T.C.

SAĞLIK BAKANLIĞI

SAĞLIK BİLGİ SİSTEMLERİ GENEL MÜDÜRLÜĞÜ

BİLGİ GÜVENLİĞİ POLİTİKALARI KILAVUZU

Sürüm 2.0

Eylül 2018

T.C. Sağlık Bakanlığı

Bilgi Güvenliği Politikaları Kılavuzu

Bakanlık Makamının 02/05/2018 tarihli ve 98813779.719.54 sayılı onayı ile Bilgi Güvenliği Politikaları Yönergesinin eki

EDİTÖRLER

Dr.M. Mahir ÜLGÜ

M. Fatih ULUÇAM

Dilek ŞEN KARAKAYA

Filiz AYDOĞDU

Burcu GÖKTÜRK

Erdal YILDIZ

ÖNSÖZ

Bakanlığımızda bilgi güvenliği çalışmaları iki ana eksen üzerine oturtulmuştur. Bunlardan ilki olan "**Bilgi Güvenliği Politikaları Yönergesi**" ile hukuki ve idari alt yapı oluşturulmuş, yönergeden alınan yetki ile bilgi güvenliğine yönelik teknik ve yönetsel tedbirlerin yer aldığı "**Bilgi Güvenliği Politikaları Kılavuzu**" hazırlanmıştır. Söz konusu dokümanların ilk sürümleri, eş zamanlı olarak 03 Mart 2014 tarihinde yayımlanarak yürürlüğe girmiştir.

Yönerge ve Kılavuz, ilk sürümlerinin yayımından bugüne kadar geçen süreçte yaşanan teknolojik gelişmeler, kullanıcılardan alınan geri bildirimler ve 694 ve 703 sayılı KHK'lar ile değişen Bakanlık merkez ve taşra teşkilatının yeni yapısı dikkate alınarak güncellenmiştir. Yönergenin en son sürümü 02 Mayıs 2018 tarihinde yayımlanmıştır. Yönergeye Sağlık Bilgi Sistemleri Genel Müdürlüğünün (SBSGM) web sayfasından erişim sağlanabilmektedir.

Bilgi teknolojilerindeki gelişmelerle birlikte, bilgi güvenliğinin sağlanmasına yönelik gereksinimler gittikçe daha karmaşık ve kapsamlı hale gelmiştir. Sınırlı bütçe ve personel kaynakları ile kapsamlı bir bilgi güvenliği çalışması yapılması için daha sistematik ve yönetsel sistemlerin uygulanması zorunluluk haline gelmiştir. Kılavuzun okumakta olduğunuz sürümü hazırlanırken teknik detaylardan kasten kaçınılmış, ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardında belirtilen madde başlıkları dikkate alınarak, güvenlik önlemlerinin kolay anlaşılabilir bir özeti sunulmuştur.

Günümüzde isimleri bilgi güvenliği ile birlikte sıkça anılan diğer iki önemli konu da "**siber güvenlik**" ve "**kişisel veri güvenliği**" alanlarıdır. Kılavuzda yer alan ve teknik personel tarafından özel yazılım, donanım ve araçlar kullanılmak suretiyle hayata geçirilen tedbirler, aslında birer siber güvenlik tedbiridir. Etkin bir BGYS tesis edilmesi için siber güvenlik ile ilgili teknik tedbirlere ilave olarak yönetsel tedbirlerin de alınması, farkındalık eğitimleri ile kurum kültürünün değiştirilmesi ve tüm bu süreçlere üst yönetimlerin de etkin katılımı ve desteği gerekir. Kılavuzda yer alan konulara ek olarak Bakanlığımız bünyesinde siber güvenlik ve siber olaylara müdahale ile ilgili hususların işleyişi, "**Kurumsal Siber Olaylara Müdahale Ekibi (SOME) Kurulum ve Yönetim Rehberi**" ile düzenlenmiştir.

Kişisel verilerin ve özellikle kişisel sağlık verilerinin kullanımı ve korunmasına ilişkin hususlar ise "**6698 sayılı Kişisel Verilerin Korunması Kanunu**" ve bu kanundan alınan yetkiyle Bakanlığımız tarafından çıkarılan "**Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik**" ile düzenlenmiştir. 6698 sayılı Kanun gereği kurulan "**Kişisel Verileri Koruma Kurulu (KVKK)**" tarafından çıkarılan tüm mevzuata Kurumun web sayfalarından erişim sağlanabilmektedir. Kılavuz hazırlanırken KVKK tarafından hazırlanan mevzuat da dikkate alınmış ve ISO 27001 standardı başlıkları altında işlenebilecek hususlar, önemli ölçüde Kılavuza aktarılmıştır.

Bilgi güvenliği ile ilgili son önemli husus, bilgi güvenliğinin üst yönetim sorumluluğunda yürütülecek bir faaliyet olduğudur. Yönerge gereği; Bakanlık merkez, bağlı kuruluşlar ve il sağlık müdürlükleri (İSM'ler) bünyesinde, bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere bilgi güvenliği alt komisyonlarının kurulması ve bilgi güvenliği yetkililerinin görevlendirilmesi gerekmektedir. Söz konusu komisyon ve bilgi güveliği yetkilisi olarak görevlendirilen kişilerin görevlerini layıkıyla yapabilmesi için bağlı oldukları kurumların en üst düzey yöneticileri tarafından kuvvetli bir şekilde desteklenmesi gerekmektedir.

POLİTİKALAR

A.1. BİLGİ GÜVENLİĞİ POLİTİKALARI

A.1.1. Temel Prensipler

A.1.1.1. T.C. Sağlık Bakanlığı; anayasa, yasalar, yönetmelikler ve ilgili diğer mevzuat çerçevesinde yürütmekte olduğu iş ve işlemlerde, ülke nüfusunun tamamı için doğum öncesinden ölüme kadar sağlıkla ilgili tüm süreçlerde çalışmakla yükümlü bir kurum olma hüviyeti ile ülkedeki her bir vatandaşa karşı sorumlulukları olan kuruluşlardan birisidir. Vatandaşlar herhangi bir sağlık kuruluşuna müracaat ettiğinde, en gizli ve mahrem sayılabilecek bilgilerine erişebilen ve bu bilgileri işleyebilen yegâne kuruluştur.

A.1.1.2. Bakanlık, hizmet verdiği vatandaşların kayıt altına aldığı her türlü bilgisini, kendisine emanet edilmiş bir değer olduğu vizyonuyla korumakla mükellef olduğunun bilinciyle hareket etmektedir. Bu suretle gerçekleştirilen faaliyetlerin ifasını verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yürütülmesi; edinilen bilgilerin bütünlüğünün, tutarlılığının, güvenilirliğinin sağlanması için uygun bilgi sistemleri ortamının tesis edilmesi, bu bilgi sistemlerinin kullanılmasından kaynaklanacak risklerin kontrol edilmesi ve tüm bu hususlarda gerekli tedbirlerin alınması usul ve esasları üzerine kurmuştur.

A.1.1.3. Bakanlık, bilgi güvenliği kapsamında yer alan basılı ve elektronik ortamdaki tüm bilgilerin, yasal mevzuat ışığında ve risk değerlendirme metotları kullanılarak "gizlilik, bütünlük ve erişilebilirlik" ilkelerine göre yönetilmesi amacıyla;

A.1.1.3.1. Bilgi güvenliği standartlarının gerekliliklerini yerine getirmek,

A.1.1.3.2. Bilgi güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,

A.1.1.3.3. Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,

A.1.1.3.4. BGYS'yi sürekli gözden geçirmek ve iyileştirmek,

A.1.1.3.5. Bilgi güvenliği farkındalığını artırmak için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirme vizyon ve misyonuyla hareket etmektedir.

A.1.1.4. Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iş olduğu gibi sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten insan kaynakları güvenliğine; iletişim ve haberleşme güvenliğinden bilgi teknolojileri güvenliğine kadar birçok konuyu da kapsar.

A.1.1.5. Bilgi güvenliği bilinçlendirme süreci, kurum içinde en üst seviyeden en alt seviyeye kadar tüm çalışanların katılımını gerektirir. Kurum çalışanları, yüklenici firma personeli, yarı zamanlı personel, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes "**kullanıcı"** kategorisine girer.

A.1.1.6. Bilgi güvenliği bilinçlendirme sürecindeki en büyük ve önemli hedef kitle kullanıcılardır. Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek kullanıcıların elindedir. Yöneticiler, bilgi güvenliği gereklerine personelinin uymasını, bilinçlendirme ve eğitim süreçleri ile destekleyerek sağlamakla sorumludur.

A.1.1.7. Başarılı ve etkin işleyen bir bilgi güvenliği bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür.

A.1.1.8. Sonuç olarak Sağlık Bakanlığı Bilgi Güvenliği Politikasının ana amacı; bilgi varlıklarını korumak, bilginin ve verinin gizliliğini sağlamak, bütünlüğünü bozmaya çalışacak yetkisiz kişilerin erişimini engellemek, ihtiyaç duyulan her alanda bilgiyi erişilebilir halde tutmak ve böylece Sağlık Bakanlığının güvenini ve itibarını sarsacak durumları bertaraf etmektir.

A.1.2. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu

A.1.2.1. Kurum ve kuruluşlarımızın hizmet sunumlarında bilgi ve iletişim sistemlerini her geçen gün daha fazla kullanmaları ile birlikte, söz konusu sistemlerin güvenliğinin sağlanması hem ulusal güvenliğimizin, hem de rekabet gücümüzün önemli bir boyutu haline gelmiştir. İnternet gibi açık ve bağlantılı bir ortamda bulunmanın artan erişilebilirlikle birlikte bazı riskleri de beraberinde getireceğini kabul etmek gerekir.

A.1.2.2. Bu risklerin önlenmesi ya da etkilerinin azaltılması için tüm paydaşları içeren bütüncül bir yaklaşımla yönetilerek siber olaylara karşı hazırlıklı olunması ve bu olaylardan en az zararla çıkılarak hizmet sürekliliğinin temininin esas alınması öncelikli şarttır.

A.1.2.3. Ülkemizde, ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonunu sağlamak görevi; 20 Ekim 2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı "Elektronik Haberleşme Kanunu" ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir.

A.1.2.4. Bu kapsamda önce 2013-2014 Eylem Planı yürürlüğe girmiş, zamanla artan güvenlik gereksinimleri nedeni ile güvenlik stratejilerinin güncellenmesi ihtiyacı doğmuş ve "2016-2019 Ulusal Siber Güvenlik Stratejisi" ve "2016-2019 Ulusal Siber Güvenlik Eylem Planı" hazırlanmıştır. 2016-2019 Ulusal Siber Güvenlik Stratejisinde sağlık sektörü kritik altyapı barındıran sektörler arasında yer almakta olup Sağlık Bakanlığı kritik altyapı işleten kamu kurumları arasında yer almaktadır.

A.1.2.5. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından 21 Haziran 2017 tarihli 30103 sayılı resmi gazete ile "KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ" yayımlanmıştır. Tebliğin amacı; "KamuNet'e dâhil edilecek kamu kurumlarının ağa bağlanan bilgi ve iletişim sistemlerine ilişkin olarak karşılaması gereken asgari gereklilikler ile bu kurumların

denetlenmesine ilişkin usul ve esaslar"ı belirlemek ve KamuNet'e bağlantı yapacak kamu kurumlarının kendi BGYS'lerini kurması, işletmesi ve kurulan BGYS için ISO 27001 standardına göre sertifikalandırılma zorunluluğu getirmektir.

A.1.2.6. SBSGM, 2014 yılından bu yana tüm faaliyetlerini kapsayacak şekilde kendi BGYS'ni kurmuş ve başarıyla uygulamaktadır. Tesis edilen sistemin ISO 27001 standardı ile uyumluluğu her yıl yapılan dış denetimler ile belgelenmekte ve güncelliği sağlanmaktadır.

A.1.2.7. Kılavuz hazırlanırken Uluslararası Standardizasyon Kuruluşu (ISO) tarafından yayımlanan ve TSE tarafından Türk Standardı olarak kabul edilen "TS ISO/IEC 27001 (2017) Bilgi Teknolojisi - Güvenlik Teknikleri - BGYS" standardında belirtilen metodoloji ve kontrol önlemleri dikkate alınmıştır.

A.1.2.8. Kılavuz başlıkları, ISO 27001 standardının EK-A'sında yer alan madde başlıklarından alınmıştır. Bu başlıklar içerisinde tüm kullanıcıları kapsayan madde başlıkları olabildiği gibi sadece sistem ve veri tabanı yöneticilerini, hizmet sağlayıcıları veya yöneticileri ilgilendiren müstakil konu başlıkları da yer almaktadır. Sağlık Bakanlığının kendine özgü ihtiyaçlarından kaynaklanan hususlar (tıbbi cihaz güvenliği, sistem akreditasyonları vb.) da en uygun madde başlığı altında, alt başlıklar olacak şekilde Kılavuza dâhil edilmiştir.

A.1.2.9. Kılavuzun her iki sürümü de Bakanlık merkez ve bağlı kuruluşlarının görüş ve önerileri dikkate alınmak suretiyle kaleme alınmıştır. Uygulama esnasında ortaya çıkan sorunlar ve olası görüş/öneriler, resmi yazı ile SBSGM'ye veya doğrudan bilgiguvenligi@saglik.gov.tr e-Posta adresine iletilebilecektir.

A.1.2.10. Bilgi güvenliği önlemlerinin hukuksal dayanaklarına ilişkin en güncel gelişme, 6698 sayılı kanunun yürürlüğe girmesi ile olmuştur. Ülkemizde kişisel verilerin korunmasının sağlanması ve buna yönelik farkındalık oluşturarak bilinç düzeyinin geliştirilmesi görevi KVKK'ya verilmiştir.

A.1.2.11. KVKK tarafından, 6698 sayılı kanunun uygulanmasına yönelik birçok ikincil mevzuat ve açıklayıcı doküman hazırlanmış ve yayımlanmıştır. Kurul tarafından yayımlanan ikincil mevzuata ve ilgili diğer bilgi ve belgelere Kurulun https://www.kvkk.gov.tr/ adresinden erişim sağlanabilmektedir.

A.1.2.12. KVKK tarafından yayımlanan mevzuata ilave olarak, kişisel sağlık verileri ile ilgili özel hususlar için Bakanlığımızca "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik" yayımlanmış durumdadır.

A.1.2.13. Kılavuz hazırlanırken; 6698 sayılı Kanun, KVKK tarafından yayımlanan ikincil mevzuat ve Bakanlığımız tarafından yayımlanmış olan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelikte yer alan ve doğrudan bilgi güvenliği ile ilişkili olan hususların Kılavuz içerisine alınması için çaba gösterilmiştir.

A.1.2.13.1. Kılavuzda yer alan bilgi güvenliği ile ilgili tüm tedbirlerin alınmış olması, kişisel verilerin mahremiyetinin sağlandığını ve hukuka uygun bir şekilde işlenmiş olacağını garanti etmemektedir.

A.1.2.13.2. ISO 27001 BGYS, kişisel verilerin korunması süreçlerini de kapsayan bir çalışmadır. KVKK kararları ve dokümanları incelendiğinde ISO 27001 standardının EK-A'sında yer alan kontrollere atıfta bulunulduğu gözlemlenmektedir. KVKK'nın maddeleri içerisinde yer alan veri sınıflaması, maskeleme, veri sızıntısını önleme, güvenli veri transferi ve erişim kontrollerine ilişkin hükümlerin; bu kılavuz uyarınca hazırlanacak olan bilgi güvenliği dokümantasyonu içerisinde ayrı başlıklar olarak veya konunun özelliğine binaen tamamen ayrı dokümanlar olarak ayrıca düzenlenmesi gerekliliği ortaya çıkmaktadır.

A.1.2.13.3. Bu kapsamda; kişisel verileri işleyen kişi ve makamlar, konuyla ilgili yukarıda belirtilen mevzuatı dikkate almak suretiyle, kılavuzda yer alan hususlar da dâhil olmak üzere her türlü tedbiri almak ve uygulamakla yükümlüdür.

A.1.3. Kurumsal BGYS Politikalarının Oluşturulması ve Uygulanması

A.1.3.1. Kılavuzda yer alan hususlar, yukarıda da açıklandığı üzere, Bakanlık ve bağlı kuruluşları ile merkez ve taşra teşkilatı için bilgi güvenliğinin sağlanmasına yönelik olarak alınması tavsiye edilen ve bu amaçla yaygın olarak kullanılan temel bazı tedbirleri içermektedir. Bilgi güvenliğinin tam olarak sağlanabilmesi için uygulayıcılar tarafından;

A.1.3.1.1. Kullanılan sistemler ve cihazlar, insan kaynakları ve nitelikleri, bilgi işleme tesislerinin fiziki özellikleri, bölgesel ve coğrafi farklılıklar vb. hususlardan kaynaklanan kuruma özgü bilgi güvenliği risklerinin ayrıntılı olarak tespit edilmesi,

A.1.3.1.2. Tespit edilen risklerin önlenmesi için Kılavuzda yer alan tedbirler başta olmak üzere gerekiyorsa ilave önlemlerin belirlenmesi,

A.1.3.1.3. Alınacak önlemlerin yazılı hale getirilerek tüm kurum personeline duyurulması,

A.1.3.1.4. Uygulamanın sürekli olarak takip edilerek varsa uygunsuzlukların ve yeni risklerin tespit edilmesi,

A.1.3.1.5. Tespit edilen uygunsuzluklar ve yeni riskler için düzeltici faaliyetlerin hayata geçirilmesi,

A.1.3.1.6. Sürekli iyileştirme için ihtiyaç duyulan çalışmaların yürütülmesi gerekmektedir.

A.1.3.2. Bakanlık Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzunun hayata geçirilebilmesi amacıyla **merkez teşkilat, bağlı kuruluşlar ve 81 ilin il sağlık müdürlükleri** tarafından asgari olarak aşağıda belirtilen faaliyetlerin yapılması gerekmektedir.

A.1.3.2.1. Kuruma Özgü BGYS Politikasının Hazırlanması

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. Kurumsal bilgi güvenliği politikasının geliştirilmesi kurumsal hafızaya sahip çalışanlar, bilgi güvenliği uzmanları ve yönetimin ortak çalışması ile yapılır. Bilgi güvenliği politikasının bilgi güvenliği hedefleri, stratejik hedefler ve hizmet kapsamı ile uyumlu olması gerekir.

Bilgi güvenliği politikası; kurumun sunduğu hizmetler, kullanılan teknoloji ve kurumun büyüklüğüne göre kurumdan kuruma değişiklik göstermekle birlikte en az aşağıdaki unsurları içerir:

- **Kurumun bilgi güvenliği vizyonu:** Kurumun bilgi güvenliği amaçları net olarak tanımlanmalı ve kurumun bilgi güvenliği politikasında yer almalıdır. Örnek; *"Bu güvenlik politikası, etkin ve yerleşmiş bilgi teknolojileri güvenlik süreçleri ve prosedürleri aracılığıyla sağlık hizmetlerinden faydalanan vatandaşa ait bilgilerin ya da kurumsal hizmetlerin icra edilmesi esnasında edinilen bilgi ve kaynakların güvenliğini, bütünlüğünü ve kullanılabilirliğini sağlamayı amaçlamaktadır."*

- **Üst Yönetim bilgi güvenliği taahhüdü**: Bilgi güvenliği politikası bilgi güvenliği ile ilgili uygulanabilir şartların karşılanması ve BGYS'nin sürekli iyileştirilmesi için bir taahhüt içermelidir. Örnek; *"BGYS'nin tüm süreçleri için gerekli yönetimsel destek ve kaynaklar sağlanır."*

- **Bilgi güvenliği faaliyetlerinin nasıl yürütüleceği**: Bilgi güvenliği politikasının nasıl uygulanacağı ve güvenlik ihlallerinin ne şekilde ele alınacağı açıkça belirtmelidir. Tercihen en üst düzey yetkili tarafından politikaya uyumluluğun sağlanmasına ilişkin gereklilik beyan edilmelidir. Örnek; "*Kurum bilgi güvenliği faaliyetlerinin etkin olarak yürütülmesi maksadıyla yaygın olarak kabul gören bilgi güvenliği standartları, ilgili yasa, mevzuat ve yönetmeliklerin gerektirdiği şartlara yönetim tarafından uyulacak, ilgili taraflarca uyulması sağlanacaktır. İç bağlamda belirtilen unsurlar, ilgili standart, mevzuat ve yönetmeliklerin getirdiği sorumluluklara uymakla yükümlüdür*."

Özetle, bilgi güvenliğine genel bir yaklaşım oluşturmak, kurum itibarını etik ve yasal sorumluluklarına uygun olarak korumak, hizmet verdiği paydaşların ihtiyaç ve beklentileri doğrultusunda kurumsal bilgi güvenliği tesis etmek gibi amaçlarla oluşturulan bilgi güvenliği politikası; kurumun en üst düzey yöneticisinin imzası ile yayımlanır.

Politikanın kurumun tüm çalışanları tarafından bilinmesi ve anlaşılması gerekir. Hizmet süreçlerinde etkileşimli olunan tüm ilgili taraflar ve dış paydaşların erişebilmesi için kurumsal web sitesi ana sayfasında ya da e-Posta ile gönderilmek suretiyle paylaşılır.

A.1.3.2.2. Kurum Bilgi Güvenliği Organizasyonunun Oluşturulması

Bilgi güvenliğinin bir yönetim sistemi mantığıyla ele alınması prensibi çerçevesinde, tüm yönetim sistemlerinde olduğu gibi bilgi güvenliği operasyonu ve uygulamasının başlatılması ve kontrol edilmesi amacıyla bilgi güvenliği rolleri ve sorumlulukları tanımlanmalı ve atamaları yapılmalıdır. Bilgi güvenliği sorumlulukları içerisinde; bilgi varlıklarının korunması, risk yönetimi faaliyetleri, iş sürekliliği gereklilikleri, tedarikçi ilişkilerinin bilgi güvenliği, kaynak bulma ve uygulama yönetimi gibi unsurların varlığı değerlendirilerek, kurumun organizasyon yapısının büyüklüğüne göre bilgi güvenliği rol ve sorumlulukları atanmalıdır. Kurumsal bilgi güvenliği politikasında bilgi güvenliği rol ve sorumluluklarına yer verilmelidir.

Kılavuzun A.2.3 (Bilgi Güvenliği Alt Komisyonları), A.2.4 (Bilgi Güvenliği Yetkilisi) ve A.2.5 (Kurumsal SOME Ekip Lideri ve Kurumsal SOME'ler) maddelerinde açıklandığı şekilde bilgi güvenliği politika ve stratejilerini belirlemek ve bu politikaların uygulanmasını sağlamak üzere bilgi güvenliği alt komisyonu oluşturulur. Alt komisyona bağlı, zaman zaman da alt komisyon adına çalışmak üzere Bilgi Güvenliği Yetkilisi ve SOME Ekip Lideri görevlendirilir.

A.1.3.2.3. Bilgi Güvenliği Eğitim Programlarının Yapılması

Kurum genelinde tüm personeli kapsayacak şekilde, sürekli güvenlik bilincinin, kurumsal güvenlik kültürünün oluşturulmasına ve korunmasına yardımcı olacak her türlü eğitim programı bilgi güvenliği yönetim sisteminin sağlanmasına yardımcı olur. Geleneksel bilgi sistemleri odaklı "son kullanıcı güvenlik eğitimleri" ve "yıllık bilgi güvenliği farkındalık eğitimleri"' iyi uygulama örnekleri olabileceği gibi kurumsal bilgi güvenliği farkındalığının oluşmasında yetersiz kalacaktır. Bu nedenle yıllık olarak hazırlanacak bilgi güvenliği eğitim planları; farkındalık broşürleri, posterler, e-Postalar, yarışmalar, sosyal mühendislik çalışmaları, oltalama saldırısı benzetimi ve benzeri farkındalığı arttırıcı faaliyetlerden uygulanabilir olanlarını kapsamalıdır.

A.1.3.2.4. Diğer BGYS Politika, Prosedür ve Talimatlarının Hazırlanması

Bilgi güvenliği politikası, bilgi güvenliği kontrollerini zorunlu tutan konuya özel politikalarla desteklenmelidir. Konuya özel politikalar kurum genelindeki süreçlerin ihtiyaçlarını karşılayacak ya da belirli konuları kapsayacak şekilde olabilir.

Bilgi güvenliği için iç politikalara duyulan ihtiyaç kurumdan kuruma değişebilir ancak, büyük ve karmaşık yapılarda özellikli süreçlere ve fonksiyonlara ait politikaların oluşturulması BGYS'nin sağlıklı tesisi için özellikle faydalıdır. Daha küçük ve konservatif yapılarda bilgi güvenliği için politikalar tek bir "bilgi güvenliği politikası" dokümanında ya da tek fakat ilgili dokümanların bir kümesinde verilebilir.

Bilgi güvenliği özellikli politikalarının kurum dışına dağıtımının icap ettiği durumlarda gizli bilgilerin ifşa edilmemesine dikkat edilmelidir.

Politika dokümanları ihtiyaca göre prosedür, talimat, yönerge gibi detaylarda oluşturulabilir. Konuya özel bilgi güvenliği politikaları hazırlanırken aşağıdaki hususları içerip içermediği kontrol edilmelidir:

- Erişim kontrolü / mobil cihazlar ve uzaktan çalışma (Kılavuz Madde A.6),
- Bilgi sınıflandırma (ve işleme) (Kılavuz Madde A.4.3),
- Fiziksel ve çevresel güvenlik (Kılavuz Madde A.8),
- Varlıkların kabul edilebilir kullanımı / temiz masa ve temiz ekran (Kılavuz Madde A.4),
- Bilgi transferi, haberleşme güvenliği (Kılavuz Madde A.10),
- Yazılım kurulumu ve kullanımı ile ilgili kısıtlamalar (Kılavuz Madde A.9),
- Yedekleme (Kılavuz Madde A.9.13),
- Kötücül yazılımlardan koruma (Kılavuz Madde A.9.6),
- Kriptografik kontrollerin kullanımı (Kılavuz Madde A.7)
- Teknik açıklıkların yönetimi (Kılavuz Madde A.9.14),
- Kişi tespit bilgisinin mahremiyeti ve korunması (Kılavuz Madde A.12),
- Tedarikçi ilişkileri (Kılavuz Madde A.11).

A.1.3.2.5. Bilgi Güvenliği Eylem Planları

- Yönerge gereği, Kılavuzda yer alan hususların hayata geçirilmesi ve takibi için SBSGM tarafından eylem planları hazırlanır ve yayımlanır.
- Yayımlanacak eylem planlarında, kurumların bilgi güvenliği alt komisyonları vasıtasıyla hazırlanması gereken BGYS politika, prosedür ve talimatları ismen sıralanır.
- Eylem planlarında yer alan hususlar, Kurum BGYS'lerinin tesisi için yapılması gereken asgari konuları içerir. Kurumlarca eylem planında belirtilmeyen konular için de BGYS politika, prosedür veya talimatları hazırlanıp uygulamaya alınabilir.

A.2. BİLGİ GÜVENLİĞİ ORGANİZASYONU

A.2.1. Bakanlık Bilgi Güvenliği Yönetim Komisyonu

A.2.1.1. Bakanlık genelinde bilgi güvenliği ve siber olaylara müdahale ile ilgili konularda en üst düzeyde koordinasyon ve karar organı olarak görev yapmak üzere, Bilgi Güvenliği Yönetim Komisyonu kurulur.

A.2.1.2. Komisyon, Sağlık Bilgi Sistemleri Genel Müdürünün Başkanlığında aşağıda belirtilen üyelerden oluşur.

Komisyondaki Görevi	Bağlı Olduğu Birim	Görevi
Başkan	SBSGM	Genel Müdür
Başkan Yrdc.	SBSGM	Genel Müdür Yardımcısı
Koordinatör	SBSGM	Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanı
Raportör	SBSGM	SOME Birim Sorumlusu
Raportör	SBSGM	BGYS Birim Sorumlusu
Üyeler	Türkiye İlaç ve Tıbbi Cihaz Kurumu Başkanlığı	Kılavuzun A.2.3 maddesi gereği bağlı bulunduğu Kurum/Genel Müdürlük adına "Bilgi Sistemleri Koordinatörü" olarak görevlendirilen en az Daire Başkanı düzeyinde personel
	Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü	
	Kamu Hastaneleri Genel Müdürlüğü	
	Halk Sağlığı Genel Müdürlüğü	
	Sağlık Hizmetleri Genel Müdürlüğü	
	Acil Sağlık Hizmetleri Genel Müdürlüğü	
	Yönetim Hizmetleri Genel Müdürlüğü	
	Sağlığın Geliştirilmesi Genel Müdürlüğü	
	Sağlık Yatırımları Genel Müdürlüğü	
	Strateji Geliştirme Başkanlığı	
	Bakanlık Hukuk Müşavirliği	

A.2.1.3. Komisyona bağlı olarak çalışmak üzere sorumluluk sahası ile ilgili çalışma grupları oluşturulabilir. Çalışma grupları oluşturulurken konunun özelliği dikkate alınarak farklı disiplinlerden personel bulundurulur.

A.2.1.4. Komisyon, Başkanın çağrısı üzerine yılda en az bir kere toplanır. Gerekli görülen durumlarda başkan komisyonu her zaman toplantıya çağırabilir.

A.2.1.5. Toplantıda kararlar oy çokluğu ile alınır. Oyların eşitliği halinde başkanın kullanmış olduğu oy esas alınır.

A.2.1.6. Komisyonun görevleri şunlardır:

A.2.1.6.1. Bakanlık genelinde uygulanacak bilgi güvenliği ve siber olaylara müdahale ile ilgili üst düzey politika ve stratejileri belirler.

A.2.1.6.2. Bakanlık Bilgi Güvenliği Politikaları Yönergesinde yer alan konuları koordine eder.

A.2.1.6.3. Bilgi güvenliği ve siber olaylara müdahale ile ilgili politika ve stratejilerin uygulanması için eylem planları hazırlar ve yayımlar.

A.2.1.6.4. Eylem planlarının uygulanmasının etkinliğini ölçer, sonuçlarını değerlendirir ve iyileştirme için ihtiyaç duyulan tedbirleri alır.

A.2.1.6.5. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı uyarınca, kritik sektörler arasında yer alan sağlık sektörü ile ilgili siber güvenlik stratejilerinin, Bakanlık dışındaki diğer paydaşlar ile koordine edilmesi faaliyetlerini yürütür.

A.2.1.6.6. SBSGM bünyesinde görev yapan Bakanlık Sektörel SOME faaliyetleri, Komisyonun gözetiminde yürütülür.

A.2.2. Sağlık Bakanlığı Sektörel SOME

A.2.2.1. Sağlık sektörü alanındaki siber güvenlik çalışmalarının planlanması, koordinasyonu ve denetimi için Bakanlık bünyesinde Sektörel SOME oluşturulur.

A.2.2.2. Sektörel SOME, sektör tecrübesine ve siber güvenlik uzmanlığına (kayıt yönetimi, siber olay yönetimi ve bilgi güvenliği yönetimi) sahip personelden oluşur.

A.2.2.3. Sektörel SOME, yıllık olarak hazırlayacağı Sektörel Siber Güvenlik Faaliyet Raporunu Bakanlık Bilgi Güvenliği Yönetim Komisyonuna sunar.

A.2.2.4. Sektörel SOME, bünyesinde faaliyet gösteren kurumsal SOME'lerden gelen Siber Olay Müdahale Raporunu Ulusal Siber Olaylara Müdahale Ekibine (USOM) iletir.

A.2.2.5. Sektörel SOME'nin görev ve sorumlulukları ile ilgili esaslar, Kurumsal SOME Kurulum ve Yönetim Rehberi'nde yer alır.

A.2.2.6. Sorumluluk alanını oluşturan sağlık sektörünü kapsayacak şekilde siber saldırı uyarısı ve güvenlik açığı duyurusu yayımlar.

A.2.3. Bilgi Güvenliği Alt Komisyonları

A.2.3.1. 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.

A.2.3.2. 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.

A.2.3.3. 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.

A.2.3.4. 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.

A.2.3.4.2. Bakanlık tarafından yayımlanan eylem planında yer alan hususların gerçekleştirilmesini sağlar.

A.2.3.4.3. Bilgi güvenliği yetkili/yetkililerini belirler ve görevlendirmesini yapar.

A.2.3.4.4. 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.

A.2.4. Bilgi Güvenliği Yetkilisi

A.2.4.1. Bakanlık merkez, bağlı kuruluşlar ve il sağlık müdürlükleri bünyesinde bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere "**bilgi güvenliği yetkilisi**" görevlendirilir.

A.2.4.2. Hangi seviyede ve hangi alt kuruluşlarda "bilgi güvenliği yetkilisi" görevlendirileceği, ilgili alt komisyonlar tarafından karar altına alınır. Bu tespit yapılırken kurum bilgi işleme tesisleri, personel sayısı, bölgesel özellikler, tespit edilen risklerin miktarı ve önem derecesi gibi ölçütler göz önüne alınarak, ölçek yaklaşımı çerçevesinde karar verilir ve görevlendirilen bilgi güvenliği yetkilisinin sorumluluk kapsamı belirlenir.

A.2.4.3. Bilgi güvenliği yetkilisi olarak; yönetim sistemleri konusunda tecrübeli, kurumda yürütülen iş süreçlerine hâkim, kurum kültürüne vakıf, tercihan bilgi sistemleri konusunda teknik eğitim almış, alt komisyondan aldığı yetkiye dayanarak bilgi güvenliği ile ilgili faaliyetleri yürütürken kurumda görev yapan tüm personel ile uygun

yöntemlerle iletişim kurabilecek, gerektiğinde otorite kullanabilecek, mümkünse yönetici düzeyinde bir personel görevlendirilir.

A.2.4.4. Bilgi güvenliği yetkilisinin ana işlevi, bulunduğu kurumdaki bilgi güvenliği faaliyetlerini alt komisyondan almış olduğu yetkiye dayanarak SBSGM ile koordineli bir şekilde yürütmektir. Bu yönüyle, bağlı bulundukları alt komisyonun bilgi güvenliği ile ilgili konulardaki icra organı olarak hareket ederler.

A.2.4.5. Bilgi güvenliği yetkilisi olarak görevlendirilen personel, SBSGM tarafından ana ilkeler konusunda eğitilir ve yönlendirilir.

A.2.5. Kurumsal SOME Ekip Lideri ve Kurumsal SOME'ler

A.2.5.1. Kurumsal SOME'ler; Bakanlık bağlı kuruluşları, il sağlık müdürlükleri ve sektörel SOME tarafından uygun görülen sağlık alanında faaliyet gösteren özel kuruluşların bünyelerinde kurulur.

A.2.5.2. Kurumsal SOME'ler, sektörel SOME tarafından koordine edilir.

A.2.5.3. Kurumsal SOME'ler, siber olaya müdahale sonrası siber olay müdahale raporunu ve yıllık faaliyet raporunu Sektörel SOME'ye iletir.

A.2.5.4. Kurumsal SOME'ler, temel sorumluluğu siber güvenlik olan bir ekip lideri koordinatörlüğünde kurulur.

A.2.5.5. Kurumsal SOME ekip liderinin en az lisans derecesine sahip olan ve siber güvenlik konusunda uzmanlaşmış personel arasından seçilmiş olması tercih edilir.

A.2.5.6. Kurumsal SOME'lerin yapısı, görevi ve sorumluluklarına ilişkin hususlar, Kurumsal SOME Kurulum ve Yönetim Rehberi'nde yer alır.

A.2.6. Üst Yönetimlerin Sorumluluğu

A.2.6.1. Bilgi güvenliği politikalarının uygulanması üst yönetim tarafından takip edilir. Bilgi güvenliği politikası kapsamında, bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi üst yönetimin sorumluluğundadır.

A.2.6.2. Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projeler üst yönetim tarafından gözden geçirilir ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanır.

A.2.6.3. Üst yönetim, bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik yeterli kaynağı tahsis eder.

A.2.6.4. Üst yönetim bilgi güvenliği ile ilgili faaliyetlerin yerine getirilmesi maksadıyla bu bölümde belirtilen bilgi güvenliği organizasyonunu kurar ve çalıştırılmasını sağlar.

A.2.6.5. Bilgi güvenliği ile ilgili süreçleri bilgi güvenliği komisyonları vasıtasıyla takip eder. Komisyon çalışmaları neticesinde üst yönetim kararı gerektiren hususlar için gerekli kararları verir ve uygulanmasını takip eder.

A.3. İNSAN KAYNAKLARI VE SON KULLANICI GÜVENLİĞİ

A.3.1. İşe Alma Öncesinde Yapılacak Kontroller

A.3.1.1. 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.

A.3.1.2. İşe alma öncesinde yapılacak güvenlik kontrollerinin amacı, çalışanların kendilerinden beklenen sorumlulukları anlamalarını sağlamak ve düşünüldükleri roller için uygun olmalarını temin etmektir.

A.3.1.3. İşe alınacak adaylar iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol (tarama yapılır) edilir.

A.3.1.4. 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.

A.3.1.5. İşe alınacak kişilerin eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilmesi için aşağıdaki yöntemlerden biri ya da birkaçı birlikte kullanılabilir.

A.3.1.5.1. Kişi özgeçmişinin doğrulanması (belgelerin tamlığı),

A.3.1.5.2. Kişinin atanacağı görevle ilgili eğitim ve tecrübe açısından gerekli yeterliliğe sahip olmasının sağlanması,

A.3.1.5.3. Beyan edilen akademik ve işle ilgili niteliklerin doğrulanması (diplomaların, referans mektuplarının, bonservis belgelerinin doğru ve geçerli olduğunun teyit edilmesi),

A.3.1.5.4. 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,

A.3.1.5.5. 657 sayılı Kanuna bağlı olmayan diğer personel için bağlı oldukları yasal mevzuatta yer alan hükümler uyarınca güvenlik incelemelerinin yaptırılması,

A.3.1.5.6. Yüklenici personeli, destek personeli vb. statüde çalışacak personelin adli sicil kayıtlarının istenmesi ve incelenmesi.

A.3.1.6. Yükleniciler ile yapılan sözleşmelerde, idare tarafından yüklenici personeli için tarama yürütüleceği ve tarama sonuçlarının menfi olması durumunda alınacak önlemler (örneğin personelin değiştirilmesi vb.) belirtilir.

A.3.1.7. 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.

A.3.1.8. 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.

A.3.2. Çalışma Esnasında Uygulanacak Kontroller

A.3.2.1. Çalışma esnasında uygulanacak güvenlik kontrollerinin amacı, çalışanların işlerini yaparken bilgi güvenliği ile ilgili sorumluluklarının farkında olmalarını ve beklenen şekilde yerine getirmelerini sağlamaktır.

A.3.2.2. İşe yeni başlayan personelin başlayış işlemlerinin eksiksiz olarak yapılmasını sağlamak için “işe başlama formu” hazırlanır ve uygulanır.

A.3.2.3. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi sorumludur.

A.3.2.4. 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. Örnek olarak kullanılabilecek bir işe başlama formu KLVZ-EK-01’dedir.

A.3.2.5. 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.

A.3.2.6. Bilgi güvenliği ile ilgili beklentiler ve sorumluluklar, çalışanların görev tanımlarına eklenir.

A.3.2.7. Çalışanların kuruluşun bilgi güvenliği politikasına uyumu izlenir.

A.3.2.8. Tüm çalışanlar ve yükleniciler için bilgi güvenliği farkındalık eğitimi programları hazırlanır ve uygulanır.

A.3.2.9. Bilgi güvenliği ihlaline neden olan kişilere yapılacak işlemler (disiplin prosedürü) önceden belirlenir ve kişilere duyurulur. İhlal oluştuğunda, disiplin prosedüründe yazan hususlar uygulanır.

A.3.2.10. Bilgi güvenliği ihlali yapan personele uygulanan yaptırımlar (kişi kimlik bilgisi verilmeden) diğer çalışanlara duyurulur ve onlar için de örnek teşkil etmesi sağlanır.

A.3.3. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri

A.3.3.1. Kurumların bilgi güvenliği yetkililerince, bilgi güvenliği teknik ve farkındalık eğitimleri için yıllık olarak uygulanmak üzere bir eğitim planı hazırlanır.

A.3.3.2. Hazırlanan plan, kurumun bilgi güvenliği alt komisyonu tarafından onaylanır.

A.3.3.3. 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.

A.3.3.4. 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.

A.3.3.5. 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.

A.3.3.6. Her yıl tüm personele en az bir kere, yüz yüze (sınıf ortamında veya konferans şeklinde) olacak şekilde bilgi güvenliği farkındalık eğitimi verilmesi tavsiye edilir.

A.3.3.7. Yüz yüze eğitimler haricinde özellikle bilgi teknolojilerinin sunmuş olduğu yetenekler/fırsatlar da kullanılmak suretiyle personelin farkındalık düzeylerinin artırılması sağlanır. Bu kapsamda;

A.3.3.7.1. Bilgi güvenliği afişleri,

A.3.3.7.2. Bilgi güvenliği broşür ve el kitapları, e-bültenler,

A.3.3.7.3. Bilgisayarların açılış ekranlarına merkezi olarak konulacak ara yüzler,

A.3.3.7.4. İnternet tabanlı eğitim,

A.3.3.7.5. Uzaktan eğitim gibi araçlar kullanılabilir.

A.3.3.8. Sunulan bilgi güvenliği teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülür ve eğitim etkililiği hususunda değerlendirme yapılır.

A.3.3.9. Eğitim katılım formları hazırlanır, katılımcılara imzalatılır ve bilgi güvenliği alt komisyonu tarafından belirlenecek süre boyunca muhafaza edilir.

A.3.4. Görev Değişikliği veya İşten Ayrılma İçin Uygulanacak Kontroller

A.3.4.1. 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.

A.3.4.2. 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.

