure Hyper Text Transfer Protocol) kullanılarak erişilebilen e-Posta (https://eposta.saglik.gov.tr) ve EBYS (https://www.ebys.saglik.gov.tr) sistemleri, yine hastanelerde laboratuvar tahlil sonuçlarının vatandaşlar tarafından doğrudan internet üzerinden sorgulanmasını sağlayan sistemler bu mimariye örnek olarak verilebilir.

6.3.8.4. Portal uygulamaları, bir veya daha fazla uygulamanın genellikle web teknolojileri kullanılan tek bir arayüz üzerinden merkezi ve güvenli olarak sunulmasını sağlar. Portal çözümlerinde; portal sunucuları kurumun halka açık sunucuların konumlandırıldığı DMZ bölgesinde, uygulamalara ve veri tabanlarına ait sunucular ise iç ağa yerleştirilir. Bu şekilde uzaktan erişim yapacak kullanıcıların, uygulamalara ve verilere güvenli olarak erişmeleri sağlanır. Portal uygulamaları, doğrudan uygulama erişimlerinin özel bir türüdür.

6.3.9. Uzak çalışma için hangi uzak erişim yönteminin veya yöntemlerinin kullanılacağına, yapılacak risk değerlendirmesine bağlı olarak kurumların bilgi güvenliği alt komisyonları tarafından karar verilir.

6.3.10. Uzaktan erişim ile ilgili yöntem/mimari belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

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

6.3.10.2. 6698 sayılı kanunun açıklanması amacıyla KVKK tarafından yayımlanan 2018/10 sayılı karar uyarınca, özel nitelikli verilerin işlendiği, muhafaza edildiği elektronik ortamlara uzaktan erişim yapılırken, en az iki kademeli kimlik doğrulama sistemi kullanılması yasal bir zorunluluktur. Diğer sistemler için de çok faktörlü kimlik doğrulama yapılması tercih edilir.

6.3.10.3. VPN işlemi (bu maksatla kullanılan ayrı bir yazılım ve/veya donanım yoksa) İl SBA Bulutu girişinde bulunan güvenlik duvarı üzerinden yapılır.

6.3.10.4. Erişim kontrollerinin uygulanabilmesi maksadıyla, hedef bilgisayarlara sabit IP adresi verilir. Yapılacak erişim "erişim yapacak kişi, hedef bilgisayar IP adresi (VLAN adresi) ve kullanılacak port/uygulama" bazında sınırlandırılır.

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

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

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

6.3.10.8. Uzak erişim için yapılan bağlantıda boşta kalma süresi 1 (bir) saati geçemez.

6.3.10.9. Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

6.3.10.9.1. Bağlantı VPN üzerinden yapılır.

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

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

6.3.10.9.4. 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.

6.3.10.9.5. 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.

6.3.10.9.6. 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.

6.3.10.9.7. Uzak bağlantı yazılımı olarak mümkün ise "Microsoft Uzak Bağlantı Programı" kullanılır.

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

6.3.11. Uzaktan çalışma için kullanılacak cihazlar belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

6.3.11.1. Uzaktan çalışma prensip olarak Bakanlığımız birimlerine ait cihazlar ile yapılır.

6.3.11.2. Uzaktan çalışacak kişi Bakanlığımız birimleri ile sözleşme/protokol imzalayan üçüncü taraf personeli ise ve kuruma ait bilgisayar verilemiyorsa, uzak çalışma için hangi tip cihazlar kullanılacağı ve bu cihazlarda alınması gereken tedbirler, ilgili sözleşme/protokollere konulur. Bu maksatla kullanılacak cihazlara ait bilgiler kuruma resmi olarak bildirilir. Kurum tarafından üçüncü taraflarda yapılacak denetimlerde belirtilen işlemlerin yapılıp yapılmadığı aranır.

6.3.11.3. Uzak çalışma kapsamında uzak masaüstü bağlantısı yapılacaksa, şahısların kendilerine ait kişisel cihazlar veya sahibi bilinmeyen/herkes tarafından erişilebilen terminaller kullanılmaz. Kullanıcıların bu tip terminaller üzerinden uzak masaüstü bağlantısı yaptıklarının tespit edilmesi halinde gerekli yasal ve idari yaptırımlar uygulanır.

6.3.11.4. Doğrudan uygulama erişimleri de dâhil uzaktan çalışmanın hiçbir çeşidinde sahibi bilinmeyen/herkes tarafından erişilebilen (internet kafe, otel bilgisayarları, kiosklar vb.) kullanılmaz.

6.3.11.5. Uzaktan çalışma için kullanılacak cihazlarda Bakanlığımıza ait gizlilik dereceli bilgiler depolanacak ise bahse konu verilerin şifreli olarak saklanmasına imkân verecek, tercihan TPM (Trusted Platform Module) yonga setine sahip, işlemci gücü yüksek bilgisayarlar kullanılır.

6.3.12. Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmış olması gerekir:

6.3.12.1. Cihazlara kişisel güvenlik duvarı kurulur ve aktif hale getirilir

6.3.12.2. İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanır.

6.3.12.3. Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir koruma yazılımı tedarik edilir. Yazılımın kendisi ve imza dosyaları güncel halde tutulur.

6.3.12.4. Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.

6.3.12.5. Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.

6.3.12.6. Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise dizüstü bilgisayar kilidi kullanılmak suretiyle çalınmaya karşı cihaz emniyete alınır.

6.3.12.7. Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (WİFİ, bluetooth, RS232 vb.) pasif hale getirilir.

6.3.12.8. 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.

6.3.12.9. 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.

6.3.12.10. Uzaktan çalışma ve uzaktan erişim için kullanılacak cihazlara çok faktörlü kimlik doğrulama yapılarak giriş yapılması tercih edilir.

6.3.12.11. Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.

6.3.12.12. Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.

6.3.12.13. Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.

6.3.12.14. Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için "jailbreak" veya "rootlama" işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.

6.3.12.15. Tüm mobil cihazlara (telefon/tablet) mutlaka lisanslı anti-virüs yazılımı kurulması gerekir.

6.3.12.16. Kullanılan her türlü mobil cihaz için üreticinin sağladığı işletim sistemi güncelleştirmeleri ve yazılım güncelleştirmeleri mutlaka periyodik olarak kontrol edilir ve uygulanır.

7. FİZİKSEL VE ÇEVRESEL GÜVENLİK

7.1. Ekipman Güvenliği

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

7.2. Belli Başlı Temiz Masa Kuralları

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

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

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

7.2.4. Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler Bilgi Güvenliği Politikaları Kılavuzu'nun A.4.5 maddesinde belirtilen yöntemler ile imha edilir.

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

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

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

7.3. Ekipman Yerleşimi Ve Koruması

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

7.3.2. Ekipmanlar, gereksiz erişimleri asgari düzeye indirecek şekilde yerleştirilir.

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

8.3.2.2. Özel koruma gerektiren ekipmanlar izole edilmiş şekilde kullanılır. A.8.3.3.5. Nem ve sıcaklık gibi parametreler izlenir.

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

8.3.2.4. Paratoner kullanılır.

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

7.4. Destek Hizmetleri

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

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

7.4.3. Kritik sistemlerde hizmet kesintisi yaşanmaması için kesintisiz güç kaynağı kullanılır.

7.4.4. Yedek jeneratör ve jeneratörün iş sürekliliği planlarında belirtilen süre boyunca çalıştırılması için yeterli düzeyde yakıt bulundurulur.

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

7.5. Kablolama Güvenliği

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

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

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

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

7.5.5. Ağ tabanlı erişim kontrol sistemleri (NAC: Network Access Control) yoksa kullanılmayan uçlar için kenar anahtar ile dağıtım paneli arasına ara bağlantı kablosu takılmaz.

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

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

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

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

7.6. Ekipman Bakımı

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

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

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

7.6.4. Bakım kayıtları düzenli olarak tutulur.

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

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

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

7.7. Kurum Dışındaki Ekipmanın Güvenliği

7.7.1. Kuruma ait bilgisayarların kurum dışına çıkarılması ya da kişisel/yüklenici firmalara ait bilgisayarların işyerlerine getirilerek kurumsal amaçlarla kullanımı için kurumun bilgi güvenliği alt komisyonu tarafından yetkilendirme yapılması gerekir.

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

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

7.7.4. Bu şekilde kullanılan ekipmanlar Kılavuzun A.4.4 (Taşınabilir Ortam Yönetimi) maddesinde belirtilen tedbirler alınmak suretiyle kullanılır. Bu ekipmanların içinde yer alan bilgilerin gizliliği için ilgili cihazlar Kılavuzun A.7.2.5 (Sabit Ortamdaki Verilerin Şifrelenmesi) maddesinde belirtilen şekilde şifrelenir.

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

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

7.8. Ekipmanın Güvenli İmhası

7.8.1. Üzerlerinde kalıcı olarak veri barındıran ekipmanlar (sunucu, masaüstü veya dizüstü bilgisayarın, merkezi veri depolama birimlerinin ve benzeri bilgi sistem cihazlarının sabit diskleri ile USB flaş sürücüsü, USB hafıza ünitesi, flash disk ya da USB hafıza olarak bilinen

taşınabilir veri depolama ortamları) Kılavuzun A.4.5 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemler kullanılarak imha edilir.

7.9. Fiziksel Ortamların Taşınması

7.9.1. Güvenilir taşıma şekli ve kuryeler kullanılır.

7.9.2. Yönetim tarafından yetkili bir kurye listesi belirlenir.

7.9.3. Kuryelerin kimliğini kontrol eden süreçler geliştirilir.

7.9.4. Paketleme, içeriğin fiziksel hasarlardan yeterince korunmasını sağlayacak şekilde yapılır.

7.9.5. Hassas bilgiler elden teslim edilir veya kurcalanmaya karşı koruma için kilitli kaplar kullanılır.

8. VARLIK YÖNETİMİ

8.1. Varlık

8.1.1. Varlık, kurum için değeri olan herhangi bir şey olarak tanımlanabilir.

8.2. Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi

8.2.1. Kurum bilgi varlıkları, içerdikleri verilerin hassasiyeti, kurum için taşıdıkları önem ve yasal zorunluluklar dikkate alınarak uygun bir şekilde sınıflandırılır/gizlilik derecesi verilir.

8.2.2. Bilgi varlıklarına (resmi yazılar dâhil) verilecek gizlilik dereceleri için 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe giren "**Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar**" dikkate alınır. Buna göre;

8.2.3.İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda kişi güvenliği veya milli güvenlik açısından saygınlık ve çıkarlarımıza **hayati derecede** zararlar verebilecek, yabancı bir devlet için faydalar temin edebilecek ve güvenlik bakımından **olağanüstü** sonuçlar doğurabilecek bilgiler "**çok gizli**",

8.2.4. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından, saygınlık ve çıkarlarımıza **büyük zarar** verebilecek, yabancı bir devlet için faydalar temin edebilecek özellikler taşıyan bilgiler "**gizli**",

8.2.5. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından saygınlık ve menfaatlere zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek bilgiler "**özel**",

8.2.6. İçerdiği bilgi itibarıyla ÇOK GİZLİ, GİZLİ veya ÖZEL gizlilik dereceleriyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi durumunda gerçek ve tüzel kişilerin itibarını sarsacak bilgiler "**hizmete özel"** olarak sınıflandırılır.

8.2.7. Çok gizli gizlilik dereceli evrak ve dokümanlar, Kurumun en üst düzey yöneticisi tarafından belirlenen ve yazılı olarak görevlendirilen kişi veya kişilertarafından hazırlanır ve özel usullere göre dağıtımı yapılır. Bu tip evrak ve dokümanlar korumalı odalarda, kasa, çelik masa veya diğer tipte çelik dolaplar içinde muhafaza edilir.

8.2.8. Gizli, özel ve hizmete özel evrakların gizlilik derecesi, yazıyı hazırlayan makam tarafından tayin edilir. Gizli ve özel evraklar kilitli çelik dolaplarda, hizmete özel evraklar ise masa gözlerinde kilitli olmak şartıyla muhafaza edilir.

8.2.9. Yukarıda sıralanan gizlilik derecelerinden hiçbirisi ile sınıflandırılmayan ve özel bir koruma gerektirmeyen evrak ve dokümanlar, "**tasnif dışı**" olarak kabul edilir.

8.2.10. Tasnif dışı bir gizlilik derecesi olmayıp, evrakın yukarıda sıralanan gizlilik derecelerinden hiç biri ile sınıflandırılmamış olduğunu belirtir. Tasnif dışı belgeler için herhangi bir erişim kısıtlaması yoktur.

8.2.11. Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, elektronik ortamda hazırlanması ve dağıtılması ile ilgili hususlar için Sağlık Bakanlığı Elektronik Belge Yönetim Sistemi Yönergesinde belirtilen kurallar uygulanır.
8.2.11. Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, kâğıt ortamda hazırlanması ve manuel (elektronik olmayan) yöntemlerle dağıtılması için Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelikte belirtilen kurallar uygulanır.

8.2.12. Resmi yazı şeklinde olmayan ancak içerdikleri bilgilerin hassasiyeti açısından sınıflandırılmaya ihtiyaç duyulan diğer bilgi varlıklarının sınıflandırılması için de yukarıda belirtilen gizlilik dereceleri kullanılır.

8.2.13. Gerek elektronik ortamda, gerekse basılı ortamda saklanan bilgilerin;

8.2.13.1. Bilgiye erişimin kayıt ve kontrol altına alınması,

8.2.13.2. İzinsiz kopyalamanın önlenmesi,

8.2.13.3. Elektronik veya basılı olarak depolama süresi ve koşullarının tanımlanması,

8.2.13.4. İletim hassasiyetinin belirlenmesi,

8.2.13.5. Gerektiğinde kanıt olarak kullanılmak üzere bütünlüğünün sağlanması,

8.2.13.6. İhtiyacın sonlanması durumunda imha edilmesi süreçlerinin tanımlanması için uygun şekil ve yöntemlerle etiketlenmesi gerekir.

8.2.13.7. Tasnif dışı bilgiler için etiketleme yapılmasına gerek yoktur.

8.2.14. Resmi yazı şeklinde olan belgelerin etiketlenmesi için yürürlükteki Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelikte belirtilen esaslar doğrultusunda hareket edilir. Bu kapsamda;

8.2.14.1. Her sayfaya gizlilik dereceleri yazılır ve damgalanır.

8.2.14.2. Ekler de yazı ile aynı gizlilik derecesini taşır.

8.2.14.3. Gizlilik dereceli bütün yazılar, zaman zaman gizlilik derecelerinin yeniden değerlendirilmesi bakımından gözden geçirilir.

8.2.14.4. Gizlilik derecelerinin indirilip yükseltilmesi yazıyı yazan makamlarca yapıldığı gibi alan makamlarca da bu hususta teklif yapılabilir.

8.2.14.5. Gizlilik dereceli ve bilhassa kontrollü yazılarda kullanılan müsveddeler, karbon kâğıtları ve yanlış yazılar muhakkak imha edilir.

8.2.14.6. Gizlilik dereceli evrak, kâğıt sepetine bütün olarak atılmaz. Kâğıt kırpa makinaları kullanılmak suretiyle imha edilir.

8.2.14.7. Gizli ve özel gizlilik derecesini haiz evrak ve belgeler izinsiz olarak çoğaltılamaz.

8.2.15. Gizlilik derecesi taşıyan bilgileri veya belgeleri görevi dışında elde eden veya belgeleri görenler, bu bilgiyi ve belge içeriğini resmi görevlerinin gerektirdiği haller dışında açıklayamaz, çoğaltamaz veya paylaşamazlar. Bu tür bir bilgiyi edinenler durumu gecikmeksizin gizlilik derecesini veren makama bildirmek ve elde ettikleri belgeleri gecikmeksizin gizlilik derecesini veren makama teslim etmek zorundadırlar.