A.3.4.3. İşten ayrılan veya görev değişikliği yapan personelin ayrılma işlemlerinin eksiksiz olarak yapılmasını sağlamak için "işten ayrılma formu" hazırlanır ve uygulanır. Örnek olarak kullanılabilecek işten ayrılma formu KLVZ-EK-02'dedir.

A.3.4.4. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi ile insan kaynakları birimi müştereken sorumludur.

A.3.4.5. 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.

A.3.4.6. 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.

A.3.4.7. Ayrılan veya görev yeri değişen personel tarafından yürütülen faaliyetlerin aksamaması için birim sorumlusu tarafından gerekli tedbirler alınır.

A.3.4.8. Mümkünse ayrılan personel ile yeni katılan personelin geçici bir süre birlikte görev yapması sağlanır.

A.3.4.9. Ayrılan kişiden teslim alınan bilgisayarlar güvenli silme işlemi yapılmadan bir başka kullanıcıya teslim edilemez.

A.3.5. Kullanıcıların Bilgi Güvenliği Sorumlulukları

A.3.5.1. 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.

A.3.5.2. 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.

A.3.5.3. 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.

A.3.5.4. 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.

A.3.5.5. Personel, edindiği bilgileri hiçbir kişi, grup, kurum veya kuruluşun menfaati için kullanamaz.

A.3.5.6. 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.

A.3.5.7. 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.

A.3.5.8. Bu yükümlülük, personelin görev yaptığı kurum ile ilişkisinin sona ermesi halinde de devam eder.

A.3.5.9. Personel, görevi nedeniyle edindiği gizli bilgiler hakkında, hiçbir sebeple yazılı veya sözlü açıklama yapamaz.

A.3.5.10. Personel, görevi kapsamında erişim hakkının bulunduğu sistemleri ve bilgileri, yetkisi içinde ya da yetkisini aşarak kendisine veya bir başkasına çıkar sağlamak amacıyla kullanamaz.

A.3.5.11. 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.

A.3.5.12. 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.

A.3.5.13. 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.

A.3.5.14. 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.

A.3.5.15. 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.

A.3.5.16. Personel, 5651 sayılı kanun gereği tutulması gereken kayıtlara ilave olarak; Bakanlık ve 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.

A.3.5.17. 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.

A.3.6. Elektronik Posta Güvenliği

A.3.6.1. Bakanlığımızda 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.

A.3.6.2. KVKK tarafından 6698 sayılı Kanunda yer alan bazı hususların açıklanması amacıyla alınan 2018/10 sayılı karar gereği, e-Posta ile aktarılacak verilerin özel nitelikli kişisel veri statüsünde olması durumunda aktarma işlemlerinin kurumsal e-Posta veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak yapılması kanuni zorunluluktur.

A.3.6.3. Bakanlığımızda görev yapan 657 sayılı Kanuna bağlı tüm kamu personeline, talep etmeleri halinde kurumsal e-Posta hesabı açılır.

A.3.6.4. Çeşitli sözleşmeler kapsamında Bakanlığımızda görev yapan ve yaptıkları iş gereği e-Posta hesabı olması gereken personele, sıralı yöneticileri tarafından onay verilmesi halinde kurumsal e-Posta hesabı açılır.

A.3.6.5. 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).

A.3.6.6. Bakanlığımız merkez ve taşra teşkilatında 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).

A.3.6.7. 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.

A.3.6.8. 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.

A.3.6.9. Bakanlık e-Posta Birimi tarafından uygulanan e-Posta yönetimi ve güvenliği ile ilgili politikalar şu şekildedir:

A.3.6.9.1. Kullanıcıların e-Posta hesaplarına tarayıcı programları, masaüstü istemci uygulaması (Office Outlook) ve cep telefonları üzerinden güvenli olarak erişebilmeleri için gerekli servisler sağlanır.

A.3.6.9.2. e-Posta hesabı ilk kez açıldığında kullanıcılara "Bakanlık e-Posta Kullanım Politikası ve e-Posta kullanımında dikkat edilmesi gereken hususlar/kullanıcı sorumluluklarını bildiren bilgilendirme yazısı" e-Posta ekinde gönderilir.

A.3.6.9.3. Kullanıcı parolalarının Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen politikalar ile uyumlu olup olmadığı denetlenir.

A.3.6.9.4. e-Posta yönetim birimi tarafından oluşturulan ve sisteme ilk kez girişte kullanılan parolanın ilk kullanımdan sonra değiştirilmesi sağlanır.

A.3.6.9.5. Kullanıcıların son kullandığı üç parolayı kullanması engellenir.

A.3.6.9.6. Kullanıcılar, altı ayda bir parolalarını değiştirmeye zorlanır. Parola değiştirme süresine beş (5) gün kala uyarı iletisi gönderilir.

A.3.6.9.7. Kullanıcılara e-Posta hesabının parolasını değiştirmek için kısa mesaj servisi (SMS) ile onay kodu gönderilir veya alternatif e-Posta aracılığı ile parola değişimi sağlanır. SMS onayı kullanıcıyı yeni oluşturacağı parola ekranına yönlendirir. Kullanıcıların daha önce sisteme kaydettiği alternatif e-Posta adresi üzerinden parola yenilenmesi tercih edilmişse, sistem tarafından parola değişikliği linki gönderilir.

A.3.6.9.8. 657 sayılı Kanun kapsamı dışında istihdam edilmiş olan personel için e-Posta hesabının ilk açılmasından itibaren aktif dizinde bir yıl kullanım süresi belirlenir. Bir yıllık süre dolduğunda aktif dizin aracılığı ile kimlik doğrulaması yapan tüm uygulamalara erişimler kapatılır.

A.3.6.9.9. Bir yıl süre ile sisteme giriş yapmayan kullanıcıların hesapları geçici olarak kapatılır. Bu hesaplar aktif dizinde pasife çekilir.

A.3.6.9.10. Kullanıcılara e-Posta hesabı ilk kez açıldığında bir GB disk alanı tanımlanır. Kota artırımı e-Posta Birimi tarafından dinamik olarak veya e-Posta Birimine e-Posta ile yapılan talepler doğrultusunda yapılır.

A.3.6.9.11. Yüksek sayıda üye içeren dağıtım gruplarına gönderilen iletilerin denetim ve onay işlemleri için "moderatör" tanımlanır. İhtiyaç olması durumunda sadece belirli kullanıcıların veya grupların söz konusu dağıtım gruplarına ileti göndermesi için detay yetkilendirmeler yapılır.

A.3.6.9.12. Yüksek sayıda üye içeren dağıtım grupları, tüm kullanıcılar tarafından görülen genel adres defterinden gizlenir.

A.3.6.9.13. Bir e-Postaya eklenebilecek en fazla alıcı sayısı 100 (yüz) e-Posta adresi ile sınırlı tutulur.

A.3.6.9.14. Gönderilen e-Posta boyutu 25 MB'yi geçemez.

A.3.6.9.15. Dağıtım gruplarının kullanım durumları (e-Posta akış trafiği) takip edilir ve bir yıl boyunca kullanılmayan gruplar tespit edilerek silinir.

A.3.6.9.16. e-Posta iletimlerinde "exe" gibi çalıştırılabilir dosyaların gönderilmesi engellenir.

A.3.6.9.17. e-Posta sistemlerinde fazla veri (data) boyutu oluşturması sebebi ile e-Posta hesaplarına profil resmi eklenmesi engellenmiştir.

A.3.6.9.18. *@saglik.gov.tr uzantılı e-Posta hesabından farklı uzantılı e-Posta adreslerine gönderilen iletilerde e-Posta Yasal Uyarı (Disclaimer) metni gönderilmektedir.

Yasal Uyarı: Bu e-Postanın içerdiği bilgiler (ekleri de dâhil olmak üzere) gizlidir. T.C. Sağlık Bakanlığı onayı olmadan içeriği kopyalanamaz, üçüncü kişilere açıklanamaz veya iletilemez. Bu mesajın gönderilmek istendiği kişi değilseniz ya da bu e-Postayı yanlışlıkla aldıysanız, lütfen yollayan kişiyi haberdar ediniz ve mesajı sisteminizden derhal siliniz. T.C. Sağlık Bakanlığı bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda bir garanti vermemektedir. Bu nedenle, bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından ve saklanmasından T.C. Sağlık Bakanlığı sorumlu değildir. Bu mesajın içeriği yazarına ait olup, T.C. Sağlık Bakanlığı görüşlerini içermeyebilir. Bu e-Posta bizce bilinen tüm bilgisayar virüslerine karşı taranmıştır.

Disclaimer: This e-mail (including any attachments) may contain confidential and/or privileged information. Copying, disclosure or distribution of the material in this e-mail without the permission of Ministry of Health of Turkey is strictly forbidden. If you are not the intended recipient (or have received this e-mail in error), please notify the sender and delete the email from your system immediately. Ministry of Health of Turkey makes no warranty as to the accuracy or completeness of any information contained in this message and hereby excludes any liability of any kind for the information contained therein or for the information transmission, reception, storage or use of such

in any way whatsoever. Any opinions expressed in this message are those of the author and may not necessarily reflect the opinions of Ministry of Health of Turkey. This e-mail has been scanned for all computer viruses known to us.

A.3.6.10. Kurumsal ve tüzel hesapların kullanımında dikkat edilmesi gereken hususlar şu şekildedir;

A.3.6.10.1. Kullanıcılar, kendilerine tahsis edilen e-Posta hesabını bir başka kişiye kullandıramaz veya devredemez.

A.3.6.10.2. Kullanıcılar, parolalarını Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen parola politikaları uyarınca oluşturur ve kullanır.

A.3.6.10.3. Kullanıcılar, kendilerine ait parolanın güvenliğinden ve söz konusu parola kullanılarak gönderilen e-Postalardan doğacak hukuki işlemlerden sorumludur.

A.3.6.10.4. Kurumsal e-Posta hesabı yalnızca kurumsal süreçlere ilişkin iş ve işlemlerde kullanılabilir. Kurumsal e-Posta hesaplarının, idari ve hukuki düzenlemelere aykırı ya da şahsi iş ve işlemlere ilişkin kullanımından kaynaklanan her türlü adli, idari, mali ve cezai sorumluluk ilgili hesap kullanıcısına aittir.

A.3.6.10.5. Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-Posta hesapları kullanılamaz. Aksine durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.

A.3.6.10.6. Konusu suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden ve sahip olduğu görev kapsamı içindeki iş ve işlemler dışındaki e-Posta hesabının kullanımından kullanıcı sorumludur.

A.3.6.10.7. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-Posta gönderilemez.

A.3.6.10.8. 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.

A.3.6.10.9. 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.

A.3.6.10.10. 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.

A.3.6.10.11. e-Posta gönderimlerinde, mesajın en alt kısmına gönderen kişinin kimlik ve iletişim bilgileri yazılır.

A.3.6.10.12. Kullanıcılar, gelen veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemek için her türlü tedbiri alır.

A.3.6.10.13. Tanınmayan elektronik postaların açılması, eklentilerinde bulunan dosya veya programların indirilip çalıştırılmasından kaynaklanabilecek güvenlik sorunlarının sorumluluğu kullanıcıya aittir.

A.3.6.10.14. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-Postalara yanıt verilmez.

A.3.6.10.15. Kaynağı bilinmeyen e-Posta ekinde gelen dosyalar kesinlikle açılmaz.

A.3.6.10.16. Kullanıcılar, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

A.3.6.10.17. 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.

A.3.7. Sosyal Mühendislik ve Sosyal Medya Güvenliği

A.3.7.1. 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.

A.3.7.2. 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.

A.3.7.3. Sosyal mühendislik saldırılarından korunmak için kişisel olarak dikkat edilmesi gereken hususlar şu şekildedir:

A.3.7.3.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunuz.

A.3.7.3.2. Bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket ediniz.

A.3.7.3.3. Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.

A.3.7.3.4. Özellikle telefonda, e-Posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi kesinlikle paylaşmayınız.

A.3.7.3.5. Parola kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-Posta ile parolanızı hiç kimseyle kesinlikle paylaşmayınız.

A.3.7.3.6. Oluşturulan dosyaya erişecek kişiler ve haklarını, “bilmesi gereken” prensibine göre belirleyiniz ve erişim kontrol tedbirleri uygulayınız.

A.3.7.3.7. Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.

A.3.7.3.8. Çöpe atılan kâğıtlara dikkat ediniz. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtları, kâğıt kırpma makinesinde imha ediniz.

A.3.7.3.9. Çok acele bilgi istendiği zaman istenen bilginin niteliğine göre teyit mekanizması kullanınız.

A.3.7.3.10. Bilgisayarınızı yabancı bir kişiye kullandırmayınız. Bu kişiler tarafından bilgisayarınıza takılacak olan USB depolama aygıtları ya da harici disklerden bilgisayarınıza zararlı yazılım bulaştırabilir.

A.3.7.3.11. Hediye olarak verilen USB depolama aygıtlarını kullanmadan önce mutlaka virüs taramasından geçiriniz.

A.3.7.4. Hastanelerde sosyal mühendislik alanında alınacak bazı önlemler şu şekilde sıralanabilir:

A.3.7.4.1. Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınır.

A.3.7.4.2. Telefon ile hasta hakkında bilgi almak isteyen kişilere, hastanın kişisel bilgileri ile ilgili açıklama yapılmaz.

A.3.7.4.3. Hasta dosyaları ilgili doktor ve hemşire dışında kimseyle paylaşılmaz. Kolay ulaşılır yerlere konulmaz.

A.3.7.4.4. Sağlık Bilgi Yönetim Sistemi (SBYS) programlarında kullanılan parolalar kimseyle paylaşılmaz.

A.3.7.5. Kişisel Sosyal Medya Güvenliği

A.3.7.5.1. Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalar farklı seçilir.

A.3.7.5.2. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.

A.3.7.5.3. Kuruma ait gizli bilgiler, resmi yazılar, çeşitli gelişmeler sosyal medya ortamında yayımlanamaz.

A.3.7.5.4. Eğitimlerde sosyal medya güvenliği ile ilgili hususlara yer verilir.

A.4. VARLIK YÖNETİMİ

A.4.1. BGYS Bakış Açısıyla Varlıklar

A.4.1.1. Varlık, kurum için değeri olan herhangi bir şey olarak tanımlanabilir.

A.4.1.2. Standart envanter yönetimi bakış açısıyla, maddi değeri olan tüm varlıklar yürürlükteki Taşınır Mal Yönetmeliği ya da Kamu İdarelerine Ait Taşınmazların Kaydına İlişkin Yönetmelik uyarınca kayıt altına alınır ve ilgili yönetmeliklerde belirtilen usuller ile takibi yapılır.

A.4.1.3. BGYS bakış açısıyla varlıklar biraz daha farklılık arz eder. Envantere kayıtlı olup olmadığına bakılmaksızın kuruma ait tüm hassas bilgiler ve bu bilgilerin işlendiği ortamlar "varlık" olarak değerlendirilir.

A.4.1.4. BGYS kapsamında varlık envanterine esas olan varlık kategorileri aşağıdaki gibidir.

A.4.1.4.1. **İş Süreçleri:** Kurumsal bilgi varlıklarının kullanıldığı, çeşitli vasıtalarla hassas bilgilerin yoğun olarak işlendiği iş süreçleri (hasta kabul, heyet işlemleri, tıbbi kayıt arşiv vb.).

A.4.1.4.2. **Kurumsal Bilgi Varlıkları:** Elektronik veya kâğıt ortamda tutulan hasta kayıtları, personel kayıt ve dosyaları, kurumsal evraklar, bilgisayarlarda saklanan ve kurum için değeri olan veriler, raporlar, listeler, çizimler, veri tabanları, veri tabanı yedekleri, faturalar, sözleşmeler, teklifler, telifler, lisanslar vb.

A.4.1.4.3. **Yazılımlar:** İşletim sistemleri, ofis uygulamaları, HBYS yazılımları, laboratuvar yazılımları, tıbbi görüntüleme yazılımları, kurumsal yazılımlar (EBYS, ÇKYS, KPS, HİTAP vb.) vb.

A.4.1.4.4. **Fiziksel varlıklar:** Sunucular, masaüstü bilgisayarlar, taşınabilir bilgisayarlar, depolama birimleri, yedekleme birimleri (kasetler, hard diskler vb.), aktif cihazlar (anahtarlama cihazı, güvenlik duvarı, yönlendirici, ağ erişim cihazı, anahtar, modem, erişim noktası vb), fakslar, fotokopiler, yazıcılar, santraller, telefonlar, evrak imha cihazları, ağa bağlı olarak çalışan veya ağa bağlanma arayüzleri olan tıbbi cihazlar vb.

A.4.1.4.5. **İnsan Kaynakları:** Çalışanlar

A.4.1.4.6. **Altyapı:** Yapısal ve elektrik kablolama altyapısı, UPS, jeneratör, iklimlendirme, giriş/çıkış kontrol sistemleri, kamera sistemleri, yangın, duman uyarı sistemleri, yangın söndürme sistemleri, destek teçhizatı vb.

A.4.1.5. **Mekânlar:** Yönetim ve hizmet odaları, sunucu odaları, arşiv odaları, tıbbi kayıt saklama odaları vb.

A.4.2. Varlık Envanterinin Tespiti

A.4.2.1. Varlık envanterinin belirlenmesi süreci, tek başına bir kişinin üstesinden gelebileceği bir faaliyet değildir. Çalışmanın bilgi güvenliği alt komisyonundan alınan yetki ve destekle, Kurumun üst yönetimi tarafından görevlendirilecek bir ekip vasıtasıyla yapılması gerekir. Ekibe kurumun bilgi güvenliği yetkilisinin başkanlık etmesi sağlanır.

A.4.2.2. Bilgi güvenliği yetkilisince, görevlendirilen ekip ile birlikte kurumun iş süreçleri analiz edilir. Başta taşınır mal sorumluları olmak üzere, teşkilatta yer alan diğer birimlerin birim sorumluları ile birlikte çalışılmak suretiyle, bilgi varlıklarının envanteri belirlenir.

A.4.2.3. Envanter belirleme işlemi bir kez yapılan ve tamamlanan bir iş değildir. Hazırlanan envanterin yazılı hale getirilmesi, farklı kaynaklardan (Çekirdek Kaynak Yönetim Sistemi/ÇKYS, Malzeme Kaynak Yönetim Sistemi/SBYS vb.) doğruluğunun kontrol edilmesi ve sürekli olarak güncel tutulması gerekir. Envanter tespit süreci, bir döngü şeklinde, periyodik olarak yapılması gereken bir faaliyettir.

A.4.2.4. Varlık envanteri, sadece fiziksel varlıklar veya bilgi sistem teçhizatından oluşmaz. Varlıklar belirlenirken, başta hassas bilgilerin işlendiği kritik iş süreçleri olmak üzere, bu süreçlere konu olan tüm kurumsal bilgi varlıklarının ortaya çıkarılması gerekir. (Örneğin İK Birimleri ile yapılacak varlık envanter çalışmasında, kurum çalışanlarının kâğıt ortamda saklanan şahsi dosyaları kurum için korunması gereken önemli bir varlık olarak gündeme getirilmişse, bu kaydın mutlaka varlık envanterinde yer alması gerekir. Eğer bu kayıt, varlık envanterine girmez ise; onunla ilgili riskler ve koruma önlemleri de tespit edilemeyecek, dolayısı ile tesis etmiş olduğumuz BGYS'nin bir bölümü eksik veya hatalı olacaktır.)

A.4.2.5. Envanterde yer alan her bir varlık için "varlık sahibi" belirlenir. Varlık sahibi gerçek bir kişi olabileceği gibi, bir birim ya da kurum da olabilir.

A.4.2.6. Varlık sahiplerince Kılavuzun A.4.3 (Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi) maddesinde belirtilen bilgi sınıflandırma kuralları uyarınca, her varlığa bir gizlilik derecesi atanır. Gizlilik derecesi yüksek varlıklar için taşıdığı yüksek risk değeri nedeniyle daha sıkı güvenlik tedbirleri uygulanır.

A.4.2.7. Kurum bilgi varlıklarının tespitinde örneği KLVZ-EK-05 Kurum Bilgi Varlıkları Envanter Çizelgesi kullanılabilir veya kurumun kendi özelliklerine uygun bir başka çizelge geliştirilebilir.

A.4.2.8. Varlık sahipleri;

A.4.2.8.1. Varlıklarını envantere doğru olarak kaydettirmekten,

A.4.2.8.2. Varlıklarına uygun gizlilik derecesi ve varlık değeri atamaktan, varlıklarının uygun şekilde korunmasından,

A.4.2.8.3. Varlıklara erişecek kişi veya süreçleri için erişim izinlerini planlamaktan, bunlarla ilgili kararları vermekten,

A.4.2.8.4. Varlıkların silinmesi ya da imha edilmesinde uygun işlemlerin uygulanmasından sorumludur.

A.4.2.9. Çalışanlar ve dış tarafların kullanıcıları; iş akitleri, sözleşmeleri veya anlaşmaları sona erdiğinde, ellerinde olan tüm kurumsal varlıkları iade etmekle mükelleftir.

A.4.3. Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi

A.4.3.1. Kurum bilgi varlıkları, içerdikleri verilerin hassasiyeti, kurum için taşıdıkları önem ve yasal zorunluluklar dikkate alınarak uygun bir şekilde sınıflandırılır/gizlilik derecesi verilir.

A.4.3.2. 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;

A.4.3.2.1. 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**",

A.4.3.2.2. 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**",

A.4.3.2.3. 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**",

A.4.3.2.4. 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.

A.4.3.2.5. 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.

A.4.3.2.6. 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.

A.4.3.2.7. Yukarıda sıralanan gizlilik derecelerinden hiçbirisi ile sınıflandırılmayan ve özel bir koruma gerektirmeyen evrak ve dokümanlar, "**tasnif dışı**" olarak kabul edilir.

A.4.3.2.8. 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.

A.4.3.2.9. 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.

A.4.3.2.10. 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.

A.4.3.2.11. Resmi yazı şeklinde olmayan ancak içerdikleri bilgilerin hassasiyeti açısından sınıflandırılmaya ihtiyaç duyulan diğer bilgi varlıklarının sınıflandırılması için de yukarıda belirtilen gizlilik dereceleri kullanılır. Bu varlıkların korunması ve erişim haklarının düzenlenmesi için alınacak tedbirler, yapılacak olan risk analiz neticesine göre belirlenir ve bu Kılavuzun A.1.3.2.1 (Kuruma Özgü BGYS Politikasının Hazırlanması) maddesinde belirtildiği şekilde kurumlar tarafından hazırlanacak Bilgi Güvenliği Politikaları Dokümanlarında ayrıntılı olarak açıklanır.

A.4.3.3. Gerek elektronik ortamda, gerekse basılı ortamda saklanan bilgilerin;

A.4.3.3.1. Bilgiye erişimin kayıt ve kontrol altına alınması,

A.4.3.3.2. İzinsiz kopyalamanın önlenmesi,

A.4.3.3.3. Elektronik veya basılı olarak depolama süresi ve koşullarının tanımlanması,

A.4.3.3.4. İletim hassasiyetinin belirlenmesi,

A.4.3.3.5. Gerektiğinde kanıt olarak kullanılmak üzere bütünlüğünün sağlanması,

A.4.3.3.6. İhtiyacın sonlanması durumunda imha edilmesi süreçlerinin tanımlanması için uygun şekil ve yöntemlerle etiketlenmesi gerekir.

A.4.3.3.7. Tasnif dışı bilgiler için etiketleme yapılmasına gerek yoktur.

A.4.3.4. Resmi yazı şeklinde olan belgelerin etiketlenmesi için yürürlükteki Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelikte belirtilen esaslar doğrultusunda hareket edilir.

A.4.3.5. Bu kapsamda;

A.4.3.5.1. Her sayfaya gizlilik dereceleri yazılır ve damgalanır.

A.4.3.5.2. Ekler de yazı ile aynı gizlilik derecesini taşır.

A.4.3.5.3. Gizlilik dereceli bütün yazılar, zaman zaman gizlilik derecelerinin yeniden değerlendirilmesi bakımından gözden geçirilir.

A.4.3.5.4. Gizlilik derecelerinin indirilip yükseltilmesi yazıyı yazan makamlarca yapıldığı gibi alan makamlarca da bu hususta teklif yapılabilir.

A.4.3.5.5. Gizlilik dereceli ve bilhassa kontrollü yazılarda kullanılan müsveddeler, karbon kâğıtları ve yanlış yazılar muhakkak imha edilir.

A.4.3.5.6. Gizlilik dereceli evrak, kâğıt sepetine bütün olarak atılmaz. Kâğıt kırpa makinaları kullanılmak suretiyle imha edilir.

A.4.3.5.7. Gizli ve özel gizlilik derecesini haiz evrak ve belgeler izinsiz olarak çoğaltılamaz.

A.4.3.5.8. 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.

A.4.3.6. 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.

A.4.3.7. Sağlık verilerinin korunmasına yönelik risk analizi yapılırken, kişisel verilerin hassasiyeti ve kanuna aykırı bir şekilde ifşası halinde uygulanacak ağır idari ve cezai yaptırımlar nedeniyle en üst düzeyde özen gösterilir.

A.4.4. Taşınabilir Ortam Yönetimi

A.4.4.1. 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.

A.4.4.2. Elektronik medya kullanımı ile ilgili olarak aşağıdaki hususlar göz önünde bulundurulur.

A.4.4.2.1. Kuruma ait veriler, kişilere ait medyalar üzerinde saklanamaz. Verilerin bir taşınabilir ortama aktarılması ihtiyacı kaçınılmaz ise bu maksatla kuruma ait medyalar kullanılır.

A.4.4.2.2. 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.

A.4.4.2.3. 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.

A.4.4.2.4. 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.

A.4.4.2.5. 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.

A.4.4.2.6. 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.

A.4.4.2.7. Gizlilik derecesi taşıyan kurumsal verilerin saklandığı medya ortamları, kişisel (şahsın kendisine ait) bilgisayarlarda kullanılamaz. Bu tip veriler kişisel bilgisayarlarda işlenemez.

A.4.4.2.8. Tüm ortamlar üretici talimatında belirtildiği şekilde toz, nem vb. çevresel şartlardan etkilenmeyecek şekilde güvenli bir ortamda saklanır.

A.4.4.3. 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.

A.4.4.4. 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.

A.4.4.5. Taşınabilir ortamların bir yerden başka yere taşınması esnasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı gerekli önlemler alınır. Bu çerçevede;

A.4.4.5.1. Güvenilir kargo/taşıma şirketleri ya da kuryeler kullanılır,

A.4.4.5.2. Yönetim tarafından yetkili kurye listeleri oluşturulur.

A.4.4.5.3. 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.

A.4.4.5.4. Ortamın içeriğini tanımlayan kayıtlar ile birlikte kaç kez transfer edildiği, transfer sorumluları ve alıcı tarafından alındığının kayıtları tutulur.

A.4.5. Ortamın Yok Edilmesi

A.4.5.1. 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.

A.4.5.2. 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.

A.4.5.3. Kaydı silinen bilgisayarların sabit diskleri, ilgili teknik birimlerden destek alınmak suretiyle sökülür.

A.4.5.4. 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:

A.4.5.4.1. **De-manyetize Etme**: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

Şekil 1 Degausser Cihazı

A.4.5.4.2. **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.

Şekil 2 Fiziksel Olarak Yok Etme

A.4.5.5. Merkez teşkilata bağlı birimlerce imhasına karar verilen sabit disklerin fiziksel imha işlemlerinin standartlara uygun şekilde yürütülmesi maksadıyla, SBSGM'de bulunan disk imha cihazı kullanılabilir. Disk imhası için imha edilecek disklere ait Kayıttan Düşme Teklif ve Onay Tutanağı (KLVZ-EK-03) ve Disk İmha Formunun (KLVZ-EK-04) resmi yazı ile SBSGM'ye gönderilmesi gerekir. Disk imha işlemleri, bizzat disklerin sahipleri veya taşınır mal sorumlularının nezaretinde yapılır.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.4.5.9. Yeniden kullanılması planlanan disklere, içlerinde yer alan bilgilerin yetkisiz kişilerin eline geçmesini engellemek maksadıyla ‘güvenli sil’ (üzerine yazma) işlemi yapılır.

A.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.

A.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.

A.4.5.12. Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

A.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,

A.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,

A.4.5.12.3. Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, hassas verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

A.5. RİSK YÖNETİMİ

A.5.1. Genel

A.5.1.1. Kurumun, stratejik hedeflerine ulaşmasını veya olağan faaliyetlerini gerçekleştirmesini belirsiz kılabilecek iç ve dış faktörler olabilir. Bu faktörlerin etkisine risk denir. Örneğin, kurumun veri koruma yükümlülüğü vardır. Veri korumadaki başarısını belirsiz kılacak faktörlerin etkisi risk olarak tanımlanır.

A.5.1.2. Kılavuzun bu bölümünde anlatılan risk değerlendirme yöntemi ISO/IEC 27005 ve TS ISO 31000 standartları referans alınarak hazırlanmış olup kurumsal bilgi varlıklarının güvenliğine ilişkin bilgi güvenliği risk yaklaşımını özetlemektedir. Anlatılan yöntem örnek niteliğinde olup idarenin kapsam ve hedeflerine bağlı olarak farklı risk yönetimi yaklaşımları da uygulanabilir.

A.5.1.3. Risk yönetimi bir tehdidin gerçekleşme olasılığı ile gerçekleşmesi halinde yol açacağı sonucun şiddetinin birlikte ele alınmasıdır.

A.5.1.4. Kurumların bilgi güvenliği alt komisyonlarınca, gerekiyorsa üst yönetim onayı da alınarak risk yönetimine ilişkin görev, yetki ve sorumlulukların tanımlanması, risklerin yönetimine ilişkin kuralların oluşturulması, görevlendirilen personel vasıtasıyla risklerin belirlenmesi ve analiz edilmesi gerekir.

A.5.1.5. Risk analizi, risklerin kapsamlı olarak anlaşılmasını sağlayan yöntemler ile risklerin belirlenmesini, risklerin oluşması halinde ortaya çıkabilecek zararın şiddetini ele alacak şekilde değerlendirilmesini ifade etmektedir.

A.5.1.6. Üst yönetim tarafından kurumun stratejik hedefleri, rapor verme süreçleri, bilgi güvenliği politikaları ve kurum kültürü bakış açısıyla sürdürülebilir ve yönetilebilir bir risk yönetimi yaklaşımı belirlenir ve risk yönetimi politikası oluşturulur. Risk çalışmasının kapsamı kurumun iş faaliyetleri ile sınırlıdır.

A.5.1.7. Belirlenen risk düzeylerine göre önlemler alınır ve iyileştirme çalışmaları yapılır. İhlal olaylarının incelenmesi, güncel tehditlerin takip edilmesi, zafiyet testleri ile zayıflık eşiklerinin ölçülmesi gibi yöntemlerle risk yönetiminin etkinliği sürekli izlenir ve iyileştirilir.

A.5.1.8. Risk analizlerinde bilhassa aşağıdaki hususlara yönelik riskler değerlendirilir:

A.5.1.8.1. Sistem, ağ ve kaynaklarına erişim kontrolünde güvenli kimlik doğrulama yöntemlerinin kullanılması,

A.5.1.8.2. Uygulama kullanıcısı, yönetici kullanıcı ve teknik kullanıcıların yetkilendirme ve erişim yöntemleri,

A.5.1.8.3. Kullanıcı ve sistem yöneticilerinin görev, sorumluluk ve yetkilerinin ayrılması,

A.5.1.8.4. Kullanılabilirlik, gizlilik ve bütünlük çerçevesinde varlıkların korunma dereceleri,

A.5.1.8.5. Sistem işletim süreçlerinde iz kayıtlarını tutma, izleme ve inkâr edememe gereksinimleri,

A.5.1.8.6. Veri sızıntısı algılama sistemleri veya kaydetme ve izleme gibi güvenlik kontrolleri,

A.5.1.8.7. Tedarik edilen hizmet ve ürünlerin de kurumsal güvenlik gereksinimlerine uyumu.

A.5.1.9. Risk yönetimi; riskin belirlenmesi, riskin analiz edilmesi ve kurumsal risk kıstaslarını sağlamak için risk iyileştirmesi yoluyla riskin değiştirilip değiştirilemeyeceğinin değerlendirilmesi aşamalarını içerir.

A.5.2. Sorumluluklar

A.5.2.1. Üst Yönetim, risk yönetimi politika ve prosedürlerinin oluşturulması, etkin şekilde uygulanması, sürekli geliştirilmesi ve risk yönetim planının gerçekleştirilmesini sağlamaktan sorumludur.

A.5.2.2. Bilgi Güvenliği Alt Komisyonu kurumsal risk çalışmasının etkin olarak yürütülmesinden ve üst yönetime raporlanmasından sorumludur.

A.5.2.3. Tüm kurum personeli icra etmekle sorumlu olduğu iş sürecine ilişkin bilgi varlıklarını bilgi güvenliği risklerine karşı korumakla, gerekli tedbirleri almakla ya da alınması için çalışma yapmakla sorumludur.

A.5.3. Risk Yönetimi

Risk yönetiminin aşamaları ve her bir aşamada yapılması gereken hususlar alt maddelerde açıklandığı şekildedir.

A.5.3.1. Varlıkların Tanımlanması

A.5.3.1.1. Bilgi güvenliği risk çalışmasına konu olan kapsam ve sınırlar içerisindeki tüm bilgi varlıklarının tanımlanması aşamasıdır.

A.5.3.1.2. BGYS bakış açısıyla varlıkların tanımlanması, Kılavuzun A.4 (Varlık Yönetimi) numaralı bölümünde ayrıntılı olarak açıklanmıştır.

A.5.3.1.3. Risk çalışmalarında, KLVZ-EK-05 Kurum Bilgi Varlıkları Envanter Çizelgesi ile kayıt altına alınan varlıklar esas alınır.

A.5.3.2. Varlıkların Değerinin Belirlenmesi

A.5.3.2.1. Varlığın kullanılmakta olduğu iş süreci, etkilediği süreçler, mali kıymeti gibi unsurlar dikkate alınarak varlık sahibi tarafından varlığa bir değer atanır. Varlık değerinin belirlenmesi risk yönetim sürecinin en önemli parçasıdır. Sonraki aşamalar bu aşama üzerine kurulur.

A.5.3.2.2. Üst Yönetim varlık değerinin belirlenmesi için etkin ve kolay kullanılabilecek bir yöntem belirler. Risk yönetimi yaklaşımında tek bir kural olmamakla birlikte kurumsal olarak farklı yöntemler kullanılabilir. En kabul görmüş yöntem, varlığın gizlilik, bütünlük ve erişilebilirlik değerlerinin en yüksek olanının alınmasıdır.

A.5.3.2.3. Varlık değeri olarak KLVZ-EK-06 Risk Hesaplama Faktörlerinde yer alan Varlık Değeri Tablosunda belirtilen ölçütler kullanılmak suretiyle bir değer atanır.

A.5.3.3. Tehdit ve Zafiyetlerin Gerçekleşme Olasılıklarının Belirlenmesi

A.5.3.3.1. Tehdit; bilgi, süreçler ve sistemlere zarar verme potansiyeline sahip her şeydir. Tehditler doğal veya insan kaynaklı, içeriden veya dışarıdan, kazara veya kasıtlı olabilir. Tehditler türlerine (yetkisiz eylemler, fiziksel hasar, teknik arıza vb.) ve kaynağına (doğal kaynaklı, insan kaynaklı vb.) göre tanımlanır.

A.5.3.3.2. Zafiyet, herhangi bir tehdidin, bilgi varlıklarının güvenliğini azaltmaya neden olabilecek zayıflıktır. Hizmet sürecinde kullanılan ağlar, bilişim temelli sistemler (kablosuz erişim cihazları, network ağ cihazları, sunucular, bilgisayarlar, yazıcılar vb.) ya da kurum personeli potansiyel olarak bir zafiyet yani açık oluşturabilir. Zafiyetler belirlenen tehditler ile ilişkilendirilir.

A.5.3.3.3. Tehditler, bu tehditlerin gerçekleşmesi durumunda etkilenecek varlıklar ve bu varlıklara ilişkin zafiyetler (zayıf noktalar) belirlenir ve riskin oluşmasına ilişkin bir olasılık değeri belirlenir. Olasılık değeri, bilgi güvenliği olayının gerçekleşme olasılığını ifade eder.

A.5.3.3.4. Bir tehdit birden fazla etkiye neden olabilir. Yani farklı bilgi güvenliği olaylarına neden olabilir. Bu nedenle her bir tehdit senaryosunun ve etkisinin olasılığını ayrı ayrı değerlendirmek ve risk analiz tablosuna ayrıca işlemek gerekir.

A.5.3.3.5. Tehdit ve zafiyetlerin gerçekleşme olasılığı için KLVZ-EK-06 Risk Hesaplama Faktörlerinde yer alan Riskin Gerçekleşme Olasılığı tablosunda belirtilen ölçütler kullanılmak suretiyle bir değer atanır.

A.5.3.4. İşe Etki Değerlerinin Belirlenmesi

A.5.3.4.1. Varlık sahibi tarafından; riskin gerçekleşmesi durumunda, varlığın kullanıldığı ve bağımlı olduğu iş süreçlerine yapacağı etkiler gizlilik, bütünlük ve erişilebilirlik açısından incelenir ve her birine ayrı bir puan verilir.

A.5.3.4.2. İşe etki değerinin belirlenmesinde gizlilik, bütünlük ve erişilebilirlik değerlerinin ortalamasının alınması ya da en yüksek değerin kullanılması gibi farklı yöntemler kullanılabilir.

A.5.3.4.3. İşe etki değeri olarak KLVZ-EK-06 Risk Hesaplama Faktörlerinde yer alan Gizlilik Etki Değeri, Bütünlük Etki Değeri ve Erişilebilirlik Etki Değeri Tablolarında belirtilen ölçütler kullanılmak suretiyle bir değer atanır.

A.5.3.4.4. Risk puanı hesaplanırken gizlilik, bütünlük ve erişilebilirlik için belirlenen etki değerlerinden en yüksek değer dikkate alınır. (Örneğin seçilen bir varlık için gizlilik etki değeri 3, bütünlük etki değeri 4, erişilebilirlik etki değeri 5 olarak belirlenmişse, işe etki değeri 5 olarak alınır)

A.5.3.5. Risk Puanı Hesaplama

A.5.3.5.1. Risk değerlendirme ve işleme için risk seviyesinin hesaplanması gerekir.

A.5.3.5.2. Risk puanı hesaplamak için birçok yöntem kullanılabilir. Örnek bir risk değeri hesaplama yöntemi aşağıdaki gibidir:

Risk Değeri = Varlık Mutlak Değeri (Varlık Değeri X İşe Etki Değeri) X Olasılık Değeri

A.5.3.6. Risk Önceliklendirme

A.5.3.6.1. Risk puanının hesaplanmasından sonraki adım, riskleri değerlendirmek ve tehdit seviyelerine göre önceliklendirmektir.

A.5.3.6.2. Risklerin değerlendirilmesi ve önceliklendirilmesi için KLVZ-EK-06 Risk Hesaplama Faktörlerinde yer alan Risk Değeri Tablosu kullanılır.

A.5.3.6.3. Risklerin anlamlandırılması ve önceliklendirilmesi aşağıdaki tabloya göre yapılır.

Risk Değeri	Risk Önceliği
1-25	Düşük
26-50	Orta
51-75	Yüksek
76-100	Çok Yüksek

A.5.3.7. Risk Kararı

A.5.3.7.1. Risk değerlendirme kararı; tanımlanmış iç ve dış paydaşların beklentileri, kurumun bilgi güvenliği hedefleri vb. unsurlar dikkate alınarak Üst Yönetim tarafından verilir. Örneğin: Bir riskin değerlendirilmesine ilişkin verilecek kararda, ilgili varlık ya da varlık grubunun desteklediği iş sürecinin ya da faaliyetinin önemi veya sözleşme, yasal ve düzenleyici gereklilikler üzerindeki rolü göz önüne alınmalıdır.

A.5.3.7.2. "Kabul edilebilir" risk seviyesi, yasal yükümlülüklere ve kurumsal politikalara uygun, kurumsal itibar zedelenmesi veya hizmeti yerine getirmeye engel olabilecek herhangi bir durum oluşturmayacak risk seviyesini ifade eder.

A.5.3.7.3. Kabul edilebilir risk seviyesi idarenin risk toleransına bağlıdır ve üst yönetim tarafından karar verilmesi gereken bir husustur. Genel olarak 25 puana kadar olan düşük seviyeli riskler kabul edilebilir risk olarak kabul edilir.

A.5.3.7.4. Risk puanının hesaplanması sonucunda elde edilen risk seviyesine, maliyet ve riskin ortadan kaldırılmasından beklenen faydaya göre risk ile ilgili karar alınır. Risk kararı seçenekleri şu şekildedir:

A.5.3.7.4.1. Risk Kabul: Risk puanı düşük seviyede ve risk puanının düşürülmesi için ek önlem alınmasına gerek yok ise veya alınacak ek önlemlerin maliyeti riskin gerçekleşmesi durumunda vereceği zarardan yüksek ise risk kabul kararı alınabilir.

A.5.3.7.4.2. Risk Azaltma: Risk puanını düşürmeye yönelik olasılık ya da etki değerini düşürecek önlemler alınmasıdır. Riski azaltma kararı alırken zaman, finans, operasyon kabiliyeti, değişikliği uygulayabilme gibi kısıtları göz önüne almak gerekir. Risk azaltma kararında yapılacak eylemler, planlanan tarih ve sorumlular açıkça belirtilmelidir.

A.5.3.7.4.3. Risk Transfer: Riski azaltmak için yapılacak eylemler bu işi daha profesyonel şekilde yönetebilecek bir dış paydaşa sözleşme ile transfer edilebilir. Riski transfer etmek, riskin gerçekleşmesi durumunda oluşacak etkiden doğacak tüm zararı transfer etmek anlamına gelmediği için transfer edilen risk sürekli izlenmeli ve kontroller denetlenmelidir.

A.5.3.7.4.4. Riskten Kaçınma: Riski azaltma için alınacak önlemler finans veya operasyon gibi kısıtlar nedeni ile uygulanabilir değil ise bu riski doğuran faaliyet veya durumdan kaçınılmalıdır. Riski doğuran faaliyetin durdurulması ya da ürünün kullanılmasından vazgeçilmesi riskten kaçınma kararıdır.

A.5.3.8. Risk İşleme

A.5.3.8.1. Risk İyileştirme Planlarının Hazırlanması

A.5.3.8.1.1. Risk iyileştirme planları; kurumsal risk haritasının çıkarılması, seçilen iyileştirme seçeneklerinin nasıl gerçekleşeceğinin planlanması ve yapılan çalışmaların kayıt altına alınması amacıyla hazırlanır.

A.5.3.8.1.2. Bu bölümde belirtilen risk işleme metodolojisi uyarınca hazırlanmış örnek bir Risk İyileştirme Planı KLVZ-EK-07'dedir.

A.5.3.8.2. Risk Analizi İletişimi ve İstişaresi

A.5.3.8.2.1. Bilgi güvenliği alt komisyonu, üst yönetim ve varlık sahipleri kurum tarafından önceden belirlenmiş zaman aralıkları ile bir araya gelerek risklerin varlığı, şiddeti, tedavisi ve kabul edilebilirliği üzerinde çalışma gerçekleştirir.

A.5.3.8.3. Bilgi Güvenliği Risklerinin İzlenmesi ve Gözden Geçirilmesi

A.5.3.8.3.1. Riskler statik değildir. Tehditler, zayıf noktalar, olasılıklar veya sonuçlar varlık yaşam döngüsü boyunca değişiklik gösterir. Riskler ve faktörlerini (varlıkların değeri, etkileri, tehditleri, zayıflıkları, risklerin ortaya çıkma ihtimalleri), iç ve dış bağlam değişikliklerini izlemek, olası değişiklikleri erken belirlemek için riskler sürekli izlenmeli ve gözden geçirilmelidir.

A.5.3.9. Raporlama ve Kayıtlar

A.5.3.9.1. Risk yönetimi boyunca riskler ile ilgili mutabakata varılan kontrol önlemlerinin ne aşamada olduğu, risk planlarının iyileştirilmesi için gerekli olan kaynaklar ve eylemler, hiçbir risk veya risk unsurunun gözden kaçırılmadığından ve gerekli önlemlerin alındığından emin olunması için risk planlarının özetleri rapor olarak üst yönetime sunulmalı ve muhafaza edilmelidir.

A.5.3.9.2. Üst Yönetim tarafından risk değerlendirme ölçütleri, etki şiddetlerini kabul etmek seviyeleri gibi temel yaklaşımları ele alan uygun bir risk yönetimi bakış açısı geliştirilir ve risk yönetim prosedüründe yazılı olarak belirtilir.

A.5.3.9.3. Hangi risk yönetim metodu kullanıldığına bakılmaksızın risk tanımlama formu ve risk analiz tablosu kayıtlarının oluşturulması, muhafazası ve güncellenmesi gerekir.

A.6. ERİŞİM KONTROLÜ

A.6.1. Erişim Kontrol Politikası

A.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.

A.6.1.2. Erişim kontrolü ile ilgili hususları açıklamak üzere, kurumun BGYS politikası ile uyumlu olacak şekilde "Erişim Kontrol Politikası" dokümanı hazırlanır. 6698 sayılı kanun kapsamında çıkarılan ikincil mevzuat uyarınca, kişisel verilere erişim için yapılan düzenlemeler söz konusu doküman içinde ayrı bir başlık/bölüm olarak ayrıntılı bir şekilde açıklanır.

A.6.1.3. Erişim kontrol politikası, kurumun bilgi güvenliği yetkilisi tarafından hazırlanır ve bilgi güvenliği alt komisyonu tarafından onaylanarak yayımlanır.

A.6.1.4. Erişim kontrol politikasının ayrılmaz bir parçası olarak "erişim yetki ve kontrol matrisi" oluşturulur. Erişim yetki ve kontrol matrisinde kimin, hangi bilgiye, hangi yetkilerle erişeceği ve erişimin kontrolü için kullanılacak yöntemler yer alır.

A.6.1.5. Erişim yetki ve kontrol matrisi gerekiyorsa "daha genel hususlardan daha özele olacak şekilde" birden fazla kademe şeklinde de hazırlanabilir.

A.6.1.6. Erişim kontrol politikası/erişim yetki ve kontrol matrisleri hazırlanırken aşağıda sıralanan prensipler dikkate alınır:

A.6.1.6.1. Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı gizlilik dereceli) bilgiler için özel bir erişim kontrol tedbiri alınmasına gerek yoktur. Bu tür bilgiler, kurumların İnternet sitelerinin vatandaşlara açık bölümlerine konulabilir. Bina ve tesislerde duyuru panosu vb. ortamlarda yayımlanabilir.

A.6.1.6.2. Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan erişim kontrol politikalarının sıkılaştırılması (zorlaştırılması) gerekir.

A.6.1.6.3. Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.

A.6.1.6.4. Bilgiye erişim talepleri ve ilgili makamlarca bu taleplere yapılan işlemlerin takip edilebilirliğini sağlamak üzere yazılı kurallar oluşturulur.

A.6.1.6.5. Erişim izinleri ile ilgili kayıtlar, varsa ilgili mevzuatta belirtilen sürelerce, yoksa varlığın sahibi tarafından belirlenecek süre boyunca saklanır.

A.6.1.6.6. Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.

A.6.1.6.7. "Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak bir kişinin kendi başına tüm bilgi varlıklarına erişimi engellenir. Teknik nedenlerle görev ayrımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır. Gerekiyorsa idari kontrol mekanizmaları oluşturulur.

A.6.1.6.8. "Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.

A.6.1.6.9. Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik sistemler için farklı kimlik doğrulama yöntemleri (token, akıllı kart, tek kullanımlık parola, parmak izi/retina/avuç içi tarama vb.) kullanılabilir.

A.6.1.6.10. Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur. Erişim ile ilgili hangi kullanıcı hareketlerinin izleneceği hususu varlık sahipleri tarafından belirlenir.

A.6.1.6.11. Sağlık Bilişim Ağı (SBA) dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.

A.6.1.6.12. Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. VTYS sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.

A.6.1.6.13. Bilgi varlıklarına fiziksel olarak yapılacak erişimler için bu yönergenin A.8 maddesinde belirtilen önlemler alınır.

A.6.1.6.14. Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için KVKK'nın 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.

A.6.2. Kullanıcı Erişimlerinin Yönetimi

A.6.2.1. Kullanıcı erişimlerinin yönetimi, sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek ve sadece yetkili kullanıcıların erişimlerini temin etmek için yapılır.

A.6.2.2. Başta kişisel sağlık verilerinin işlendiği bilgi sistemleri olmak üzere erişim kontrolüne tabi tutulacak tüm sistem ve hizmetler için "kullanıcı erişim yönetimi esasları" belirlenir. Belirlenen esaslar, ilgili tüm taraflara (muhtemel kullanıcılara) resmen duyurulur. Kullanıcı erişimi ile ilgili hususlar Kurumun "Erişim Kontrol Politikası" ve/veya her bir sistem/hizmet için ayrı ayrı hazırlanacak "kullanıcı/işletim el kitapları/kılavuzları" içinde yer alır.

A.6.2.3. Kullanıcı erişimleri ile ilgili yönetim esasları belirlenirken aşağıdaki hususlar dikkate alınır:

A.6.2.3.1. Hizmet veya sisteme erişim için nasıl müracaat edileceği,

A.6.2.3.2. Müracaat esnasında hangi bilgilerin isteneceği,

A.6.2.3.3. Kullanıcıların yetkilendirilmesinde kullanılan roller ve haklarının neler olduğu,

A.6.2.3.4. Yetki değişiklik taleplerinin hangi koşullarda ve nasıl yapılacağı,

A.6.2.3.5. Ayrıcalıklı erişim taleplerinin nasıl değerlendirileceği,

A.6.2.3.6. Kullanıcı erişimlerinin izlenmesi için alınmış olan tedbirler,

A.6.2.3.7. Kullanıcı hesaplarının kapatılması/silinmesi için yapılacak işlemler.

A.6.2.4. Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir. Bilmesi gereken prensibi uyarınca gereksiz olarak verilmiş yetkilerin kaldırılması sağlanır.

A.6.2.5. İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en az 6 (altı) aylık aralıklarla yapılır.

A.6.2.6. Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilir.

A.6.2.7. Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili incelemeler, 3 (üç) ayı aşmayacak şekilde daha sık yapılır.

A.6.2.8. 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır. Bu süre kurumların bilgi güvenliği alt komisyonları tarafından değiştirilebilir. Her bir sistem için belirlenecek süreler, kurumların erişim kontrol politikası içinde yazılı olarak kayıt altına alınır.

A.6.2.9. Ayrıcalıklı erişim hakkı verilen kullanıcı sayısı (etki alanı yöneticisi, veri tabanı yöneticisi vb.) asgari düzeyde tutulur. Mümkün olduğu yerlerde, rutin ve düzenli sistem yönetim işlevlerinin otomatik araçlarla (batch/otomatik kod yazılması, sistem yeteneklerinin kullanılması vb.) yapılması sağlanır.

A.6.2.10. Ayrıcalıklı erişim hakları, düzenli iş faaliyetleri için kullanılan kullanıcı kimliğinden farklı bir kullanıcı kimliğine tahsis edilir. Düzenli iş faaliyetleri, ayrıcalıklı kullanıcı kimliği ile yapılmaz.

A.6.2.11. Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanır ve sıkı bir şekilde kontrol edilir.

A.6.2.12. Programların kaynak kodları ve ilgili öğelere (tasarımlar, özellikler, doğrulama planları ve geçerleme planları gibi) erişim (yetkisiz işlevsellik girişini ve istenmeyen değişiklikleri önlemenin yanı sıra değerli fikri mülkiyet haklarının gizliliğini sağlamak için) sıkı bir şekilde kontrol edilir.

A.6.3. Parola Güvenliği

A.6.3.1. Kurumların Bilgi Güvenliği Yetkililerince kendi kurumlarına özgü "Parola Politikası" oluşturulur ve yazılı hale getirilir. Hazırlanan "Parola Politikası" kurumun Bilgi Güvenliği Alt Komisyonu tarafından onaylanır ve tüm çalışanlara duyurulur.

A.6.3.2. Parola politikaları belirlenirken, sistem ve uygulamaların, kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmaya zorlamaları sağlanır.

A.6.3.2.1. Parolalar en az 8 (sekiz) karakterden oluşur. Sistem yönetim işlemlerinde kullanılan parolaların (root, administrator, sysadmin vb.) en az 12 karakterden oluşması tavsiye edilir.

A.6.3.2.2. İçerisinde en az 1 (bir) tane büyük ve en az 1(bir) tane küçük harf bulunur.

A.6.3.2.3. İçerisinde en az 1 (bir) tane rakam bulunur.

A.6.3.2.4. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !,?,A,+,$,#,&,/,{,*,-,],=,...)

A.6.3.2.5. Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, abababab...)

A.6.3.2.6. Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf,1234,zxcvb...)

A.6.3.2.7. Kişisel bilgiler veya klavye kombinasyonları ile basitçe üretilebilecek karakter dizilerinin kullanılması engellenir. (Örneğin 12345678, qwerty, doğum tarihi, çocuğun adı, soyadı gibi)

A.6.3.2.8. Sözlükte bulunabilen kelimelerin kullanılması engellenir.

A.6.3.2.9. Kullanıcının son 3 (üç) parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir.

A.6.3.2.10. Sistem ve uygulamalarda oturum kontrolü yapılarak bir kullanıcı adı ve parolasının aynı anda birden çok bilgisayarda kullanılması engellenir.

A.6.3.3. VTYS, aktif dizin sunucusu, uygulama sunucusu, ağ cihazları gibi sistem hesaplarına ait parolalar (root, administrator, sysadmin vb.) en geç 3 (üç) ayda bir değiştirilir.

A.6.3.4. Kullanıcı hesaplarına ait parolalar (örnek: HBYS, e-Posta, web, masaüstü bilgisayar vb.) en geç 6 (altı) ayda bir değiştirilmesi sağlanır.

A.6.3.5. Sistem yöneticileri ayrıcalıklı işlemleri normal kullanıcı adı ve parola ile yapmaz. Bu maksatla farklı kullanıcı adı ve parola kullanılır.

A.6.3.6. Parolalar, e-Posta iletilerine veya herhangi bir elektronik forma eklenmez.

A.6.3.7. Parolalar gizli bilgi olarak muhafaza edilir. Kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.

A.6.3.8. Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu bölümde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.

A.6.3.9. İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.

A.6.3.10. Yazılım uygulamalarında erişim yetkisi tanımlanan kullanıcılara, gönderilen parola sıfırlama linkinin, aktivasyon işlemi başlatıldıktan (linke tıklandıktan) sonra en geç 15 dk. içerisinde tamamlanacak şekilde ayarlanması gerekir.

A.6.4. Sağlık Bakanlığı Uygulamalarına OGN

A.6.4.1. Ortak Giriş Noktası (OGN), Sağlık Bakanlığı tarafından geliştirilen uygulamalara tek bir noktadan erişim imkânı sunan bir web sitesidir. OGN'ye https://giris.saglik.gov.tr/ adresinden erişim sağlanır.

A.6.4.2. Kullanıcılar OGN'ye aşağıda belirtilen beş farklı yöntemden herhangi biri ile kimliğini doğrulattığında, OGN ile bütünleşmesi tamamlanmış tüm Bakanlık uygulamalarını görür. Buradan istenilen uygulamaya, ayrıca bir kimlik doğrulama yapılmaksızın erişim sağlanır.

A.6.4.3. OGN ile kullanıcılara Aktif Dizin, T.C. Kimlik Kartı, e-Devlet Kapısı, Elektronik İmza (e-İmza) ve Mobil İmza olarak beş farklı kimlik doğrulama yöntemi sunulur.

A.6.4.3.1. Aktif Dizin ile kimlik doğrulama yöntemi kullanılarak giriş işleminin yapılabilmesi için kullanıcıların *@saglik.gov.tr uzantılı e-Posta adresine sahip olmaları gereklidir. Bakanlığımız e-Posta Biriminden temin edilecek kurumsal e-Posta ve şifreleri ile giriş yapılır.

A.6.4.3.2. E-imza ile giriş işlemi için nitelikli elektronik sertifikası (NES) olan (e-İmza işlemi yapma imkânına sahip) kullanıcıların, öncelikle kullandıkları işletim sistemi ile uyumlu "e-İmza" uygulamasını bilgisayarlarına yüklemeleri gerekmektedir. e-İmza uygulaması yüklendikten sonra e-İmza ile giriş seçeneği seçildiğinde, ekranda bilgisayara takılı kartlar listelenir. Seçilen kart ile sisteme giriş yapılır.

A.6.4.3.3. Mobil İmza ile giriş işlemi için GSM işletmecileri tarafından sunulan mobil imzaya sahip kullanıcılar, cep telefonlarına ve hatlarına tanımlı mobil imzaları ile sisteme giriş yapabilir.

A.6.4.3.4. T.C. Kimlik Kartı ile giriş işlemi için kimlik kartlarına e-İmza tanımlı kullanıcıların öncelikle kullandıkları işletim sistemi ile uyumlu "e-İmza" uygulamasını indirip bilgisayarlarına yüklemeleri gerekmektedir. e-İmza uygulaması yüklendikten sonra T.C. Kimlik Kartı ile giriş seçeneği seçildiğinde, ekranda bilgisayara takılı kartlar listelenir. Seçilen kart ile sisteme giriş yapılır.

A.6.4.3.5. e-Devlet ile giriş işlemi için; e-Devlet giriş seçeneği seçilerek gelen ekrandan "e-Devlet Girişi için Tıklayınız" butonuna tıklanarak kullanıcı e-Devlet giriş ekranına yönlendirilir. e-Devlet üzerinden başarılı giriş yapıldığı taktirde sistem kullanıcıya OGN'de tanımlı Bakanlık uygulamalarını listeler. Kullanıcı tercih ettiği uygulamayı seçerek işlemlerine devam eder.

A.6.4.4. Bakanlık merkez teşkilatı ve bağlı kuruluşlar tarafından sunulan tüm web tabanlı uygulamaların OGN ile entegre edilmesi zorunludur.

A.6.5. Merkezi Aktif Dizin ve E-Posta Sistemine Erişim

A.6.5.1. SBSGM tarafından Bakanlık merkez teşkilatı birimlerinin etki alanı hizmetlerinin gerçekleştirilmesi, tüm Bakanlık kullanıcılarına *@saglik.gov.tr uzantılı e-Posta hesaplarının açılması maksadıyla "Merkezi Aktif Dizin ve e-Posta sistemi" kurulur ve işletilir.

A.6.5.2. Aktif dizinde kurumsal birim (Organizational Unit: OU) yaratma, silme, değiştirme; OU'lar altında yeni kullanıcı tanımlama, kullanıcı hesabını askıya alma (disable), silme, kullanıcı özelliklerini değiştirme, kullanıcıyı teşkilat ağacında bir noktadan diğer noktaya taşıma; kullanıcı için e-Posta hesabı açma, e-Posta hesabını askıya alma, e-Posta hesabını silme gibi işlemler SBSGM tarafından (Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı) yapılır.

A.6.5.3. Merkezi aktif dizin hizmetinin e-Posta işlemleri dışında başka maksatlarla kullanılması gerektiğinde (örneğin geliştirilen bir uygulama için kullanıcı erişim yetkilendirmesi) yazılı talepte bulunulur. Bu tür erişim taleplerinde prensip olarak sadece "okuma yetkisi" ile erişim izni verilir. Farklı yetkiler ile aktif dizin erişim taleplerine, SBSGM BGYS politikaları kapsamında yapılacak risk değerlendirmesinde alınacak karara istinaden işlem yapılır.

A.6.5.4. Gerçek kişiler için kurumsal e-Posta hesap işlemleri:

A.6.5.4.1. Bakanlık merkez ve taşra teşkilatı ve bağlı kurumlarda görev yapan gerçek kişiler, ÇKYS/İKYS sisteminde kayıtlı iseler, kişisel olarak https://eposta.saglik.gov.tr/ adresindeki "Kayıt Ol" menüsündeki adımları takip etmek suretiyle "*@saglik.gov.tr uzantılı" "kurumsal e-Posta hesabı" açarlar.

A.6.5.4.2. ÇKYS/İKYS sisteminde kayıtlı olmayan personel için "KLVZ-EK-08 e-Posta Talep Formu / Gerçek Kişiler" ilgili birimler tarafından doldurularak üst yazı ile SBSGM'ye gönderilir.

A.6.5.4.3. SBSGM tarafından formda isimleri yazan personelin ÇKYS/İKYS kayıtlarında olup olmadığı ve hâlihazırda anılan kişi adına açılmış bir e-Posta hesabı bulunup bulunmadığı kontrol edilir.

A.6.5.4.4. Talep edilen "kurumsal e-Posta hesapları" açılır. Hesaplara ait tek kullanımlık erişim şifreleri kapalı zarf içinde resmi yazı ile talep yapılan birimlere iletilir.

A.6.5.4.5. Tek kullanımlık şifrelerin, gizliliği bozulmadan hesap açılan gerçek kişilere ulaştırılması, resmi yazıya işlem yapan birimin sorumluluğundadır.

A.6.5.5. Ortak kullanım için tüzel e-Posta hesap işlemleri:

A.6.5.5.1. Tüzel e-Posta hesapları birden fazla gerçek kişi tarafından erişilebilen ve belli bir görevin icrası veya bir birim adına yürütülen faaliyetlerin gerçekleştirilmesi (satınalma@saglik.gov.tr, ik@saglik.gov.tr, bilgiguvenligi@saglik.gov.tr gibi) için açılır.

A.6.5.5.2. Tüzel e-Posta hesaplarına kimin hangi yetki ile erişeceği "KLVZ-EK-09 E-Posta Talep Formu/Tüzel Kişiler" doldurulmak suretiyle, üst yazı ile SBSGM'ye gönderilir.

A.6.5.5.3. Tüzel e-Posta hesabının açılmasını müteakip yetki verilen kişiler, ortak posta kutusunu, kişisel olarak kullandıkları kurumsal e-Posta kutuları altında ikinci bir posta kutusu olarak görmeye ve kullanmaya başlarlar.

A.6.5.5.4. Ortak posta kutusuna erişecek kişiler ve erişim yetkisi değişiklik talepleri, ortak posta kutusundan epostayonetim@saglik.gov.tr adresine bildirilmesi suretiyle yapılır.

A.6.5.6. Kullanıcı hesaplarının ve posta kutularının yönetimi

A.6.5.6.1. Sistem yönetim araçları ile aktif dizin kullanıcı hesapları taranarak bir yıldan daha uzun süredir kullanılmayan kullanıcı hesapları pasife alınarak kullanıma kapatılır.

A.6.5.6.2. Kurumdan ayrılan, emekli olan, ilişiği kesilen personelin kullanıcı hesapları pasife alınarak kullanıma kapatılır.

A.6.6. Veri Merkezi ve Sunucu Barındırma Hizmetlerine Erişim

A.6.6.1. SBSGM tarafından, Bakanlık merkez teşkilatı birimleri ve bağlı kuruluşlar tarafından geliştirilen/tedarik edilen uygulamaların sunucu ve depolama ihtiyaçlarını karşılamak üzere veri merkezi ve sunucu barındırma hizmeti verilir.

A.6.6.2. Bakanlık ve bağlı kuruluşlarının merkez birimlerinden uygulama sunucusu talepleri EBYS üzerinden alınır. Sunucu hizmeti talepleri için KLVZ-EK-10 Sunucu Talep Formu kullanılır. Form doldurularak resmi yazı ile SBSGM'ye gönderilir.

A.6.6.3. Gelen talepler Sistem Yönetimi Birimi tarafından incelenir, gerekiyorsa başvuru yapan birim ile irtibata geçilerek ilave bilgiler istenir. Mevcut kaynaklar yapılan talebi karşılayamayacak durumda ise sonucu resmi yazı ile ilgili makama bildirilir.

A.6.6.4. Talebin karşılanabileceğine karar verilmesi durumunda sunucu kurulumu yapılarak ilgilisine tahsis edilir. Aksi takdirde, neden sunucu tahsis edilemeyeceği ile ilgili gerekçeler, resmi yazı ile talep yapan uygulama sahibine bildirilir.

A.6.6.5. Sunucuya erişim sağlayacak kullanıcının etki alanı hesabı var ise yetkilendirme yapılır. Eğer sunucuda yerel/tekil kullanıcı tanımlanmışsa parola bilgisi SMS ile gönderilir.

A.6.6.6. Sunucuda yetkilendirilmiş kullanıcının görev yerinin değiştiği veya görevden ayrıldığı bilgisinin herhangi bir şekilde SBSGM'ye ulaşması durumunda, ayrıca bir bildirim beklenmeksizin ilgili kişinin erişim hakları derhal iptal edilir.

A.6.7. Merkezi Veri Tabanı Yönetim Sistemine Erişim

A.6.7.1. SBSGM tarafından, Bakanlık merkez teşkilatı birimleri ve bağlı kuruluşlar tarafından geliştirilen/tedarik edilen uygulamaların veri tabanı ihtiyaçlarını karşılamak üzere merkezi veri tabanı yönetim sistemi (VTYS) işletilir.

A.6.7.2. Taşra teşkilat birimleri tarafından kullanılan uygulamaların veri tabanı ihtiyaçları, uygulama/sistemin sahipleri tarafından karşılanır. Bu ihtiyaçlar için merkezi VTYS kullanılmaz.

A.6.7.3. Yeni geliştirilen ilk defa hizmete verilecek bir uygulama/sistem için merkezi VTYS'den yararlanmak maksadıyla yapılması gereken işlemler şu şekildedir:

A.6.7.3.1. Merkezi VTYS'den yararlanmak için "KLVZ-EK-11 Veri Tabanı/Kullanıcı Oluşturma Talep Formu" doldurulur ve resmi yazı ile SBSGM'ye gönderilir. KLVZ-EK-11'in doldurulması ile ilgili açıklamalar, formun son kısmında ayrıntılı olarak yer almaktadır.

A.6.7.3.2. SBSGM Veri Tabanları ve Orta Katman Yönetimi Birimi tarafından yapılan talep incelenir, gerekiyorsa başvuru yapan birim ile irtibat kurularak ilave bilgiler alınır. Elde mevcut yazılım ve donanım kaynaklarının talebi karşılama kabiliyeti değerlendirilir. Talebin karşılanabileceğine karar verilmesi durumunda aşağıdaki şekilde işlemlere devam edilir. Aksi takdirde, neden veri tabanı oluşturulamayacağı ile ilgili gerekçeler resmi yazı ile talep yapan makama bildirilir.

A.6.7.3.3. Merkezi VTYS'de veri tabanı oluşturulabilmesi için KLVZ-EK-11 ile veri tabanına erişim yetkisi verilen kişilerin KLVZ-EK-12 Personel Gizlilik Sözleşmesi ve erişim yapacak kişiler firma personeli ise ilgili sözleşmeye ait KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesinin resmi evrak ile SBSGM'ye gönderilmiş ve Genel Müdürlük tarafından işletilen Sözleşme Takip Uygulamasına girilmiş olması gerekir.

A.6.7.3.4. Sözleşme takip uygulamasında yapılan kontrollerin neticesinin olumlu olması halinde merkezi VTYS üzerinde talep edilen veri tabanı ve kullanıcılar oluşturulur, gerekli yetkilendirmeler yapılır. Olumsuz olması durumunda, talep yapan birim ile iletişim kurularak gizlilik sözleşmeleri ile ilgili eksikliklerin tamamlanması istenir.

A.6.7.3.5. Yeni oluşturulan veri tabanına ait bilgiler (sunucu adı, IP adresi, port numarası, kullanıcı adı, kullanıcı erişim bilgileri, standart yedekleme planı, yedekleme ve yedekten geri dönüş testlerinin ilgili kullanıcılara bildirim yöntemi vb.) resmi yazı ile talep yapan birime bildirilir.

A.6.7.3.6. Veri tabanına erişim için tanımlanan kullanıcı adı ve parola bilgileri, SMS ile ilgili kişilere iletilir.

A.6.7.3.7. VTYS'de saklanan veriler, SBSGM yedekleme politikaları uyarınca son 15 (on beş) gün içerisinde herhangi bir güne dönülebilecek şekilde yedeklenir. Uygulama sahiplerinin yedekleme ve yedekten geri dönüş ile ilgili konuları, ilgili birim ile birebir koordine etmeleri ve varsa özel ihtiyaçlarını SBSGM'ye belirtmeleri gerekir.

A.6.7.4. Mevcut bir veri tabanına erişen kullanıcıların yetkilerinin değiştirilmesi, yeni kullanıcı eklenmesi veya mevcut bir kullanıcının silinmesi için yapılması gereken işlemler şu şekildedir:

A.6.7.4.1. Veri tabanında kullanıcı ve yetki işlemleri için KLVZ-EK-14 Veri Tabanı Kullanıcı İşlemleri ve Yetkilendirme Talep Formu doldurulur ve resmi yazı ile SBSGM'ye gönderilir. E-posta ile yapılan taleplere işlem yapılmaz.

A.6.7.4.2. Kişilere yetki verilebilmesi için KLVZ-EK-12 Personel Gizlilik Sözleşmesinin SBSGM'ye gönderilmiş ve Genel Müdürlük tarafından işletilen Sözleşme Takip Uygulamasına girilmiş olması gerekir.

A.6.7.4.3. Yeni açılan kullanıcıların kullanıcı ismi ve parolaları SMS ile talepte bulunan kişilere iletilir. Yapılan tüm işlemlerin sonuçları resmi yazı ile talepte bulunan makama iletilir.

A.6.7.5. Kişinin görev yerinin değiştiği veya görevden ayrıldığı bilgisinin herhangi bir şekilde SBSGM'ye ulaşması durumunda (e-Posta bildirimi, KLVZ-EK-02 İşten Ayrılma Formu, sözleşme takip uygulamasından alınan uyarı vb.) ayrıca bir bildirim beklenmeksizin ilgili kişinin erişim hakları derhal iptal edilir.

A.6.8. Elektronik Belge Yönetim Sistemine Erişim

A.6.8.1. Elektronik Belge Yönetim Sistemi (EBYS), Sağlık Bakanlığı merkez teşkilatı ve bağlı kuruluşları ile taşra teşkilatı tarafından yürütülen faaliyetler esnasında her türlü dokümanın kayıt altına alınarak bu bilgilerin bilgisayar ortamda paylaşılmasına ve kullanıcısı olan tüm personelin her zaman ve her yerden bu bilgilere kolaylıkla ulaşabilmesine imkân veren bir sistemdir.

A.6.8.2. Evrakın EBYS üzerinden hazırlanması ve yayımlanması ile ilgili usul ve esaslar, EBYS Yönergesinde açıklanmıştır. Yönergeye SBSGM web sayfasında bulunan "Mevzuat" bağlantısından erişim sağlanmaktadır.

A.6.8.3. EBYS uygulamasında kullanıcılar rollerine göre üç kategoride yer alır:

A.6.8.3.1. **Sistem Yöneticisi:** EBYS ve e-İmza Biriminde görev yapan tüm personel, sistem yöneticisi olarak tanımlanmıştır. Sistem yöneticileri, tüm EBYS üzerinde yönetim hakkına sahiptir.

A.6.8.3.2. **İl EBYS Yetkilisi:** Taşra teşkilatındaki EBYS iş süreçlerini yönetebilmek için il sağlık müdürlükleri tarafından belirlenen kullanıcılardır. Bahse konu kullanıcıların tanımlanması işlemi resmi yazı ile yapılır.

A.6.8.3.3. **Standart Kullanıcı:** Sağlık Bakanlığı teşkilatı içerisinde kendi biriminde belge oluşturma yetkisine sahip olan tüm kullanıcılardır.

A.6.8.4. EBYS'de kullanıcı tanımlama işlemleri merkez teşkilatta EBYS sistem yöneticileri, taşra teşkilatında il EBYS yetkilileri tarafından yapılır.

A.6.8.5. İl EBYS yetkilileri, sorumlu olduğu il ile ilgili sistemsel tanımlamaları (birim listeleme, yeni birim oluşturma, birim güncelleme, kullanıcı birim yetkisi listeleme ve kullanıcı birim yetkisi güncelleme) ve kullanıcı işlemlerini (kullanıcı listeleme, yeni kullanıcı oluşturma, kullanıcı güncelleme ve vekâlet işlemleri) yapar.

A.6.8.6. Standart kullanıcı oluşturma talepleri https://yazilimdestek.saglik.gov.tr/ sistemi üzerinden yapılır. EBYS kullanılırken karşılaşılan hataların bildirilmesi, yeni geliştirme talepleri ve yardım masası hizmetleri için de aynı adres kullanılır.

A.6.8.7. Kullanıcı tanımlama işlemi için "kullanıcının kimlik numarası, adı ve soyadı, *@saglık.gov.tr uzantılı e-Posta adresi, birimi, unvanı" bilgilerinin bildirilmiş olması gerekir.

A.6.8.8. Kullanıcılar sisteme; masaüstü uygulaması olarak çalışan EBYS istemci yazılımı, https://ebys.saglik.gov.tr/ adresinde yer alan web tabanlı istemci yazılımı veya cep telefonları için geliştirilen (Android, IOS ve Windows tabanlı) EBYS mobil istemci yazılımı üzerinden erişebilir.

A.6.8.9. Kullanıcılar EBYS uygulamalarına merkezi etki alanında tanımlı kullanıcı adı/parolası, e-İmza işlemlerinde kullanılan NES veya mobil imza işleminde kullanılan NES ile giriş yaparlar.

A.6.8.10. e-İmza ve mobil imza işlemlerinde TÜBİTAK UEKAE tarafından işletilen Kamu Sertifikasyon Merkezi (KamuSM) tarafından üretilen NES'ler kullanılır.

A.6.8.11. NES talepleri, kurumların "E-İmza Kurum Yetkilisi" üzerinden KamuSM'ye yapılır. KamuSM'ye NES başvurusu yapılması ve NES kullanmak suretiyle e-İmza atılırken karşılaşılan sorunlar ile ilgili detaylı bilgiler adresinde, http://www.kamusm.gov.tr/, EBYS ile ilgili detaylı bilgiler http://www.ebysportal.saglik.gov.tr/ adresinde yer almaktadır.

A.6.9. Kimlik Paylaşım Sistemine Erişim

A.6.9.1. Sağlık Bakanlığı tarafından geliştirilen uygulamalarda, gerçek kişilere ait kimlik ve adres bilgileri, İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü MERNİS veri tabanı ile entegre bir şekilde çalışan Sağlık Bakanlığı Kimlik Paylaşım Sistemi (KPS) vasıtasıyla sağlanır.

A.6.9.2. KPS'nin kuruluş amacı, çalışma ve yetkilendirme esasları, gizlilik ve kullanıcı sorumlulukları "KPS Usul ve Esasları Hakkında Yönerge"de açıklanmıştır. Yönergeye http://www.sbsgm.saglik.gov.tr/TR,13124/yonergeler.html adresinden erişim sağlanabilmektedir.

A.6.9.3. KPS, kimlik doğrulamasına ihtiyaç duyan tüm kamu sağlık teşkilatları (il sağlık müdürlükleri, hastaneler, aile hekimlikleri vb.) tarafından kullanılır.

A.6.9.4. Üniversite hastaneleri ve özel hastaneler, kimlik doğrulama işlemleri için doğrudan İçişleri Bakanlığı tarafından sunulan servisleri kullanır. Bu kurumlarca, söz konusu servislere erişim için doğrudan İçişleri Bakanlığına müracaat edilir.

A.6.9.5. KPS mimarisi gereğince, her kuruma (il sağlık müdürlükleri, hastaneler, aile hekimlikleri vb.) bir kullanıcı tanımlanmakta ve kimlik doğrulamaya ihtiyaç duyan kişiler, kuruma tanımlanan kullanıcı üzerinden sorgulama yapmaktadır.

A.6.9.6. Kurumlara tanımlanan kullanıcının, belli bir IP adresi üzerinden sorgulama yapması gerekmektedir.

A.6.9.7. KPS'de web servis kullanıcısı oluşturma, yetkilendirme, silme gibi işlemler taşra teşkilatı için il sağlık müdürlüklerinde bulunan KPS il yöneticileri tarafından, Bakanlık merkez teşkilatı için KPS Birimi tarafından yapılmaktadır.

A.6.9.8. Kullanıcılar tarafından yapılan web servis sorgulamaları sistem tarafından kayıt altına alınmaktadır.

A.6.9.9. KPS kullanacak kurum veya kişilerin, yetki ve sorumlulukları şu şekildedir:

A.6.9.9.1. Alınan bilgiler, tanımlanmış hizmetlerin yerine getirilmesi amacı dışında başka hiçbir amaçla kullanılmaz ve ilgilisi dışında kimse ile paylaşılmaz.

A.6.9.9.2. Bilgilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek, bilgilerin muhafazasını sağlamak amacıyla uygun güvenlik tedbirleri alınır.

A.6.9.9.3. KPS web servisleri sadece doğrulama amaçlı kullanılır. Bu servislerden elde edilen bilgiler üçüncü şahıslar ile paylaşılmaz.

A.6.9.9.4. Yapılan iş ve işlemlerde, 6698 sayılı kanun dikkate alınır.

A.6.9.10. KPS ile ilgili her türlü iletişim kps@saglik.gov.tr adresine e-Posta atılarak veya https://yazilimdestek.saglik.gov.tr/ adresi üzerinden talep açılarak sağlanır.

A.6.10. e-Nabız, USS Bilgi Yönetim Sistemi ve KDS Raporlarına Erişim

A.6.10.1. Ulusal Sağlık Sistemi (USS); 6698 sayılı kanun ve 663 sayılı KHK ile Sağlık Bakanlığına verilen görevler çerçevesinde kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla; Bakanlığımız birimleri

tarafından ulusal ölçekte tesis edilen ve birbiri ile entegre olarak çalışan muhtelif veri kayıt ve bilgi sistemlerinin tamamı için kullanılan genel bir ifadedir.

A.6.10.2. e-Nabız Projesi ülke genelinde birinci, ikinci ve üçüncü basamakta faaliyet gösteren ve sağlık hizmeti sunmakta olan bütün sağlık tesisleri tarafından işlenen kişisel sağlık verilerinin **merkezi bir veri kayıt sisteminde toplanması** ve toplanan verilerin çeşitli uygulamalar ve raporlar aracılığı ile verinin sahibi olan vatandaşlara ve yetkilendirilen Sağlık Bakanlığı çalışanlarına sunulması amacıyla gerçekleştirilmektedir. USS'yi oluşturan diğer bilgi sistemleri de A.6.10.1 maddesinde belirtilen amaçlar doğrultusunda, merkezi veri kayıt sistemine veri gönderir.

A.6.10.3. Merkezi veri kayıt sistemi üzerinde toplanan verileri kullanan uygulamalar ve kullanım maksatları şu şekildedir:

A.6.10.3.1. **e-Nabız Kişisel Sağlık Sistemi:** Merkezi veri kayıt sistemi üzerinde toplanan sağlık verilerine vatandaşların ve sağlık profesyonellerinin internet ve mobil cihazlar üzerinden erişebildikleri uygulamadır.

A.6.10.3.2. **USS Bilgi Yönetim Sistemi:** Bakanlık merkez ve taşra teşkilatında görev yapan yetkilendirilmiş personel tarafından kullanılan, standart sorgulama ve raporlama arayüzlerinin olduğu sistemdir. Birinci basamak sağlık hizmeti veren sağlık personeline ait performans verileri de bu uygulama üzerinden görüntülenir ve ihtiyaç duyulan düzenlemeler yapılır.

A.6.10.3.3. **Karar Destek Sistemi (KDS) Raporları**: USS Bilgi Yönetim Sistemi ile sağlanamayan, Bakanlık merkez ve taşra teşkilatında görev yapan üst yönetime ve diğer yetkili personel tarafından alınacak kararlara destek olmak üzere hazırlanmış olan özel ve kapsamlı raporların ve istatistiklerin yer aldığı sistemdir.

A.6.10.4. **e-Nabız Kişisel Sağlık Sistemine Erişim:**

A.6.10.4.1. e-Nabız kişisel sağlık sistemine https://enabiz.gov.tr/ adresinden, e-Devlet kapısı (https://www.turkiye.gov.tr/) üzerinden veya cep telefonlarına yüklenecek e-Nabız mobil uygulaması vasıtası ile erişim sağlanır.

A.6.10.4.2. İlk kez e-Nabız kullanıcısı olacak kişiler, e-Devlet üzerinden e-Nabız'a giriş yaparak profil ayarları üzerinden e-Nabız parolası oluşturur ya da kendi aile hekimine başvurarak e-Nabız için geçici şifre edinebilir.

A.6.10.4.3. NES sahibi olan kullanıcılar, e-İmza araçlarını kullanmak suretiyle e-Nabız kişisel sağlık sistemine erişim sağlayabilir.

A.6.10.4.4. E-nabız sistemindeki bilgiler, sadece kişilerin yetkilendirdiği hekimler veya sistemde bulunan "Paylaş" seçeneğini kullanarak ilgili kişi tarafından sürekli ya da geçici izin verilen kişiler tarafından görülebilir. Paylaşım seçenekleri ve anlamları şu şekildir.

- **Hiçbir Hekim Verilerimi Görmesin**: Kişi e-Nabız sisteminde bu seçeneği işaretlediyse Sağlık Bakanlığında bulunan hiçbir hekim SMS ile doğrulama yapmadan hastanın sağlık verilerine erişim yetkisine sahip değildir.

- **Aile Hekimim Verilerimi Görsün**: Kişi e-Nabız sisteminde bu seçeneği işaretlediyse hastanın aile hekimliği birimine atanmış (asaleten, vekâleten, geçici) aile hekimleri ilgili hastanın sağlık verilerine erişme yetkisine sahiptir.

- **Muayene Olduğum Hekim Verilerimi Görsün:** Kişi e-Nabız sisteminde bu seçeneği işaretlediyse sadece hastanın son 24 saat içerisinde muayene olduğu hekim sağlık verilerine erişme yetkisine sahiptir.

- **Muayene Olduğum Hastanedeki Tüm Hekimler Verilerimi Görsün**: Kişi e-nabız sisteminde bu seçeneği işaretlediyse hastanın son 24 saat içerisinde muayene olduğu sağlık tesisindeki tüm hekimler hastanın sağlık verilerine erişme yetkisine sahiptir.

- **Sağlık Bakanlığındaki Tüm Hekimler Verilerimi Görsün**: Kişi e-Nabız sisteminde bu seçeneği işaretlediyse Sağlık Bakanlığında bulunan tüm hekimler hastanın sağlık verilerine erişim yetkisine sahiptir.

A.6.10.4.5. e-Nabız kişisel sağlık sistemine aile hekimlerinin erişimi ile ilgili iş akışını gösteren çizelge KLVZ-EK-15'de, sağlık tesisi hekimlerinin erişimi ile ilgili iş akışını gösteren çizelge KLVZ-EK-16'dadır.

A.6.10.4.6. Uygulamanın çevrimiçi yardım dokümanı https://enabiz.gov.tr/Yardim/ adresinde ve kullanım kılavuzu https://enabiz.gov.tr/document/KILAVUZ_.pdf adresinde yer almaktadır.

A.6.10.5. USS Bilgi Yönetim Sistemine Erişim:

A.6.10.5.1. USS Bilgi Yönetim Sistemine https://ussyonetim.saglik.gov.tr/ adresinden veya Bakanlık OGN (https://giris.saglik.gov.tr/) üzerinden erişim sağlanabilir.