8.2.16. İlgili mevzuat tarafından verilen yetkiye dayanılarak Bakanlığımıza bağlı sağlık hizmet sunucuları tarafından işlenen kişisel sağlık verileri; verinin ait olduğu kişi, ne maksatla istendiği vb. özel durumlar da dikkate alınmak suretiyle yukarıda tanımlanan gizlilik derecelerinden en az "ÖZEL" gizlilik derecesi ile etiketlenir.

8.3 Taşınabilir Ortam Yönetimi

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

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

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

8.3.2.2. 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.

8.3.2.3. 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.

8.3.2.4. ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL veriler, taşınabilir ortamda saklanamaz. Özellikle bu tür ortamlarda saklama zorunluluğu var ise bu Kılavuzun A.7.2.5 (Sabit Ortamdaki Verilerin Şifrelenmesi) maddesinde belirtilen şekilde şifreli olarak saklanır.

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

8.3.2.6. 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.

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

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

8.3.3. Taşınabilir ortamda yer alan verilerin bütünlüğünün sağlanması (değişmediğinin garanti altına alınması) için Kılavuzun A.7.2.1.3 (Özetleme İşlemleri) maddesinde belirtilen standartta uygun bir özetleme (hash) algoritması kullanılmak suretiyle verilerin bir özeti (parmak izi) alınır. Alınan özet, kullanılan algoritma ve anahtar ile birlikte bir tutanak ile kayıt altına alınır ve taşınabilir ortam ile birlikte muhafaza edilir. İhtiyaç duyulan durumlarda verinin tekrar özeti alınarak herhangi bir değişiklik olup olmadığı kontrol edilir.

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

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

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

8.3.5.2. Yönetim tarafından yetkili kurye listeleri oluşturulur.

8.3.5.3. 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.

8.3.5.4. Ortamın içeriğini tanımlayan kayıtlar ile birlikte kaç kez transfer edildiği, transfer sorumluları ve alıcı tarafından alındığının kayıtları tutulur.

8.4 Ortamın Yok Edilmesi

8.4.1. 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.

8.4.2. 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.

8.4.3. Kaydı silinen bilgisayarların sabit diskleri, ilgili teknik birimlerden destek alınmak suretiyle sökülür.
8.4.4. Sökülen sabit disklerden daha önce ilgili teknik birimler tarafından "onarımı mümkün değil" şeklinde rapor verilenler ile sağlam olmakla birlikte "yeniden kullanımı düşünülmeyen" cihazlar aşağıda belirtilen yöntemlerden biri ya da birkaçı birlikte kullanılmak suretiyle imha edilir:

8.4.4.1. De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

8.4.4.2. Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.

8.4.5.6. Bilgisayarların sabit diskleri dışında hassas veri bulundurma ihtimali olan diğer depolama ortamları, ortam türüne bağlı olarak aşağıda yer alan yöntemlerden biri kullanılarak yok edilir.

8.4.5.6.1. Ağ cihazları (anahtarlama cihazı, yönlendirici vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

8.4.5.6.2. Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanarak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemi ile ya da Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

8.4.5.6.3. Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

8.4.5.6.4. Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

8.4.5.6.5. Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta ancak çoğunda yok etme komutu bulunmamaktadır. Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

8.4.5.6.6. Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
8.4.5.6.7. Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre Kılavuzun A.4.5.4 Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

8.4.5.6.8. Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

8.4.5.7. Kâğıt ve mikrofiş ortamlarındaki veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

8.4.5.8. Orijinal kâğıt formattan tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

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

8.4.5.10. 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.

8.4.5.11. Bulut ortamındaki sistemlerde yer alan hassas verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılamaz hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

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

8.4.5.12.1. İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan verilerin Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

8.4.5.12.2. Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

8.4.5.12.3. Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, hassas verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

9. İŞLETİM GÜVENLİĞİ

9.1. Sunucu ve Sistem Güvenliği

9.1.1. Sunucuların ve sistemin güvenliğini sağlamak için gerekli güvenlik koşullarının tanımlandığı, güvenlik ilkelerinin belirlendiği "Sistem Güvenlik Politikası" oluşturulur.

9.1.2. İş sürekliliği ve acil durum planlaması için ilgili otoritelerle iletişim yöntemleri tanımlanır ve yazılı hale getirilir. Acil durumlarda erişilmesi gereken kişilerin irtibat numaraları ilgili personelin kolayca ulaşabileceği bir şekilde bulundurulur.

9.1.3. Yeni teknolojileri, uygulamaları, tehdit veya açıklıkları takip etmek için dernek, forum siteleri, e-Posta grupları gibi özel ilgi grupları belirlenir ve ilgili personel tarafından takip edilir. USOM tarafından yayımlanan https://www.usom.gov.tr/tehdit.html adresinden yaygın kullanılan yazılım ve donanımlarla ilgili güvenlik bildirimleri takip edilebilir. Aynı şekilde Bakanlığımız BGYS ve SOME birimleri tarafından yayımlanan https://bilgiguvenligi.saglik.gov.tr ve https://some.saglik.gov.tr adreslerinden güvenlik haberleri takip edilebilir.

9.1.4. Sistem yöneticisine sistem ile ilgili genel ve tam bir bakış açısı sağlayabilmesi açısından sistemdeki işletim sistemi, yüklü servisler, kaç sunucu (sanal ve fiziksel) olduğunu gösteren varlık döküm listesi oluşturulur. Sistemde bulunan her varlığa mutlaka bir sahip atanır. Hazırlanan varlık envanter listesi sadece ilgili personelin erişebileceği bir şekilde saklanır.

9.1.5. Varlık envanter listesinde sunucuların isimleri, IP adresleri, yeri, ana görevi, üzerinde çalışan uygulamalar, sahibi; işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personelin isimleri ve telefon numaraları gibi sıklıkla ihtiyaç duyulan bilgiler yer alır.

9.1.6. Sunuculara ve uygulamalara erişim sağlayan kullanıcıların erişim hakları, erişimlerin iptal edilmesi veya erişim yetkisinin değiştirilmesi gibi kuralların tanımlandığı bir "erişim matrisi" oluşturulur.

9.1.7. Sunucularda zorunlu kalmadıkça "administrator" ve "root" gibi genel sistem hesapları kullanılmaz.

9.1.8. Sunuculara yapılan erişimlerin raporlanması, mesai saati dışındaki erişimlerin işaretlenmesi gibi detaylar gözlenir. Kullanıcılara olması gerekenden fazla yetki tanımlanmaz.

9.1.9. Sunucularda açılan oturumlar için kurallar tanımlanır. Sunuculara ve uygulamalara yapılan başarılı ve başarısız girişimlerin kayıtları tutulur. Kaba kuvvet ataklarına engel olmak maksadıyla sunuculara 5 (beş) başarısız oturum açma denemesi yapıldığında ilgili hesap belirlenerek bir süre boyunca askıya alınır.

9.1.10. Sunucularda oturum açmış kullanıcı hesapları ile herhangi bir işlem yapılmadığı takdirde 10 (on) dakika sonra ekran kilitlenir ve ilgili kullanıcının oturum açma ekranına düşmesi sağlanır. 1 (bir) saat boyunca işlem yapılmadığı takdirde, ilgili kullanıcının oturumu otomatik olarak sonlandırılır.

9.1.11. Sistem hesaplarına ait parolalar için Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen yönetici hesaplarına ilişkin kurallar dikkate alınır.

9.1.12. Sunucuda varsayılan yönetici adı (administrator) değiştirilir. Bir sunucuda mümkün olduğu kadar az sayıda kullanıcı hesabı bulundurulur ve gereksiz hesap açılmaz. Güvenlik amacıyla başkaca bir zorunluluk yok ise misafir (Guest) hesabı kapalı olarak tutulur. Misafir (Guest) ve Yönetici (Administrator) hesaplarının isimleri değiştirilir. Açılmış fakat kullanılmayan kullanıcı hesapları kapalı duruma (disabled) getirilir veya silinir.

9.1.13. Sunucuların güvenliğini sağlayabilmek için kullanılmayan uygulamalar veya servisler kapatılır. Gerekli servis ve hizmetler dışında başka bir servis çalıştırılmaz.