A.6.10.5.2. Kullanıcılar USS Bilgi Yönetim Sistemine erişirken sisteme;

- Yönetici yetkisine sahip kullanıcılar tarafından tanımlanan kullanıcı adı ve parola,

- Kurumsal (*@saglik.gov.tr) e-Posta ve parola,

- e-Devlet Kapısı (T.C. Kimlik No ve e-Devlet şifresi) (OGN üzerinden girişlerde),

- e-İmza kullanmak suretiyle giriş yaparlar.

A.6.10.5.3. Kullanıcıların sisteme tanıtılması, yetkilerinin verilmesi, yetkilerinin izlenmesi, gereksiz yetkilerin kaldırılması ve kullanıcı hesaplarının kapatılması/pasife

alınması işlemleri “Merkez, İSM veya Toplum Sağlığı Merkezi (TSM) Yöneticileri” tarafından yapılır.

A.6.10.5.4. Kullanıcı yetkilendirme işlemleri, ilgili kullanıcının sistemde tanımlı Yetki Grupları (Grup Bilgileri) ile ilişkilendirilmesi suretiyle gerçekleştirilir. Kullanıcılara ‘bilmesi gereken’ prensibi doğrultusunda mümkün olan en az yetkinin verilmesinden yetkiyi veren “Merkez, İSM veya TSM Yöneticisi” sorumludur.

A.6.10.5.5. Merkez, İSM veya TSM yöneticilerinin tanımlanması ve iptal işlemleri resmi yazı ile talep edilir. e-Posta veya yardım masası üzerinden bu maksatla yapılan taleplere işlem yapılmaz.

A.6.10.5.6. USS bilgi yönetim sistemi ile ilgili genel duyurular, https://ussyonetim.saglik.gov.tr/ ana sayfasında herhangi bir menü seçilmeden ekrana ilk gelen pencerede yer alır. Herhangi bir menüde Sağlık Bakanlığı logosu veya sol üst köşedeki kullanıcı ismine tıklandığında duyuru sayfasına ulaşılabilir.

A.6.10.5.7. USS bilgi yönetim sistemi kullanım kılavuzuna, sisteme giriş yapıldıktan sonra yardım menüsü altından erişim sağlanır.

A.6.10.5.8. USS bilgi yönetim sistemi ile ilgili her türlü yardım masası işlemleri (soru sorma, sorun bildirme, yeni işlevsellik ihtiyaçları vb.), Bakanlık Yazılım Destek Uygulaması (https://yazilimdestek.saglik.gov.tr/) üzerinden yapılır.

A.6.10.6. KDS Raporlarına Erişim

A.6.10.6.1. OBIEE (Oracle Business Intelligence Enterprise Edition) KDS sistemi kullanıcı yönetimi konusunda USS Yönetim Web uygulamasına bağlıdır. Kullanıcı oluşturma ve yetkilendirme işlemleri USS Yönetim Web sistemi üzerinden yapılır. Kullanıcı tanımlama/yetkilendirme yetkisi Nabız birimi ile birlikte KDS alt birimlerinin belirlediği destek personellerinden bulunur.

A.6.10.6.2. Kullanıcılar KDS raporlarına erişirken sisteme, yönetici yetkisine sahip kullanıcılar tarafından tanımlanan kullanıcı adı ve parola ile kds.sagliknet.saglik.gov.tr adresi üzerinden giriş yapabilir.

A.6.10.6.3. Kullanıcı tanımlama istekleri resmi yazı, e-posta ve yazılım destek (https://yazilimdestek.saglik.gov.tr/) aracılığı ile yapılır. Kullanıcı tanımlamaları ve yetkilendirmeleri KDS birim personeli ve il adminleri tarafından gerekli kontroller yapıldıktan sonra sağlanır.

A.6.10.6.4. Kullanıcı yetkilendirme işlemleri, ilgili kullanıcının sistemde tanımlı Yetki Grupları (Grup Bilgileri) ile ilişkilendirilmesi suretiyle gerçekleştirilir. Kullanıcı sistemlere sahip olduğu yetki çerçevesinde erişim sağlar.

A.6.10.6.5. SİNA raporlarına erişim sina.saglik.gov.tr adresinden veya Bakanlık OGN(ortak giriş noktası) https://giris.saglik.gov.tr/ üzerinden erişim sağlanabilir.

A.6.10.6.6. KDS ile ilgili genel duyurular, www.e-saglik.gov.tr ana sayfasında herhangi bir menü seçilmeden ekrana ilk gelen pencerede veya OBIEE girişinde yer alan pop-up pencerelerinde yer alır. Herhangi bir menüde Sağlık Bakanlığı logosu veya sol üst köşedeki kullanıcı ismine tıklandığında duyuru sayfasına ulaşılabilir**.**

A.6.10.6.7. KDS ile ilgili her türlü yardım masası işlemleri (soru sorma, sorun bildirme, yeni işlevsellik ihtiyaçları vb.) Bakanlık Yazılım Destek Uygulaması (https://yazilimdestek.saglik.gov.tr/) üzerinden yapılır.

A.6.11. Halk Sağlığı Yönetim Sistemine Erişim

A.6.11.1. Halk Sağlığı Yönetim Sistemi (HSYS); Halk Sağlığı Genel Müdürlüğüne bağlı birimler, İSM'lerde birinci basamak sağlık hizmetlerinin koordinasyonu ile görevli birimler ve birinci basamak sağlık hizmet sunucuları için geliştirilmiş bir yazılımdır.

A.6.11.2. HSYS yazılımları güncel yazılım metodolojileri kullanılarak, uluslararası standart ve kalitede geliştirilmiştir. Tüm uygulama ve modüller tek merkezden yönetilebilecek şekilde, bütünleşik bir yapıda, veri bütünlüğünü sağlayacak şekilde tasarlanmıştır. Kullanıcılarına standart veri gerişi, analizi ve raporlama araçları sağlar.

A.6.11.3. HSYS yazılımları ile ilgili ihtiyaçlar Halk Sağlığı Genel Müdürlüğü tarafından belirlenir. Yazılımların geliştirilmesi ve işletilmesi süreçleri Sağlık Bilgi Sistemleri Genel Müdürlüğü Halk Sağlığı Bilişimi Dairesi Başkanlığı tarafından gerçekleştirilir.

A.6.11.4. HSYS'ye https://hsys.saglik.gov.tr/ adresinden veya Bakanlık OGN (https://giris.saglik.gov.tr/) üzerinden erişim sağlanabilir.

A.6.11.5. Kullanıcılar HSYS'ye erişirken kendilerini sisteme;

A.6.11.5.1. HSYS tarafından tanımlanan kullanıcı adı ve parola,

A.6.11.5.2. Kurumsal (*@saglik.gov.tr) e-Posta ve parola,

A.6.11.5.3. e-Devlet Kapısı (T.C. Kimlik No ve e-Devlet şifresi) (OGN üzerinden girişlerde),

A.6.11.5.4. e-İmza kullanmak suretiyle tanıtabilir.

A.6.11.6. Kullanıcıların yetkilendirme işlemleri, kullanıcıların sistemde tanımlı olan rol/rol grupları ile ilişkilendirilmesi suretiyle yapılır. Hangi uygulamaya, hangi rol/rol grubunun hangi yetkiler ile erişebileceği, analiz safhasında belirlenir ve analiz dokümanları ile kayıt altına alınır.

A.6.11.7. Kullanıcıların sisteme tanıtılması, yetkilerinin verilmesi, yetkilerinin izlenmesi, gereksiz yetkilerin kaldırılması ve kullanıcı hesaplarının kapatılması/pasife alınması işlemleri "il HSYS yöneticileri" tarafından yapılır.

A.6.11.8. İl HSYS yöneticilerinin tanımlanması ve iptal işlemleri resmi yazı ile talep edilir. e-Posta veya yardım masası üzerinden bu maksatla yapılan taleplere işlem yapılmaz.

A.6.11.9. Uygulamalara erişecek rol/rol gruplarının yeniden düzenlenmesi ile ilgili ihtiyaçlar, Halk Sağlığı Genel Müdürlüğündeki ilgili Daire Başkanlığı ve SBSGM Halk Sağlığı Bilişimi Dairesi Başkanlığınca müşterek olarak ele alınır. Erişim yetkilerinde değişiklik yapılmasına karar verilmesi halinde yeni yetkiler analiz dokümanlarına işlenir.

A.6.11.10. HSYS ile ilgili genel duyurular, sisteme giriş yapıldıktan sonra görülebilen HSYS ana sayfası veya her bir uygulamanın kendi ana sayfası üzerinden yapılır.

A.6.11.11. Uygulamaların kullanım kılavuzlarına, sisteme giriş yapıldıktan sonra her bir uygulamanın ana sayfasından erişim sağlanır.

A.6.11.12. HSYS ile ilgili her türlü yardım masası işlemleri (soru sorma, sorun bildirme, yeni işlevsellik ihtiyaçları vb.), Bakanlık Yazılım Destek Uygulaması (https://yazilimdestek.saglik.gov.tr/) üzerinden yapılır.

A.6.12. Merkezi Web İçerik Yönetim Sistemine Erişim

A.6.12.1. Merkezi web içerik yönetim sistemi; Bakanlık merkez, bağlı kuruluşlar ve taşra teşkilatının (ASM'ler hariç) web sitelerinin tek merkezden yönetilmesi ve güvenli bir ortamda barındırılmasını sağlamak amacıyla SBSGM tarafından verilen bir hizmettir.

A.6.12.2. Web içerik yönetim sistemi ile Bakanlığımıza bağlı farklı birimlerin ihtiyaçlarını görecek şekilde standart web sitesi tasarımları hazırlanmış ve birimlerin kendilerine uygun tasarımı seçerek kullanmalarına imkân sağlanmıştır.

A.6.12.3. Web içerik yönetim sisteminde var olan kullanıcı yetkilendirme ara yüzleri ile web içeriği hazırlayan ve yayımlayan kullanıcıların farklı yetkiler (örneğin belge ekleme, silme, yayım için onay verme vb.) ile sistemi kullanmaları imkânı bulunmaktadır.

A.6.12.4. Kullanıcı tanımlama işlemleri, taşra teşkilatları için "İl Web İçerik Yöneticileri" vasıtasıyla; merkez teşkilat için doğrudan SBSGM (Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı) tarafından yapılmaktadır.

A.6.12.5. Kullanıcılar tarafından yapılan önemli işlemler (kullanıcı oluşturma, silme, yetkilendirme, doküman/bilgi ekleme, yayımlama vb.) ile ilgili iz kayıtları web içerik yönetim sistemi tarafından tutulmaktadır.

A.6.12.6. İl web içerik yöneticileri ve merkez teşkilatındaki kullanıcıların eğitimleri SBSGM tarafından yapılır. Son kullanıcıların web içerik hazırlama ve yayımlama ile ilgili eğitimleri il web içerik yöneticileri tarafından verilir.

A.6.12.7. Taşra teşkilatına bağlı birimlerin (hastaneler, il ve ilçe sağlık müdürlükleri, laboratuvarlar, 112 komuta kontrol merkezleri vb.) web içerik yönetim sistemini kullanmaları için takip etmeleri gereken süreç şu şekildedir:

A.6.12.7.1. İhtiyaç sahibi birim, web sitesi talebini resmi yazı ile il web içerik yöneticisine bildirir.

A.6.12.7.2. İl web içerik yöneticisi, sistem üzerinden web sitesi talebini yapar. Talep edilen site ile ilgili bilgileri sisteme girer. Ayrıca resmi yazı ile ihtiyacı SBSGM'ye bildirir.

A.6.12.7.3. Talep edilen web sitesi SBSGM tarafından hazırlanır. Sitenin hazır olduğu bilgisi web içerik yönetim sistem üzerinden il web içerik yöneticisine otomatik olarak bildirilir. Ayrıca resmi yazı ile de bilgi verilir.

A.6.12.7.4. İl web içerik yöneticisi, web sitesini kullanacak personeli ve yetkilerini sisteme tanımlar ve kullanıcı eğitimi verir.

A.6.12.7.5. Kullanıcılar tarafından sisteme doküman/bilgi girişleri yapılır. Sitenin kullanıma hazır olduğu il web içerik yöneticisine bildirilir.

A.6.12.7.6. İl web içerik yöneticisi webyonetim@saglik.gov.tr adresine e-Posta göndererek sitenin kullanıma hazır olduğunu SBSGM'ye bildirir.

A.6.12.7.7. SBSGM tarafından site açılır ve alan adıyla birlikte il yetkilisine dönüş yapılır.

A.6.12.8. Web içerik yönetim sistemi uygulamalarına giriş e-Devlet Kapısı kimlik doğrulama servisi üzerinden veya OGN (https://giris.saglik.gov.tr) üzerinden yapılır.

A.6.12.9. Kullanıcıların sisteme doğru şekilde tanımlanmasından ve takibinin yapılmasından il web içerik yöneticileri, web sitelerinde yayımlanan içerikten ise ilgili web sitesinde yayımı yapan kullanıcılar sorumludur.

A.6.12.10. Web sitelerinin herkese açık bölümlerinde sadece tasnif dışı (gizliliği olmayan) bilgiler yayımlanabilir.

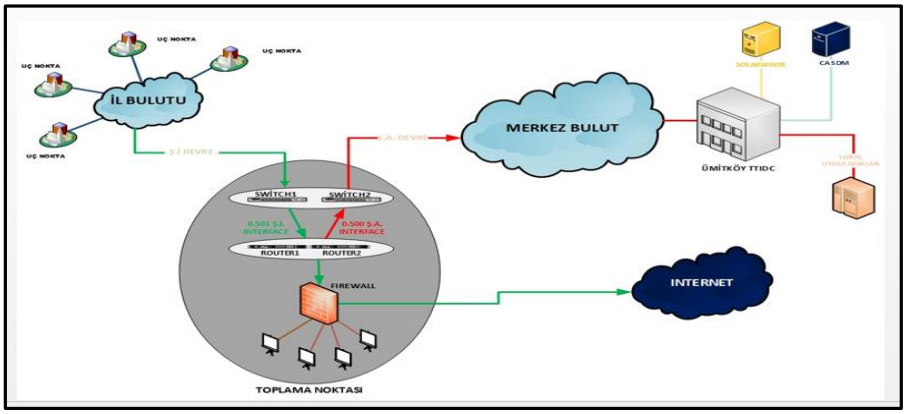
A.6.12.11. Web içerik yönetim sistemi ile iletişim ihtiyaçları webyonetim@saglik.gov.tr adresine e-Posta göndermek suretiyle karşılanır. *@saglik.gov.tr uzantılı e-Posta adresleri haricinde başka adreslerden gelen taleplere işlem yapılmaz.

A.6.13. Sağlık Bilişim Ağına Erişim

A.6.13.1. Sağlık Bilişim Ağı (SBA), Sağlık Bakanlığı ve bağlı kuruluşlarının veri iletişiminin güvenilir ve hızlı bir kanal üzerinden sağlanması amacıyla tesis edilen, KamuNet'e bağlı olarak çalışan, internet erişiminin kontrollü olarak sağlandığı kapalı bir ağdır.

A.6.13.2. SBA, Bakanlık birimlerinin iletişim teknolojilerinden en üst seviyede, hızlı ve en ekonomik şekilde faydalanması amacıyla en güncel teknolojiler kullanılarak tesis edilmiştir.

A.6.13.3. SBA projesinin işletme ve yönetim faaliyetleri SBSGM tarafından yerine getirilir. Ağın bulut mimarisindeki görünümü Şekil 3'tedir.



Şekil 3 SBA Bulut Mimarisi

A.6.13.4. İl seviyesinde tesis edilmiş olan bulutların işletme ve yönetim faaliyetleri, İSM'ler tarafından görevlendirilen "SBA İl Bulut Sorumluları" vasıtasıyla yapılır.

A.6.13.5. İl Bulut Sorumluları, kendi bulutlarının yönetilmesinden, buluta bağlı lokasyonların izlenmesinden, http://sba.saglik.gov.tr adresi vasıtasıyla SBA projesi ile ilgili duyuruların takip edilmesi ve işlem yapılmasından sorumludur.

A.6.13.6. İl Bulut sorumlularınca;

A.6.13.6.1. SBA yönetim faaliyetleri kapsamında https://sbayonetim.saglik.gov.tr/ adresinde yer alan uygulama vasıtasıyla "lokal bulut bağlantı hattı kapasitesi, yeni lokasyon talebi, uç nokta iptal talebi, nakil talebi" vb. işlemler yapılır.

A.6.13.6.2. SBA izleme faaliyetleri kapsamında https://sbanms.saglik.gov.tr adresinde yer alan uygulama vasıtasıyla il ve buluta bağlı olan lokasyonların "up/down" durumu, veri aktarım grafiği, CPU, RAM değerleri gibi teknik veriler izlenir.

A.6.13.6.3. SBA projesi kapsamında kurulumları Türk Telekom tarafından yapılan cihazların sürekli çalışır kalması, yüklenicinin taahhütlerinin ölçülmesi açısından önem arz etmektedir. Bu nedenle enerji sorunu bulunan yerlerde gerekli tedbirler alınarak cihazların 7/24 esasına göre çalıştırılması sağlanır.

A.6.13.7. SBA il Bulut Sorumluları ile ilgili tüm işlemler (yetkilendirme, yetki iptal, görev değişikliği vb.) resmi yazı ile yapılır. Bu maksatla SBSGM'ye gönderilecek yazılarda görevlendirilen kişinin "adı, soyadı, görevi ve unvanı, *@saglik.gov.tr uzantılı e-Posta adresi, iş ve cep telefonu numarası" bilgileri mutlaka yer alır.

A.6.13.8. SBA'ya bağlanan lokasyonlarda asgari olarak bu kılavuzda yer alan bilgi güvenliği politikalarının uygulanması gerekir.

A.6.14. Uzaktan Çalışma ve Erişim

A.6.14.1. 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.

A.6.14.2. 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.

A.6.14.3. Uzaktan çalışma ile ilgili esaslar belirlenirken, uzaktan çalışmanın ne tür fiziki ortamlarda yapılacağı göz önüne alınır. Muhtemel uzak çalışma ortamları aşağıda sıralanmıştır.

A.6.14.3.1. Bakanlığımıza ait ancak SBA bağlantısı olmayan yerler (aktif cihaz sayısı 10'dan az olan müstakil bina ve tesisler),

A.6.14.3.2. Çalışanların evleri veya (tedarikçiler, iş ortakları için) ofisleri,

A.6.14.3.3. Herkese açık alanlar (kafeler, lokantalar, oteller vb.),

A.6.14.3.4. 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).

A.6.14.4. Uzaktan çalışma işlemi, yapısı itibarı ile güvensiz olarak kabul edilir ve bilgi güvenliğini sağlamak için ek önlemler alınması gerekir.

A.6.14.5. Uzaktan çalışma ile ilgili kontrol tedbirleri belirlenirken aşağıda sıralanan dört temel tehdit unsuru/modeli dikkate alınır.

A.6.14.5.1. Uzak çalışma ortamlarının fiziki güvenliğindeki yetersizlikler,

A.6.14.5.2. Uzak bağlantının güvenli olmayan ağ ortamları (çoğunlukla internet) üzerinden yapılması,

A.6.14.5.3. Kurum güvenlik politikaları uygulanmamış güvenilir olmayan cihazların iç ağa bağlanması,

A.6.14.5.4. İç ağdaki kaynaklara dışarıdan erişim.

A.6.14.6. Günümüzde teknolojinin bizlere sağlamış olduğu yetenekler kullanılmak suretiyle, farklı yöntemler kullanılarak uzak bağlantı yapılması mümkündür.

A.6.14.7. Uzaktan erişim için en uygun yöntemin belirlenmesi amacıyla, her ihtiyacın kendine özgü şartları ve risklerinin ayrıntılı olarak değerlendirilmesi gerekir.

A.6.14.8. Uzaktan erişim yöntemi olarak aşağıda açıklamaları verilen tünelleme, uygulama portalleri, uzak masaüstü erişim veya doğrudan uygulama erişimi yöntemlerinin biri veya birkaçı birlikte kullanılabilir.

A.6.14.8.1. 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.

A.6.14.8.2. 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.

A.6.14.8.3. 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.

A.6.14.8.4. 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.

A.6.14.9. Uzak çalışma için hangi uzak erişim yönteminin veya yöntemlerinin kullanılacağına, yapılacak risk değerlendirmesine bağlı olarak kurumların bilgi güvenliği alt komisyonları tarafından karar verilir ve kurumun BGYS Politikası içerisinde (veya ayrı bir politika olarak) yazılı olarak belirtilir.

A.6.14.10. Uzaktan erişim ile ilgili yöntem/mimari belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

A.6.14.10.1. Bakanlığımızda genel bir politika olarak uzak masaüstü işlemleri VPN bağlantısı üzerinden yapılır. VPN bağlantısı yapılmadan doğrudan uzak masaüstü bağlantısı yapılmasına hiçbir şekilde izin verilmez.

A.6.14.10.2. 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.

A.6.14.10.3. VPN işlemi (bu maksatla kullanılan ayrı bir yazılım ve/veya donanım yoksa) İl SBA Bulutu girişinde bulunan güvenlik duvarı üzerinden yapılır.

A.6.14.10.4. 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.

A.6.14.10.5. VPN bağlantılarına ilişkin iz kayıtları tutulur ve söz konusu iz kayıtları en az iki yıl süre ile saklanır.

A.6.14.10.6. Uzak bağlantı yapılacak uygulamalara/kaynaklara erişimin daha kontrollü olarak yapılması gerekiyorsa, bağlantılar bu amaçla ayrılan bir terminal/vekil sunucu üzerinden de yapılabilir.

A.6.14.10.7. Uzak bağlantı yapacak istemci bilgisayarların IP adresleri/blokları biliniyorsa, hedef bilgisayara sadece belirtilen IP adreslerinden erişim yapılması için gerekli ayarlar yapılır.

A.6.14.10.8. Uzak erişim için yapılan bağlantıda boşta kalma süresi (herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre sınırlanır. Bu süre 1 (bir) saati geçemez.

A.6.14.10.9. Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

A.6.14.10.9.1. Bağlantı VPN üzerinden yapılır.

A.6.14.10.9.2. Bağlantı yapan kişinin, hedef bilgisayarda oturum açma iznine sahip bir kullanıcı olması gerekir.

A.6.14.10.9.3. Hedef bilgisayara kullanıcı adı ve parola girilerek oturum açılır. Anonim girişlere izin verilmez.

A.6.14.10.9.4. 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.

A.6.14.10.9.5. 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.

A.6.14.10.9.6. 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.

A.6.14.10.9.7. Uzak bağlantı yazılımı olarak mümkün ise "Microsoft Uzak Bağlantı Programı" kullanılır.

A.6.14.10.9.8. 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.

A.6.14.11. Uzaktan çalışma için kullanılacak cihazlar belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir:

A.6.14.11.1. Uzaktan çalışma prensip olarak Bakanlığımız birimlerine ait cihazlar ile yapılır.

A.6.14.11.2. 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.

A.6.14.11.3. 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.

A.6.14.11.4. Doğrudan uygulama erişimleri de dâhil uzaktan çalışmanın hiçbir çeşidinde sahibi bilinmeyen/herkes tarafından erişilebilen (internet kafe, otel bilgisayarları, kiosklar vb.) kullanılmaz.

A.6.14.11.5. 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.

A.6.14.12. Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmış olması gerekir:

A.6.14.12.1. Cihazlara kişisel güvenlik duvarı kurulur ve aktif hale getirilir.

A.6.14.12.2. İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanır.

A.6.14.12.3. 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.

A.6.14.12.4. Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.

A.6.14.12.5. Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.

A.6.14.12.6. Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise dizüstü bilgisayar kilidi kullanılmak suretiyle çalınmaya karşı cihaz emniyete alınır.

A.6.14.12.7. Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (WİFİ, bluetooth, RS232 vb.) pasif hale getirilir.

A.6.14.12.8. 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.

A.6.14.12.9. 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.

A.6.14.12.10. Uzaktan çalışma ve uzaktan erişim için kullanılacak cihazlara çok faktörlü kimlik doğrulama yapılarak giriş yapılması tercih edilir.

A.6.14.12.11. Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.

A.6.14.12.12. Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.

A.6.14.12.13. Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.

A.6.14.12.14. Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için “jailbreak” veya “rootlama” işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.

A.6.14.12.15. Tüm mobil cihazlara (telefon/tablet) mutlaka lisanslı anti-virüs yazılımı kurulması gerekir.

A.6.14.12.16. Kullanılan her türlü mobil cihaz için üreticinin sağladığı işletim sistemi güncelleştirmeleri ve yazılım güncelleştirmeleri mutlaka periyodik olarak kontrol edilir ve uygulanır.

A.7. KRİPTOGRAFİK KONTROLLERİN KULLANIMI

A.7.1. Kriptografik Politikalar

A.7.1.1. Elektronik ortamda yer alan bilgiler;

A.7.1.1.1. Kurum için taşıdığı değer nedeniyle HİZMETE ÖZEL ve üstü gizlilik derecesi ile sınıflandırılmış ise,

A.7.1.1.2. Kaybı halinde yasal olarak yaptırımlara uğranması riski varsa,

A.7.1.1.3. CD, DVD, USB bellek, dizüstü bilgisayar vb. taşınabilir ortamlarda saklanıyorsa,

A.7.1.1.4. Herkesin kolayca erişebileceği web sayfaları vb. yerlerde tutuluyorsa,

A.7.1.1.5. İnternet üzerinden e-Posta, dosya aktarım protokolü (FTP:File Transfer Protocol) vb. yöntemlerle bir başka kişiye veya web servisleri vb. araçlarla bir başka sisteme aktarılması gerekiyorsa,

A.7.1.1.6. **6698 sayılı Kanun ile tanımlanan özel nitelikli kişisel veri** kategorisinde ise standart olarak kullanılan erişim kontrollerine ilave olarak daha iyi koruma sağlanması için kriptografik tekniklerin kullanılması gerekir.

A.7.1.2. Sadece taşınabilir cihazlar değil aynı şekilde masaüstü bilgisayarlar ve sunucuların da herhangi bir nedenle kurum dışına çıkarılması gerekiyorsa ve bunların disklerinde yer alan hassas bilgilerin başka türlü korunma imkânı yok ise aynı şekilde kriptografik araçların kullanımı göz önünde bulundurulur.

A.7.1.3. Kriptografik kontroller;

A.7.1.3.1. Bilgilerin gizliliğini sağlamak,

A.7.1.3.2. Bütünlüğünü korumak,

A.7.1.3.3. Gönderici ve alıcının kimliklerini doğrulamak ve

A.7.1.3.4. Yapılan işlemlerin hiçbir şekilde inkâr edilmemesini,

A.7.1.3.5. Özgünlük ve güvenilirliği garanti etmek amacıyla kullanılır.

A.7.1.4. Şifreleme, bilgilerin gizliliğini sağlamak amacıyla yapılır. Şifrelenmiş bir bilgi, kötü niyetli bir kişinin eline geçse dahi okunamayacağı, erişilemeyeceği için önemli bir koruma sağlar.

A.7.1.5. Veri özeti (hash), bütünlüğü korunacak bilginin sabit boyutta bir parmak izinin (özetinin) çıkarılmasını sağlar. Bilginin bir harfinin (veya bir bitinin) bile değişmesi

durumunda, yeni çıkarılacak özet, aslından farklı olacağı için bilginin değişmediği garanti edilmiş olur.

A.7.1.6. Elektronik (sayısal) sertifikalar, imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır. Bu bağlamda sertifika, ilgili kişi veya cihazın elektronik ortamdaki kimlik kartlarına benzetilebilir. Bilgisayar ortamında yapılacak işlemler tarafların sayısal sertifikaları ile yapılıyor ise ilgili kişilerin kimlikleri kesin olarak doğrulanabilir.

A.7.1.7. e-İmza, sayısal sertifika kullanılarak üretilir ve imzayı atan kişinin yaptığı işlemi inkâr etmesini önler. NES kullanılarak atılan imzalar, güvenli elektronik imza olarak adlandırılır ve 5070 sayılı Elektronik İmza Kanunu uyarınca elle atılan imza ile eşdeğerdir.

A.7.1.8. Tüm bu kriptografik işlemler (simetrik/asimetrik şifreleme, özetleme, e-İmza vb.) çeşitli yazılım ve bazen de donanımların kullanılması suretiyle yapılır. Yapılan kriptografik işlemin beklenen faydayı sağlaması için güçlü kriptolama algoritmaları seçmek ve seçilecek algoritmaya göre yeterli koruma sağlayacak uzunlukta anahtar kullanmak gerekir. Zayıf bir algoritma ve yeteri kadar uzun olmayan bir anahtar ile yapılan işlemler güçlü bilgisayarlar ile kolayca çözülebilir.

A.7.2. Kriptografik Araç ve Yöntemler

A.7.2.1. Algoritma ve Anahtar Uzunlukları:

A.7.2.1.1. Açık anahtar altyapısı teknikleri kullanılarak yapılacak asimetrik şifreleme işlemlerinde;

- RSA (Ron **R**ivest, Adi **S**hamir ve Leonard **A**dleman) ve eliptik eğri kriptolojisi (ECC:Elliptic Curve Cryptography) algoritmalarından birisi kullanılır.

- RSA algoritması kullanılacaksa anahtar uzunluğu en az 1024 bit, tercihen 2048 bit olarak seçilir.

- ECC algoritması kullanılacaksa “n” değeri olarak en az 224 bit seçilir.

A.7.2.1.2. Blok (simetrik) şifreleme işlemlerinde, gelişmiş şifreleme standardı (AES:Advanced Encryption Standard) kullanılır ve anahtar boyu en az 256 bit olur.

A.7.2.1.3. Veri özeti (hash) işlemlerinde;

- Özetleme algoritması olarak blok boyu en az 256 olacak şekilde güvenli özetleme algoritmasının (SHA: secure hash algorithm) ikinci veya üçüncü sürümü (SHA2 veya SHA3) kullanılır.

- SHA2 algoritmasını kullanan sistem ve uygulamaların, SHA3’e yükseltilmesine gerek yoktur.

A.7.2.1.4. Anahtar değişimi ve doğrulama (authentication) işlemlerinde;

- Diffie-Hellman (DH) , internet anahtar değişim (IKE: İnternet Key Exchange) veya eliptik eğri kullanan DH (ECDH: Elliptic Curve Diffie-Hellman) algoritmalarından birisi seçilir. Anahtar boyutu olarak 2048 bit anahtar kullanılır.

- Anahtar üretim ve değişim öncesinde uç noktaların birbirlerini doğrulamaları gerekir. Doğrulama için tarafların X.509 Ver3 standardında üretilen sertifikalar kullanılır.

- Kimlik doğrulama için kullanılan sunuculara bilinen güvenilir bir sertifika otoritesi tarafından imzalanmış geçerli bir sayısal sertifika yüklenir.

- SSL veya TLS kullanan tüm sunucular ve uygulamaların, bilinen güvenilir bir sertifika otoritesi tarafından imzalanmış geçerli bir sayısal sertifikası olması gerekir.

A.7.2.1.5. Sunucu ve istemci doğrulama işlemlerinde kullanılacak sayısal sertifikalar:

- X.509 Ver3 standardında olmalıdır.

- Son kullanıcı sertifikaları Kamu Sertifikasyon Merkezinden alınır.

- Bakanlık tarafından geliştirilen/kullanılan uygulamalarda, sertifikaların geçerliliğini kontrol etmek için çevrimiçi sertifika durumu protokolü (OCSP:Online Certificate Status Protocol) veya sertifika iptal listesi (CRL: Certificate Revocation List) metotlarından biri ya da her ikisi birlikte kullanılır.

- Sertifika geçerlilik kontrolünde kullanılan SİL ve OCSP'lerin farklı durumlara göre birbirlerine üstünlükleri vardır. CRL'ler belirli aralıklarla yayınlandıkları için bazı kontrollerde bazı sertifikaların geçerlilik durumları doğru anlaşılamamaktadır. Bu yüzden eğer bir internet bağlantısı varsa öncelikle OCSP kullanılması gerekir.

- Sertifika geçerlilik kontrolünün sık yapıldığı durumlarda, CRL dosyalarının her sertifika kontrolü için yeniden indirilip içerisinden kontrol yapılması kurum için birçok yük getirecektir. Bu yüzden Sertifika Deposu dediğimiz depolama yönteminin kullanılması kurum için çok büyük kolaylık getirecektir. Sertifika Deposunda, geçerlilik kontrolü yapılan her sertifika için kontrol sırasında gerekli olan tüm kök sertifikalar, çekilen CRL'ler ya da OCSP cevapları güvenliği sağlanmış bir veri tabanı gibi bir depo içerisine kaydedilir. Aynı sertifika için tekrar geçerlilik kontrolü yapılmak istendiğinde gerekli olan tüm bilgiler depoda bulunmaktadır ve bu bilgileri tekrar internetten çekmeye gerek yoktur.

A.7.2.2. Web Trafiği Güvenliği:

A.7.2.2.1. İşletilen tüm web sunucuları için kimlik doğrulama ve şifreleme işlemlerinde kullanılmak üzere, X.509 Ver3 tabanlı sayısal sertifika temin edilir ve kullanılır.

A.7.2.2.2. Tedarik edilecek sayısal sertifikanın, son kullanıcılar açısından yaygın olarak kullanılan tarayıcılar tarafından ayrıca bir işlem yapmadan tanınan bir sertifika üreticisi tarafından verilmiş olmasına dikkat edilir.

A.7.2.2.3. Web trafiğinin korunması için HTTPS kullanılır.

A.7.2.2.4. Https protokolü TLS 1.2 veya üstü bir protokol ile birlikte kullanılır. Tüm web sunucularında SSL ve TLS 1.2 altındaki servisleri kapatılır. Uyumluluk açısından tüm işletim sistemindeki tarayıcılar güncel versiyona yükseltilir.

A.7.2.2.5. HTTPS trafiğinin şifrelenmesinde anahtar boyu en az 256 bit olacak şekilde AES algoritması kullanılır. DES, 3DES, RC4 algoritması kullanıma kapatılır.

A.7.2.2.6. Veri özetleme işlemleri için MD5 ve SHA1 kullanan “cipher suit”ler devre dışı bırakılır.

A.7.2.2.7. CRIME saldırısını önlemek için TLS sıkıştırması (compression) devre dışı bırakılır.

A.7.2.2.8. Oturum anahtarlarının güvenliği için kusursuz iletme gizliliği (PFS: Perfect Forward Secrecy) özelliği aktive edilir.

A.7.2.2.9. Sunucunun özel anahtarını korumak için mümkün olan en üst düzey önlemler alınır.

A.7.2.2.10. Herkesin erişimine açık ve HTTPS kullanan web sitelerinde EV SSL sertifikaları veya SSL site mührü kullanılması tercih edilir.

A.7.2.3. FTP İşlemleri Güvenliği:

A.7.2.3.1. Standart FTP hizmeti, doğası gereği güvensiz olduğu için hiçbir şekilde kullanılmaz.

A.7.2.3.2. Güvenli FTP işlemleri için sFTP (Secure FTP), SCP (Secure Copy) veya FTPS (TLS/SSL üzerinden FTP) protokollerinden birisi kullanılır.

A.7.2.3.3. SFTP/FTPS/SCP protokolleri kullanılırken şifreleme algoritması olarak AES-256 seçilir.

A.7.2.3.4. Gizlilik dereceli bilgi değişimi olacaksa sunucu tarafı kimlik doğrulaması için sayısal sertifika kullanılır. İstemci tarafı için de tercihen sayısal sertifika ile veya form tabanlı (kullanıcı adı/parola) yöntemler kullanılarak kimlik doğrulaması yapılır.

A.7.2.3.5. FTPS yapılırken kontrol ve data kanallarının her ikisi de şifrelenir.

A.7.2.4. Uzaktan Yönetim Faaliyetleri:

A.7.2.4.1. Kimlik doğrulaması için temelde iki bağlanma yöntemi mevcuttur. Bunlardan birincisi kullanıcı adı ve şifre ile oturum sağlanan yöntem, ikincisi ise SSH key (SSH açık/gizli anahtar) yardımı ile oturumun sağlandığı yöntemdir. İlk yöntemin yeni kullanıcılar için anlaşılması kolaydır. Ancak kötü niyetli kullanıcılar genellikle art

arda şifre denemeleri ile güvenlik tavizlerine yol açabilir. Bu yöntem yerine SSH anahtarı yardımı ile oturum sağlanması daha güvenlidir.

A.7.2.4.2. SSH Protokolü içerinde şifreleme algoritması olarak AES-256 kullanılır.

A.7.2.4.3. SSH kullanılırken, istemci ve sunucu arasında kimlik doğrulaması yapılır.

A.7.2.4.4. Daha güvenli uzaktan erişim ve yönetim işlemleri için standart SSH portunun (22 nolu port) değiştirilmesi, port yönlendirmelerinin kapatılması, kullanıcı/adı parola ile SSH bağlantılarının engellenmesi, "root" erişimlerinin kapatılması gibi sıkılaştırmalar yapılır.

A.7.2.5. Sabit Ortamdaki Verilerin Şifrelenmesi:

A.7.2.5.1. Windows tabanlı sistemlerde tam disk şifreleme işlemleri için;

- Bitlocker kullanılır.
- Bitlocker etkinleştirilecek cihazlarda (eğer varsa) şifreleme anahtarının saklanmasında kullanılan TPM (Trusted Platform Module) yonga seti aktif hale getirilmelidir.
- TPM yonga setine erişimi kısıtlamak için kullanıcıların bilgisayarlarındaki temel giriş/çıkış sistemi (BIOS: **B**asic **I**nput/**O**utput **S**ystem) ayarlarını değiştirmeleri engellenir.

A.7.2.5.2. GNU/Linux Cent OS tabanlı sistemlerde tam disk şifreleme işlemleri için LUKS (Linux Unified Key Setup) kullanılır.

A.7.2.5.3. Apple Mac OS X tabanlı sistemlerde tam disk şifreleme işlemleri için FileVault kullanılır.

A.7.2.5.4. Disk şifreleme için SBSGM tarafından hazırlanan ve https://bilgiguvenligi.saglik.gov.tr/Home/KullaniciElKitaplari adresinde yayımlanan sürücü şifreleme kullanıcı el kitapları kullanılır.

A.7.2.6. Dosya ve klasör şifreleme işlemleri için;

- Güvenilir bir kaynak tarafından yayımlanmış ve AES-256 algoritmasını destekleyen herhangi bir yazılım (Winrar (5.0 veya üstü), Winzip (9.0 veya üstü) veya 7-zip) kullanılabilir.
- 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.

A.8. FİZİKSEL VE ÇEVRESEL GÜVENLİK

A.8.1. Genel Hususlar

A.8.1.1. Günümüzde bilgiler büyük oranda bilgi sistemleri vasıtasıyla işlenmekte ve sayısal ortamlarda saklanmaktadır. Bu nedenle bilgi güvenliği ile ilgili tedbirlerin önemli bir kısmını bilgi sistemleri ve ağlarının korunmasına yönelik siber güvenlik önlemleri oluşturmaktadır. Bununla birlikte, fiziksel ortamda saklanan bilgilerin veya elektronik ortamda saklanmakla birlikte bunların muhafaza edildiği bilişim sistemleri ve ağlarının güvenliği için fiziksel ve çevresel önlemlerin alınması kaçınılmazdır.

A.8.1.2. İş ve işyerlerinin fiziksel ve çevresel güvenliği ile ilgili hususlar çeşitli yönetmelik, yönerge ve talimatlar ile düzenlenmiş durumdadır. Bu mevzuatın bir kısmı şu şekildedir:

A.8.1.2.1. İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik (Resmî Gazete, Tarih/Sayı: 17.07.2013-28710),

A.8.1.2.2. İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği (Resmî Gazete, Tarih/Sayı: 29.12.2012-28545),

A.8.1.2.3. İşyerlerinde Acil Durumlar Hakkında Yönetmelik (Resmî Gazete, Tarih/Sayı: 18.06.2013-28681),

A.8.1.2.4. Binaların Yangından Korunması Hakkında Yönetmelik (Resmî Gazete, Tarih/Sayı:19.12.2007-26735),

A.8.1.2.5. Hastane Afet ve Acil Durum Planları (HAP) Uygulama Yönetmeliği (Resmî Gazete, Tarih/Sayı:20.03.2015-29301),

A.8.1.2.6. Hastane Afet ve Acil Durum Planı (HAP) Hazırlama Kılavuzu

A.8.1.2.7. Sağlıkta Kalite Standartları –Hastane/ADSH.

A.8.1.3. Bu bölümde yer alan hususlar, esas olarak ISO 27001 standardında yer alan “bilgi varlıklarının fiziksel ve çevresel güvenlik önlemleri ile korunması için kontroller” dikkate alınarak hazırlanmıştır. Aynı zamanda yukarıda sıralanan ilgili diğer mevzuat da dikkate alınmıştır. Kılavuzda yer alan kontrollerin uygulanması esnasında yürürlükteki diğer mevzuat ile çelişen bir husus ile karşılaşılması durumunda, normlar hiyerarşisi dikkate alınarak üst seviye norm dikkate alınır. Yine de tereddütte kalınması halinde kurumun bilgi güvenliği alt komisyonunda değerlendirilerek karar verilir.

A.8.2. Güvenli Alanlar

A.8.2.1. Fiziksel ve çevresel güvenlik tedbirlerinin belirlenmesi ve uygulamaya alınmasının ön koşulu hassas veya kritik bilgi ve bilgi işleme tesislerini barındıran güvenli alanların tespit edilmesi ve bu alanların güvenlik sınırlarının tanımlanmasıdır.

A.8.2.2. Güvenlik sınırları belirlenirken kademeli bir yaklaşım kullanılır. Gerekiyorsa iç içe güvenli alanlar oluşturularak daha hassas ve kritik bilgilerin işlendiği alanlara erişim için birden fazla fiziksel sınırdan geçilmesi zorunlu hale getirilir.

A.8.2.3. Güvenlik sınırları belirlenirken kişilerin kontrolsüz olarak giriş çıkış yapabilecekleri herhangi bir boşluk bulunmamasına dikkat edilir. Bu tür boşlukların kapatılması/korunması için ilave tedbirler alınır.

A.8.2.4. Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunur.

A.8.2.5. Göreceli olarak daha az hassas varlıkların yer aldığı dış güvenlik sınırında alınan güvenlik tedbirleri ile kritik varlıkların yer aldığı iç güvenlik sınırlarındaki tedbirler farklılaştırılır.

A.8.2.6. Güvenli alanlar, fiziksel güvenlik engelleri ile çevrili, kilitlenebilir bir ofis ya da birkaç oda olabilir. Birden fazla kuruluşun aynı bina içerisinde olduğu durumlarda fiziksel erişim güvenliğine özel dikkat gösterilir.

A.8.2.7. Fiziksel koruma, bir ya da daha fazla fiziksel engel konularak gerçekleştirilir. Birden fazla fiziksel engel kullanımı (kartlı geçiş sistemleri, turnikeler, kayar kapılar, kilitli odalar vb.) ilave koruma sağlayarak tek bir engelin başarısızlığı durumunda güvenliğin tehlikeye girmesini önler.

A.8.2.8. Giriş kontrolleri, korunacak tesis veya varlığa göre değişir.

A.8.2.8.1. Sağlık hizmeti sunumu yapan tesislerde en dışta yer alan güvenlik sınırlarının geçiş noktaları, sadece gözle veya elektronik tarama araçları ile korunur. Burada amaç, vatandaşların gereksiz giriş kontrolleri ile uğraşmadan en kısa yoldan sağlık hizmetine eriştirilmesidir. Bununla birlikte sürekli gözetim yapılarak şüpheli durumlarda, güvenlik personeli vasıtası ile gerekli müdahalelerde bulunulur. Bölgesel koşullar dikkate alınarak ilave güvenlik tedbirleri alınabilir.

A.8.2.8.2. Bakanlık merkez yerleşke, bağlı kuruluşlar, il sağlık müdürlükleri gibi sağlık hizmeti sunumu yapılmayan ancak sağlık hizmetinin sunumu için destek hizmetlerinin verildiği bina ve yerleşkelerde, en dış güvenlik sınırında yer alan geçiş noktalarında sadece yetkili personele erişim izni verilmesini temin edecek giriş kontrolleri yapılır.

A.8.2.9. Kapsamı ve yöntemi idareler tarafından belirlenecek şekilde ziyaretçilerin giriş ve çıkışlarının tarih ve saatleri kayıt altına alınır. Daha önce erişimi onaylanmadığı sürece tüm ziyaretçiler denetlenir. Ziyaretçilere sadece belirli, yetkilendirildikleri amaçlar için erişim verilir. Ziyaretçilerin kimliği uygun bir yöntem ile doğrulanır.

A.8.2.10. Sunucu odaları, güvenlik kontrol merkezleri, arşiv odaları vb. hassas bilgilerin işlendiği veya saklandığı alanlar kolayca ulaşılamayacak yerlere kurulur. Bu alanlara erişim uygun yöntemler kullanılarak sınırlandırılır.

A.8.2.11. Özel bir gereksinim yoksa bu tür tesis ve odaların ne maksatla kullanıldığını gösteren işaretlerin konulmasından sakınılır. Bu gibi yerlere giriş için iki faktörlü kimlik doğrulama mekanizmaları kullanılır.

A.8.2.12. Kapsam ve yöntemi idarelerce belirlenmek suretiyle tüm personel ve ziyaretçilerin güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartları hazırlanır ve kullanılır.

A.8.2.13. Refakat edilmeyen bir ziyaretçi ile karşılaşıldığında veya kimlik takmayan bir kişi görüldüğünde hemen güvenlik personeline bilgi verilir.

A.8.2.14. Dış taraf destek personeline güvenli alanlara veya gizli bilgi işleme tesislerine erişim izni, sadece gerekli olduğu durumlar için geçici süre ile verilir. Bu tür erişimlerde, mümkün olduğu kadar erişim kısıtlaması yapılır ve takip edilir.

A.8.2.15. Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilir.

A.8.2.16. Güvenli alanlara erişim hakları düzenli olarak gözden geçirilir. Gereksiz erişim izinleri iptal edilir veya yetki kısıtlaması yapılır.

A.8.2.17. Gizli bilgi işleme tesislerinin yerlerini belirten krokiler ve dâhili telefon rehberleri herkes tarafından kolayca erişilebilir yerlere konulmaz.

A.8.2.18. Sahipsiz güvenli alanlar fiziksel olarak kilitlenir ve periyodik olarak gözden geçirilir.

A.8.2.19. Yetki verilmediği sürece, fotoğraf, video, ses ve diğer kayıt cihazları ve mobil cihazlardaki kameralara izin verilmez.

A.8.2.20. Yetkisiz kişilerin teslimat ve yükleme işlemleri için güvenli alanlara giriş yapmasını engellemek üzere güvenli alan dışında olacak şekilde teslimat ve yükleme alanları oluşturulur.

A.8.2.21. Postacı, kurye personeli, dağıtıcı gibi kişilerin tesis içlerine kontrolsüz olarak girmesi engellenir. Teslimat ile ilgili kurallar oluşturulur. Teslimat işlemlerinin kurum içinde belirlenecek noktalarda yapılması için tedbir alınır.

A.8.2.22. Personel güvenliği ve sağlığı için ilgili yönetmelikler uygulanır.

A.8.2.23. Yangın, sel, deprem, patlama ve diğer doğal afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınır ve uygulanır.

A.8.2.24. Giriş/çıkış yapılan yerler ve ortak kullanım alanları güvenlik kameraları ile kayıt altına alınır.

A.8.3. Ekipman Güvenliği

A.8.3.1. 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.

A.8.3.2. Belli başlı temiz masa kuralları

A.8.3.2.1. 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.

A.8.3.2.2. Yetkisiz kişilerin erişiminin engellenmesi için bilgisayar başından ayrılma durumunda ekran kilitlemesi yapılır. Otomatik ekran kilitlemesi devreye alınır.

A.8.3.2.3. Sistemlerde kullanılan parola, telefon numarası ve T.C. kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulundurulmaz.

A.8.3.2.4. Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler A.4.5 maddesinde belirtilen yöntemler ile imha edilir.

A.8.3.2.5. Faks makinelerine gelen yazılar sürekli kontrol edilir ve makinede yazı bırakılmaması için tedbir alınır.

A.8.3.2.6. 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.

A.8.3.2.7. Fotokopi ve diğer çoğaltma teknolojilerinin (tarayıcı, sayısal kamera vb.) yetkisiz kullanımını önlemek için uygun idari ve teknik tedbirler alınır.

A.8.3.3. Ekipman Yerleşimi ve Koruması

A.8.3.3.1. Yüksek maliyetli, özel koruma gerektiren elektronik cihazların (tıbbi cihazlar dâhil) yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine dikkat edilir.

A.8.3.3.2. Ekipmanlar, gereksiz erişimleri asgari düzeye indirecek şekilde yerleştirilir.

A.8.3.3.3. Kritik veri içeren araçlar, yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilir.

A.8.3.3.4. Özel koruma gerektiren ekipmanlar izole edilmiş şekilde kullanılır.

A.8.3.3.5. Nem ve sıcaklık gibi parametreler izlenir.

A.8.3.3.6. Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanır.

A.8.3.3.7. Paratoner kullanılır.

A.8.3.3.8. Bilgi işlem araçlarının yakınında yeme, içme ve sigara kullanımı konularını düzenleyen kurallar oluşturulur ve uygulanır.

A.8.3.4. Destek Hizmetleri

A.8.3.4.1. Elektrik, su, kanalizasyon ve iklimlendirme sistemlerinin, destekledikleri bilgi işlem birimi için yeterli düzeyde olmasına dikkat edilir.

A.8.3.4.2. Ekipmanların elektrik arızalarından korunması için ana besleme noktalarında elektrik şebekesine yedekli bağlantı yapılır.

A.8.3.4.3. Kritik sistemlerde hizmet kesintisi yaşanmaması için kesintisiz güç kaynağı kullanılır.

A.8.3.4.4. Yedek jeneratör ve jeneratörün iş sürekliliği planlarında belirtilen süre boyunca çalıştırılması için yeterli düzeyde yakıt bulundurulur.

A.8.3.4.5. Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

A.8.3.5. Kablolama Güvenliği

A.8.3.5.1. Güç ve iletişim kablolarının (ağ kabloları, güç kaynağı kabloları, telefon kabloları, vb.) fiziksel etkilere ve dinleme faaliyetlerine karşı korunması için önlemler alınır.

A.8.3.5.2. Kablolar binalar arası geçişte yeraltında, bina içlerinde kablo kanalları veya tavalar içerisinden geçirilir.

A.8.3.5.3. Karışmanın (interference) olmaması için güç ve iletişim kabloları fiziksel olarak ayrılır.

A.8.3.5.4. Hatalı bağlantıların olmaması için ekipman, kablolar ve prizler görülebilecek bir şekilde etiketlenir ya da işaretlenir.

A.8.3.5.5. Ağ tabanlı erişim kontrol sistemleri (NAC: Network Access Control) yoksa kullanılmayan uçlar için kenar anahtar ile dağıtım paneli arasına ara bağlantı kablosu takılmaz.

A.8.3.5.6. Kablolama yapılırken gelecekteki ihtiyaçlar dikkate alınarak yedekli olarak kablo çekilir.

A.8.3.5.7. Bina içindeki yerel alan ağı ana omurgası fiziksel olarak yedekli bir şekilde çalıştırılır.

A.8.3.5.8. Dağıtım panelleri ve kenar anahtarların konulduğu kabinler yetkisiz erişime karşı kilitli olarak bulundurulur.

A.8.3.5.9. Bahse konu kabinlerin de kesintisiz güç kaynağı ve jeneratör altyapısından faydalanması sağlanır.

A.8.3.6. Ekipman Bakımı

A.8.3.6.1. Kurumda kullanılmakta olan ekipmanların yıllık bakım planları oluşturulur. Planda yer alan ekipman listesinin envanter ile uyumlu olması kontrol edilir.

A.8.3.6.2. Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılır.

A.8.3.6.3. 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.

A.8.3.6.4. Bakım kayıtları düzenli olarak tutulur.

A.8.3.6.5. 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.

A.8.3.6.6. Ekipmanlar sigortalıysa, sigorta şartlarının sağlanması için gerekli özen gösterilir.

A.8.3.6.7. Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınır ve takip edilir.

A.8.3.7. Kurum Dışındaki Ekipmanın Güvenliği

A.8.3.7.1. 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.

A.8.3.7.2. Bu şekilde kullanılan ekipmanların ve kullanıcıların listesi oluşturulur ve takip edilir.

A.8.3.7.3. Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenir.

A.8.3.7.4. 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.

A.8.3.7.5. Tesis dışına çıkarılan ekipmanın gözetimsiz bırakılmamasına ve seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilir.

A.8.3.7.6. Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulur.

A.8.3.8. Ekipmanın Güvenli İmhası

A.8.3.8.1. 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.

A.8.3.9. Fiziksel ortamların taşınması

A.8.3.9.1. Güvenilir taşıma şekli ve kuryeler kullanılır.

A.8.3.9.2. Yönetim tarafından yetkili bir kurye listesi belirlenir.

A.8.3.9.3. Kuryelerin kimliğini kontrol eden süreçler geliştirilir.

A.8.3.9.4. Paketleme, içeriğin fiziksel hasarlardan yeterince korunmasını sağlayacak şekilde yapılır.

A.8.3.9.5. Hassas bilgiler elden teslim edilir veya kurcalanmaya karşı koruma için kilitli kaplar kullanılır.

A.9. İŞLETİM GÜVENLİĞİ

A.9.1. Yazılı İşletim Prosedürleri

A.9.1.1. Yapılan işlemlerin standart hale getirilmesi, iş sürekliliğinin sağlanması, kurumsal hizmetlerin sunumuna yönelik süreçlerin planlanması ve süreçlerin yazılı kurallara uygun olarak yerine getirilmesi gibi amaçlarla ihtiyaç duyulan işletim dokümanları hazırlanır.

A.9.1.2. Oluşturulan dokümanların onaylanması, yayınlanması, sürüm güncelleme ve/veya imha edilmesi süreçleri tanımlanır. Belge, kayıt ve dokümanlar için etkili bir yönetim sistemi oluşturulur ve sürekliliği sağlanır.

A.9.1.3. Dokümanlarda Kurumun ve Bakanlığın logosu, doküman adı, doküman kodu, sürüm numarası, yayın tarihi, sayfa numarası, hazırlayan, kontrol eden, onaylayan gibi başlık bilgileri bulunur.

A.9.1.4. Dokümanların yürürlük durumu ve güncel sürümlerinin takibi için (geçerli doküman listesi, iptal edilen ve değiştirilen doküman listesi hazırlamak gibi) kontroller oluşturulur.

A.9.1.5. Bilgi teknolojileri alanında; sistem ve ağların yönetimi, değişiklik kuralları, güvenlik gereklilikleri gibi süreçlerde işletim kurallarının yazılı hale getirilmesi ve ilgili kişilerin kolayca erişebileceği bir yöntemle muhafaza edilmesi gerekir.

A.9.1.6. Hazırlanacak dokümantasyon, işletimsel hataları engellemek, beklenmeyen sorunların ortaya çıkması durumunda sistemi kullanıcı bağımsız yeniden başlatabilmek, otomasyonun işletilemediği durumlarda süreci manuel olarak yürütebilmek gibi amaçlara cevap verecek şekilde düzenlenir.

A.9.1.7. Yazılı işletim prosedürleri, sunucu açma-kapatma, sistem kurulumu ve yapılandırılması, yedekleme, yedekten geri dönme gibi işletimsel konularda olabileceği gibi işletme sırasında oluşabilecek hatalara yanıt verme, bilgi güvenliği ihlal olaylarına müdahale, sistem destek programlarının kullanımı ile ilgili kısıtlamalar, güvenli imha yöntemleri gibi konularda da hazırlanabilir.

A.9.1.8. Sistem ana bileşenleri ve önemli süreçlere ilişkin kullanım kılavuzu niteliğinde dokümanların hazırlanması gerekir.

A.9.1.9. Denetimsiz veya yetkisiz olarak sistemlere erişilmesi ya da değişiklik yapılmasının engellenmesi için yazılı işletim prosedürlerinde işletim yöntemi, sorumlusu ve gerekli olan diğer detaylara mutlaka yer verilir.

A.9.2. Değişiklik Yönetimi

A.9.2.1. Bilgi teknolojilerindeki değişiklikler ile birlikte sistem, sunucu veya yazılım değişiklikleri veya güncellemeleri de kaçınılmazdır. Ancak bu değişikliklerin kontrolsüz bir şekilde yapılması, bilgi güvenliği açısından riskleri de beraberinde getirir.

İş sürekliliğine ilişkin açıklamalar kılavuzun A.13 (İş Sürekliliği) numaralı bölümünde açıklanmıştır. Değişikliklerin yönetimsel bir süreci takip etmemesi iş sürekliliğini tehdit eden bir unsurdur.

A.9.2.2. Değişiklik yönetiminin amacı, süreç ve yöntemi tanımlanmış olan bilgi sistemleri değişikliklerinin bilgi güvenliği prensipleri çerçevesinde gerçekleştirilmesini sağlamaktır. Bunun için en iyi yol, takip edilmesi gereken adımları tanımlayan yazılı işletim prosedürleri mantığıyla hazırlanan değişiklik yönetimi dokümanının oluşturulmasıdır.

A.9.2.3. Değişiklik Türleri

A.9.2.3.1. Yazılım Değişiklikleri

A.9.2.3.1.1. Kurumsal yazılım geliştirme yaşam döngüsü boyunca ele alınan değişikliklerdir.

A.9.2.3.1.2. İşleyiş hataları, kullanıcı gereksinimlerinin kodlamaya uygun olmaması, yeni ya da değişen istekler gibi nedenlerle yazılımlar üzerinde değişiklik yapma ihtiyacı oluşabilir.

A.9.2.3.2. Donanım ve Altyapı Değişiklikleri

A.9.2.3.2.1. Bilgi işlem ekipmanının kurulumu, değiştirilmesi, çıkarılması veya yeniden konumlandırılması, ilave donanım kurulumları, altyapıdan donanımın kaldırılması, sistem yapılandırma değişiklikleri ve lokasyon değişiklikleri, sistemler üzerinde yazılım ürünleri kurulumu, yaması, yükseltilmesi veya kaldırılması gibi nedenlerle değişiklik yapma ihtiyacı oluşabilir.

A.9.2.3.2.2. Talep tarihi, nedeni, değişiklik bilgisi, ilgili sistem/sistemler ve gerekli diğer bilgileri içeren talep yazısı düzenlenir ya da otomatik platform üzerinden hazırlanır. Sistem sorumlusu tarafından süreç ve teknik açıdan değerlendirilir. Birimler arası etkileşim, kullanılan ek kaynaklar, ne zaman/nerede/ne yapıldığı/kimin yaptığını içeren değişiklik kontrolü raporlaması kurumsal olarak belirlenen bir sistem üzerinden ya da detaylı raporlar aracılığıyla kayıt altına alınmalıdır.

A.9.2.3.3. Veri Tabanı Değişiklikleri

A.9.2.3.3.1. Veri tabanı objelerinin (kullanıcı, şema, tablo vb.) güncellenmesi, silinmesi veya yeni tablo, obje, kayıt yaratılması, veri tabanına yapılacak eklemeler, taşımalar, yeniden düzenlemeler gibi ihtiyaçlardan kaynaklanan değişikliklerin tek tek kaydedilerek, geçmişe dönük olarak saklanması, istenilen zamanda kontrol edilip incelenmesi ve raporlanması gerekir.

A.9.2.4. Değişiklik yapılırken, türünden bağımsız olarak aşağıdaki adımların takip edilmesi gerekir.

A.9.2.4.1. Değişiklik nedeninin yazılı olarak tanımlanması: Her değişiklik, değişiklik talep eden personel ya da uygulama sahibi tarafından değişim isteği talep yazısı veya varsa kullanılan standart form ile başlatılır.

A.9.2.4.2. Değişiklik etki analizi: Değişiklikler kurum varlıklarını (donanım, yazılım, ağlar, vb.) aynı zamanda süreçleri, hizmetleri, anlaşmaları, vb. hususları etkileyebilir. Bu nedenle değişikliğin maliyet, zaman ve risk açısından etkilerinin araştırılarak dokümante edilmesi gerekir. Değişiklik talebi öncelikle sistemlerin yürütülmesinden sorumlu personel tarafından analiz edilir. Değişimden etkilenecek diğer varlıklar, değişikliğin başlatılması veya sistemlerin kapatılması üzerindeki etkilerini, acil durum planları üzerindeki etkilerini, yedekleme gereksinimlerini, depolama gereksinimlerini ve işletim sistemi gereksinimlerini içeren değişiklik planının teknik bütünlüğünün ve performans/kapasite/güvenlik/işlevsellik üzerinde yapacağı etkilerin gözden geçirilmesi gerekir. Bu süreçte yedekten geri dönme testleri yapılarak değişiklik sürecinin geri çekilmesi durumu da planlanır.

A.9.2.4.3. Değişiklik onay süreci: Sorumlu personel tarafından yapılan değişiklik analiz çalışması yönetici onayına sunulur. Yönetici değişikliği onaylayabilir, reddedebilir ya da ek bilgi talep edebilir. Etkileşimde olan diğer sistem sorumlularının, kendi sorumlukları dâhilinde olan sistemler için gerekli önlemleri alması ve yazılı olarak önlemleri aldığını bildirmesi beklenir. Değişiklik onayı yöneticiden alındıktan sonra değişiklik çalışmalarına başlanır.

A.9.2.4.4. Değişimin planlanması ve test edilmesi: Kabul edilen değişikliklerin gerçekleştirilmesi için planlama yapılır. Tüm değişiklikler öncelikle test edilir. Test aşaması, kurumun teknoloji altyapısının tüm bileşenlerinin güvenilirliğini ve performansını sağlamak için test ve kalite güvencesinin sağlanması amacıyla gerçekleştirilir. Test aşaması yöneticiye rapor edilir ve bir sonraki adım olan uygulama safhasına geçip geçmemek konusunda onay alınır. Planlama, test ve uygulama safhaları teknolojik bir platform üzerinden ya da kayıtlar ile delil niteliğinde dokümante edilir.

A.9.2.4.5. Uygulama: Test edilen değişiklik, yönetici onayı ile uygulamaya alınır.

A.9.2.4.6. Uygulama sonrası inceleme: Değişikliğin istenen hedeflere ulaşıp ulaşmadığını sağlamak için uygulama sonrası gözden geçirme yapılır. Uygulama sonrası eylemler, değişikliği kabul etmeye, değiştirmeye veya geri almaya karar vermeyi içerir.

A.9.2.5. Aşağıdaki değişiklikler, operasyonel bir süreç gerektirmekle birlikte değişim yönetimi süreci gerekliliklerine dâhil değildir:

A.9.2.5.1. Günlük idari süreçte yapılan değişiklikler (parola sıfırlama, e-Posta grubuna kullanıcı ekleme/silme/gözden geçirme, dosya izni değişiklikleri)

A.9.2.5.2. Acil durum olağanüstü durum kurtarma

A.9.2.5.3. Sistem yapılandırmasında gerek duyulmadan yapılan masaüstü değişiklikleri.

A.9.3. Kapasite Yönetimi

A.9.3.1. Bilişim, bilginin işlenmesi, depolanarak saklanması, teknik araçlarla en hızlı ve kolay yoldan iletilerek bilgi akışının sağlanması demektir. Sağlık sistemi içerisinde her türlü bilginin iletimi ve etkin şekilde kullanımı için sağlık bilişim sistemlerine ihtiyaç duyulmaktadır. Sağlık hizmetleri 24 saat yaşayan ve çalışan teknolojik bileşenler üzerinde çalışmaktadır. Bu bileşenlerin en hızlı ve ekonomik şekilde kullanımı için kapasitenin izlenmesi ve yönetilmesi şarttır.

A.9.3.2. Kapasite yönetimi ile ayakta kalabilirlik/kullanılabilirlik (uyarılar ile hataların proaktif olarak düzeltilmesi ve iş sürekliliğinin sağlanması) ve ölçeklenebilirlik (yürütülen iş sürecinin veri hacmi büyüdükçe veri merkezinin ölçeklendirilmesi için gerekli kaynakların öngörülebilmesi) sağlanır.

A.9.3.3. Kapasite yönetimi, kaynakların izlenmesi, sistem performansını temin etmek için kapasite yönetiminin yapılması ve sürekli olarak gözden geçirilmesi şeklinde gerçekleştirilir.

A.9.3.4. Sistem izleme, bilgi teknolojileri altyapısı ile ilgili kritik iş uygulamalarının çalışır olmasını, performansının optimize edilmesini ve sistem güvenliğini sağlamak için gereklidir. Temel amaç, çeşitli ana bilgisayarların, ağ sistemlerinin ve depo ünitelerinin sorunsuz çalışmasını ve her sistem ve bileşenin ne kadar yüklü olduğunu ve ne kadar verimli kullanıldığını, darboğaza yol açan kullanımların sistem güvenliğini tehdit edip etmediğini bilmektir. Sistemlerin kapasitesinin izlenmesi bilgi güvenliğinin sağlanması ve iş sürekliliğinin sağlanması için girdi oluşturur.

A.9.3.5. İzleme için öncelikle kaynaklara karar verilmelidir. Uzun tedarik sürelerine ve yüksek maliyetlere sahip kaynaklar için özel ilgi gerekir. Bu nedenle önemli sistem kaynaklarının kullanımı özellikle izlenmelidir. Sunucular, veri tabanları, uygulamalar, web sunucuları ve web servisleri yanı sıra farklı türde uygulamalar ve daha birçok kaynaktan performans metriği alınabilir. Ancak, sürecin optimizasyonu için minimum; sanal ve fiziksel sunucular, veri tabanı ve ağ cihazları gibi kaynakların ayakta olup olmadığı, kapasite oranı (RAID grubunda kalan alan miktarı, depolama dizilerinde kullanılabilir disk alanı miktarı, kullanıcılara tahsis edilen dosya sistemi veya posta kutusu kotası miktarı) ve performans (CPU -İşlemci- kullanımı, bellek kullanımı, disk I/O kullanımı) ve ağ güvenliği (sisteme hatalı giriş denemeleri, yetkisiz veri tabanı yapılandırması, güvenlik ihlalleri) açısından izlenmesi gerekir.

A.9.3.6. Dosya sunucularında yeterli alanın azalması idari dikkat için uyarı gerektirirken, bellek hatası, disk hatası gibi alarmlar derhal müdahale gerektirir. Bu nedenle izlenen sistemlere ilişkin minimum kabul edilebilir eşik değerlerin belirlenmesi ve uyarı önceliklerinin belirlenmesi gerekir. (Örneğin; “90 dakika boyunca işlemci kullanımı %90’ın üzerinde olursa kritik alarm üret” ya da “veri tabanı kullanım oranı %80’i geçerse yöneticiye bilgi ver” gibi)

A.9.3.7. Gelecekteki sistem ihtiyaçları ve ileriye yönelik planlanan yeni iş uygulamaları mevcut kapasite göz önüne alınarak değerlendirilir. Mevcut kapasitenin optimizasyonu için disk alanından saklanma süresi dolan verinin silinmesi, uygulama mantığının ya da veri tabanı sorgularının optimize edilmesi, kaynak tüketen hizmetlerden kritik

olmayanlar için reddetme ya da bant genişliği sınırlaması gibi çözüm yöntemleri uygulanabilir.

A.9.4. Geliştirme, Test ve İşletim Ortamlarının Ayrılması

A.9.4.1. Yanlışlıkla yapılan değişiklikler, yapılandırma uyumsuzlukları veya yetkisiz erişim gibi riskleri azaltmak için geliştirme, test ve işletim (canlı) ortamları mutlaka birbirinden ayrılır.

A.9.4.2. Bu ortamlar aşağıdaki hususlar dikkate alınarak değerlendirilir;

A.9.4.2.1. Yazılım geliştirme, test ve işletim ortamları, farklı etki alanlarında, farklı sistem ve bilgisayarlarda ve hatta verinin hassasiyetine göre farklı ağlarda çalıştırılır.

A.9.4.2.2. İstisnai durumlar dışında, testler işletimdeki sistemler üzerinde yapılmaz.

A.9.4.2.3. İşletimdeki sistemler üzerinden derleyici, editör ve diğer geliştirme araçları veya sistem programlarına erişim izni verilmez.

A.9.4.2.4. Geliştirme, işletim ve test sistemi için farklı kullanıcı profilleri ve kimlik doğrulama anahtarları kullanılır.

A.9.4.2.5. Test ortamında gerçek veriler kullanılmaz.

A.9.4.2.6. Hassas verilerin, gerçek ortamla eşdeğer bir test ortamında kontrol edilmeden işletime alınmaması gerekir.

A.9.5. Etki Alanı Kurulum ve Yönetimi

A.9.5.1. Yönetilebilirlik, ölçeklenebilirlik, genişletilebilirlik, güvenlik entegrasyonu, diğer etki alanları ile birlikte çalışabilme, güvenli kimlik doğrulama ve yetkilendirme, grup politikaları ile yönetim, DNS ve DHCP gibi servislerle birlikte çalışabilme gibi avantajları nedeniyle etki alanları kurulur ve işletilir.

A.9.5.2. Merkez teşkilata bağlı birimlerin etki alanı hizmetleri SBSGM tarafından işletilen merkezi etki alanı vasıtasıyla sağlanır.

A.9.5.3. SBSGM tarafından sunulan merkezi etki alanı ve veri merkezi/sunucu barındırma ile ilgili hususlar, Kılavuzun A.6.5 (Merkezi Aktif Dizin ve e-Posta Sistemine Erişim) ve A.6.6 (Veri Merkezi ve Sunucu Barındırma Hizmetlerine Erişim) numaralı maddelerinde açıklanmıştır.

A.9.5.4. Bakanlık bağlı kuruluşları ve il sağlık müdürlüklerinin her birinin müstakil birer etki alanı ile yönetilmesi hedeflenir. Geçmiş dönemlerde çeşitli nedenlerle birden fazla etki alanı kuran ve çalıştıran birimlerce, söz konusu etki alanlarının birleştirilmesi, birleştirilemiyorsa birlikte çalışması için gerekli önlemler alınır.

A.9.6. Sunucu ve Sistem Güvenliği

A.9.6.1. Sunucuların ve sistemin güvenliğini sağlamak için gerekli güvenlik koşullarının tanımlandığı, güvenlik ilkelerinin belirlendiği "Sistem Güvenlik Politikası" oluşturulur.

A.9.6.2. 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.

A.9.6.3. 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.

A.9.6.4. 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.

A.9.6.5. 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.

A.9.6.6. Sunuculara ve uygulamalara erişim sağlayan kullanıcıların erişim hakları, erişimlerin iptal edilmesi veya erişim yetkisinin değiştirilmesi gibi kuralların tanımlandığı bir "erişim matrisi" oluşturulur.

A.9.6.7. Sunucularda zorunlu kalmadıkça "administrator" ve "root" gibi genel sistem hesapları kullanılmaz.

A.9.6.8. Sunuculara yapılan erişimlerin raporlanması, mesai saati dışındaki erişimlerin işaretlenmesi gibi detaylar gözlenir. Kullanıcılara olması gerekenden fazla yetki tanımlanmaz.

A.9.6.9. 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.

A.9.6.10. 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.

A.9.6.11. Sistem hesaplarına ait parolalar için Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen yönetici hesaplarına ilişkin kurallar dikkate alınır.

A.9.6.12. 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.

A.9.6.13. Sunucuların güvenliğini sağlayabilmek için kullanılmayan uygulamalar veya servisler kapatılır. Gerekli servis ve hizmetler dışında başka bir servis çalıştırılmaz.

A.9.6.14. 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.

A.9.6.15. Sertifika kullanım süresi, son kullanım süresi yaklaşan sertifikaların takibi gibi işlemler hazırlanacak bir sertifika takip listesi vasıtasıyla takip edilir.

A.9.6.16. 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.

A.9.6.17. Sunucuda depolanan veriler, işletim sisteminin çalıştığı disk bölümünden farklı bir disk bölümünde tutulur.

A.9.6.18. Sunucuların arka planda çalışan servisleri ile birlikte o servislerinde kullandığı portlar kontrol edilir. Gereksiz portlar kapatılır. Mümkün olduğu surette uygulamaların varsayılan portları değiştirilir.

A.9.6.19. 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.)

A.9.6.20. 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.

A.9.6.21. 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.

A.9.6.22. Mutlaka zorunlu değil ise sunucuların internete erişimleri kapatılır.

A.9.6.23. 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.

A.9.6.24. 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.

A.9.6.25. Kullanıcıların bilgisayarlarının saat ve tarih ayarlarını değiştirmesi engellenir.

A.9.6.26. Virüs vb. zararlı yazılımlardan korunmak ve kurumsal bilgilerin kurum dışına sızmasını engellemek amacıyla gerekiyorsa USB bellek gibi taşınabilir cihazların kullanımı engellenir.

A.9.6.27. Kullanıcıların ".exe/.bat" gibi çalıştırabilir dosyaları çalıştırmaları engellenir.

A.9.6.28. 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.

A.9.6.29. Kullanıcıların bilgisayar ayarlarını değiştirmelerini önlemek amacıyla denetim masasına ve C dizinine erişimleri engellenir.

A.9.6.30. Kullanıcıların DNS adreslerini değiştirmeleri engellenir.

A.9.6.31. Sunuculara yapılacak uzak masa üstü bağlantılarında Kılavuzun A.6.14 (Uzaktan Çalışma ve Erişim) maddesinde belirtilen hususlara dikkat edilir.

A.9.6.32. 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)

A.9.6.33. 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.

A.9.6.34. 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.

A.9.6.35. 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.

A.9.6.36. 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.

A.9.6.37. Tüm bilgisayarlar lisanslı anti-virüs yazılımı ile korunur. Anti-virüs yazılımının virüs veritabanı güncel tutulur.

A.9.6.38. 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.

A.9.6.39. 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.

A.9.6.40. 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.

A.9.6.41. 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.

A.9.6.42. 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.

A.9.6.43. Sunucuların üretici tarafından tavsiye edilen/teknik dokümanlarında belirtilen süreler dikkate alınarak yıllık bakım planları hazırlanır. Bakımlar yetkili uzmanlar tarafından yapılır ve kayıt altına alınır.

A.9.6.44. 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.

A.9.7. Ağ İşletim Güvenliği

A.9.7.1. Ağ mimarisi ve aktif ağ cihazlarının yönetimi, güvenlik ilke ve kuralları, erişim haklarının yazılı olduğu "Ağ Güvenliği Politikası" oluşturulur.

A.9.7.2. 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.

A.9.7.3. 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.

A.9.7.4. 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.

A.9.7.5. 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.

A.9.7.6. 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.

A.9.7.7. 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.

A.9.7.8. Güvenlik ve ağ cihazlarına yapılacak uzaktan erişimler için yönergenin A.6.10 maddesinde belirtilen hususlara dikkat edilir.

A.9.7.9. Uzaktan erişim verilen kullanıcılara bağlantı zamanı ve süresi ile ilgili kısıtlamalar getirilir. Kurumdaki görevi gereği kullanıcıların bağlantı süreleri farklı olabilir.

A.9.7.10. Güvenlik duvarları, ana omurga cihazları gibi kritik sistemlere yapılacak erişimler için yerel kullanıcılar yerine ikincil bir kimlik doğrulamasının kullanılması tavsiye edilir.

A.9.7.11. 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.

A.9.7.12. 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.

A.9.7.13. Güvenlik ve ağ cihazlarının kurulumunu, yapılandırmasını ve sistemde karşılaşılan hataları gidermek için izlenilen yöntemleri anlatan kılavuz dokümanları hazırlanır. Bu kılavuzlardan bilgi havuzu oluşturulur.

A.9.7.14. 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.

A.9.7.16. 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.

A.9.7.17. 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.

A.9.7.18. Telnet gibi güvensiz bağlantılara izin verilmez. SSH protokolünü kullanan bağlantılarda SSH Ver2 kullanılır.

A.9.7.19. 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.

A.9.7.20. Güvenlik duvarı ve ağ cihazları için kontrol listeleri (ACL, güvenlik ürünleri erişim kısıtlaması vb.) tanımlanır.

A.9.7.21. Güvenlik ve ağ cihazlarının fiziksel güvenliğini sağlamak için gerekli tedbirler alınır.

A.9.7.22. 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.

A.9.7.23. Güvenlik ve ağ cihazları üzerindeki gereksiz ve kullanılmayan tüm servisler kaldırılır.

A.9.7.24. Cihazları kaba kuvvet saldırılarından korumak için 5 (beş) yanlış deneme sonrasında oturum belirli bir süre kilitlenecek şekilde ayarlama yapılır.

A.9.7.25. Doğru yapılandırılmış zaman damgası için cihazlar NTP sunucu ile senkronize olarak çalıştırılır.

A.9.7.26. 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.

A.9.7.27. 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.

A.9.7.28. 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.

A.9.7.29. Dış ağdan sunucular üzerindeki servislere, sunucu yönetim protokolleri (RDP, SSH) ile erişim engellenir. Sunucular, sadece belirli portlardan erişim sağlanacak şekilde yapılandırılır.

A.9.7.30. Kurum bünyesinde barındırılan ve hizmet veren uygulamalara HTTPS üzerinden bağlanılır.

A.9.7.31. Güncel atak metotlarından korunmak için saldırı tespit ve önleme sistemleri, ağ hizmetlerine erişim ilkelerinin belirlenmesi için Güvenlik Duvarı kullanılır.

A.9.7.32. 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:

A.9.7.32.1. Basın yayın organlarını takip ederek idareye raporlamakla sorumlu personel haricindeki tüm personelin dizi, film ve TV erişimlerinin kapatılması,

A.9.7.32.2. Kurum sosyal medya hesaplarını yönetmekle sorumlu personel dışındaki tüm personelin Facebook, Twitter, İnstagram vb. uygulamalara erişimlerinin engellenmesi veya bant genişliği sınırlaması yapılması,

A.9.7.32.3. Youtube, Vimeo, Dailymotion gibi platformlarda erişimlerle ilgili olarak sadece ihtiyaç duyan personele izin verilmesi, bu yapılamıyorsa bu platformlara erişimlere bant genişliği sınırlaması yapılması önerilir.

A.9.8. Veri Tabanı Güvenliği

A.9.8.1. Kılavuzun A.6.1 (Erişim Kontrol Politikası) maddesi gereği hazırlanacak Erişim Kontrol Politikasının bir parçası olarak; veri tabanına erişim sağlayan kullanıcıların erişimlerini tanımlayan, veri tabanında hesap oluşturma kurallarını belirleyen, kullanıcı kaydı girme, kullanıcı kaydı silme gibi erişim yetkilerinin tanımlandığı bir erişim dokümanı oluşturulur. Verilen erişim yetkileri erişim politikasında belirtilen aralıklarla kontrol edilir.

A.9.8.2. SBSGM tarafından merkezi bir hizmet olarak sunulan veri tabanı hizmetlerinden yararlanmak için yapılması gereken işlemler bu kılavuzun A.6.7 (Merkezi VTYS'ye Erişim) maddesinde açıklanmıştır.

A.9.8.3. SBYS yazılımlarının işletimi başta olmak üzere bağlı kuruluşlar, il sağlık müdürlükleri ve sağlık hizmet sunucuları tarafından tesis edilen VTYS'ler için de A.6.7 (Merkezi VTYS'ye Erişim) maddesinde belirtilen süreçlere benzer süreçler oluşturulur.

A.9.8.4. Veri tabanında kullanıcı hesabı oluşturma ve kullanıcılara erişim yetkisi tanımlama talepleri resmi yazı ile yapılır.

A.9.8.5. Kurumun veri tabanına erişen kullanıcılar (veri tabanı yöneticileri, uygulama geliştiriciler, yedekleme operatörleri vb.) ile mutlaka gizlilik sözleşmesi imzalanır ve erişim hakkı edindikten sonra almış olduğu sorumluluklar kullanıcıya bildirilir.

A.9.8.6. Veri tabanında sorgu seviyesindeki erişim denetimleri belirli aralıklar ile kontrol edilir. Erişim denetiminin tablo seviyesinde mi yoksa satır/sütun seviyesinde mi olduğu kullanıcının rolüne göre belirlenir ve kurum erişim kontrol politikasında belirtilen kurallar dâhilinde yetki tanımlaması yapılır.

A.9.8.7. Veri tabanına erişim sağlayan kullanıcılar için kimlerin nereye erişim sağlayacağı gibi erişimlerin sınıflandırılması yapılır. Zaman içerisinde değişen kullanıcı erişim yetkileri, audit (izleme/denetim) kurallarıyla takip edilir.

A.9.8.8. Veri tabanına bağlanan kullanıcıların, görüntülediği verileri aktarma veya tablo dışına çıkarma gibi yetkileri/işlemleri için kontrol mekanizmaları sağlanır. Verilerin elektronik kopyasının alınması gerekli ise verilen yetkiler gözden geçirilir.

A.9.8.9. Veri tabanına erişen ortak kullanıcı hesaplarına izin verilmez.

A.9.8.10. Uygulama sunucuları üzerinden gelen veri tabanı kullanıcılarının, sadece ilgili uygulama sunucularından bağlantı sağlaması, okuma, yazma, silme ve değiştirme yetkileri olması; yeni tablo/nesne oluşturma, şema değişikliği yapma gibi yetkilerinin kaldırılması gerekir.

A.9.8.11. Benzer şekilde veri tabanı sunucularına kod geliştiren kullanıcı için oluşturulan veri tabanı kullanıcılarının da yeni tablo/nesne oluşturma, şema değişikliği yapma gibi yetkilerinin olması bunun dışında canlı/gerçek veriye erişerek bu veriler üzerinde okuma, yazma, silme ve değiştirme gibi yetkilerinin olmaması gerekir.

A.9.8.12. Veri tabanında yer alan tüm kullanıcı hesaplarının durumlarına bakılır. Veri tabanında oluşturulmuş isimsiz hesaplar, geçmişte açılmış fakat kullanılmayan hesaplar özellikle kontrol edilir. Kurumdan ayrılan çalışanlara ait veri tabanı hesapları kilitlenir veya silinir.

A.9.8.13. Veri tabanına son girilen başarılı ve başarısız oturum bilgilerinin giriş kayıtları tutulur.

A.9.8.14. Veri tabanında kritik rollere sahip kullanıcıların yetkileri ve görevleri, kurum erişim kontrol politikasında belirtilen aralıklarla düzenli olarak kontrol edilir. Varsa gereğinden fazla verilmiş olan yetkilerin kaldırılması sağlanır.

A.9.8.15. “Select” yetkisi dışında yetkisi olan kullanıcılar ayrıştırılarak bu kullanıcılar kurum erişim kontrol politikasında belirtilen aralıklarla kontrol edilir. Veri tabanı sunucuları için kod geliştiren kullanıcılar dışında diğer kullanıcıların veri tabanına bağlanıp sorgu yapmaları engellenir. (örnek; Kullanıcıların tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmaları engellenir.)

A.9.8.16. Veri tabanında “sysdba, sysoper, admin” yetkisine sahip olan kullanıcı hesaplarının kontrolleri yapılır. En yetkili kullanıcıların veri tabanında yaptığı işlemler kayıt altına alınır.

A.9.8.17. SQL Server kurulumu ile gelen varsayılan “SA” kullanıcısı pasife alınır.