9.1.14. Sunuculara güvenli bağlantı yapılabilmesi için SSL sertifikası yüklenir. Sunuculara SSH bağlantısı yapılacak ise kullanılan anahtarlar belirli aralıklarla değiştirilir. Sertifika ve anahtar yönetimi ve kriptografik işlemler için Kılavuzun A.7.2 (Kriptografik Araç ve Yöntemler) maddesinde belirtilen hususlara dikkat edilir.

9.1.15. Sertifika kullanım süresi, son kullanım süresi yaklaşan sertifikaların takibi gibi işlemler hazırlanacak bir sertifika takip listesi vasıtasıyla takip edilir.

9.1.16. BIOS güncellemeleri takip edilir. Sunucuların BIOS ayarlarının girişi parola ile korunur. Sunucuların varsayılan olarak CD-ROM, DVD-ROM veya flash disk gibi harici kaynaklardan başlatılması engellenir.

9.1.17. Sunucuda depolanan veriler, işletim sisteminin çalıştığı disk bölümünden farklı bir disk bölümünde tutulur.

9.1.18. Sunucuların arka planda çalışan servisleri ile birlikte o servislerinde kullandığı portlar kontrol edilir. Gereksiz portlar kapatılır. Mümkün olduğu surette uygulamaların varsayılan portları değiştirilir.

9.1.19. Kılavuzun A.9.15 (Sistem Güvenlik Testleri) maddesinde belirtilen güvenlik testleri yapılarak sunucular ve sistem ile ilgili açıklıklar tespit edilir. Tespit edilen açılıkların kapatılması sağlanır. (Sunucuda Windows işletim sistemi kullanıyor ise “Netstat –an”, Linux işletim sistemi kullanıyor ise “Netstat –tulp” komutu ile açık veya kullanılan portlar listelenerek kontrol edilebilir.)

9.1.20. Sunucu işletim sistemleri, güvenlik açıklarına karşı güncel tutulur. Güncellemelerde değişiklik yapılacak ise bu değişiklikler Kılavuzun A.9.2 (Değişiklik Yönetimi) maddesinde belirtilen değişiklik yönetimi kuralları çerçevesinde, onay ve uygulama sahipleri tarafından test mekanizmasından geçirildikten sonra uygulanır.

9.1.21. Etki alanındaki sunucu ve istemci bilgisayarların yama yönetiminin merkezi bir sunucu üzerinden otomatik olarak yapılması için gerekli olan sistem tesis edilir. Bu amaçla

üreticiler tarafından yayımlanan yamalar merkezi bir sunucuya çekilir ve bu sunucu vasıtası ile diğer bilgisayarlara dağıtımı yapılır.

9.1.22. Mutlaka zorunlu değil ise sunucuların internete erişimleri kapatılır.

9.1.23. Sistem kaynaklarının uygun seviyede planlanması, sürdürülebilmesi ve etkin kullanılabilmesi için Kılavuzun A.9.3 (Kapasite Yönetimi) maddesinde belirtildiği şekilde kapasite yönetimi yapılır. Kapasite yönetim planları uyarınca sunucuların performans gereklilikleri belirlenir. Sistemde belli aralıklarla disk birleştirmesi (defragment) ve disk temizlemesi yapılır. Yasal bulundurma süresi dolan veya sistem tarafından geçici olarak yaratılan dosyalar silinir. Disklerin doluluğu, ram ve işlemci kullanımı ve bunlara ilişkin kullanım parametreleri kontrol edilir.

9.1.24. Her etki alanı için NTP (Ağ Zaman Protokolü) sunucusu kurularak sistemdeki tüm aktif cihazların bu servis üzerinden tarih ve saat eşleştirmesi yapması sağlanır. İllerdeki NTP sunucuları, SBSGM tarafından sunulan NTP servisi ile senkronize edilir.

9.1.25. Kullanıcıların bilgisayarlarının saat ve tarih ayarlarını değiştirmesi engellenir.

9.1.26. Virüs vb. zararlı yazılımlardan korunmak ve kurumsal bilgilerin kurum dışına sızmasını engellemek amacıyla gerekiyorsa USB bellek gibi taşınabilir cihazların kullanımı engellenir.

9.1.27. Kullanıcıların ".exe/.bat" gibi çalıştırabilir dosyaları çalıştırmaları engellenir.

9.1.28. Kullanıcıların kısa yolu olmayan uygulamaları açmalarını önlemek için komut satırı olarak da bilinen ve Windows işletim sistemli cihazlarda yer alan MS-Dos tabanlı konsola (cmd) erişimleri engellenir.

9.1.29. Kullanıcıların bilgisayar ayarlarını değiştirmelerini önlemek amacıyla denetim masasına ve C dizinine erişimleri engellenir.

9.1.30. Kullanıcıların DNS adreslerini değiştirmeleri engellenir.

9.1.31. Sunuculara yapılacak uzak masa üstü bağlantılarında Kılavuzun A.6.14 (Uzaktan Çalışma ve Erişim) maddesinde belirtilen hususlara dikkat edilir.

9.1.32. Sunucuda paylaşıma açılmış klasörlerde izin verilen kullanıcı ve gruplar kontrol edilir. Kullanıcılara, gruplara verilen izinler ve kullanıcıların baskın izin seçeneğini nerden aldığı incelenir. Herkes (everyone) isimli kullanıcı grubuna izin atanmaz. İzinler kullanıcılardan ziyade gruplara verilir. Kullanıcıların bilgisayarlarını günlük işlerini yapmalarını sağlayacak seviyede en az yetki ile çalıştırmaları sağlanır. Aynı izinlere sahip olması gereken kullanıcılar bir grupta toplanır. (Satın Alma, İnsan Kaynakları gibi)

9.1.33. Geliştirme ve test ortamları esas çalışma ortamından ayrılır. Yapılması planlanan işlemler öncelikle test ortamında denenir. Kurumun yapısına göre test ortamları için farklı VLAN'lar oluşturulabilir.

9.1.34. Kurumda işletilen sistemler için Kılavuzun A.9.13 (Yedekleme Yönetimi) maddesinde belirtildiği şekilde yedekleme politikası hazırlanır. Kurumun yedekleme politikasında belirtilen kurallara göre yedekleme işlemi yapılır.

9.1.35. Sunucularda yapılan işlemlerin iz kayıtlarına erişmek için olay günlükleri (event logs) tutulur. İz kayıtları, Kılavuzun A.9.12 (İz Kayıtları Yönetimi) maddesinde belirtildiği şekilde saklanır.

9.1.36. Sunucu ve sistem güvenliğini sağlayabilmek için lisanslı yazılımlar kullanılır. Kurumun yazılım lisans varlıklarının sayısı, bu lisanların hangilerinin aktif kullanıldığı, kullanılmayan lisansların bilgisinin tutulması gibi ayrıntıları içeren listeleme ile aktif lisans yönetimi yapılır.

9.1.37. Tüm bilgisayarlar lisanslı anti-virüs yazılımı ile korunur. Anti-virüs yazılımının virüs veritabanı güncel tutulur.

9.1.38. Özellikle Bakanlık merkez teşkilatı birimleri ve il sağlık müdürlükleri gibi idari faaliyetlerin yapıldığı kurumlarda, her bir bilgisayara küçük tip yerel yazıcı bağlamak yerine, merkezi bir yazıcı yönetim sistemine bağlı ortak kullanılan büyük tip yazıcıların kullanılması tavsiye edilir. Yazıcıların USB bağlantıları ve kurum dışı adreslere e-Posta göndermesi engellenir. Yazıcılara erişim için PIN kodu veya kartlı tanımlama gibi bir güvenlik kontrolü oluşturulur.

9.1.39. Sunucuların fiziksel güvenliğini sağlamaya yönelik tedbirler alınır. Sunucu/sistem odalarında alınması gereken tedbirler bu Kılavuzun A.9.9.1 (Sunucu/Sistem Odası Güvenliği) maddesinde olduğu gibidir. Sunucu odası dışında sunucu bulundurulmaz. Sunucu/Sistem odalarına yapılan giriş çıkışlar kontrol edilir, giriş-çıkışların kayıtları tutulur.

9.1.40. Sistemde hata ile karşılaşıldığında hataları gidermek adına izlenilen yöntemler, aynı hata ile tekrar karşılaşıldığında hızlı aksiyon alınabilmesi ve iş sürekliliğinin sağlanabilmesi için yazılı hale getirilir. Hata ve çözümlerinin bulunduğu merkezi bir havuz oluşturulur.

9.1.41. Sunucu kurulumları ve sunucu üzerinde yapılan konfigürasyonlardan oluşan bir sistem bilgi bankası oluşturulur. Hazırlanmış olan bilgi bankasında yapılan işlemler takip edilebilir ve yeni bir yapılandırma işleminde bu bilgi bankası kullanılabilir.

9.1.42. Sunucular üzerinde yapılacak değişiklikler bu Kılavuzun A.9.2 (Değişiklik Yönetimi) maddesinde belirtilen değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanır. Önemli sistem ayarlarının yetkisiz kişiler tarafından değiştirilmesini engellemek, yetkili kullanıcılar tarafından yapılan değişiklikleri izlemek, değişikliklerden meydana gelebilecek olan güvenlik açıkları veya sistem problemlerini önceden belirleyerek önlem almak gibi amaçlarla kayda dayalı değişiklik yönetimi uygulanır.

9.1.43. Sunucuların üretici tarafından tavsiye edilen/teknik dokümanlarında belirtilen süreler dikkate alınarak yıllık bakım planları hazırlanır. Bakımlar yetkili uzmanlar tarafından yapılır ve kayıt altına alınır.

9.1.44. Sunucuların erişilebilirlik (availability) seviyesini artırmak için herhangi bir sunucunun çalışmaması durumunda diğer bir sunucunun onun yerine amaçlanan şekilde

çalışmasını sağlayacak kümelenmiş (cluster) mimari yapıda yapılandırılması gerekir. Yüksek maliyet ya da yönetimsel zorluklar nedeni ile sunucular kümelenmiş yapıda tesis edilemiyorsa en azından disklerin kümelenmiş olarak yapılandırılması tavsiye edilir.

9.2. Ağ İşletim Güvenliği

9.2.1. Ağ mimarisi ve aktif ağ cihazlarının yönetimi, güvenlik ilke ve kuralları, erişim haklarının yazılı olduğu "Ağ Güvenliği Politikası" oluşturulur.

9.2.2. İş sürekliliği ve acil durum planlaması süreçlerinde ilgili otoritelerle iletişim yöntemleri tanımlanır ve yazılı hale getirilir. Acil durumlarda erişilmesi gereken kişilerin irtibat numaraları personelin kolayca ulaşabileceği bir şekilde bulundurulur.

9.2.3. Yeni teknolojileri, uygulamaları tehdit veya açıklıkları takip etmek için dernek, forum siteleri, e-Posta grupları gibi özel ilgi grupları belirlenir ve ilgili personel tarafından takip edilir.

9.2.4. Ulusal Siber Olaylara Müdahale ekibi (USOM) tarafından sağlanan https://www.usom.gov.tr/tehdit.html adresinden ürünler ile ilgili güvenlik güncelleştirmeleri, https://www.usom.gov.tr/zararli-baglantilar/1.html adresinden zararlı bağlantılar takip edilebilir. Ayrıca https://some.saglik.gov.tr/ ve https://bilgiguvenligi.saglik.gov.tr adreslerinde yayınlanan güvenlik haberleri takip edilebilir.

9.2.5. Güvenlik ve ağ cihazlarına erişim sağlayan kullanıcılar için cihazlara giriş yapmadan önce bilgilendirme sayfası açılması gerekir. Açılacak bu sayfada sadece yetki verilen kişiler tarafından erişilebilecek bir cihaz olduğu, izinsiz erişimlerde kanuni işlem yapılacağı gibi hususları bildiren bir sorumluluk metni oluşturulur.

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

9.2.7. Güvenlik ve ağ cihazlarında yönetici olarak erişim yetkisine sahip olan kullanıcılar yazılı olarak tanımlanır. Bu erişim yetkisine sahip kullanıcı hesaplarındaki değişiklikler kontrol edilir. Sistemler üzerinde ortak erişim yetkisi olan hesaplar açılmaz. Sahibi bilinmeyen hesaplar kaldırılır.

9.2.8. Güvenlik ve ağ cihazlarına yapılacak uzaktan erişimler için yönergenin A.6.10 maddesinde belirtilen hususlara dikkat edilir.

9.2.9. Uzaktan erişim verilen kullanıcılara bağlantı zamanı ve süresi ile ilgili kısıtlamalar getirilir. Kurumdaki görevi gereği kullanıcıların bağlantı süreleri farklı olabilir.

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

9.2.11. Güvenlik ve ağ cihazları için varlık envanter listesi oluşturulur. Listede cihaz/ürünün adı, marka ve modeli, kullanım maksadı, IP ve MAC adresi, bulunduğu yer, sorumlusu gibi bilgiler yer alır.

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

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

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

A.9.7.15. Sistemi etkileyecek bir çalışma yapılması gerekiyorsa mesai saati dışında yapılır. Bu çalışmadan etkilenecek kurum/firma ya da kişilere bilgi verilir.

9.2.16. Aktif ağ cihazlarından bilgi toplamak için kullanılan SNMP protokolünün (Simple Network Management Protocol) v2 veya v3 sürümü kullanılır. SNMP v2 protokolü kullanılacak ise SNMP protokolü topluluk anahtarı (community string) ile sorgulama yapar ve varsayılan olarak "public" ve "private" olarak gelen "snmp community" değerleri değiştirilir. Değiştirilen "snmp community" değeri açık (clear-text) bir şekilde gönderildiği için mümkün ise daha güvenli bir versiyon olan SNMPv3 tercih edilir.

9.2.17. Kablosuz ağlara giriş yapan tüm kullanıcılar sisteme kimlik tanımlı olarak kaydedilmelidir. Kimlik doğrulamasında bağlantı yapacak kullanıcının kimlik bilgileri ve ne kadar süre ağda kalacağı gibi bilgiler alınır. 5651 sayılı kanun ve Bakanlık BGYS politikaları uyarınca, ağa dâhil olan tüm kullanıcılar kaydedilir ve bu bilgiler belirlenen süreler boyunca saklanır.

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

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

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

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

9.2.22. Güvenlik ve ağ cihazlarının yazılım güvenliğini sağlamaya yönelik tedbirler alınır. Cihazlar ilk kurulduğunda varsayılan olarak atanmış olan kullanıcı adı ve parolalar değiştirilir. Parolalar, Kılavuzun A.6.3 (Parola Güvenliği) maddesinde yer alan sunucular için güçlü parola ilkeleri esaslarına göre oluşturur.

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

9.2.24. Cihazları kaba kuvvet saldırılarından korumak için 5 (beş) yanlış deneme sonrasında oturum belirli bir süre kilitlenecek şekilde ayarlama yapılır.

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

9.2.26. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Kanunu uyarınca tutulması gereken trafik bilgileri (iz kayıtları) ile ilgili hususlar Kılavuzun A.14.4 numaralı maddesinde detaylı olarak açıklanmıştır.

9.2.27. Saldırganların yerel ağda kendilerini ağ geçidi olarak tanımlayarak trafiği kendi üzerinden geçirerek bilgilere erişim sağlamasını önlemek için ağda kullanılan anahtarlarda "DHCP snooping" ve "arp inspection" özelliği aktif edilir.

9.2.28. Kurum ağı, IEEE 802.1x port bazlı kimlik doğrulama sistemine göre yapılandırılır. Port tabanlı kimlik doğrulama ile yerel ağların dinlenilmesi, istenmeyen erişimlerin ağa bağlanması engellenir.