A.9.8.18. Veri tabanında sahip olduğu yetkileri bir başka kullanıcıya (“with admin option” ya da “with grant option” gibi seçeneklerle) devretme yetkisi olan kullanıcı hesapları özellikle takip edilir. Mutlak zorunluluk yok ise kullanıcılara bu tür yetkiler verilmez.

A.9.8.19. “Yedek alabilme” hakkına sahip kullanıcı hesapları, kurum erişim kontrol politikasında belirtilen aralıklarla kontrol edilir.

A.9.8.20. Veri tabanları arasında veri aktarımı yapmak için kullanılan database linkleri “private” olarak oluşturulur. Güvenlik açığı teşkil etmesi nedeniyle “public” olarak oluşturulmuş linkler, “private” olarak değiştirilir. Tüm linkler belirli aralıklarla kontrol edilir.

A.9.8.21. Güvenlik paketleri ve yamalar, kontrollü olarak uygulanır. Sistemde hangi yamaların uygulanıp uygulanmadığı kontrol edilir.

A.9.8.22. Veri tabanı güncelleştirmeleri takip edilir. Sistem üzerinde kod çalıştırabilen ve yetki yükseltilebilen zafiyetlerin giderilmesine öncelik verilir.

A.9.8.23. Yama ve güncelleme çalışmaları yapılmadan önce tüm ilgili kişi ve kurumlara bildirimde bulunulur ve sonrasında ilgili uygulama kontrolleri gerçekleştirilir.

A.9.8.24. Veri tabanı kullanıcısının kaynakları, limit parametreleri belirli aralıklarla kontrol edilir.

A.9.8.25. Veri tabanına yapılan erişimlerde kaba kuvvet saldırılarına karşı, kullanıcı hesabının kitlenmesi için giriş kontrolü yapılır (5 (beş) yanlış deneme sonrası kullanıcı hesabının kilitlenmesi gibi).

A.9.8.26. İstemci, veri tabanı ve uygulama sunucuları arasındaki ağ trafiği şifrelenir. Veri tabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar kullanılır.

A.9.8.27. Veri tabanı sunucusu sadece SSH, RDP, SSL ve veri tabanının orijinal yönetim yazılımına açık tutulur. Bunun dışında FTP, TELNET vb. gibi açık metin şifreli bağlantılara kapatılır.

A.9.8.28. Veri tabanına dinamik içerikli web sitelerinden gelen istekler için Kılavuzun A.9.9 (Yazılım Güvenliği) maddesinde belirtilen güvenlik tedbirleri alınır.

A.9.8.29. Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılarak uygun yedekleme politikaları oluşturulur. Yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli olarak alınması kontrol altında tutulur.

A.9.8.30. Veri tabanından alınan yedeklerin başarılı olarak alındığı iz kayıtları üzerinden kontrol edilir. Kurumun bilgi güvenliği alt komisyonu tarafından belirlenecek yedekleme politikaları uyarınca geri dönüş testleri yapılır.

A.9.8.31. Veri tabanında parola politikasında kullanılan parametrelerin tanımları ve varsayılan değerleri değiştirilir. Veri tabanı üzerinde oluşturulan her kullanıcı profili için parola parametrelerinin tanımlanması gerekir.

A.9.8.32. Veri tabanı kullanıcı profillerine göre tanımlanması gereken diğer parola parametreleri ve önerilen değerleri şu şekildedir:

A.9.8.32.1. Kullanıcı hesabının kilitlenmesi için gerekli maksimum başarısız oturum açma girişim sayısı 5 (beş),

A.9.8.32.2. Parolanın geçerli sayılacağı maksimum gün sayısı 90 gün,

A.9.8.32.3. Kullanıcı parola süresi dolmadan önce kullanıcıya parolasını değiştirmesi için hatırlatma gönderme süresi 7 (yedi) gün,

A.9.8.32.4. Parolanın tekrar kullanılabilmesi için tanımlanması gereken minimum farklı parola sayısı 3 (üç),

A.9.8.32.5. Parolanın tekrar kullanılabilmesi için geçmesi gereken minimum süre 90 gün,

A.9.8.32.6. Maksimum sayıdaki başarısız oturum açma girişimlerinden sonra, hesabın ne kadar süreyle kilitli kalacağı süre 10 (on) dakika.

A.9.8.33. Veri tabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlantı yapılır.

A.9.8.34. Veri tabanı kullanıcıları ilk kez tanımlanan hesaplarıyla oturum açtıklarında parola değiştirmeye zorlanır.

A.9.8.35. Kullanılan uygulamaların kurulumu ve yapılandırmasının anlatıldığı kılavuz dokümanları hazırlanır. (Oracle Kurulum, SQL Kurulum, bağlantı dokümanları gibi)

A.9.8.36. Mümkün olduğu takdirde Oracle Listener servisinin varsayılan portu olan 1521 portunun değiştirilmesi ve parola ile bu servisin güvenlik kontrolünün sağlanması tavsiye edilir.

A.9.8.37. Mümkün olduğu takdirde veri tabanının MySQL servisi 3306, MongoDB 27017 servisleri gibi varsayılan portlarının, güvenlik tedbirlerini artırmak amacıyla port numaralarının değiştirilmesi tavsiye edilir.

A.9.8.38. Veri tabanı sunucusu üzerindeki gereksiz olan servisler kapatılır.

A.9.8.39. Sistem üzerinde bilgi toplanmasına neden olabilecek başlık bilgileri ve hata mesajlarının açık bırakılması önlenir.

A.9.8.40. Veri tabanı yönetim sistemlerinin, alanında uzman ve eğitim almış personel tarafından yönetilmesi sağlanır.

A.9.9. Yazılım Güvenliği

A.9.9.1. Uygulama yazılımlarına erişen kullanıcıların erişim yetkileri ve rol yönetimi yazılı olarak tanımlanır. Kullanıcı erişim talepleri onay mekanizmasından geçirilir.

A.9.9.2. 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.

A.9.9.3. Uygulamalarda yönetici ve kullanıcı hesap yetkilerinin tanımlanması, her proje için yazılı kurallar doğrultusunda yapılır. Yetki tanımlanan kullanıcıların yetki kısıtlamaları belirli aralıklarla takip edilir.

A.9.9.4. Uygulama yazılımlarında roller oluşturularak erişim kontrol (yetkilendirme) matrisi oluşturulur. Rol tabanlı yetkilendirmeler yapılır. Kullanıcıların sadece yetkilendirildiği rol kapsamındaki verilere erişim sağlayacak şekilde düzenleme yapılır.

A.9.9.5. 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.

A.9.9.6. Kurulumla birlikte gelen varsayılan (default) kullanıcı hesapları ve rolleri silinir veya pasif hale getirilir.

A.9.9.7. Güvenlik fonksiyonları ile alakalı görüntüleme ve yapılandırma sayfalarına sadece güvenlikten sorumlu ve yetkilendirilmiş hesaplar tarafından erişim yapılır. Kullanıcılara, sadece yetkisi ve izni olan servisleri ve verileri gösterecek şekilde ayarlama yapılır.

A.9.9.8. Program kaynak kütüphaneleri işletimdeki sistemler dışında ayrıca farklı bir yerde saklanır. Kaynak kodlara erişim yapan hesaplar yazılı olarak tanımlanır ve bu hesapların hareketleri izlenir. Program kaynak kütüphanelerine erişim yapan kullanıcıların tüm erişimlerinin iz kayıtları tutulur.

A.9.9.9. Geliştirme ve test işlemlerinin, kullanıma aktarılmadan önce belirli kuralları kapsadığı yazılı bir doküman hazırlanır. Geliştirme ve test ortamları esas çalışma ortamından ayrılır. Yazılım projelerinde yapılan değişiklikler öncelikle test ortamında kontrol edilir, gerekli test aşamaları tamamlandıktan sonra yapılan düzenlemeler canlı ortama aktarılır. Test işlemlerinde gerçek kişisel veriler kullanılmaz. Bütün yazılım projeleri için test senaryoları hazırlanır ve testlerde çıkan hataların kontrolü yazılı olarak tutulur.

A.9.9.10. Yazılım paketlerinde yapılacak değişiklik öncesi test hazırlık sürecinde roller ve sorumluluklar belirlenir. Değişiklik talepleri alındıktan sonra onay merciinden geçirilir. Orijinal yazılımda değişiklik gerekli ise yazılımın orijinal hali saklanır. Versiyon değişiklikleri (Minor ve Major değişiklik gibi) kayıt altına alınır ve değişikliklerde risk değerlendirmesi önceden yapılır.

A.9.9.11. İş sürekliliğini sağlamak adına uygulamaların hata kayıtlarını ve çözümlerini içeren bir hata havuzu oluşturulur.

A.9.9.12. Yedekleme politikası uyarınca bilgi ve yazılımlar yedeklenir. Yedekler belirlenen kurallar doğrultusunda test edilir.

A.9.9.13. Uygulama yazılımları, kullanıcıların parolasını parola politikasına göre oluşturması yönünde zorlayıcı şekilde tasarlanır. Yazılımlar kullanıcıya parolasını değiştirme yetkisi verecek şekilde yapılandırılır.

A.9.9.14. Uygulama yazılımları kullanıcıya parola kurtarma seçeneği ile kullanıcının yeniden parola oluşturmasına olanak sağlayacak şekilde tasarlanır. Kurtarma parolası kullanıcı tarafından sisteme tanımlanmış olan kurumsal e-Posta adresine veya cep telefonuna gönderilecek parolayı sıfırlama gibi bir fonksiyon sunulur.

A.9.9.15. Kullanıcılara tanımlanan geçici parola, güçlü parola politikasına göre ve sınırlı geçerlilik süresine göre verilir.

A.9.9.16. Kurumda kullanılan uygulamalarda tanımlı süre boyunca aktif olmayan oturumlar otomatik olarak kapatılır ve yazılım projeleri türüne göre oturum süreleri belirlenir.

A.9.9.17. Kullanıcı sayısının fazla olduğu ve yoğun olarak kullanılan sistemlerde kimlik yönetim servislerinin yük dengeli (load-balancer) olarak çalıştırılması tavsiye edilir.

A.9.9.18. Uygulama yazılımları başka kaynaklara bağlanırken (veri tabanı vb.) erişim için kullandığı parolalar şifrelenmiş (encrypted) bir halde saklanır. Parolaların şifrelerini çözmek için gereken anahtarlar, yetkisiz erişimden korunur. Parolalar hiçbir durumda uygulamanın kaynak kodu içinde saklanmaz. Son kullanıcıların ya da istemci durumundaki uygulama servislerini kullanan diğer sistemlerin kimliklerini doğrulamak için kullandığı parolalar kriptografik özet halinde (hash) saklanır.

A.9.9.19. Yazılım projelerinde teknik açıkla ilgili kontroller sağlanır. Zafiyetlerin yayınları takip edilir. Uygulama projelerinde güvenliği sağlamak için yazılımlar KLVZ-EK-17 Güvenli Yazılım Geliştirme Kontrol Listesi ile kontrol edilir.

A.9.9.20. Oturum açılması gereken uygulamalarda belirli sayıda yanlış kimlik doğrulama denemesinden sonra captcha uygulaması ile kullanıcıdan doğrulama talep edilir. Belirli sayıda hatalı kimlik doğrulama denemesinin ardından hesap geçici olarak kilitlenir. (Örneğin 5 yanlış deneme)

A.9.9.21. Son kullanıcı ile uygulama sunucusu arasındaki trafik şifrelenir. SSL protokolünün güncellenmiş son sürümü kullanılır.

A.9.9.22. Uygulama yazılımlarında kullanıcıya dönen hata sayfalarında, kullanıcıya sistem hakkında bilgi verilmemesi ve hata kontrolü yapılması (versiyon bilgisi gibi) için tedbir alınır.

A.9.9.23. Uygulama yazılımları kullanıcıya az bilgi ile geri bildirim yapacak şekilde tasarlanır. Kullanıcıya dönen hata sayfalarında “kullanıcı adı yanlış” gibi hatanın nerden kaynaklı olduğunu söyleyen bilgiler değil de “kullanıcı adı veya parola yanlış” gibi hata kaynağını göstermeyen bilgiler verilir.

A.9.9.24. Kullanıcı ve yönetici hesap hareketlerinin iz kayıtları tutulur. İz kayıtları yetkisiz kişiler tarafından değiştirilmeye karşı korunur.

A.9.9.25. KVKK'nın 2018/10 sayılı kararı uyarınca özel nitelikli kişisel verilerin işlendiği yazılımlarda;

A.9.9.25.1. Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

A.9.9.25.2. Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

A.9.9.25.3. Veriler üzerinde gerçekleştirilen tüm hareketlerin iz kayıtlarının bir başka ortamda güvenli olarak saklanması,

A.9.9.25.4. Verilerin bulunduğu ortamlara (örneğin VTYS sunucuları) ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin (sızma testleri) düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

A.9.9.25.5. Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması (sızma testleri, kaynak kod analizleri), test sonuçlarının kayıt altına alınması,

A.9.9.25.6. Verilere uzaktan erişim gerekiyorsa en az 2 (iki) kademeli kimlik doğrulama sisteminin sağlanması gerekir.

A.9.10. Sunucu/Sistem Odası Güvenliği

A.9.10.1. 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.

A.9.10.2. Bir sistem odasının en temel özellikleri;

A.9.10.2.1. 7×24 kesintisiz çalışabilirlik,

A.9.10.2.2. Güç yönetimi ve ağ bağlantılarında farklı kanallardan yedeklilik,

A.9.10.2.3. Ağ güvenliği, fiziksel erişimlerde yetkilendirme ve görüntülü gözetleme,

A.9.10.2.4. Çevre şartlarının kontrol altında tutulması,

A.9.10.2.5. Yangına karşı duman algılama gibi erken uyarı sistemleridir.

A.9.10.3. Sistem odasının kesintisiz çalışmasına; sıcaklığın normal aralığın dışına çıkması, yangın, su baskını, deprem, yetkisiz kişilerin sistem odasına girmesi, odadaki herhangi bir cihazın arızalanması engel olabilir. Tüm bu olumsuz durumların yaşanmasının önlenmesi ve hizmetlerin sağlıklı çalışabilmesi için standartlara (ANSI/TIA/EIA-942 standardı gibi) uygun bir sistem odası oluşturulması ve ana bilgisayar, sunucu ve diğer hizmet sürecindeki bileşenlerin güvenli olarak bu alanlarda konumlandırılması gerekir. Bahse konu "ANSI/TIA-942 Standardı", veri merkezlerinin sınıflandırılabildiği 4 (dört) tip katman içerir. Her aşama kendisinden bir önceki aşamada bulunması gereken koşulları sağlamalıdır. Bu katmanlar şunlardır;

A.9.10.3.1. Katman-1 Temel Altyapı (Tier-1) : Tek bir kapasiteye sahip bileşenlere ve bilgisayar ekipmanına hizmet veren tek, yedeksiz bir dağıtım yoluna sahip bir veri merkezidir. Fiziksel olaylara karşı sınırlı korumaya sahiptir.

A.9.10.3.2. Katman-2 Yedek Kapasite Bileşen Altyapı (Tier-2): Yedek kapasite bileşenlerine ve bilgisayar ekipmanına hizmet veren tek, yedeksiz bir dağıtım yoluna sahip bir veri merkezidir. Fiziksel olaylara karşı gelişmiş koruma sağlar.

A.9.10.3.3. Katman-3 Eşzamanlı Olarak Erişilebilir Altyapı (Tier-3): Yedek ekipman bileşenlerine ve bilgisayar ekipmanına hizmet veren çoklu bağımsız dağıtım yollarına sahip bir veri merkezidir. Tipik olarak, sadece bir dağıtım yolu bilgisayar ekipmanına her zaman hizmet eder. Site aynı anda sürdürülebilmektedir, bu da dağıtım yolunun bir parçası olan unsurları içeren her bir kapasite bileşeninin, bilgi ve iletişim teknolojilerinin sahip olduğu yeteneklerini son kullanıcıya zarar vermeden planlı bir şekilde çıkarılabileceği/değiştirilebileceği/servis edilebileceği anlamına gelir. Çoğu fiziksel olaylara karşı korumaya sahiptir.

A.9.10.3.4. Katman-4 Arıza Toleranslı Altyapı (Tier-4): Tümü aktif olan bilgisayar ekipmanına hizmet veren yedek kapasite bileşenleri ve çoklu bağımsız dağıtım yollarına sahip bir veri merkezidir. Veri merkezi, kurulum sırasında arıza süresine neden olmadan eşzamanlı bakım ve 1 (bir) arızaya izin vermektedir. Neredeyse tüm fiziksel olaylara karşı korumaya sahiptir.

A.9.10.4. Sistem odası ile ilgili aşağıdaki ölçütlere dikkat edilmesi gerekir;

A.9.10.4.1. 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.

A.9.10.4.2. 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.

A.9.10.4.3. 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.

A.9.10.4.4. 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.

A.9.10.4.5. 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.

A.9.10.4.6. 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.

A.9.10.4.7. 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.

A.9.10.4.8. **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.

A.9.10.4.9. **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.

A.9.10.4.10. **Deprem Kontrolü:** Kabinler yere veya duvara sabitlenmeli, kabinler arası yerleşim deprem ve havalandırma şartlarına uygun tasarlanmış olmalı, deprem yönetmeliği şartları sağlanmalıdır.

A.9.10.4.11. **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.

A.9.10.4.12. **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.

A.9.10.4.13. **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.

A.9.11. Tıbbi Cihaz Güvenliği

A.9.11.1. Hastanelerin Bilgi İşlem/Biyomedikal Birimleri Tarafından Takip Edilmesi Gereken Hususlar[1]

A.9.11.1.1. Tıbbi cihazlara fiziksel erişim sadece yetkili kişiler ile sınırlandırılır. Cihazların çalınmasını, kurcalanmasını engelleyebilmek için düzenli olarak güvenlik kontrolleri yapılır.

A.9.11.1.2. Tıbbi cihaz envanteri çıkarılır. Cihazlara ait temel bilgiler tespit edilerek kullanıldığı yer ile birlikte kayıt altına alınır.

A.9.11.1.3. Tedarik safhasında bilgi güvenliği yapılandırma imkânı sağlayan cihazlar tercih edilir ve bu husus hazırlanacak tıbbi cihaz tedarik şartnamelerine konulur.

A.9.11.1.4. Cihaz yaşam döngüsü boyunca bilgi teknolojileri ile ilgili cihaz yapılandırma ihtiyaçları için üretici firma desteği alınır.

A.9.11.1.5. Tıbbi cihazların bağlı olduğu ağın geniş alan ağı çıkışına sınır güvenliğini sağlamak üzere güvenlik duvarı kurulur. Tıbbi cihazlar söz konusu güvenlik duvarı vasıtasıyla oluşturulan DMZ bölgelerine konumlandırılarak cihazlara dış ağdan yapılacak erişimler engellenir veya asgari düzeye indirilir.

A.9.11.1.6. Sağlık hizmet sunucusunun sınır güvenliğini sağlayan bir güvenlik duvarı yok ise tıbbi cihazlar ayrı bir VLAN'a (veya VLAN'lara) konulur. Ağ cihazlarının sağladığı imkânlar çerçevesinde dış ağdan yapılacak erişimler engellenir veya asgari düzeye indirilir.

A.9.11.1.7. Yerel alan ağının VLAN'lara bölünerek yönetilmesi, VLAN'lar için ACL'ler oluşturularak trafiğin yönetilmesi tıbbi cihazlar için iç ağdan kaynaklanabilecek (bilinçli veya bilinçsiz) tehlikeleri önemli ölçüde azaltır.

A.9.11.1.8. İz kaydı üretme imkânı olan tıbbi cihazların iz kayıtları sadece yerel cihazda değil merkezi bir iz kaydı saklama sunucusuna da aktarılmak suretiyle saklanır.

---

[1] Bu başlık altında yazılı olan gereksinimler Open Web Application Security Program (OWASP) tarafından yayınlanmış "Secure Medical Device Deployment Standart" isimli doküman esas alınarak hazırlanmıştır. Söz konusu dokümanın İngilizce ve Türkçe Sürümlerine https://www.owasp.org/index.php/OWASP_Secure_Medical_Device_Deployment_Standard adresinden erişim sağlanabilmektedir.

A.9.11.1.9. Tıbbi cihazlar tarafından üretilen iz kayıtları, (varsa) Merkezi Kayıt ve Olay Yönetim Sistemi (SIEM) vasıtasıyla diğer sistemler tarafından üretilen iz kayıtları ile ilişkilendirilir ve gerekli analizler yapılır.

A.9.11.1.10. Tıbbi cihazların düzgün bir şekilde yapılandırıldıklarından emin olmak ve güncelliğini yitirmiş yazılımlardan kaynaklanan tehlikelerin hedefi haline gelmeyeceklerini garanti altına alabilmek için düzenli olarak zafiyet taramaları yapılır. Tespit edilen açıklıklar üretici firmalardan da destek alınmak suretiyle giderilir.

A.9.11.1.11. Tıbbi cihazlar genellikle en fazla bir ya da birkaç tane bilgisayar ile haberleşme ihtiyacı duyarlar. Sahte DNS ile ilgili ataklardan korunmak maksadıyla, bağlanılacak sunucu ve/veya terminallerin isim ve IP adresleri tıbbi cihazların "host" dosyalarına yazılarak cihazın DNS bağlantıları kesilir.

A.9.11.1.12. Cihazın ağ bağlantısı yapılmadan önce mutlaka varsayılan değer bilgileri (device host name, admin, user, supervisor vb.) değiştirilir. Parola vb. bilgileri cihazların yazılımları içine değiştirilemez bir şekilde gömülü cihazlar kesinlikle kullanılmaz.

A.9.11.1.13. Cihazlara hesap kilitleme ilkesi uygulanır. Ardı ardına üç defadan fazla hatalı giriş halinde, hesaplar kilitlenir veya belirlenecek bir süre için askıya alınır.

A.9.11.1.14. Cihazlar, verilerin sadece güvenli bir format ve en güncel SSH gibi güvenli iletişim protokolleri aracılığı ile gönderilmesini mümkün kılacak şekilde yapılandırılır. FTP, Telnet veya http gibi güvenli olmayan iletişim protokolleri yerine HTTPS veya sFTP protokolleri kullanılır. Güvenli olmayan ağ protokolleri devre dışı bırakılır.

A.9.11.1.15. Cihazın bellenimi (firmware) ve önemli konfigürasyon bilgileri harici olarak yedeklenir.

A.9.11.1.16. Cihazın belleğindeki veriler mümkün ise şifreli olarak muhafaza edilir.

A.9.11.1.17. Yönetici hesabı ve kullanıcı hesapları ayrılır. Mümkün ise ağ üzerinden yönetici hesabı ile cihaza erişim yapılması engellenir.

A.9.11.1.18. Güncelleme mekanizmaları oluşturulur. İşletim sistemleri de dâhil cihaz üzerindeki yazılımlar güncel halde tutulur.

A.9.11.1.19. Cihaz üzerindeki kullanılmayan arayüzler, yazılımsal veya mümkün olmuyorsa donanımsal olarak kapatılır.

A.9.11.1.20. Tıbbi cihazlara uzaktan erişim yapmaya yetkili personelin kimlikleri belirlenir, bu personel ile kişisel gizlik sözleşmesi imzalanır. Uzak bağlantılar Kılavuzun A.6.14.2 (Uzaktan Çalışma ve Erişim) maddesinde belirtilen tedbirler alınmak suretiyle yapılır.

A.9.11.1.21. Tıbbi cihazlara uzaktan müdahalede bulunan firma çalışanları ile gizlilik sözleşmesi yapılır.

A.9.11.2. Tıbbi Cihaz Tedarik Planlaması Yapan Birimler Tarafından Dikkat Edilmesi Gereken Hususlar:

A.9.11.2.1. Mevcut tıbbi cihazlar, siber güvenlik yetenekleri yönüyle incelenir ve iyileştirmek için bir strateji uygulanır.

A.9.11.2.2. Tıbbi cihazlardaki yazılım ve donanım güncelleme işlemleri için üretici firma veya yetkili temsilcilerinin desteği alınır.

A.9.11.2.3. Yeni tıbbi cihaz tedariklerinde siber güvenlik konusu, mutlaka göz önünde bulundurulur. Üreticilerin ve cihazların siber güvenlik konusundaki yetenekleri araştırılır. Kurumsal bilgi güvenliği politikalarının uygulanamayacağı cihazlar tedarik edilmez.

A.9.11.2.4. Envanterde yer alan ve siber güvenlik tedbirleri uygulanamayan cihazların yenilenmesi veya ağ bağlantısı ihtiyacı olmayan yerlerde kullanılması için planlama yapılır.

A.9.11.2.5. Yeni yapılacak tıbbi cihaz bakım ve onarım sözleşmelerine; yazılım/donanım güncellemelerinin yapılması, sıkılaştırma işlemleri ile ilgili hususlar da eklenir.

A.9.11.2.6. Tıbbi cihazlarda siber güvenliğin sağlanması için bilgi işlem ve biyomedikal birimlerinden oluşan ekipler kurulur. Biyomedikal birimlerde görev yapan personelin bilgi teknolojileri/siber güvenlik konularında eğitim alması için gerekli tedbirler alınır.

A.9.11.2.7. Tıbbi cihazlar, üreticilerinin öngördüğü kullanım amacı ve varsa kullanım kılavuzunda belirtilen öneriler dikkate alınarak kullanılır.

A.9.11.2.8. Tıbbi cihazların güvenli kullanımını sağlamak için üreticinin öngördüğü hususlar dikkate alınarak gerekli eğitimler yapılır.

A.9.12. İz Kayıtları (Log) Yönetimi

A.9.12.1. 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.

A.9.12.2. Kurumun iz kayıtları politikası yazılı hale getirilir. İz kayıtlarının tutulması ve yönetilmesi (iz kayıtlarının üretilmesi, aktarılması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi gibi süreçler) sadece erişim yetkisi verilen bir birim/kişiler tarafından yapılır. Bu yetkilerin tercihen Kurumsal SOME'lere verilmesi uygundur.

A.9.12.3. 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.

A.9.12.4. 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.

A.9.12.5. 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.

A.9.12.6. Kritik olaylara ilişkin iz kayıtlarının merkezi sunucuya eş zamanlı olarak (olay oluştuğu zaman) gönderilmesi sağlanır.

A.9.12.7. 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.

A.9.12.8. Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemleri hayata geçirilir.

A.9.12.9. Teknik olarak mümkün olması durumunda, iz kayıtları gizlilik ve hassasiyet seviyelerine göre sınıflandırılarak, ilgili kullanıcıların sadece verilen yetkiler çerçevesinde iz kayıtlarına bakmaları sağlanır.

A.9.12.10. Kayıt üreten ortamlarla iz kayıtları saklama merkezleri arasında, verilerin teknik imkânlar dâhilinde şifreli olarak transfer edilmesi sağlanır.

A.9.12.11. 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.

A.9.12.12. 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.

A.9.12.14. İz kayıtlarının tek yönlü kriptografik özet değerleri (hash) hesaplatılır ve iz kayıtları güvenli ortamlarda saklanır.

A.9.12.15. Olay sonrası incelenmek üzere güvenilir delillerin elde edilmesi için tutulacak kayıtların asgari niteliklerinin aşağıdaki gibi olması gerekir:

A.9.12.15.1. 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),

A.9.12.15.2. Sanal ortam kayıtları,

A.9.12.15.3. Bilişim sistemleri tarafından üretilen kayıtlar, SBYS'ler,

A.9.12.15.4. Güvenlik duvarları,

A.9.12.15.5. Antivirüs yazılımları,

A.9.12.15.6. Saldırı tespit/önleme sistemleri,

A.9.12.15.7. Yönlendiriciler ve anahtarlama cihazları,

A.9.12.15.8. Sunucular,

A.9.12.15.9. Diğer iş uygulamaları (kritik kurumsal projeler),

A.9.12.15.10. Veri tabanları,

A.9.12.15.11. VPN iz kayıtları.

A.9.12.16. Tutulması gereken asgari iz kayıtları;

A.9.12.16.1. Kaydı oluşturan sistem,

A.9.12.16.2. Kaydın oluşturulma zamanı (tarih, saat, zaman dilimi),

A.9.12.16.3. Kaydı oluşturan olay,

A.9.12.16.4. Kaydın ilişkili olduğu kişi (IP/Port bilgisi, MAC adresi, işlemi yapan tekil kullanıcı adı veya sistemin adı).

A.9.12.17. 5651 sayılı kanun ve bu kanuna dayanarak yayımlanan ikincil mevzuat ile kurumun tutmak zorunda olduğu iz kayıtları Kılavuzun A.14.4 (5651 Sayılı Kanun ile Uyum) maddesinde ayrıntılı olarak açıklanmıştır.

A.9.13. Yedekleme Yönetimi

A.9.13.1. Yedekleme Politikası

A.9.13.1.1. Verilerin yedeklenmesi iş sürekliliğinin en temel prensipleri arasında yer alır. Donanım arızaları, yazılım hataları, kullanıcıdan kaynaklanan sorunlar ya da doğal tehditler gibi nedenlerle veri kayıpları yaşanabilir. Başarılı bir yedekleme işlemi ve yedeklenen verinin ihtiyaç anında veri kaybı olmadan kurtarılabilmesi veri yedekleme sistemlerinin en temel iki bileşenidir.

A.9.13.1.2. Yedeklerin kurumun gereksinimleri dikkate alınarak hazırlanmış olması, yönetimin konuya bakış açısını yansıtan bir yedekleme politikası doğrultusunda alınıp güvenliğinin sağlanması, saklanması ve belirli sıklıkta geri dönüş testlerinin yapılması veri kaybı riskini minimum seviyeye indirecektir. Yedekleme sisteminin kurulumu; yedeklenecek veri miktarı, yedekleme sıklığı, yedeklenen verinin zaman içerisinde değişme oranı, kabul edilebilir maksimum veri kaybı gibi parametrelere bağlıdır.

A.9.13.1.3. Her kurumun;

A.9.13.1.3.1. Kendisine özgü yasal veya sözleşmeden doğan gereksinimlerini,

A.9.13.1.3.2. İlgili verinin saklanma ve korunma gerekliliklerini belirlemesi ve bu gereklilikleri karşılayacak şekilde bir politika oluşturması gerekir.

A.9.13.1.4. Yedekleme politikası; olası bir felaket durumu ya da sistem hatası sonrası gerekli tüm verilerin geri getirilebilmesini sağlayacak şekilde yedekleme kuralları tanımlanmış, etkin, yönetilebilir ve izlenebilir bir yedekleme sistemi kurulması ve işletilmesine imkân verecek şekilde hazırlanmalıdır.

A.9.13.1.5. Yedekleme politikasında aşağıdaki tabloda yer alan başlıkların tanımlanmış olması gerekir.

S.Nu.	Yedeklenen Sistem	Tam Yedek	Fark Yedek	Artırımlı Yedek	Transactional /Log Yedek	Saklama Süresi
1	Veri Tabanları					
2	Sanallaştırma Sunucuları					
3	Dosya Paylaşım Platformu					
4	Aktif Dizin					

A.9.13.1.6. Yedekleme politikasının yerine getirilmesi için detaylı bir yedekleme analiz çalışması yapılmalı ve politikayı sağlayacak bir yedekleme planı ortaya koyulmalıdır. Yedekleme planının asgari aşağıdaki bilgileri içermesi gerekmektedir;

A.9.13.1.6.1. Yedekleme sıklığı,

A.9.13.1.6.2. Hangi saklama ortamında ne kadar süre tutulacağı,

A.9.13.1.6.3. Hangi yedekleme türü ile yedekleneceği,

A.9.13.1.6.4. Kabul edilebilir geri dönüş süresi,

A.9.13.1.6.5. Kabul edilebilir veri kaybı süresi.

A.9.13.2. Veri Analiz Çalışması

A.9.13.2.1. Yedekleme sistemi oluşturulmasının ilk adımı detaylı bir veri analiz çalışmasıdır.

A.9.13.2.2. Analiz çalışmalarında öncelikle kuruma ait veriler kategorize edilir.

A.9.13.2.3. Kategoriler; sanal sunucular, fiziksel sunucular, veritabanları, dosyalar, PACS görüntüleri, güvenlik duvarı, saldırı tespit sistemi (IPS) gibi tüm ağ ve güvenlik cihazlarının iz kayıtları, sistem erişimlerine ilişkin iz kayıtları vb. şekilde düzenlenebilir.

A.9.13.2.4. Kategorize edilen verilerin önem dereceleri bilgi güvenliği alt komisyonu tarafından belirlenir.

A.9.13.2.5. Kritik verilerin varlık envanteri özel önem gösterilmesi gereken bir hususdur. Bunun için kılavuzun A.13 (İş Sürekliliği Yönetimi) maddesi referans alınarak kritik varlık listesi oluşturulmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.

A.9.13.2.6. Oluşturulan varlık envanterinde hangi sistemlerde ne tür uygulamaların çalıştığı, yedeği alınacak dizin ve dosyalar, yetkili personel ve yetki seviyeleri yer almalıdır.

A.9.13.3. Yedekleme Listelerinin Oluşturulması

A.9.13.3.1. Yedekleme sistemlerinin ve networkün gereksiz yere meşgul edilmemesi, kapasitenin verimsiz kullanılmaması, kapasite artış gereksinimlerinin öngörülebilmesi ve yedekleme yazılımı lisansının tüketilmemesi adına yedekleme listesi oluşturulur. Yedekleri alınacak sistem, dosya ve verilerin belirlenip yedekleme listesinin oluşturulmasında analiz çalışmalarından faydalanılır.

A.9.13.3.2. Kurumun sistem gereklilikleri göz önüne alınarak; Sunucular, Sanal Sunucular, Veri Tabanları, Aktif Dizin/ Etki Alanı Denetleyicisi, Güvenlik ve Ağ Cihazları gibi veri içeren platformların yedeklenmesi planlanmalıdır.

A.9.13.3.3. Yedeklenecek veriler bilgi işleme süreci içerisinde değişiklik gösterebileceğinden yedekleme listesi en az yılda 2 (iki) kez gözden geçirilmeli ve güncellenmelidir.

A.9.13.3.4. Yedekleme üniteleri üzerinde gereksiz yer ve lisans işgal edilmemesi için uygulama sahiplerinin yazılı onayı alınarak kritiklik düzeyi düşük olan ve sürekli büyüyen iz kaydı dosyaları yedekleme listesine dâhil edilmemelidir.

A.9.13.3.5. Yedekleme listeleri kapasite yönetimi planlanması için referans oluşturur. Kapasite yönetimi ile ilgili hususlar kılavuzun A.9.3 maddesinde yer almaktadır.

A.9.13.4. Yedekleme Planlarının Oluşturulması

A.9.13.4.1. Başarılı bir yedekleme sistemi için kategorize edilmiş ve önceliklendirilmiş verilerin yedekleme planları oluşturulur.

A.9.13.4.2. Yedekleme planları asgari olarak; yedeklenecek bileşenin adı (host name), ulaşım yolu (ip adresi), yedekleme tipi ve sıklığı, yedek geri dönüş testi raporları gibi bilgileri içerir. Örnek bir Yedekleme Planı KLVZ-EK-18'de verilmiştir.

A.9.13.4.3. Kurumun gereklilikleri doğrultusunda hazırlanmış olan Yedekleme Planına göre yedeklerin düzenli aralıklarla alınması ve sürekli olarak gözden geçirilmesi gerekir.

A.9.13.5. Yedekleme Çalışmaları

A.9.13.5.1. Kritik veriler yedeklenirken iki farklı şekilde yedeklenmek üzere bir yedekleme sistemi oluşturulmalıdır. Bunlardan ilki; canlı çalışma ortamında eş zamanlı olarak kümelenmiş disk sisteminin farklı disk bölümlerine; ikincisi ise, çevrimdışı olarak varsa yedekleme sunucusu yoksa şifrelenmiş olarak harici depolama ortamlarında yedeklenmesidir.

A.9.13.5.2. Kritik olmayan veriler yedeklenirken, verilerin bir kopyası mevcut sunucular üzerinde, diğer bir kopyası çevrimdışı olarak yedekleme sunucusu veya harici depolama ortamlarında tutulur.

A.9.13.5.3. Yedekleme politikası ve planları doğrultusunda yapılan yedekleme işlemleri düzenli olarak kontrol edilmeli ve Yedekleme Kontrol Listesi ile kayıt altına alınmalıdır. Örnek bir Yedekleme Kontrol Listesi KLVZ-EK-19'da verilmiştir.

A.9.13.5.4. Kurumun yedekleme işlemlerinin başarısının ölçülmesi ve rapor oluşturulması amacıyla yedekleme başarısızlıkları izlenmeli ve kayıt altına alınmalıdır.

A.9.13.5.5. Özel nitelikli kişisel veri kategorisinde bulunan sağlık kayıtlarının yer aldığı yedekleme ortamları Kılavuzun A.7 (Kriptoloji) maddesinde yer alan usullere göre şifrelenir.

A.9.13.5.6. Yedekleme medyalarının acil durumlarda kullanılması gerekebileceğinden güvenilir ürünlerden seçilmeli ve düzenli periyotlarda test edilmelidir.

A.9.13.5.7. Yedekleme medyalarının bulundurulduğu ortamların fiziksel uygunluğu ve güvenliği sağlanmalı ve herhangi bir felaket anında etkilenmeyecek şekilde bilgi işlem odalarından farklı odalarda veya binalarda saklanmalıdır.

A.9.13.6. Geri Dönüş Testleri

A.9.13.6.1. Yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için belirli aralıklarla geri dönüş testlerinin yapılması gerekir.

A.9.13.6.2. Yılda en az 2 (iki) kez geri dönüş testi yapılarak tutanakla kayıt altına alınır. Tutanakta; sunucu adı, test tarihi, önceki test tarihi, yedek türü ve yedek durumu, geri yükleme testlerinin kimler tarafından ne zaman yapıldığı, başarılı olup olmadığı gibi asgari bilgiler yer almalıdır.

A.9.13.6.3. Yedekten geri yükleme testlerinin, başarısız olması nedeniyle veri kaybı olabileceği durumu göz önüne alınarak, canlı ortamda değil gerçek ortamın aynısı olan test ortamında yapılması gerekmektedir.

A.9.13.7. Yedekleme Süreci Görev ve Sorumlulukları

A.9.13.7.1. Yedekleme politikasının işletilmesi ve zaman içerisinde günün ihtiyaçlarına göre güncellenmesi veri kaybı durumunda kurumun göreceği zararı en aza indirecektir.

A.9.13.7.2. Bu nedenle, yedekleme sistemlerinin yönetiminden, yedekleme politikasının ve yedekleme planının hazırlanmasından, uygulanmasından ve güncellenmesinden sorumlu personelin görevlendirilmesi gerekmektedir.

A.9.13.7.3. Yedekleme işleminin gerekli eğitimi almış personel tarafından yapılması sağlanmalıdır.

A.9.14. Teknik Açıklık Yönetimi

A.9.14.1. "Teknik açıklık" bir bilgi güvenliği terimidir. Kelime anlamı olarak "bir varlık veya kontrolde bulunan ve potansiyel olarak bir ya da daha fazla tehdit unsuru tarafından istismar edilebilecek herhangi bir kontrol zafiyetidir". Aynı şekilde "tehdit" de "bir sisteme ya da organizasyona zarar verebilecek herhangi bir istenmeyen olayın potansiyel nedeni" olarak tanımlanabilir.

A.9.14.2. Teknik açıklıklar; bir varlık veya kontrolün tasarımı, uygulanması, konfigürasyonu veya çalışması sırasında dikkatsizlik nedeniyle veya kasıtlı olarak yaratılan kusurlardır.

A.9.14.3. Teknik açıklıkların tespiti bazen herhangi bir masraf yapmadan çok kolay şekilde olabilir. Bilhassa ürünün tasarımından kaynaklanan açıklıklar üreticiler tarafından yayımlanan yamalar ile düzeltilir. Envanterde yer alan bir yazılım veya işletim sisteminin yamalarının yapılarak en güncel sürümünün kullanılması, ilave bir çaba göstermeden olası pek çok teknik açıklığı önler. Sunucu ve sistem güvenliği kapsamında, yama yönetimi yapılması ile ilgili hususlar Kılavuzun A.9.6 (Sunucu ve Sistem Güvenliği) maddesinde açıklanmıştır.

A.9.14.4. Bununla birlikte yanlış uygulama ve konfigürasyonlardan kaynaklanan hataların giderilmesi, genellikle daha zor ve masraflıdır. Bu tür açıklıkların tespiti için teknik uzmanlardan yararlanılması, açıklık taramalarının yapılması veya bu Kılavuzun A.9.15 (Güvenlik Testleri) maddesinde belirtilen güvenlik testlerinin yapılması gerekir.

A.9.14.5. Teknik açıklıların önlenmesi, tespiti ve giderilmesi için aşağıda sıralanan faaliyetler yapılır:

A.9.14.5.1. Olası teknik açıklıklar; başta Bakanlık Sektörel SOME, istihbarat sağlayan kurum ve kuruluşlar tarafından e-Posta ve resmi yazı ile yapılan bildirimler, üretici firmalar tarafından yayımlanan duyurular, forumlar ve özel ilgi grupları vasıtasıyla takip edilir.

A.9.14.5.2. Alınan tüm önlemlere rağmen çeşitli nedenlerle oluşabilecek açıklıkların tespit edilmesi için işletilen sistemler ticari veya ücretsiz açık kaynak kodlu güvenlik açığı tarama yazılımları ile taramaya tabi tutulur. Bu amaçla ağa bağlanan cihazlar

üzerindeki açıklıkların tespiti için OpenVas, MetaSploit Framework, Nessus, Nexpose; web uygulamaları için Wapiti, Arachni, w3af, Acunetix, Netsparker gibi yazılımlar kullanılır.

A.9.14.5.3. Bakanlık Sektörel SOME ya da kurumların aldığı hizmet veya Kurumsal SOME'ler tarafından kurumların bilgi sistemleri yukarıda belirtilen araçlarla açıklık tarama işlemine tabi tutulur ve tespit edilen eksiklikler ilgili kurumlara yazılı ve elektronik olarak gönderilir.

A.9.14.5.4. Teknik açıklıkların önlenmesi ve giderilmesi için takip edilen kaynaklarda belirtilen/tavsiye edilen önlemler alınır. Bu amaçla yama ve güncelleştirmeler yapılır, cihaz/sistem konfigürasyonları önerilen şekilde ayarlanır. Çok sayıda açıklık tespit edilmesi durumunda öncelikle çok yüksek ve yüksek risk oluşturan açıklıkların giderilmesi hedeflenir.

A.9.14.5.5. Açıklıkların kapatılması sonrasında aynı araçlar ile tekrar tarama yapılarak alınan önlemlerin yeterlilik durumunun doğrulanması gerekir.

A.9.14.5.6. Teknik açıklıkların yönetiminde kullanılan yazılımların lisanssız ya da güvenlik açığı yaratabilecek korsan yazılım olmamasına dikkat edilir.

A.9.15. Sistem Güvenlik Testleri

A.9.15.1. Sistem güvenlik testleri, açıklık tarama araçları tarafından ve manuel olarak tespit edilen teknik eksikliklerin özel yazılım ve tekniklerle istismar edilmesi ve sistemlere erişim sağlanması amacıyla yapılır. Bu testler yaygın kullanımıyla "sızma testi" veya "penetrasyon testi" olarak da bilinir.

A.9.15.2. Bakanlığımıza bağlı tüm merkez ve taşra birimleri tarafından geliştirilen veya kaynak kodları ile birlikte tedarik edilen yazılımların "kaynak kod analiz" işlemleri de sistem güvenlik testlerinin bir parçası olarak gerçekleştirilir.

A.9.15.3. KVKK'nın özel nitelikli kişisel verilerin güvenliği için alınması gereken tedbirler kapsamında yayımlanan 2018/10 sayılı kararı uyarınca bu veriler elektronik ortamlarda saklanıyor ise;

A.9.15.3.1. Verilerin bulunduğu ortamlara (örneğin VTYS sunucuları) ait güvenlik güncellemelerinin sürekli takip edilmesi, **gerekli güvenlik testlerinin (sızma testleri) düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması**,

A.9.15.3.2. Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, **bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması (sızma testleri, kaynak kod analizleri), test sonuçlarının kayıt altına alınması** kanuni bir zorunluluktur.

A.9.15.4. Bakanlık merkez ve taşra teşkilatı ile bağlı kuruluşlara bağlı birimlerde yapılacak sistem güvenlik testleri, önceden makam onayı almak ve ilgili birimlere bilgi vermek şartıyla, Bakanlık Sektörel SOME vasıtasıyla gerçekleştirilir. Sektörel SOME tarafından yapılacak güvenlik testleri (USOM veya Bakanlık ihlal olayları bildirim

sistemi vasıtası ile bildirilen olayların çözümlenmesi, Bakanlık Üst Yönetim tarafından verilen direktifler vb.) özel ihtiyaçlara binaen istisnai olarak yapılır.

A.9.15.5. Bakanlık bağlı kuruluşlar ile taşra teşkilatları, önceden kendi üst yönetimlerinden onay almak ve ilgili birimlere bilgi vermek şartıyla, kurumsal SOME'leri vasıtasıyla kendilerine bağlı birimlerde sistem güvenlik testi yapar veya yaptırabilir.

A.9.15.6. Güvenlik testi için hizmet alımı yapılması halinde, ilgili firma ve personeli ile mutlaka gizlilik sözleşmesi yapılır.

A.9.15.7. Yapılacak kontrol ve testler, "TSE 13638 Sızma Testi Yapan Personel ve Firmalar İçin Şartlar" standardına bağlı kalınarak yürütülür.

A.9.15.8. Testler, TS 13638'de tanımlandığı şekilde aşağıda belirtilen uzman/ sertifikalı personel tarafından yapılır.

A.9.15.8.1. Stajyer Sızma Testi Uzmanı

A.9.15.8.2. Kayıtlı Sızma Testi Uzmanı

A.9.15.8.3. Sertifikalı Sızma Testi Uzmanı

A.9.15.8.4. Kıdemli Sızma Testi Uzmanı

A.9.15.9. Güvenlik testleri iç ağdan (internal) ve dış ağdan (external) olacak şekilde ayrı ayrı yapılır ve en az aşağıdaki hususların test edilmesi gerekir.

A.9.15.9.1. Ağ ve sistem altyapısı sızma testi,

A.9.15.9.1.1. Yerel ağ sızma testleri ağ sızma testi,

A.9.15.9.1.2. İnternet üzerinden sızma testleri,

A.9.15.9.1.3. Güvenlik sistemleri (antivirüs, IPS/IDS, güvenlik duvarı vb.) sızma testi,

A.9.15.9.1.4. İşletim sistemleri sızma testi,

A.9.15.9.1.5. Kablosuz ağ sızma testi.

A.9.15.9.2. Mobil uygulama sızma testi,

A.9.15.9.3. Veri tabanı testleri,

A.9.15.9.4. Hizmet aksatma saldırı (DoS/DDoS) testleri,

A.9.15.9.5. Endüstriyel kontrol sistemi (SCADA) sızma testi,

A.9.15.9.6. Sosyal mühendislik testleri,

A.9.15.9.7. Web uygulama sızma testleri ve yazılım kaynak kod analizleri (kaynak kodları olan yazılımlar için).

A.9.15.10. Kaynak kod analizlerinin sadece otomatik kod analiz araçları ile yapılması yeterli bir işlem olarak kabul edilmez. Kodların yetkin personel tarafından manuel olarak gözden geçirilmesi gerekir. Bu amaçla TÜBİTAK'ın yayımlamış olduğu güncel Güvenli Yazılım Geliştirme Kılavuzu veya KLVZ-EK-17 Güvenli Yazılım Geliştirme Kontrol Listesinde yer alan ölçütler kullanılır.

A.9.15.11. Yapılan testler sonucunda ortaya çıkan sonuçlar, önem derecesine göre raporlanır. Bu raporların oluşturulmasında TSE 13638 standart raporlama örneği temel alınır. Raporda en az aşağıda belirtilen hususların yer alması gerekir.

A.9.15.11.1. Kapak Sayfası (testlerin yapıldığı zaman dilimini içerir),

A.9.15.11.2. Yönetici Özeti (Kısa bir okuma ile rapordaki önemli bilgilere ulaşmak isteyen okuyuculara (özellikle yöneticilere) yönelik bir bölümdür),

A.9.15.11.3. Genel Bilgiler,

A.9.15.11.4. Test Ekibi,

A.9.15.11.5. Kapsam ve IP Adresleri,

A.9.15.11.6. Genel Değerlendirme,

A.9.15.11.7. Genel Test Metodolojisi,

A.9.15.11.8. Risk Derecelendirmesi (Sayısal olarak veya farklı renklendirme şeklinde, TSE 13638 Standartlarına göre (Acil, Kritik, Yüksek, Orta, Düşük) yapılarak kurumun risklerin giderilmesinde önceliklendirme yapılmasına imkân vermek üzere hazırlanır),

A.9.15.11.9. Genel Bulgular,

A.9.15.11.10. Teknik Bilgiler (Raporun teknik detaylarının verildiği kapsamlı bir bölümdür. Teknik bilgilerin aşağıdaki alt bölümleri içermesi tavsiye edilir)

A.9.15.11.10.1. Giriş,

A.9.15.11.10.2. Bilgi toplama,

A.9.15.11.10.3. Açıklık analizi,

A.9.15.11.10.4. Kullanma /açıklık onayı,

A.9.15.11.10.5. Kullanma sonrası etki,

A.9.15.11.10.6. Varsa diğer testler (sosyal mühendislik/fiziksel sızma testi/DoS/DDoS vb.),

A.9.15.11.10.7. Kullanılan araçlar.

A.9.15.11.11. Testlere ait grafiksel gösterimler,

A.9.15.11.12. Tavsiye özeti.

A.9.15.12. Sızma testi raporları yukarıda bahsi geçen maddeler asgari kalmak suretiyle kurumun ihtiyaçlarına göre değiştirilebilir.

A.9.15.13. Sızma testi raporunun stajyer sızma testi uzmanı dışındaki diğer uzmanlar tarafından hazırlanması ve imzalanması gerekir.

A.9.15.14. Oluşturulan rapor, Kurumsal SOME Ekip lideri ve Bilgi Güvenliği Yetkilisi tarafından değerlendirilerek acil eylem planı oluşturulur ve açıklıkların kapatılması için çalışmalar başlatılır.

A.9.15.15. Yapılan çalışmalar sonucunda ortaya çıkan sonuçlar, kurumun bilgi güvenliği alt komisyonuna sunulur. Kapatılamayan zafiyetler risk tablosuna işlenir ve riskin azaltılması için mümkün olan önlemler alınır.

A.9.15.16. Hazırlanan raporlar GİZLİ gizlilik derecesi ile sınıflandırılır. Gerek yazılı kopyaları gerekse elektronik kopyaları mutlaka güvenli bir ortamda saklanır.

A.10. HABERLEŞME GÜVENLİĞİ

A.10.1. Ağ Güvenliği

A.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.

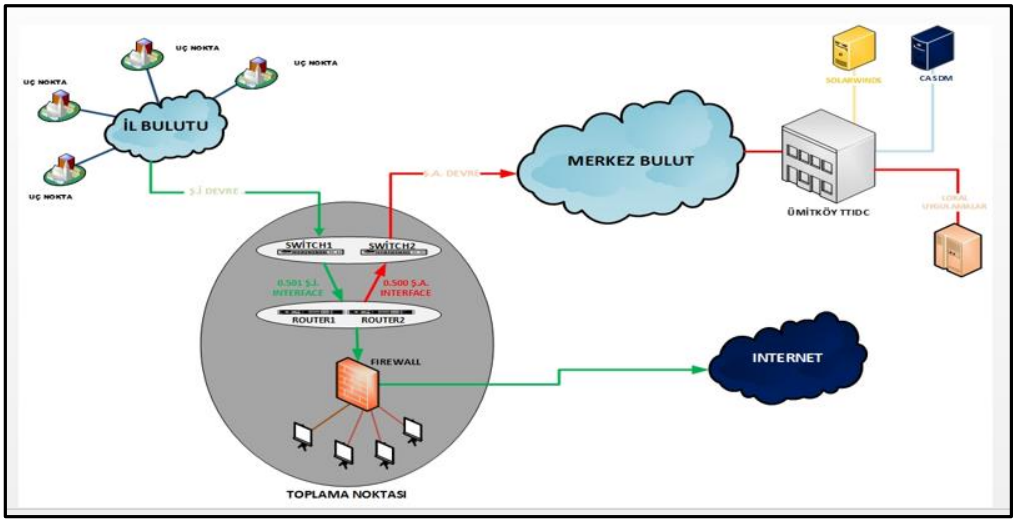
A.10.1.2. Ağ güvenliği, bir kuruluşun bilgisayar ağına bağlı olarak çalışan varlıklarının ve ağ trafiğinin güvenliğini sağlamak üzere, uygulamakta olduğu politikalar ve kontrol önlemleridir. Ağ güvenliği, bilgi güvenliğinin sağlanması için en önemli bileşenlerden biridir.

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

A.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.

A.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.

A.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 Şekil 34'te gösterildiği gibidir.



Şekil 4: SBA Bulut Mimarisi

A.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.

A.10.1.8. Aktif cihaz sayısının 10'dan az olması nedeniyle SBA İl bulutuna doğrudan bağlı olmayan yerlerde, İnternet bağlantısında kullanılan aktif ağ cihazlarının desteklemesi durumunda, internet trafiği il toplama noktasında bulunan güvenlik duvarı ile tesis edilen IPSec VPN benzeri bir tünel üzerinden geçirilerek, trafiğin filtrelenmesi ve iz kayıtlarının tutulması imkânı sağlanır.

A.10.1.9. 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.

A.10.1.10. 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.

A.10.2. Uç Nokta (Yerel Alan Ağı) Ağ Güvenliği

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

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

A.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.

A.10.2.4. 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.

A.10.2.5. Yerel alan ağlarında, port kısıtlaması yapılamayan, yönetim yeteneği olmayan ağ dağıtım kutuları (hub) veya eski nesil kenar anahtarlar kullanılmaz.

A.10.2.6. NAC tabanlı çözümlerin olmaması durumunda, kullanılmayan portlar kenar anahtar üzerinde yazılımsal olarak kapatılır.

A.10.2.7. Yerel alan ağları performans, güvenlik ve ölçeklenebilirlik avantajlarını kullanmak üzere VLAN'lara bölünerek yönetilir.

A.10.2.8. 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.

A.10.2.9. 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.

A.10.2.10. 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.

A.10.2.11. Bakanlık yazılı onayı alınmaksızın yukarıda belirtilen şekilde internet bağlantılarının yapıldığının tespit edilmesi halinde, ilgililer hakkında idari ve yasal işlemler yapılır.

A.10.2.12. 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.

A.10.2.13. Bu noktalarda tesis edilen güvenlik duvarlarının yönetimi, uç noktalardaki bilgi işlem yöneticileri tarafından yapılır.

A.10.2.14. Hastanelerin misafir ağları ile SBA'ya bağlanan yerel alan ağları fiziksel olarak ayrı ağlar olarak tesis edilir. Misafir ağlarına bağlı kullanıcıların SBA ağına erişimine izin verilmez.

A.10.3. Kablosuz Ağ Güvenliği

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

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

A.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;

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

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

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

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

A.10.4. Veri Aktarımı Güvenliği

A.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.

A.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.

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

A.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.

A.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.

A.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.

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

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

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

A.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.

A.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.

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

A.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.

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

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

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

A.10.4.16.1. Şifreli olarak aktarılması gereken dosyalar, aktarım öncesinde tek tek veya topluca, AES-256 veya üstü bir şifreleme aracı kullanılmak suretiyle şifrelenir.

A.10.4.16.2. 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.

A.10.4.16.3. 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.

A.10.4.16.4. 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.

A.10.4.16.5. Şifrelenen dosyanın parolası, şifreli dosyanın aktarımında kullanılan sistemden farklı bir araç/ortam kullanılmak suretiyle alıcısına ulaştırılır (örneğin; e-Posta ile aktarılan şifreli bir dosyanın parolası SMS ile, dosya sunucusu ile paylaşılan şifreli bir dosyanın parolası e-Posta ile gönderilebilir.)

A.10.4.17. e-Posta ile Veri Aktarımı:

A.10.4.17.1. Hedef kişi, Sağlık Bakanlığı çalışanı ise ve "*@saglik.gov.tr" uzantılı kurumsal e-Posta hesabı varsa, dosya aktarımı için en pratik yöntem olarak Sağlık Bakanlığı Kurumsal e-Posta Sistemi tercih edilir.

A.10.4.17.2. Hedef adres "*@saglik.gov.tr" uzantılı tüzel e-Posta adresi ise bu hesaba birden fazla kişinin ulaşabileceği dikkate alınır ve gönderme işlemi konusunda daha fazla hassasiyet gösterilir.

A.10.4.17.3. ÇOK GİZLİ, GİZLİ ve ÖZEL gizlilik derecesindeki bilgiler önce A.10.4.16'de belirtilen şekilde şifrelenmeyi müteakip e-Posta eki olarak gönderilir. HİZMETE ÖZEL bilgilerin şifrelenmesine gerek yoktur.

A.10.4.17.4. Hedef adres, halka açık e-Posta servislerinden alınan bir adres veya bir başka kuruma ait kurumsal e-Posta adresi ise HİZMETE ÖZEL olanlar da dâhil gizlilik derecesi taşıyan tüm bilgiler, gönderilmeden önce mutlaka yukarıda belirtilen şekilde şifrelenir.

A.10.4.18. Dosya Paylaşım Ortamları ile Veri Aktarımı:

A.10.4.18.1. FTP yapısı itibarıyla güvenli bir paylaşım ortamı olarak kabul edilmez.

A.10.4.18.2. Bilgi paylaşımı için mutlaka FTP sistemlerinin kullanılması gerekiyor ise HİZMETE ÖZEL olanlar da dâhil gizlilik derecesi taşıyan tüm bilgiler, paylaşılmadan önce mutlaka yukarıda belirtilen şekilde şifrelenir.

A.10.4.19. Taşınabilir Medya ile Veri Aktarımı:

A.10.4.19.1. Bakanlık taşınabilir medya kullanım politikası, A.4.4'te açıklandığı gibidir.

A.10.4.19.2. Taşınabilir medya yapısı itibarıyla çalınma, kaybolma gibi tehditlere maruz kalma ihtimali nedeniyle, başka bir aktarım yöntemi olmadığı durumlarda kullanılır.

A.10.4.19.3. ÇOK GİZLİ, GİZLİ ve ÖZEL gizlilik derecesindeki bilgiler taşınabilir medya ortamında şifreli olarak muhafaza edilir.

A.10.4.19.4. Kurum Kontrolünde Olmayan Ortamlar Üzerinden Veri Aktarımı:

A.10.4.19.5. Halka açık e-Posta servisleri (Hotmail, Gmail vb.), bir başka kuruma ait kurumsal e-Posta sistemleri ve halka açık bulut depolama ortamları (Google Drive, Dropbox, Apple iCloud vb.) prensip olarak güvensiz olarak kabul edilir.

A.10.4.19.6. Gizli kalması gereken bilgiler hiçbir şekilde açık (şifresiz) olarak bu ortamlarda tutulamaz ve aktarılamaz

A.10.4.19.7. Aktarım yapılacak kişi/kurumun Bakanlığımız kontrolündeki sistemlere erişim izni yok ise HİZMETE ÖZEL olanlar da dâhil daha üst düzey gizlilik derecesi

taşıyan tüm bilgiler, yukarıda belirtilen şekilde şifrelenmek suretiyle kurum kontrolünde olmayan sistemler üzerinden paylaşılabilir.

A.10.4.20. Web Servisleri Üzerinden Veri Aktarımı

A.10.4.20.1. Web servislerine erişimin sadece yetkilendirilmiş taraflar arasında yapılması sağlanır. Bu kapsamda gerekli her türlü bileşen kullanılarak (anahtarlama cihazı, yönlendirici, güvenlik duvarı vb.) gerekli erişim ayarları (güvenlik kuralları, güvenlik konfigürasyonları) yapılır ve her türlü fiziksel ve mantıksal güvenlik önlemleri alınır.

A.10.4.20.2. Web servisleri ile yapılacak olan iletişim şifreli olarak yapılır. Bu kapsamda yapılacak iletişim, SSL/TLS protokolleri üzerinden gerçekleştirilir. Web servis iletişiminin kriptografik yöntemler kullanılarak güvenli bir şekilde yapılması için Kılavuzun A.7.2 (Kriptografik Araç ve Yöntemler) maddesinde belirtilen hususlara dikkat edilir.

A.10.4.20.3. Yönetimsel olarak uygulanabilir olması halinde, web servislerine iletişim için zaman ve/veya IP adresi bazında filtre kullanılması hususu dikkate alınır.

A.10.4.20.4. Web servisi kapsamında kullanılan mesajlar bir doğrulama mekanizmasından geçirilir. XML (Extensible Markup Language) servisler için belirlenen XML şemasına uygun olduğu denetlenir. Şema doğrulamasından geçemeyen istekler kabul edilmez.

A.10.4.20.5. Web servislerine erişim ve ilgili fonksiyonların kullanımı, servis içinde tanımlanmış doğrulama ve yetkilendirme mekanizmaları ile kontrol edilir. Yetkisiz erişim ve kullanımlar engellenir.

A.10.4.20.6. Doğrulama ve yetkilendirme mekanizmaları için kullanılan kullanıcı adı parola bilgileri, SSL/TLS içinde şifreli olarak gönderilir. Hiçbir zaman açık olarak gönderilmez.

A.10.4.20.7. Web servislerinin yoğun kullanımı durumunda hizmetin erişilebilirliğinin sağlanması amacıyla gerekli alt yapı kurulur. Gelen istekler için yük dengelemesi yapılarak web servislerine erişimin sürekliliği sağlanır.

A.10.4.20.8. Web servisleri kapsamında giden ve gelen XML mesajların büyüklüğü, kullanılan web servis fonksiyonları bazında veya bir mesaj kapasitesi olarak belirlenir. Gelen web servis istekleri belirlenen mesaj kapasitesini aşıyorsa reddedilir.

A.10.4.20.9. Web servisleri kapsamında giden, gelen mesajlar herhangi bir zararlı yazılım ve kötü niyetli kod parçacığına karşı taranır. Zararlı içerik taşıyan istekler reddedilir.

A.10.4.20.10. Web servislerine yapılan her türlü erişim için iz kayıtları oluşturulur ve saklanır. Bu kapsamda asgari olarak “erişim yapan IP, erişim zamanı, erişim yapılan fonksiyon, erişimi gerçekleştiren kullanıcı” gibi bilgiler kayıt altına alınır.

A.10.4.20.11. Web servisleri sürekli olarak kontrol edilir ve değişen teknoloji ve ihtiyaçlara göre gerekli güvenlik güncellemeleri yapılır.

A.10.4.20.12. Ayrıca alınan kayıtlar düzenli olarak incelenir. Varsa yetkisiz erişimler tespit edilerek güvenlik önlemleri arttırılır.

A.10.5. Gizlilik Sözleşmeleri

A.10.5.1. Bakanlığımıza ait gizli kalması gereken bilgilerin korunması maksadıyla, Bakanlık merkez ve taşra teşkilatı ile bağlı kuruluşlarda görev yapan 657 sayılı Kanuna bağlı personel de dâhil kendilerine herhangi bir nedenle kurumun bilgi ve bilgi işleme tesislerine erişim yetkisi verilen tüm çalışanlar ve tedarikçiler ile gizlilik sözleşmeleri yapılır.

A.10.5.2. Gerçek kişiler ile personel gizlilik sözleşmesi, tüzel kişiler ile kurumsal gizlilik sözleşmesi imzalanır. Staj vb. nedenlerle geçici olarak çalışanlar da dâhil tüm personel ile gizlilik sözleşmesi yapılması esastır.

A.10.5.3. Aynı şekilde resmi bir sözleşme veya protokol olmasa bile yasal bir gerekçeye istinaden geçici olarak kendilerine hassas bilgiler verilen/hassas bilgilere erişim izni verilen tüzel kişiler ile gizlilik sözleşmesi yapılması gerekir.

A.10.5.4. Korunacak bilginin niteliği ve durumun özelliğine göre, imzalanacak gizlilik sözleşmelerinin içeriği değişebilir. Bununla birlikte hazırlanacak olan gizlilik sözleşmelerinde mutlaka aşağıda sıralanan hususların bulunması gerekir.

A.10.5.4.1. Korunacak bilginin tanımı,

A.10.5.4.2. Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dâhil olmak üzere anlaşma süresi,

A.10.5.4.3. Anlaşma sona erdiğinde yapılması gereken eylemler,

A.10.5.4.4. Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar,

A.10.5.4.5. Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,

A.10.5.4.6. Gizli bilgilerin kullanım izni ve bilgileri kullanmak için tarafların hakları,

A.10.5.4.7. Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,

A.10.5.4.8. Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesi halinde diğer tarafın bilgilendirme zorunluluğu ve bildirimin nasıl yapılacağı,

A.10.5.4.9. Teslim edilen bilgilerin iade veya imhasına ilişkin hükümler,

A.10.5.4.10. Sözleşmenin ihlali durumunda yapılması beklenen eylemler.

A.10.5.5. Kamu personeli ile yapılacak gizlilik ve ifşa etmeme düzenlemelerinde, personelin statüleri gereği bağlı oldukları başta 657 sayılı Devlet Memurları Kanunu olmak üzere diğer yasal mevzuat dikkate alınır.

A.10.5.6. Kişisel ve kurumsal gizlilik sözleşmesi olarak;

A.10.5.6.1. Sözleşmeli olarak çalışan personel için KLVZ-EK-12 Personel Gizlilik Sözleşmesi,

A.10.5.6.2. Firmalar ve diğer kurum ve kuruluşlar için KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesi,

A.10.5.6.3. 657 sayılı Devlet Memurları Kanununa bağlı personel için KLVZ-EK-18 Bilgi Güvenliği Farkındalık Bildirgesi kullanılır.

A.10.5.7. Söz konusu sözleşmeler, SBSGM için hazırlanmış olup her kurumun kendi ihtiyaçlarına özgü olarak güncellemesi gerekir.

A.10.5.8. Kişi ve kurumlar ile yapılan gizlilik sözleşmeleri, protokol ve benzeri dokümanlar, ilgili birimler tarafından yürürlük süresince ve sonrasında ilgili alt komisyonlar tarafından belirlenecek süreler boyunca saklanır.

A.10.6. Veri Aktarım Anlaşmaları

A.10.6.1. Kamu kurumu veya kuruluşu ile Bakanlığımız arasında veri aktarımı yapılırken aşağıda belirtilen hususlar göz önünde bulundurulur.

A.10.6.2. Bakanlıktan veya Bakanlığa yapılacak veri aktarımının değerlendirilmesinde 6698 sayılı kanuna, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğe ve ilgili diğer mevzuata uyum aranır.

A.10.6.3. Bakanlıktan veya Bakanlığa yapılmak istenen kişisel sağlık verisi aktarımı işlemleri, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'te öngörüldüğü şekilde, izin süreçlerinin tamamlanması sonrasında yapılır.

A.10.6.4. Veri aktarımının ilgili mevzuata uygun olduğunun değerlendirilmesi halinde veri aktarımı ancak 6698 sayılı kanunda yer alan ilkelere uygun olarak yapılır.

A.10.6.5. Bakanlıktan veya Bakanlığa yapılacak veri aktarımları bir Protokol çerçevesinde gerçekleşir.

A.10.6.6. Hangi verilerin, hangi amaç veya amaçlarla, ne şekilde ve ne süreyle aktarılacağı gibi sorulara ilişkin cevapların da yer aldığı Protokol, taraflarca imza altına alınır.

A.10.6.7. Web servisler aracılığı ile aktarılmayacak olan verilerin aktarılmasında, uluslararası standartlarla yüksek güvenlikli olduğu belirlenen sistemler kullanılır.

A.10.6.8. Aktarılan verilerin farklı amaçlar için kullanılmasını engelleyecek yeterli güvenlik önlemleri alınır. Bu önlemlerin, KVKK tarafından açıklanan önlemleri de içermesi gerekir.

A.10.6.9. Protokol kapsamında elde edilen kişisel verilerin üçüncü kişilere hiçbir şekilde aktarılamayacağına ilişkin bir gizlilik sözleşmesi imzalanır veya Protokol'de buna ilişkin hükümler bulunur.

A.10.6.10. Kişisel verilerin, KVKK tarafından belirlenen kriterlere uygun bir şekilde anonim hâle getirilmesi hâlinde bu veriler, herhangi bir Protokol imzalanmaksızın aktarılır.

A.10.6.11. Aktarılıp aktarılmamasında hukuka uygunluğun net bir şekilde tespit edilemediği veriler hakkında Bakanlıktan görüş alınır. İhtiyaç olması halinde KVKK'dan resmi görüş talep edilir.

A.11. TEDARİKÇİ İLİŞKİLERİ

A.11.1. Mal ve Hizmet Alımları Güvenliği

A.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.

A.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:

A.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.

A.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.

A.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.

A.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.

A.11.1.2.5. Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, "Personel Gizlilik Sözleşmeleri" idareye teslim edildikten sonra tanımlanır.

A.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.

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

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

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

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

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

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

A.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.

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

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

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

A.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.

A.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.

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

A.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.

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

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

A.11.2. SBYS Firmaları ile İlişkilerde Dikkat Edilecek Hususlar

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

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

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

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

A.11.2.5. SBYS yazılım üreticileri, Bakanlık Kayıt Tescil Sistemine (KTS) kayıt olarak akredite olurlar. Üreticilerin KTS'ye kayıt olabilmesi için istenilen sertifikalar ve belgeler ilgili mevzuatta belirtilmiştir.

A.11.2.6. Bakanlık tarafından istenilen sertifika ve belgeleri teslim eden SBYS yazılım üreticileriyle, KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesi imzalanır ve üretici firma KTS'ye kaydedilir.

A.11.2.7. KTS'ye kayıt olan SBYS yazılım üreticileri Bakanlık tarafından yayımlanan sağlık bilişimi standartlarına uygunluk açısından denetlenir.

A.11.2.8. Sağlık bilişimi standartlarına ve ilgili mevzuatlara uyumlu olmayan; bilgi, belge, sertifika ve doküman eksiği olan SBYS yazılım üreticileri, KTS web sayfasında pasif listeye alınır. Eksiği olmayan SBYS yazılım üreticileri ise aktif listede yer alır.

A.11.2.9. İlgili mevzuat kapsamında SBYS yazılım üreticilerine eksikliklerini gidermeleri için süre verilir. Bu süre içerisinde eksikliklerini gideren SBYS yazılım üreticileri aktif listeye alınır.

A.11.2.10. Kullanılmasına karar verilen sağlık bilişimi standartları ve veri gönderiminde dikkat edilecek hususlar SBSGM web sayfasında yayımlanır ve güncellenir.

A.11.2.11. Sağlık hizmeti sunucularınca SBYS yazılım üreticilerinden, ürettiği SBYS yazılımının minimum şartlara uyum sağladığını gösteren "KTS Kayıt Belgesi" istenir. KTS kayıt belgesinin geçerliliği KTS web sayfası üzerinden sorgulanır.

A.11.2.12. KTS yetki belgesi olmayan, geçersiz yetki belgesi ibraz eden ya da KTS web sayfasında pasif listede yer alan SBYS yazılım üreticileri ile sözleşme imzalanmaz.

A.11.2.13. Sağlık kuruluşları ile SBYS yazılım üreticisi arasında yaşanabilecek uyuşmazlıklarda uygulanacak cezai şartların SBYS yazılım üreticisi ile yapılacak sözleşmelerde yer alması sağlanır.

A.11.2.14. Sağlık kuruluşları ve aile hekimleri, SBYS yazılım üreticisi ve bayileriyle ayrıca gizlilik sözleşmesi imzalamalıdır. Sağlık tesisleri ve aile hekimleri bu maksatla KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesini kullanabilecekleri gibi kendileri de sözleşme metinlerini oluşturabilirler.

A.11.2.15. SBYS'lerin ilk kurulumu esnasında uzaktan destek ile kurulum talepleri kabul edilmez.

A.11.2.16. SBYS yazılım üreticisi, ilk kurulum esnasında çalıştıracağı personel ile ilgili planlamayı kurulum ve proje planında detaylı olarak açıklamak zorundadır.

A.11.2.17. Kurulum ve proje planının işletmeye alınacağı tarihe, sağlık kuruluşları tarafından karar verilir. Sözleşme imzalandıktan sonra SBYS'nin işletmeye alınacağı tarih, sağlık kuruluşları tarafından hazırlanan şartnamelerde belirtilir.

A.11.2.18. Sağlık kuruluşları, HBYS tedarikçilerinden en az altı ayda bir kez olacak şekilde son alınan yedek üzerinden veri kurtarma testi yapmasını istemeli ve gerekli kontrolleri yapmalıdır.

A.11.2.19. Herhangi bir sebeple mevcut SBYS yazılımının kullanımına son verilirse, verilerin tamamı orijinal veri tabanı formatında, kolay ve sorunsuz okunabilir bir medya ortamında, 3 (üç) kopya halinde sağlık kuruluşuna teslim edilmek zorundadır.

A.11.2.20. Kritik alanlardaki değiştirme ve silme işlemlerinin, ancak yetki ölçüsünde yapılması gerekir. Değişikliklere sonradan erişim ve geri düzeltme için mutlaka iz kaydı dosyaları detayları olarak tutulmalı veya VTYS katmanındaki denetleme (audit) uygulama yazılımından da desteklenir olmalıdır.

A.11.2.21. Kişisel sağlık verileri özel nitelikli kişisel veriler kapsamında olması sebebiyle; sözleşme süresince veya sonrasında kayıtlı tüm veriler hiçbir surette, hiçbir zaman SBYS üreticisinde kalmak üzere kopyalanamaz, çıktı alınamaz, firma sunucularına aktarılamaz, ifşa edilemez.

A.11.2.22. SBYS yazılımları tüm sistem genelindeki kullanıcı, işlem ve bilgi düzeylerinde bilgi gizliliğini ve güvenliğini sağlamak zorundadır. Her kullanıcının gerektiğinde değiştirilebilir kişisel bir parolası olmalıdır. Bu parola ile farklı bir lokasyonda oturum açıldığında ilk oturum otomatik olarak kapatılmalıdır. Bir kişiye ait parolanın birden çok kişi tarafından kullanılmasına izin verilmemelidir.

A.11.2.23. Çeşitli yetki düzeyleri ve grupları tanımlanabilmeli, yetki değişimi SBYS Yöneticisi tarafından yapılabilmelidir. Verilere erişim bu tanımlamalar çerçevesinde yapılmalıdır.

A.11.2.24. SBYS'de kullanıcılar için saat bazında sisteme giriş sınırlandırması yapılabilmelidir.

A.11.2.25. SBYS'de kullanıcıların otomasyona giriş-çıkış zamanları ve geçersiz giriş denemeleri istenildiğinde raporlanabilmelidir.

A.11.2.26. Poliklinik, Klinik, Laboratuvar bazında yetkilendirmeler yapılabilmelidir. Kullanıcının yetki verilmeyen bir poliklinikteki hasta listesine erişimi engellenmelidir.

A.11.2.27. SBYS yazılımlarında Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen parola özellikleri tanımlanabilmeli ve bu kurala uymayan parolalar kabul edilmemelidir.

A.11.2.28. Sağlık kuruluşu ile ilişiği kalıcı olarak kesilen tüm personelin SBYS erişim yetkisi tamamen ve otomatik olarak iptal edilmelidir.

A.11.2.29. Geçici olarak sağlık kuruluşunda bulunmayan (izin, rapor, geçici görev kurs, eğitim vb.) personelin SBYS'ye girişi otomatik olarak engellenmelidir.

A.11.2.30. Sunucu işletim sistemi, sunucu yazılımları, veri tabanında yapılacak yapısal değişiklikler gibi tüm sistemi etkileyen güncellemeler mesai saatleri dışında veya hasta yoğunluğunun en az olduğu saatlerde yapılmalıdır. Acil müdahale edilmesi gereken bir arıza durumunda ise mesai saatleri içinde güncelleme yapılabilir.

A.12. BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

A.12.1. İhlal Bildirimi ve Olay Yönetimi

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

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

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

A.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.

A.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.

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

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

A.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.

A.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.

A.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.

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

A.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.

A.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.

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

A.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.

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

A.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.

A.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.

A.12.2. Kanıt Toplama

A.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.

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

A.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.

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

A.12.2.5. Olay yerindeki bilgisayar kapalı ise kesinlikle açılmaz.

A.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.

A.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.

A.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.

A.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.

A.12.2.10. Yedeklenecek diskin hafızası şüpheli bilgisayar diskinden büyük olur.

A.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.

A.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)

A.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.

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

A.13. İŞ SÜREKLİLİĞİ YÖNETİMİ

A.13.1. İş Sürekliliği Genel Yaklaşımı

A.13.1.1. İş sürekliliği; kurumun vermekte olduğu kritik bilişim hizmetlerinin sunumuna kesintisiz bir şekilde devam etmesi veya türü ve nedeni ne olursa olsun, herhangi bir kesinti ya da olay durumunda, önceden belirlenmiş kritik iş süreçlerini, önceden tanımlanmış kabul edilebilir seviyede sunma yeteneğini sağlayan yöntemdir. Kurum iş süreçlerinde hizmet sürekliliği yeteneğini; etkin bir risk yönetimi, öncelikli hizmetlerini kesintiye uğratabilecek olayların tanımlanması, bu olayların bertaraf edilmesi için gerekli tedbirlerin alınması, olay anında ve sonrasında kritik hizmetlerin en hızlı ve etkin nasıl ayağa kaldırılacağının senaryolarla planlanması ve bu senaryoların tatbikatlarla test edilmesi ile elde eder.

A.13.1.2. Bu bölümde anlatılan iş sürekliliği, bilgi varlıklarının iş sürekliliğinin sağlanmasına yönelik tedbirleri kapsamaktadır. Yaşanacak her türlü afet ve acil durumda sunulan hizmetlerin sürdürülebilir olması, fiziksel ve fonksiyonel olarak afet ve acil durumlara hazırlıklı olunması, zamanında, hızlı ve etkili müdahalede bulunularak en kısa sürede olağan işleyişe dönülmesi için alınması gereken tedbirler ve yapılması gereken çalışmalar “Hastane Afet ve Acil Durum Planı (HAP) Hazırlama Kılavuzu”nda ayrıntılı olarak anlatılmış, örnek planlar verilmiştir.

A.13.1.3. İş sürekliliği kurma nedenleri; hizmet sürekliliğini sağlamak ve kesintilere yeterli şekilde yanıt verme kabiliyetini kazanmak olabileceği gibi yasa, yönetmelik ve sözleşmelerden kaynaklanan sorumlulukları yerine getirmek de olabilir.

A.13.1.4. Etkin bir bilgi güvenliği iş sürekliliği sistemi kurulduğunda kurumun şu çıktıları elde etmesi beklenir;

- Kritik süreç ve varlıkların hizmet sürekliliğinin sağlanması,

- Dokümante edilmiş ve tatbikatlarla test edilmiş bir olay/kriz yönetim kabiliyeti,

- Hizmet verdiği ve/veya yükümlü olduğu paydaşlarının gereksinimlerini anlamış ve bu gereksinimlere cevap verecek iş süreçlerinin kurulmuş olması.

A.13.1.5. Kritik iş sürekliliği yönetimi sadece iş sürekliliği planı hazırlanması, yedekleme yapılması, felaket merkezi oluşturulması, prosedürler, detaylı talimatlar oluşturulması değil; bunların bütünleşik olarak hizmet sürekliliğinin iyileştirilmesi amacıyla uygulanmasıdır.

A.13.1.6. İş sürekliliği planları, verilen hizmetleri önceliklendirme, olası tehdit ve zafiyetleri değerlendirerek gerekli önlemleri almak suretiyle hizmet sürekliliğini sağlama, hizmetlerin kesintiye uğramasına neden olan olaylara önceden tanımlanmış senaryolarla müdahale etme, süreçleri onarma ve planlı olarak yeniden başlatma konularında kılavuzluk yapan dokümante prosedürlerdir.

A.13.1.7. İş sürekliliği planları, felaket kurtarma çözümleri değil, felaketin olumsuz sonuçlarının oluşmasını önlemeye odaklanan eylem planlarıdır. Felaket kurtarma senaryoları iş sürekliliği planlarının bir parçasıdır. Felaket kurtarma çözümleri, felaket sonrasında verilerin kurtarılmasına odaklanırken, iş sürekliliği çözümleri, hem verilerin erişilebilirliğini gözetir hem de kurumun felaket sonrasında en hızlı şekilde yeniden hizmet verebilmesine odaklanır.

A.13.2. İş Sürekliliği Adımları

A.13.2.1. Kurumsal iş sürekliliği yönetim sisteminin kurulması ve işletilmesi için öncelikle iş sürekliliği kapsamının belirlenmesi gerekir. Bunun için ilk adım kritik iş süreçlerinin çıkarılması ve önceliklendirilmesidir. İş sürekliliği kapsamı bu şekilde oluşturulur.

A.13.2.2. Kapsam belirlendikten sonra bu iş süreçlerine ilişkin mevcut durum analizi yapılır. Mevcut durum analizinde kurumun kritik iş süreçlerinin fotoğrafı çekilir. Yürütülen bu hizmetleri kesintiye uğratabilecek tehditler var mı, bu tehditlerle ilgili süreçte zayıf noktalar var mı gibi hususlar incelenir ve detaylı analiz edilir. Başarılı bir mevcut durum analizi için kurumsal risk yönetimi sürecinin kurum kültürü olarak benimsenmiş, risk haritaları çıkarılmış ve kurumsal kabul edilebilir risk seviyesi belirlenmiş olmalıdır.

A.13.2.3. İş sürekliliğinin kapsamının belirlenip, mevcut durum analizi yapıldıktan sonra, hangi iş sürecinin kesintisiz hizmet verebilmesi için hangi kaynaklara ihtiyaç olduğunun dokümante edilmesi ile kaynak planlaması ortaya koyulur.

A.13.2.4. Her başarılı süreç yönetiminde olması gerektiği gibi iş sürekliliği süreci için roller ve sorumluluklar atanır.

A.13.2.5. Atanmış olan sorumlular tarafından hizmetleri kesintiye uğratabilecek olumsuz senaryolar tatbikatlarla test edilir, sonuçlar değerlendirilir, varsa aksaklıklar giderilir ve sürekli takip edilir.

A.13.2.6. Kritik Varlıkların / Süreçlerin Tanımlanması

A.13.2.6.1. Kurum tarafından gerçekleştirilen tüm iş süreçleri önemli kabul edilirken, bir olay meydana gelmesi durumunda, kurum mevcudiyeti ve itibarı açısından kritik önem taşıyan süreçlerin ayağa kaldırılmasına öncelik verilir. İş sürekliliği yönetimi için öncelikle kritik iş süreçlerinin ve bu süreçlerde kullanılan sistemlerin belirlenmesi ve listesinin oluşturulması gerekir.

A.13.2.6.2. Yürütülen iş, işlem ve sürecin kritik olabilmesi için aşağıda belirlenen durumlardan en az birine uygun olması gerekir;

A.13.2.6.2.1. İş sürecinin kesintiye uğraması ya da yavaşlaması durumunda kurum için yasal, finansal, operasyonel ve benzeri büyük riskler oluşur.