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

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

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

9.2.32. Kurumsal kaynakların etkin olarak kullanılması, 5651 sayılı kanundan kaynaklanan uyum zorunlulukları, veri güvenliğinin sağlanması, zararlı içerik ve yazılımlardan korunma vb. maksatlarla internet erişimi kısıtlamaları yapılabilir. Kısıtlama ile ilgili politikalar, kurumların bilgi güvenliği alt komisyonları tarafından belirlenir. Kısıtlama ile ilgili planlama yapılırken aşağıdaki hususlar dikkate alınır:

9.2.32.1. Basın yayın organlarını takip ederek idareye raporlamakla sorumlu personel haricindeki tüm personelin dizi, film ve TV erişimlerinin kapatılması,

9.2.32.2. Kurum sosyal medya hesaplarını yönetmekle sorumlu personel dışındaki tüm personelin Facebook, Twitter, İnstagram vb. uygulamalara erişimlerinin engellenmesi veya bant genişliği sınırlaması yapılması,

9.2.32.3. Youtube, Vimeo, Dailymotion gibi platformlarda erişimlerle ilgili olarak sadece ihtiyaç duyan personele izin verilmesi, bu yapılamıyorsa bu platformlara erişimlere bant genişliği sınırlaması yapılması önerilir.

9.3. Yazılım Güvenliği

9.3.1. Uygulama yazılımlarına erişen kullanıcıların erişim yetkileri ve rol yönetimi yazılı olarak tanımlanır. Kullanıcı erişim talepleri onay mekanizmasından geçirilir.

9.3.2. Uygulama yazılımlarına erişim sağlayan kullanıcıların aldıkları erişim hakları, erişimlerin iptal edilmesi veya erişim yetkisinin değiştirilmesi gibi kurallar yazılı hale getirilir. İşten ayrılma veya görev değişikliği olması durumunda kullanıcı hesapları iptal edilir ve tanımlanan yetkiler görev değişikliği doğrultusunda güncellenir.

9.3.3. Uygulamalarda yönetici ve kullanıcı hesap yetkilerinin tanımlanması, her proje için yazılı kurallar doğrultusunda yapılır. Yetki tanımlanan kullanıcıların yetki kısıtlamaları belirli aralıklarla takip edilir.
9.3.4. Uygulama yazılımlarında roller oluşturularak erişim kontrol (yetkilendirme) matrisi oluşturulur. Rol tabanlı yetkilendirmeler yapılır. Kullanıcıların sadece yetkilendirildiği rol kapsamındaki verilere erişim sağlayacak şekilde düzenleme yapılır.

9.3.5. Uygulamada, kullanıcıların yetkilerinin sistem yöneticisi ya da yetkilendirilmiş kişiler tarafından ayarlanabildiği kimlik yönetimi ekranı bulunur. Kimlik yönetim ekranlarında, belirlenen kullanıcılar ve yetkiler dışında yetkilendirme bulunmaz.

9.4. Sunucu/Sistem Odası Güvenliği

9.4.1. Hizmet sunumunun sürekliliğinin sağlanması için kesintisiz ve sürekli çalışan elektronik ve donanımsal altyapı ihtiyacı bulunmaktadır. Donanım, elektronik altyapı ya da çevresel faktörlerden kaynaklanabilecek sorunlar hizmetlerin sunumuna birçok açıdan zarar verebilir ve olumsuz etkilerin giderilmesi gerek maliyet gerek zaman açısından çok zor olabilir. Bu nedenle, hizmet sunumunda yer alan tüm aktif ve pasif donanımın; sadece sunuculara tahsis edilmiş, yetkisiz personelin girişinin engellendiği, sıcaklık ve nemin kontrol edildiği, elektrik kaynağının stabilize edildiği, özel şekilde iklimlendirilmiş ve güvenliği sağlanmış sunucu/sistem odasında konumlandırılması gerekir. Sistem odalarındaki donanımların hizmet sürekliliğinin sağlanması için yedekli bir güç kaynağı sistemi, yedekli haberleşme bağlantıları, ısı, nem gibi çevre değişkenlerinin kontrolü için iklimlendirme cihazları ve güvenlik cihazları yer alır.

9.4.2. Bir sistem odasının en temel özellikleri;

9.4.2.1. 7×24 kesintisiz çalışabilirlik,

9.4.2.2. Güç yönetimi ve ağ bağlantılarında farklı kanallardan yedeklilik,

9.4.2.3. Ağ güvenliği, fiziksel erişimlerde yetkilendirme ve görüntülü gözetleme,

9.4.2.4. Çevre şartlarının kontrol altında tutulması,

9.4.2.5. Yangına karşı duman algılama gibi erken uyarı sistemleridir.

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

9.4.3.1. 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.

9.4.3.2. 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.

9.4.3.3. 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.

9.4.3.4. 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.

9.4.3.5. 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.

9.4.3.6. 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.

9.4.3.7. 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.

9.4.3.8. 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.

9.4.3.9. 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.

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

9.4.3.11. 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.

9.4.3.12. 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.

9.4.3.13. 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.

9.5. İz Kayıtları (Log) Yönetimi

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

9.5.2. İz kayıtlarının tutulması ve yönetilmesi (iz kayıtlarının üretilmesi, aktarılması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi gibi süreçler) sadece erişim yetkisi verilen bir birim/kişiler tarafından yapılır. Bu yetki Kurumsal SOME'dir.

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

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

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

9.5.6. Kritik olaylara ilişkin iz kayıtlarının merkezi sunucuya eş zamanlı olarak (olay oluştuğu zaman) gönderilmesi sağlanır.

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

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

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

9.5.10. Kayıt üreten ortamlarla iz kayıtları saklama merkezleri arasında, verilerin teknik imkânlar dâhilinde şifreli olarak transfer edilmesi sağlanır.

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

9.5.12. İz kayıtları periyodik olarak yedeklenir ve yedeklerin uygun şekilde muhafaza edilmesi sağlanır. A.9.12.13. Merkezi iz kaydı sunucusu sadece yeni iz kayıtlarının saklanması için fonksiyonlar içerir. Bu sunucuda iz kayıtlarının silinmesi/değiştirilmesi amaçlı erişimlere izin verilmez.

9.5.14. İz kayıtlarının tek yönlü kriptografik özet değerleri (hash) hesaplatılır ve iz kayıtları güvenli ortamlarda saklanır.

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

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

9.5.15.2. Sanal ortam kayıtları,

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

9.5.15.4. Güvenlik duvarları, A.9.12.15.5. Antivirüs yazılımları, A.9.12.15.6. Saldırı tespit/önleme sistemleri,

9.5.15.7. Yönlendiriciler ve anahtarlama cihazları,

9.5.15.8. Sunucular,

9.5.15.9. Diğer iş uygulamaları (kritik kurumsal projeler),

9.5.15.10. Veri tabanları,

9.5.15.11. VPN iz kayıtları.

9.5..16. Tutulması gereken asgari iz kayıtları;

9.5.16.1. Kaydı oluşturan sistem,

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

9.5.16.3. Kaydı oluşturan olay,

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

10. HABERLEŞME GÜVENLİĞİ

10.1. Ağ Güvenliği

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

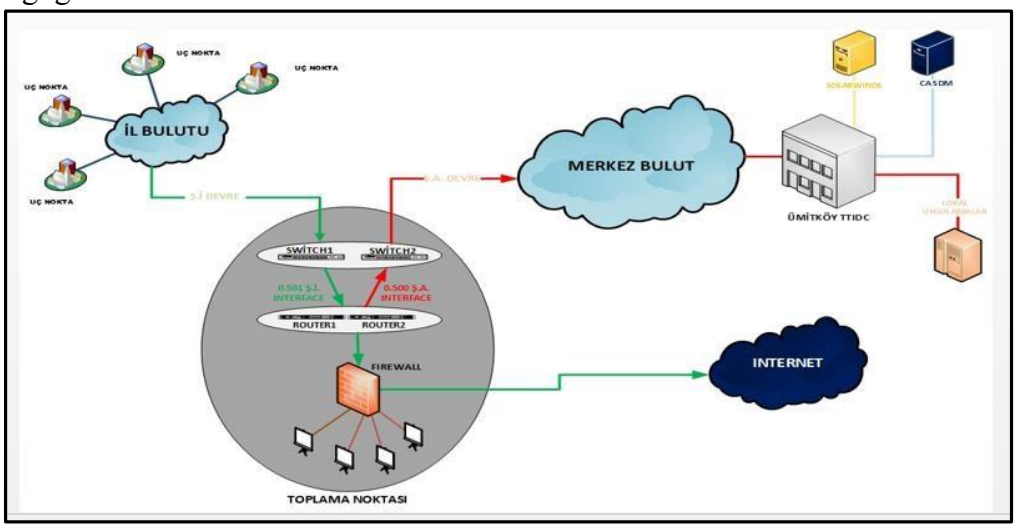
10.1.2. Ağ güvenliği, bir kuruluşun bilgisayar ağına bağlı olarak çalışan varlıklarının ve ağ trafiğinin güvenliğini sağlamak üzere, uygulamakta olduğu politikalar ve kontrol önlemleridir. Ağ güvenliği, bilgi güvenliğinin sağlanması için en önemli bileşenlerden biridir.

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

10.1.4. Daha güvenli bir iletişim ortamı sağlamak maksadıyla (Aile Sağlığı Merkezleri, 112 Komuta Kontrol Merkezleri, müstakil bir binada çalışan ve ağa bağlı aktif cihaz sayısı 10'dan az olan birimler hariç) Bakanlığımıza bağlı tüm kurum ve kuruşların geniş alan ağı bağlantıları, internet erişimleri SBA üzerinden sağlanır.

10.1.5. Aile Sağlığı Merkezleri, 112 Komuta Kontrol Merkezleri, müstakil bir binada çalışan ve ağa bağlı aktif cihaz sayısı 10'dan az olan birimlerin internet erişimleri doğrudan ADSL aboneliği vb. yöntemlerle sağlanır.

10.1.6. SBA mimarisi uyarınca illere bağlı uç noktalar, (istisnai bazı büyük iller hariç) her il için birer adet olacak şekilde tesis edilmiş "toplama noktası" olarak adlandırılan yapılar üzerinden, SBA Merkez Bulutuna ve internete bağlanır. SBA bulut mimarisi aşağıdaki şekilde gösterildiği gibidir.



10.1.7. Buluta bağlı kullanıcıların internet erişimleri il toplama noktasında bulunan internet bağlantısı üzerinden gerçekleştirilir. Bu noktada sınır güvenliği için tesis edilmiş olan güvenlik duvarının yönetimi, bağlı kuruluşlar/il sağlık müdürlüklerince görevlendirilen personel tarafından yapılır.

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

10.1.9. Uzaktan çalışma maksadıyla internet üzerinden SBA'ya bağlı cihazlara erişim yapılması halinde alınması gereken güvenlik tedbirleri, Kılavuzun A.6.14.2 (Uzaktan Çalışma ve Erişim) maddesinde açıklanmıştır.

10.2. Uç Nokta (Yerel Alan Ağı) Ağ Güvenliği

10.2.1. SBA'ya bağlı olsun veya olmasın, bir yerel alan ağında ağ güvenliği ile ilgili uygulanması gereken tedbirler takip eden maddelerde sıralanmıştır.

10.2.2. Yerel alan ağının fiziki güvenliği için Kılavuzun A.8.3.5 (Kablolama Güvenliği) maddesinde belirtilen tedbirler alınır.

10.2.3. Kablosuz sistemler kullanılarak tesis edilen yerel alan ağları için burada yazılı olan hususlara ilave olarak Kılavuzun A.10.3 (Kablosuz Ağ Güvenliği) maddesinde belirtilen tedbirler alınır.

10.2.3. Ağa bağlanacak bilgisayarların ağ yöneticileri tarafından belirlenecek ölçütleri taşıyan, kimliği tanımlanmış ve doğrulanmış olması gerekir. Bu maksatla mümkünse ağ tabanlı erişim kontrol sistemleri (NAC) kullanılır. NAC tabanlı çözümlerin olmaması durumunda, ağa bağlanacak cihazların MAC adresleri, bağlanacağı kenar anahtarın ilgili portuna elle tanımlanarak yetkisiz, kimliği bilinmeyen cihazların ağa erişimi engellenir.

10.2.4. Yerel alan ağlarında, port kısıtlaması yapılamayan, yönetim yeteneği olmayan ağ dağıtım kutuları (hub) veya eski nesil kenar anahtarlar kullanılmaz.

10.2.5. NAC tabanlı çözümlerin olmaması durumunda, kullanılmayan portlar kenar anahtar üzerinde yazılımsal olarak kapatılır.

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

10.2.7. Ağa bağlanan tıbbi cihazlar, sunucular ve istemci bilgisayarlar farklı VLAN'lara konulur. Çok kritik ve hassas verilerin bulunduğu, izole edilmesi gereken cihaz ve sistemler için gerekiyorsa mikro segmentasyon yapılır.

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

10.2.9. Herhangi bir nedenle böyle bir bağlantı ihtiyacı olması halinde, söz konusu bağlantı için SBSGM'nin yazılı onayı alınması ve yazılı onayda belirtilen ilave güvenlik tedbirlerinin uygulanması gerekir.

10.2.10. Bakanlık yazılı onayı alınmaksızın yukarıda belirtilen şekilde internet bağlantılarının yapıldığının tespit edilmesi halinde, ilgililer hakkında idari ve yasal işlemler yapılır.

10.2.11. Yerel alan ağlarının SBA'ya bağlandığı noktalarda sınır güvenliğinin sağlanması için asgari tedbir olarak bir adet güvenlik duvarı kurulur. Bu maksatla açık kaynak kodlu yazılımlar kullanılabilir.

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

10.3. Kablosuz Ağ Güvenliği

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

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

10.3.3. Bağlantı ayarları için şifreleme etkinleştirilir. Şifreleme seçeneği etkinleştirilirken ağa erişim için kullanılmak üzere üçüncü taraflar tarafından tahmin edilemeyecek karmaşık bir parola belirlenir. Şifreleme yöntemi olarak;

10.3.4. Öncelikle WPA3 Güvenlik protokolü kullanılır. WPA3 desteklemeyen cihazlarda üretici firmaların yayımlamış olduğu güncel yazılım sürüme yükseltilir.

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

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

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

10.4. Veri Aktarımı Güvenliği

10.4.1. 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.

10.4.2. 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.

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

10.4.4. 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.

10.4.5. 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.

10.4.6. Belirlenen amaç için gerekli olandan daha fazla bilgi aktarılmaz. Aktarılacak bilginin bir paragraf veya belirli sütunlar olması durumunda, yalnızca "kolay" olduğu için istenen bilgilerin yer aldığı dokümanın veya tablonun tamamı gönderilmez.

10.4.7. İstenen amacı karşılaması halinde, gerçek veri yerine anonim hale getirilmiş verinin aktarılması tercih edilir.

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

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

10.4.10. 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.

10.4.11. 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.

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

10.4.13. Aktarım yapılacak hedef kişi/kurumun Bakanlığımız kontrolündeki sistemlere erişim izni olmaması halinde, gizli kalması gereken bilgiler uygun şekilde şifrelenmek şartıyla, diğer paylaşım ortamları kullanılarak paylaşılabilir.

10.4.14. Herkese açık (TASNİF DIŞI) bilgiler en kolay ve en düşük maliyetli yöntemle aktarılır.

10.4.15. Özel nitelikli kişisel verilerin (sağlık verileri) aktarımı yapılırken KVKK'nın 2018/10 sayılı kararında belirtilen tedbirlerin alınmış olması gerekir.

10.4.16. Şifreleme araçları olarak A.7.2'de belirtilen kriptografik yöntemler kullanılır. Bu çerçevede;

10.4.17. Şifreli olarak aktarılması gereken dosyalar, aktarım öncesinde tek tek veya topluca, AES-256 veya üstü bir şifreleme aracı kullanılmak suretiyle şifrelenir.

10.4.18. Şifreleme için WINRAR (5.0 veya üstü), WINZIP (9.0 veya üstü) veya 7-ZIP programlarından herhangi biri kullanılabilir. Ya da gönderici ve alıcının üzerinde mutabık kalacakları aynı şartları sağlayan bir başka şifreleme aracı kullanılabilir.

10.4.19. Microsoft Office (Word, Excel, PowerPoint) tarafından sağlanan şifre koyma yeteneği, AES-128 algoritmasını kullandığı için özellikle zayıf bir parola seçilmesi durumunda şifrenin kırılması ihtimaline karşı yeterince güvenli olarak kabul edilmez.

10.4.20. Şifrelemede kullanılacak parolanın, A.6.3.2'de detayları verilen parola politikasında belirtilen ölçütler (en az 8 karakter, büyük ve küçük harf karışık, en az bir özel karakter, en az bir rakam, kelime anlamı olmayan vb.) ile uyumlu olması gerekir. Bu şartları sağlamayan bir parola kullanılması durumunda, şifre kırma yazılımları ile şifreli verilere ulaşılması ihtimali olduğu dikkate alınır.

10.4.21. Şifrelenen dosyanın parolası, şifreli dosyanın aktarımında kullanılan sistemden farklı bir araç/ortam kullanılmak suretiyle alıcısına ulaştırılır (örneğin; ePosta ile aktarılan şifreli bir dosyanın parolası SMS ile, dosya sunucusu ile paylaşılan şifreli bir dosyanın parolası e-Posta ile gönderilebilir.

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 ve/veya Kurum Bilgi Güvenliği Yetkilisi) 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 SBSGM tarafından kullanılan ve örneği Kılavuzun ekinde 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, kurumların 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.

12. BİLGİ GÜVENLİĞİ VE İHLAL OLAYI YÖNETİMİ

12.1. İhlal Bildirimi ve Olay Yönetimi

12.1.1. Bakanlık 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.

12.1.2. Merkezi ihlal birim sistemi dışında, Bakanlığın diğer birimlerince bilgi güvenliği ihlal olaylarının bildirimi için ayrı bir sistem/yazılım kurulmasına gerek yoktur. Merkezi sisteme girilen olayların, USOM tarafından işletilen SOME İletişim Platformuna (SİP) girilmesi ile ilgili esaslar, Sektörel SOME tarafından ayrıca belirlenir.

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

12.1.4. Merkezi ihlal bildirim sistemine girilen olaylar, SBSGM ekipleri tarafından ön değerlendirmeye tabi tutulur. Bildirim yapan kişiyle irtibat kurularak aynı zamanda ilgili kurumun bilgi güvenliği yetkilisine de bilgilendirme yapılır. İlgili bilgi güvenliği yetkilisi kendi arşivini tutmak amacıyla KLVZ-EK-21 Olay Bildirim ve Müdahale Formunun 1'inci Bölümünü (Olay Bildirimi) doldurur ve kurumsal ihlal bildirimi hafızası oluşturmak üzere saklar.

12.1.5. Küçük çaplı, yalnızca kendi kurumunu ilgilendiren ve bilgi güvenliği yetkilisi ya da kurumsal SOME tarafından kendi imkânları ile yerel olarak çözülebilecek olaylara kurumun SOME'si veya bilgi işlem personeli tarafından gerekli müdahale yapılır. Müdahale sonrasında KLVZ-EK-21'in 2'nci Bölümü (Olay Müdahale) doldurularak e-Posta ile bilgiguvenligi@saglik.gov.tr adresine gönderir.

12.1.6. 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 Sektörel SOME'den görüş/destek alır. Olayın çözümünde KLVZ-EK-21'in 2'nci Bölümünü (Olay Müdahale) doldurarak bilgiguvenligi@saglik.gov.tr adresine gönderir.

12.1.7. Yaşanılan olayın Sağlık Bakanlığı, diğer sağlık tesisleri ya da kamu kurum ve kuruluşlarını etkileyecek boyutta olması durumunda, Sektörel SOME sürece dâhil olur. Gerekli müdahaleyi yapar ya da yaptırılmasını sağlar. Sektörel SOME tarafından KLVZ-EK-21'in 2'nci Bölümü (Olay Müdahale) doldurularak kayıt altına alınır.

12.1.8. Merkezi ihlal bildirimi sistemine girilen tüm ihlal olaylarının süreç ve sonuçları BGYS Birimi tarafından takip edilir.

12.1.9. Merkezi ihlal bildirim sisteminde yer alan olay türleri ve açıklamaları şu şekildedir:

12.1.9.1. Servis Dışı Bırakma Saldırısı (DoS/DDoS): Saldırının amacı hedef alınan sistemi hizmet veremeyecek hale getirecek yöntemlerle, ilgili servisi hizmet dışı bırakmaktır. Kullanılan temel yöntem, ilgili hizmet servisine olağan dışı miktarda (çok sayıda) paket gönderip, engellemektir.

12.1.9.2. Bilgi Sızdırma (Data Leakage): Kurumun ürettiği, kullandığı ya da işlediği verilerin bilinçli veya bilinçsiz olarak yanlış hedefe gönderilmesi, çalınması ve/veya sızdırılmasıdır.

12.1.9.3. Zararlı Yazılım (Malware): Her türlü bilgi işleme yapabilen sistemlere zarar vermek, veri çalmak ve/veya yok etmek için üretilen yazılımlardır.

12.1.9.4. Sahtecilik (Fraud): Daha çok finansal sistemlerde karşılaşılan, aldatma amacı ile yapılan kasıtlı eylemlerdir.

12.1.9.5. Port Tarama: Ağa bağlı olarak çalışan aktif cihazlarda çalışan servislerin varlığını tespit etmek, bilgi toplamak ve tespit edilecek zafiyetler ile zararlı bir işlem yapma amacı ile gerçekleştirilen eylemlerdir.

12.1.9.6. Veri Tabanı Saldırısı: VTYS yazılımları, VTYS'nin çalıştığı donanımlar veya VTYS ile ilişkili uygulama yazılımlarında bulunan açıklıkların kullanılması suretiyle yetkisiz bir şekilde verilerin ele geçirilmesini hedefleyen saldırılardır. SQL Injection saldırısı buna örnek verilebilir.

12.1.9.7. Web Uygulamaları Güvenlik İhlalleri: Siteler arası betik çalıştırma (XSS: Cross-Site Scripting) saldırıları, kötü amaçlı dosya çalıştırılması, güvenli olmayan direk nesne referanslama, sunucu taraflı çapraz kod çalıştırma (CSRF: Cross Site Request Forgery), bilgi sızdırma ve uygun olmayan hata kontrolü, İhlal edilmiş kimlik doğrulama ve oturum yönetimi, güvensiz iletişimler gibi ihlaller bu madde altında değerlendirilir.

12.1.9.8. Sosyal Mühendislik: Kişilerin zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye yönelik teknikler içerir.

12.1.9.9. Veri Kaybı/İfşası: Gizli bilgilerin e-Posta aracılığı ile iletimi, ağ üzerinden iletilen bilgilerin yetkisiz ya da yanlış alıcıya iletimi, internet üzerinden güvenli olmayan kanallar aracılığıyla veri iletimi, ortak kullanım yazıcılarından alınan çıktıların sahiplenilmemesi ya da güvenliğine önem verilmemesi, masaüstü ya da ortak alanlarda basılı kopyaların denetimsiz bırakılması vb. durumları ifade eder.

12.1.9.10. Zararlı Elektronik Posta (SPAM): Kişinin bilgisi ve talebi dışında, ticari içerikli veya politik bir görüşün propagandasını yapmak ya da bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-Posta iletileridir.

12.1.9.11. Parola Ele Geçirme: Depolanmaması gereken bir yerde depolanan parolaların herhangi bir saldırı yöntemi ile ele geçirilmesidir.

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

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

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

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

12.2. Kanıt Toplama

12.2.1. 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.

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

12.2.3. 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.

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

12.2.5. Olay yerindeki bilgisayar kapalı ise kesinlikle açılmaz.

12.2.6. 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.

12.2.7. 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.

12.2.8. 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.

12.2.9. 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.

12.2.10. Yedeklenecek diskin hafızası şüpheli bilgisayar diskinden büyük olur.

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

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

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

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