A.13.2.6.2.2. İş sürecinin etkilediği ya da etkilendiği sistem ya da paydaşlar, stratejik olarak önemli ya da geniş kitlelerdir.

A.13.2.6.2.3. İş süreci insan hayatını ya da toplum sağlığını etkilemektedir.

A.13.2.6.2.4. İş sürecinin kesintiye uğraması kurumsal itibarı maddi ya da manevi olumsuz bir şekilde etkileyecek niteliktedir. (Örneğin SBYS'ler)

A.13.2.6.3. Kritik varlıklar / süreçler belirlenirken;

A.13.2.6.3.1. Süreç ile ilgili iç ve dış yükümlülükler,

A.13.2.6.3.2. Süreçten yararlanan / hizmet alan paydaşların hizmet sürekliliği ihtiyaçları,

A.13.2.6.3.3. Yasal ve düzenleme amaçlı atanan sorumluluklar,

A.13.2.6.3.4. Protokollerle anlaşmaya varılmış hizmet zorunlulukları,

A.13.2.6.3.5. Hizmetin sürdürülmesinde başarısız olunması durumunda sonuçlarının ne büyüklükte olacağı gibi hususlar dikkate alınarak KLVZ-EK-22 İş Sürekliliği Formları arasında yer alan "Kritik Süreçler / Varlıklar Listesi" oluşturulur ve iş sürekliliği kapsamı belirlenir.

A.13.2.6.4. Kritik iş süreçlerinin tanımlanmasında yararlanılacak ve kritik süreçler / varlıklar listesi ile ilişkilendirilecek dokümanlar;

A.13.2.6.4.1. Varsa hizmet bekleyen ve yasal yükümlülüklerle bağlı olunan dış paydaşlarla yapılan protokollerin listesi,

A.13.2.6.4.2. Tedarikçiler ile yapılan sözleşmeler,

A.13.2.6.4.3. Kurumdan beklenen kritik hizmetlerin sağlanmasını destekleyen tüm iş süreçlerinin / faaliyetlerin envanteridir.

A.13.2.7. Mevcut Durum Analizi

A.13.2.7.1. Kritik iş süreçlerinin sürekliliğinin sağlanmasına ilişkin gerekli olan koşulların ortaya koyulduğu ve iş sürekliliğine engel olabilecek olası tehditlerin tespit edildiği aşamadır.

A.13.2.7.2. İş etki analizleri ve risk işleme çalışmalarının değerlendirilmesi ile mevcut durum ortaya koyulur.

A.13.2.7.3. İş etki analizi, iş kesintisine neden olabilecek durumlar ve bunların etkilerinin değerlendirilmesidir. Kesintiye neden olabilecek durumlar, darboğazlar, zafiyetler göz önüne alınarak süreçlerin kapsamlı bir fotoğrafı çekilir, sınıflandırılır (az önemliden en önemliye doğru sıralanır) ve buna yönelik olarak risk işleme çalışmaları yapılır.

A.13.2.7.4. İş sürekliliğinin temelinde risk yönetimi vardır. İş etki analizinden edinilen bilgilere göre kesintiye yol açabilecek olayların riskleri tanımlanır. Risk yönetimi, iş etki

analizleri ile ilişkilendirilmiş risk değerlendirme raporunun hazırlanması vb. süreçler Kılavuzun A.5.3 (Risk Yönetimi) maddesinde açıklanmıştır. İş sürekliliği için planlama yapılırken kurumsal risk yönetimi dikkate alınır.

A.13.2.7.5. İş etki analizleri ve risk değerlendirme çalışmaları neticesinde; kritik iş süreçlerine yönelik tehditler, zafiyetler, olasılıklar ve alınacak önlemler ile mevcut durum analizi ortaya koyulur.

A.13.2.8. Kaynak Planlaması

A.13.2.8.1. Kritik iş süreçlerinin en temel fonksiyonlarının, en az veri kaybı ile en kısa sürede tekrar hizmet verebilir duruma getirilmesinin sağlanması için hangi kaynaklara ne kadar ihtiyaç duyulduğunun ve bu kaynakların maliyetinin çıkarılması gerekir.

A.13.2.8.2. Kaynak planlaması yapılırken o işin sürekliliğinin sağlanması için ihtiyaç duyulan tüm mali kaynaklar, teknoloji, alt yapı, tedarik edilecek malzemeler, bina, ulaşım ve benzeri kaynak tipleri ve tanımlanmış yetkinlikleri ile beraber personel detaylı olarak belirlenir ve KLVZ-EK-22 İş Sürekliliği Formları içinde örneği yer alan “Kaynak İhtiyaç Listesi” oluşturulur.

A.13.2.8.3. İş sürekliliği kaynak ihtiyaç listesi, 24 saat – 72 saat – 1 hafta gibi iş kurtarma fazları için ayrı ayrı detaylı olarak oluşturulabilir. 24 saat fazında en temel ihtiyaçlar planlanırken, devam eden fazlarda daha detaylı ihtiyaç duyulacak kaynaklar belirtilebilir.

A.13.2.8.4. Kaynak planlarken kriz yönetim merkezi olarak kullanılabilecek 7X24 kullanıma uygun, internet bağlantısı, telefon/mobil telefon, taşınabilir bilgisayar, projeksiyon cihazı, yazı tahtası, muhtelif kırtasiye donanım ve imkanlarının hazır bulundurulduğu kriz yönetim merkezinin de belirlenerek kararının alınması gerekir.

A.13.2.9. Roller ve Sorumluluklar

İş sürekliliği süreçlerinin standartlara uygun ve etkin şekilde işletilebilmesi için ı gereken oluşturulması gereken organizasyon yapısı ve roller Şekil 5’te açıklanmıştır.

A.13.2.9.1. Üst Yönetim;

A.13.2.9.1.1. Üst Yönetim kritik iş süreçlerinin sürekliliğinin sağlanmasından birinci derecede sorumludur.

A.13.2.9.1.2. Bilgi güvenliği alt komisyonu tarafından belirlenen iş sürekliliği hedeflerini onaylar. (Örnek iş sürekliliği hedefi: X faaliyetlerinin Y zamanda ayağa kaldırılması, X faaliyeti felaket senaryosunun Y kez tatbikatlar ile test edilmesi vb.)

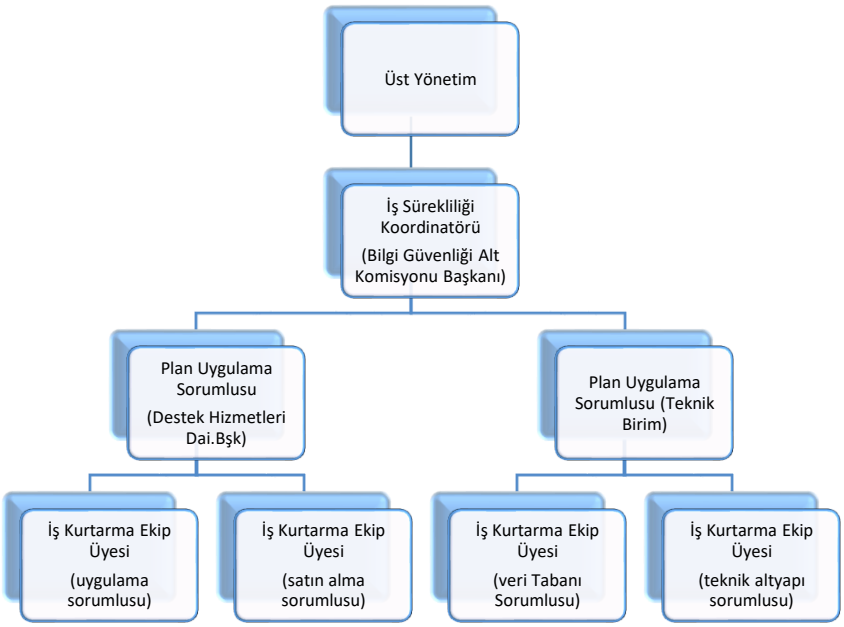
A.13.2.9.1.3. İş sürekliliğinde yer alacak personelin görev yetki ve sorumluluklarını belirler.

A.13.2.9.1.4. Kritik iş süreçlerinin, iş sürekliliği gereksinimlerini ve iş ihtiyaçlarını belirler veya görevlendirmiş olduğu personel tarafından belirlenmesini sağlar.

A.13.2.9.1.5. Belirlenen kaynakların sağlanmasını taahhüt eder.

A.13.2.9.1.6. İş sürekliliğinin sağlanması için sürekli test ve tatbikatları destekler ve bunun için gerekli faaliyetlerin gerçekleştirilmesini sağlar ve kontrol eder.

A.13.2.9.1.7. İş sürekliliği hedeflerini, rol ve sorumlulukları, iş sürekliliği taahhüdünün bulunduğu iş sürekliliği politikasını oluşturur ve yayımlar.



Şekil 5: İş Sürekliliği Organizasyonu

A.13.2.9.2. İş Sürekliliği Koordinatörü;

A.13.2.9.2.1. Bilgi güvenliği alt komisyonu başkanı aynı zamanda kurumun iş sürekliliği koordinatörü olarak görev yapar.

A.13.2.9.2.2. Felaket ya da kesintiye neden olan büyük çaplı olayların nasıl yönetileceği ve verilen hizmet ve faaliyetlerin belirlenen sürelerde nasıl geri döndürüleceğini tanımlayan İş Sürekliliği Planlarının oluşturulmasından ve işletilmesinden sorumludur.

A.13.2.9.2.3. Kurumun bağlı olduğu güncel mevzuat, yasa, yönetmelik ve sözleşmelerden doğan yaptırım ve yükümlülükleri takip ederek İş Sürekliliği Planlarının güncellenmesini sağlar.

A.13.2.9.2.4. İş sürekliliği planlarının test edilmesi için tatbikatlar düzenler, kayıt altına alınmasını sağlar.

A.13.2.9.2.5. İş sürekliliğini etkileyecek ya da iş sürekliliğinden etkilenebilecek taraflarla iletişimi sağlar.

A.13.2.9.2.6. İş sürekliliğinin sağlanabilmesi için plan uygulama sorumluları ve iş kurtarma ekiplerinin görev dağılımını belirler ve ekiplerin yetkinliğini arttırmak amacıyla iş sürekliliği eğitimlerini planlar.

A.13.2.9.2.7. Planın devreye alınması ve hasar onarımı sonrası normal çalışma durumuna geri dönülmesi kararlarını verir.

A.13.2.9.3. Plan Uygulama Sorumluları;

A.13.2.9.3.1. Kurum organizasyon şemasındaki ilgili yöneticiler ve onların atadıkları sorumlulardan oluşur.

A.13.2.9.3.2. Planın uygulanmasında, İş Sürekliliği Koordinatörü tarafından verilen görevlerin gerçekleştirilmesinden sorumludur.

A.13.2.9.3.3. Acil ve beklenmedik bir durumla karşılaşıldığında kendisine bağlı personeli koordine eder. İş sürekliliği koordinatörüne bilgi akışını sağlar.

A.13.2.9.3.4. İş sürekliliği planının uygulanması için ilgili iş sürecinden sorumlu olan personel ve yedeklerinin yer aldığı iş kurtarma ekiplerini oluşturur.

A.13.2.9.3.5. Yedekten geri dönme işlemleri, ağ konfigürasyonunun restorasyonu, iş uygulamalarının sunucular üzerine kurulum ve konfigürasyonu gibi süreçlerin gerçekleştirilmesinden sorumludur.

A.13.2.9.4. İş Kurtarma Ekipleri

A.13.2.9.4.1. Plan uygulama sorumlularının vermiş olduğu işlerden sorumludur.

A.13.2.9.5. Genel Sorumluluklar;

A.13.2.9.5.1. Hizmetlerin erişilebilirliğinin sağlanması için planlamalar doğru bir şekilde yapılır.

A.13.2.9.5.2. Hizmetlerin erişilebilirlik ve sınıflandırma ile ilgili gereksinimleri hizmet sahipleri tarafından belirlenir.

A.13.2.9.5.3. Kritik iş süreçlerinde yer alan personel, iş sürekliliği planlarında belirtilen görevleri yerine getirmekle ve iş süreklilik tatbikatlarına katılmakla sorumludur.

A.13.3. İş Sürekliliği Stratejisi Belirleme

A.13.3.1. İş sürekliliği planları geliştirilirken; kritik hizmetleri sunan ve bu hizmetlerden faydalanan/faydalanacak iç ve dış paydaşların ihtiyaç ve gereksinimleri, toplantı veya anket gibi çalışmalar ile analiz edilir. Analizler için KLVZ-EK-22 İş Sürekliliği Formları içinde örneği yer alan “Kritik Varlık/Süreç Analiz Formu” kullanılır. Anket veya toplantılardan elde edilecek sonuçlarda asgari olarak aşağıdaki soruların yanıtları elde edilmelidir;

A.13.3.1.1. İşin yürütülmesi için ihtiyaç duyulan yazılım, donanım ve diğer teknolojik bileşenler ve bilgi işlem araçları nelerdir? Ekipman ve sistem gereklilikleri nelerdir? (Bu aşamada "İş Sürekliliği Kaynak İhtiyaç Listesi" kesinleştirilir)

A.13.3.1.2. Özel sözleşme ya da yasa ve mevzuatlara bağlı olarak yerine getirilmesi gereken minimum yükümlülükler nelerdir?

A.13.3.1.3. Sürecin çıktısı olan hizmetin kullanıcıları kimlerdir?

A.13.3.1.4. Hizmet sürekliliğinin sağlanması için bağımlı olunan hizmetler, iş sürekliliğini etkileyebilecek dâhili ve harici taraflar kimler/nelerdir? Sürecin iş sürekliliğinin sağlanması için hangi sistemlere sürekli erişim gereklidir?

A.13.3.1.5. Elektronik verilerin korunması nasıl sağlanmaktadır? Bu veriler korunamazsa nasıl sonuçlar ortaya çıkar? İlgili veriler sürekli erişim için gerekli midir?

A.13.3.1.6. Personelin temel yeterlilik seviyesi nedir? Herhangi bir felaket durumunda başka birimlerden/dış kaynaklardan personel alınması mümkün müdür? Mümkünse hangi birim ya da kaynaklarla iş birliği yapılabilir?

A.13.3.2. Bu aşamada ayrıca iş sürekliliğine engel olabilecek felaket senaryoları oluşturulur ve bu senaryolara nasıl müdahale edileceği yani kurtarma operasyonlarının (nerede yönetilecek, kim yönetecek ve kime raporlayacak) nasıl yönetileceği belirlenir. Kurtarma öncelikleri ve kurtarma zaman hedefleri, müdahale eylem planları ve sorumluları KLVZ-EK-22 İş Sürekliliği Formları içinde yer alan "İş Kurtarma Planı" örneğinde olduğu gibi detaylı olarak dokümante edilir.

A.13.3.3. İş sürekliliği planları; varlık envanteri, bilgi sınıflandırma, bilgi aktarımı, yedekleme, kapasite yönetimi, varlıkların kabul edilebilir kullanımı, risk yönetimi, yasal gereksinimler ve standartlara uyum, konfigürasyon ve değişim yönetimi, fiziksel ve çevresel güvenlik gibi operasyonel faaliyetlerde kullanılan bilgi güvenliği dokümanları göz önüne alınarak hazırlanmalıdır.

A.13.4. İş Sürekliliği Planı Oluşturma

A.13.4.1. Bu bölümde şu ana kadar anlatılan tüm bilgiler; iş sürekliliği planı oluşturulması için idarenin "hangi süreçler kritik, bu süreçlerin sürekliliğini sağlamak için yasa, mevzuat ve sözleşmelerden doğan zorunluluklar neler, iş sürekliliğini tehdit edebilecek unsurlar neler olabilir ve bu tehditleri bertaraf etmek için nasıl hazırlık yapılmalı" gibi durumları analiz ettiği ve iş sürekliliği planını desteklemek için dokümantasyon oluşturduğu süreçleri içerir.

A.13.4.2. İş sürekliliği planları; kesinti anında bütün ihtiyaç duyulabilecek gereksinimlerin tanımlı olduğu ve ilgili tüm taraflar tarafından bilinen ve uygulanması sırasında karmaşaya neden olmayacak şeklinde hazırlanır. İş sürekliliği planları aşağıdaki içeriğe sahip olmalıdır;

- Amaç ve kapsam,

• İş sürekliliği hedefleri,

• Planın hangi koşullarda hayata geçirileceği,

• Olağanüstü durumda kurtarma çalışmalarında kimlerin görev alacağı ve hangi kurtarma adımlarını gerçekleştireceği,

• Olağanüstü durumlarda, gerek organizasyon için gerekse organizasyon dışında iletişime geçilecek kişi ve kurumlar, aynı zamanda iletişimin nasıl sağlanacağı bilgisi,

• İç ve dış bağımlılıklar,

• Planın hayata geçirilmesi için gerekli olan kaynaklar,

• Tanımlanmış iletişim adımları.

A.13.4.3. İş sürekliliği planının, dokümante edilmiş tüm liste ve formların (kritik varlıklar/süreçler listesi, kaynak ihtiyaç listesi, acil durum iletişim listesi, süreç analiz formu vb.) genel çerçevesini sunan tek bir ana doküman olarak hazırlanması, planın amacının, kapsamının ve hedeflerinin uygulayıcılar tarafından daha anlaşılır olmasını sağlar.

A.13.4.4. İş sürekliliği planlarında;

A.13.4.4.1. İş sürekliliği planında acil veya olağanüstü durumların neler olduğunun ve "çok acil, acil ve normal" seviyelerin neler olduğunun tanımlanmış olması gerekir.

A.13.4.4.2. Herhangi bir olağanüstü durum anında iş sürekliliği planında yazılı olan faaliyetleri gerçekleştirecek olan kişilerin rolleri, sorumlukları ve yetkileri önceden belirlenmiş ve tanımlı olmalıdır.

A.13.4.4.3. Yapılan olağanüstü durum tanımları uyarınca, iş sürekliliği planının hangi koşullarda aktive edilmesi gerektiği ve rol bazında yapılması gerekenlerin belirlenmiş olması gerekir.

A.13.4.4.4. Olağanüstü durumun sona ermesi sonrasında iş süreçlerinin olağanüstü durum öncesine dönmesi için yapılması gerekenlerin tanımlanması gerekir.

A.13.4.4.5. Olağanüstü durumun olağan çalışma ortamını kullanılamaz hale getirmesi durumunda alternatif çalışma lokasyonları ve kriz merkezi planlamasının yapılması gerekir.

A.13.4.4.6. İş sürekliliği ekibinde bulunan çalışanların iletişim bilgileri (telefon, e-Posta, adres), kendilerine ulaşılamadığı durumlarda alternatif olarak kullanılacak iletişim bilgilerine nasıl ulaşılacağının plana dâhil edilmesi gerekir.

A.13.4.4.7. Olağanüstü durum ile ilgili medya ve kamu bilgilendirmesinin nasıl yapılacağına ilişkin kurumsal iletişim stratejisinin de planda yer alması gerekir.

A.13.4.5. Kritik iş sürekliliği yönetimi, bütünleşik olarak hizmet sürekliliğinin iyileştirilmesi amacıyla uygulanır. Bir yönetim sistemi mantığı ile işletilmesi gerekir. Bu nedenle bu süreç önceden hazırlanması ve sürekli gözden geçirilmesi gereken bir takım dokümanlarla desteklenmelidir. İş sürekliliği dokümanları;

A.13.4.5.1. Bilgi güvenliği tehdit listesi ve ihlal olayları olay müdahale süreç dokümanları,

A.13.4.5.2. Kritik varlıklar / süreçler listesi,

A.13.4.5.3. Kaynak ihtiyaç listesi,

A.13.4.5.4. Kritik tedarikçiler, acil durum ilk müdahale ekip üyeleri ve yedeklerinin yer aldığı acil durum iletişim listesi,

A.13.4.5.5. Uzmanlık, yetkinlikler ve tanımlanmış sorumlulukları ile iş sürekliliğinin sağlanmasından sorumlu personel ve yedeğinin yer aldığı iş telefonu, ev telefonu, cep telefonu, iş ve kişisel e-Postası ve normal iletişimin kullanılamayacağı durumlarda irtibat kurmanın yollarını içeren acil durum iletişim listesi,

A.13.4.5.6. Felaket sonrası kritik faaliyetler için kurtarma sırası (acil veya olağanüstü durum yönetimi (kurtarma), devam etme ve normale dönüş) içeren olay müdahale planları, tatbikat ve testlerin kayıtları,

A.13.4.5.7. Sistem kapasitesi ve eşik değerlerin izlenme raporları,

A.13.4.5.8. Kritik hizmetin sürdürülmesine destek olan altyapı envanteri (donanım, yazılım, teknik ekipmanlar, sunucular, veri tabanları, internet vb.) ve yedekleme planları

A.13.4.5.9. Tatbikat test uygulama formu,

A.13.4.5.10. İş süreklilik planı sonrası yapılan değerlendirme formu.

A.13.5. İş Sürekliliği Planlarını Tatbikatlar ile Test Etme

A.13.5.1. Tatbikatlar öngörülen risklere karşı hazırlık seviyesinin ölçüldüğü aktivitelerdir. Kapsamlı bir hazırlık süreci gerektirir aksi halde ciddi kesintilerin yaşandığı olumsuz durumlar ile karşılaşılabilir.

A.13.5.2. Tatbikat türleri maliyet, zaman, karmaşıklık, efor ve normal operasyonda oluşacak kesintiler açısından farklı özelliklere sahiptir.

A.13.5.3. Tatbikat türleri ve açıklamaları Tablo-1'de verilmiştir.

Tatbikat Türü	Tanım
Kavramsal tatbikat	İş sürekliliği planı ve ilgili dokümantasyonun gözden geçirilmesidir.
Detaylı kavramsal tatbikat	Kavramsal tatbikatın daha detaylı olarak yerine getirilmesidir. Bu tatbikat türünde planda yer alan her adımın üzerinden geçilerek eksiklikler tespit edilmeye çalışılır.
Simülasyon	Bu tatbikat türünde örnek bir olay üzerinden iş sürekliliği planı çalıştırılır. Tatbikat sırasında süreç veya sistemlerde herhangi bir kesinti gerçekleştirilmez. İş sürekliliği planı kesinti gerçekleşmiş gibi düşünülerek çalıştırılır ve tatbikatı yapılır.
Bileşen veya servis tatbikatı	İş süreçlerinin bir kısmı için gerçekleştirilir. İş süreçlerinde kesintiye neden olabilecek bir olay gerçekleştirilir ve süreç tekrar çalışır hale getirilir. Bu tatbikat çalışan bir sistem üzerinde gerçekleştirildiğinden, kurumun acil durum tatbikatı kapsamında olmayan operasyonunu aksatmayacak biçimde planlanması gereklidir.
Tam tatbikat	İş sürekliliği planının tamamının test edilmesidir. Tam tatbikat kurum süreçlerinin felaketten kurtarma merkezinde tekrar çalıştırılmasını da kapsayan detaylı bir tatbikattır.

Tablo 1 Tatbikat Türleri

A.13.5.4. İş sürekliliği tatbikatları; tatbikata hazırlık, tatbikatın gerçekleştirilmesi ve tatbikatın değerlendirmesi olmak üzere üç adımda gerçekleştirilir.

A.13.5.5. Tatbikata hazırlık: Varsa daha önce gerçekleştirilen tatbikat planları ve sonuçları incelenir. Tatbikat zamanı, senaryosu, değerlendirme ölçütleri ortaya koyulur. Tatbikat riskleri değerlendirilir ve tatbikat programı yapılır. KLVZ-EK-22 İş Sürekliliği Formları içinde yer alan Tatbikat Test Uygulama Formu, yapılacak tatbikata özgü ihtiyaçlara göre özelleştirilmek suretiyle kullanılabilir.

A.13.5.6. Tatbikatın gerçekleştirilmesi: Tatbikatlar bir önceki adımda hazırlanan plana uygun olarak icra edilir. Tatbikat kanıtları kayıt altına alınır. Tatbikatın bitmesi sonrasında ilgili taraflar ve katılımcılar bilgilendirilir.

A.13.5.7. Tatbikatın değerlendirilmesi: Tatbikat bulguları incelenerek tatbikat değerlendirme raporu hazırlanır. Varsa yaşanan sıkıntılar, iş sürekliliğinde görev alan personelin performansı, kullanılan kaynak ve ortamın yeterliliği gibi hususlar raporda belirtilir.

A.13.5.8. Sürekli iyileştirmenin sağlanması için planlar belirli sıklıklarla tatbikatlar ile test edilir. Planların test edilme sıklığı planlarda belirtilmelidir.

A.13.5.9. Tatbikatlardan elde edilen bulgular, kurumların bilgi güvenliği dokümantasyonuna ve bir sonraki eğitime dâhil edilir.

A.13.5.10. Tatbikat sonuçlarına göre planlar tekrar gözden geçirilir, gerekiyorsa düzeltici faaliyet planlanır, ihlal olayları müdahale süreçleri ve risk çalışmalarına yansımaları değerlendirilir.

A.14. UYUM

A.14.1. Yasal Gereksinimlere Uyum

A.14.1.1. İdarenin kanuniliği ilkesi, hukuk devletinin temel ilkelerindendir. Bu ilke gereğince idarenin iş ve işlemleri bir kanuna dayanmalı, aynı zamanda bu iş ve işlemler kanunlara aykırı olmamalıdır. Yani kanunlar, idarenin faaliyette bulunabilmesinin hem şartı, hem de sınırı durumundadır. Burada "kanunlar" ifadesinden salt TBMM tarafından çıkarılan kanunları değil normlar hiyerarşisi gereği "anayasa, uluslararası sözleşmeler, kanun, kanun hükmünde kararname, tüzük, yönetmelik, yönerge/genelge ve idare tarafından çıkarılan diğer yazılı talimatları anlamak gerekir.

A.14.1.2. İdarenin kanuniliği ilkesi gereği, Bakanlığımız merkez teşkilatı ve bağlı kuruluşlar tarafından yapılacak her türlü iş ve işlemin kanuni bir dayanağının bulunması, bu iş ve işlemlerin mevzuata aykırı olmaması ve kanunlarca zorunlu tutulan konuların yerine getirilmesi için gerekli tedbirlerin alınması; özetle yasal gereksinimlere uyum sağlanması gerekmektedir.

A.14.1.3. İdare için makul güvenlik tedbirlerinin alınması, yalnızca siber olaylara ilişkin tedbirlerin alınması olarak algılanmamalıdır. Yasal yükümlülükleri ihmal ya da ihlal davaları, cezalar veya olumsuz medya haberlerinin de kurumsal imajı ya da değerleri siber olaylarla aynı oranda tehdit edebileceği göz önünde bulundurulmalıdır.

A.14.1.4. İdare, ilgili tüm kanuni yasal, düzenleyici, sözleşmeye dayalı şartlar ve bu gereksinimleri karşılama yaklaşımını açıkça tanımlamak, yasal düzenlemelerin gerekliliklerine uyum için talimat ya da prosedürleri yayımlamak ve güncel tutmakla sorumludur.

A.14.1.5. Yasal gereksinimler; bilgi teknolojileri ile ilgili güvenlik gereksinimleri, fikri mülkiyet hakları / telif hakları yasaları, gizlilik, veri şifreleme ve verileri koruma yasaları şeklinde olabilir. Yasa ve yönetmeliklerin takip edildiğinden emin olmak için öncelikle tüm uyum gerektiren düzenlenmelerin yer aldığı bir liste oluşturulmalıdır. Örnek liste KLVZ-EK-23 Yasal Mevzuat Uyumu İçin Takip Listesinde yer almaktadır.

A.14.1.6. Kanunlar ve yönetmelikler, güvenlikle ilgili olayların sıklığı ve etkisinin büyüklüğü, gelişen teknoloji ve ihtiyaçlara bağlı olarak değişebilen yaşayan varlıklardır. Siber suçların Türk Ceza Kanunu'nda ilk yer alışı 6 Haziran 1991 tarihli 3756 Sayılı Türk Ceza Kanununun bazı maddelerinin değiştirilmesine dair kanun ile olmuştur. Bu değişikliğin 20. maddesi ile "Bilişim Alanında Suçlar" başlığı altında bir bölüm eklenmiş ve bir bilgisayardan programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru olarak kabul edilmiştir. Takip eden süreçte yeni teknolojilerin kullanılmaya başlanması ile güvenlik ihtiyaçları farklılaşmış ve yeni mevzuatlar eklenmiş ve teknoloji gelişmeye devam ettiği sürece eklenmeye devam edecektir. Bu nedenle, oluşturulan listenin güncellenmesinden sorumlu olacak bir yetkili personel ya da ekibin belirlenmesi gerekmektedir. Uyulması gereken yasal mevzuatların belirlenmesi ve takibi süreci yalnızca bilgi sistemleri veya bilgi güvenliği birimlerinin işi olarak değerlendirilmemeli, hukuk, insan kaynakları, idari mali işler gibi birimlerden de destek alınması gerekmektedir.

A.14.1.7. Hangi şartların kurumu etkileyebileceğinin belirlenmesinin ardından geçerli güvenlik önlemlerinin uyumluluk için yeterli olup olmadığının veya gereksinimleri karşılamak için ek önlemlerin alınması gerekip gerekmediğinin belirlenmesi gerekir. Örneğin, 5651 no'lu yasa ile ilgili, Bilgi Teknolojileri Kurumu (BTK) her kurum için bazı yükümlülükler getirmiştir. Bu yükümlülüklerden biri de zaman ve tarih mührü ile erişim iz kayıtlarının tutulmasıdır. İdare ilgili yasa gereği; öncelikle yükümlülüklerini anlamalı, uygulamakta olduğu bir iz kayıt yöntemi varsa yasanın gerekliliklerini karşılayıp karşılamadığını kontrol etmeli ve eğer gerekiyorsa ek önlemler almalıdır.

A.14.2. Lisanslama ve Fikri Mülkiyet Hakları

A.14.2.1. Fikri mülkiyet insan zekâsının, entellektüel birikiminin, zihinsel yaratıcılığının ortaya çıkarmış olduğu müzikten, edebiyata, endüstriyel tasarımlardan bilimsel buluşlara kadar uzanan geniş bir yelpaze içinde yer alan ürünleri kapsar. Bu ürünler düşünce safhasında kaldığı ve üreticisi dışındakilerle paylaşılmadığı sürece korumaya konu olmazlar. Ancak bu düşüncelerin ve ürünlerin, uygun şekilde kayıt altına alınmalarını takiben diğer kişilerle paylaşılmaları ve özellikle bu ürünlerin kazanç amacıyla ticarete konu olmaları söz konusu olduğu zaman korunmaları gerekir.

A.14.2.2. Fikri mülkiyet, sınai mülkiyet hakları ve telif hakları olmak üzere iki ana başlık altında incelenir.

A.14.2.3. Sınai mülkiyet hakları; teknolojik buluşlar, patentler, mal ve hizmetlerin ticari markaları, modeller, endüstriyel tasarımları ve coğrafi işaretleri kapsar. Bu haklar 6769 Sayılı Sınai Mülkiyet Kanunu ile korunur. Tescil işlemleri, Türk Patent ve Marka Kurumu tarafından koordine edilir.

A.14.2.4. Telif hakları; edebiyat, müzik, sanat ürünleri ve görsel-işitsel ürünler, filmler, bilgisayar program ve yazılımlarını ortaya çıkaran kişilerin bu ürünler üzerindeki haklarını içerir. Bu haklar 5846 sayılı Fikir ve Sanat Eserleri Kanunu ile korunur. Konu ile ilgili faaliyetler, T.C. Kültür ve Turizm Bakanlığı Telif Hakları Genel Müdürlüğü tarafından yürütülür.

A.14.2.5. Bakanlığımıza bağlı tüm birimlerce yapılan her türlü iş ve işlemlerde, fikri mülkiyet haklarına saygılı davranılır. Bu hakların korunması için gerekli tedbirler alınır.

A.14.2.6. Lisanslı yazılım kullanımı ile ilgili hususlarda Başbakanlık'ın 2008/17 sayılı Genelgesinde belirtilen esaslara dikkat edilir. Genelge ile lisanslı yazılım kullanımı ile ilgili işlerde "birinci derecede" sorumluluğun "ilgili kamu kurum ve kuruluşunda bilgi işlem ünitesi veya bu işten sorumlu birimde çalışanlara" verilmiş olduğu dikkate alınır.

A.14.2.7. Çeşitli maksatlar için tedarik edilen yazılımlar, kurumların taşınır kayıt birimleri tarafından envantere alınmak suretiyle kayıt altına alınır. Ayrıca kılavuzun Varlık Yönetimi başlıklı bölümünde belirtilen KLVZ-EK-05 Kurum Bilgi Varlıkları Envanter Çizelgesine işlenir.

A.14.2.8. Yazılımlara ait lisans belgeleri, yazılımın üreticisi firma tarafından sağlanan lisans takip/indirme sayfasına erişim şifresi, varsa CD/DVD ve benzeri materyal, USB dongle vb. anahtarlar, ilgili projenin yürütüldüğü birimde muhafaza edilir.

A.14.2.9. Herhangi bir proje veya faaliyet kapsamında yeni bir yazılım tedarik edilmesi ihtiyacı olduğunda, tedarik faaliyetine başlanmadan Kurumun bilgi işlem sorumlusu ve taşınır kayıt birimi ile koordinasyon kurulur.

A.14.2.10. Bakanlığımıza ait hiçbir cihazda, üreticisi tarafından açıklanmış lisanslama politikasına aykırı bir şekilde (lisanslama/kullanım anahtarının kırılması, yazılımın izinsiz olarak kopyalanması vb.) yazılım kullanılamaz.

A.14.2.11. Lisans çerçevesinde izin verilen kullanıcı sayısının aşılmaması için gerekli tedbirler alınır. Lisans sözleşmesi çerçevesinde izin verilen lisans birim sayısının aşılması (işlemci, disk, sunucu, kullanıcı, adet vb.) durumunda A.9.3. maddesinde belirtilen Kapasite Yönetimi ve A.13.2.8. maddesinde belirtilen Kaynak Planlaması süreçleri devreye alınır.

A.14.2.12. Çeşitli isimler altında (open source, freeware, shareware) ücretsiz olarak dağıtılan yazılımlar, zararlı öğeler barındırma ihtimaline karşı test edilmeden kuruma ait bilgisayarlara kurulmaz.

A.14.2.13. Bakanlık çalışanlarınca, görev tanımlarının bir parçası olarak resmi bir hizmetin ifası için kurum kaynakları kullanılmak suretiyle üretilen (her türlü bilgi, belge, rapor, doküman, grafik, kitapçık, sunum, tasarım, proje, yazılım vb.) fikri mülkiyete konu olabilecek varlıkların mülkiyeti, Bakanlığımıza aittir. Bakanlık söz konusu varlıkları, ilgili mevzuat uyarınca kendi adına tescil ettirebilir. Kişiler, söz konusu varlıklar üzerine kişisel bir hak iddia edemezler.

A.14.2.14. Aksi kararlaştırılmadıkça, tedarik sözleşmeleri kapsamında yüklenici firmalar tarafından yapılan/yaptırılan tasarım, geliştirme ve/veya eklemelere ilişkin ortaya çıkan fikri mülkiyet hakları Bakanlığımıza aittir. Bu kapsamda, yükleniciler tarafından geliştirilen (tasarım, yazılım, yazılım kodu, algoritma vb.) fikri mülkiyete konu olabilecek varlıklar, sözleşme süresi sonunda idare tarafından teslim alınır. Yükleniciler ve/veya çalışanları, söz konusu varlıklar üzerinde kişisel/kurumsal bir hak iddia edemezler. Bakanlık, söz konusu fikri mülkiyet haklarından Yükleniciyi bir lisans sözleşmesi çerçevesinde (bedeli mukabili veya bedelsiz olarak) faydalandırabilir.

A.14.2.15. Yüklenici firmalar, sözleşmeler kapsamında Bakanlığımız için yaptıkları iş ve işlemlerde üçüncü taraflara ait herhangi bir fikri mülkiyet hakkını ihlal edemezler. Bu husus sözleşmelere konulmak suretiyle garanti altına alınır.

A.14.2.16. Telif hakları kapsamında korunan kitaplar, makaleler, raporlar ve diğer belgeler hiçbir şekilde kopyalanamaz, çoğaltılmaz ve dağıtılamaz.

A.14.2.17. Fikri mülkiyet haklarının ihlal edilmesi ile ilgili şikâyetler www.bilgiguvenligi.saglik.gov.tr adresinde yer alan Olay Bildirim Uygulaması vasıtasıyla Bakanlığa iletilir.

A.14.3. Kişisel Verilerin Korunması Mevzuatı

A.14.3.1. Anayasa'nın 20'ci maddesinin, 6698 sayılı kanunun ve Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin, kişisel verilerin korunmasına ilişkin hükümlerine azami düzeyde hassasiyet gösterilir.

A.14.3.2. Kişisel verilerin ve kişisel sağlık verilerinin işlenmesinde, 6698 sayılı kanunun 4'üncü maddesinde yer alan genel ilkelere; ayrıca kişisel verilerin işlenmesinde Kanun'un 5'inci maddesinde, kişisel sağlık verilerinin işlenmesinde ise Kanun'un 6'ncı maddesinde yer alan hükümlere riayet edilir.

A.14.3.3. Kişisel verilerin ve kişisel sağlık verilerinin aktarılmasında, 6698 sayılı kanunun 8'inci ve 9'uncu maddesinde yer alan hükümlere riayet edilir.

A.14.3.4. 6698 sayılı kanunun 12'nci maddesinin birinci fıkrası uyarınca veri sorumlusu; verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek, verilerin muhafazasını sağlamak amaçlarıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

A.14.3.5. 6698 sayılı kanunun 12'nci maddesinin ikinci fıkrası uyarınca veri sorumlusu (İdare), kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişiler (sağlık hizmet sunucularında HBYS işletimi hizmeti veren yüklenici) ile birlikte müştereken sorumludur.

A.14.3.6. 6698 sayılı kanunun 12'nci maddesinin üçüncü fıkrası uyarınca veri sorumlusu, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Dolayısı ile Kanun hükümlerine uyumluluğun sağlanıp sağlanmadığı hususunda veri sorumlusu, veri işleyeni (HBYS işletimi hizmeti veren yüklenici) denetleyebilir.

A.14.3.7. 6698 sayılı kanunun 12'nci maddesinin dördüncü fıkrası uyarınca veri sorumlusu ile veri işleyen (HBYS işletimi hizmeti veren yüklenici), öğrendiği kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

A.14.3.8. Kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ile 140'ıncı madde hükümleri uygulanır.

A.14.3.9. 6698 sayılı kanun hükümlerine uygunsuzluk nedeniyle KVKK tarafından verilecek idari para cezaları ile ilgili kişiler tarafından açılacak davalarda hükmedilecek maddi ve manevi tazminat davaları, kusurlu olması hâlinde veri işleyen (SBYS işletimi hizmeti veren yüklenici) tarafından ödenir.

A.14.4. 5651 Sayılı Kanun ile Uyum

A.14.4.1. Türkiye'de internet ile ilgili en kapsamlı düzenleme 2007 yılında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile sağlanmıştır.

A.14.4.2. 5651 sayılı kanun ile temel olarak aşağıdaki hususlarda düzenlemeler yapılmıştır:

A.14.4.2.1. İnternet aktörlerinin (içerik sağlayıcı, yer ve erişim sağlayıcı, toplu kullanım sağlayıcı) tanımı yapılmış ve bu aktörlerin hak ve sorumlulukları belirlenmiştir.

A.14.4.2.2. Yasada suçlar bakımından erişimin engellenmesi usul ve esasları düzenlenmiştir.

A.14.4.2.3. İnternet ortamında yayımlanan içerik nedeniyle haklarının ihlal edildiğini iddia eden kişilere ilişkin; içeriğin yayından çıkarılmasını sağlama ve cevap hakkı uygulamalarına ilişkin usul ve esaslara yer verilmiştir.

A.14.4.2.4. Konusu suç teşkil eden (ve/veya küçükler için zararlı olan) içerik kapsamında filtreleme usulü öngörülmüştür.

A.14.4.2.5. Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen katalog suçlara ilişkin şikâyetlerin yapılabileceği internet bilgi ihbar merkezi (ihbarweb.org.tr) kurulmuştur.

A.14.4.3. Bakanlığımız bağlısı kurum ve kuruluşlarda tesis edilmiş olan ağların hemen hemen tamamına yakını bir şekilde internet ortamına bağlı olarak çalışmakta ve Kanunda belirtilen internet aktörlerinden "**içerik sağlayıcı, yer sağlayıcı** veya **toplu kullanım sağlayıcı**" rollerinden bir veya birkaçına girebilmektedir.

A.14.4.4. "Erişim sağlayıcı" kuruluşlar, abonelerine ticari olarak internet erişimi sağlayan telekomünikasyon firmaları olup Bakanlığımıza bağlı hiçbir kurum bu kategoriye girmemektedir.

A.14.4.5. İçerik Sağlayıcı, İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir. Bakanlık merkez teşkilatı, bağlı kuruluşlar ve taşra teşkilatı birimleri web sayfaları vasıtası ile kullanıcılara içerik sundukları için "**İçerik Sağlayıcı**" konumundadır.

A.14.4.6. İçerik Sağlayıcı;

A.14.4.6.1. İnternet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

A.14.4.6.2. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur.

A.14.4.7. Yukarıda belirtilen nedenlerle; Bakanlığımıza bağlı kurum ve kuruluşların web sayfalarında yer alan her türlü içeriğin mutlaka bir sahibi olmalı ve kayıt altına alınmalı, kurumun web sayfasında içerik yayımlama ile ilgili usul ve esaslar belirlenmeli, yazılı hale getirilmeli ve titizlikle uygulanmalıdır.

A.14.4.8. Kılavuzun A.6.12 numaralı maddesinde belirtilen Merkezi Web İçerik Yönetim Sistemi vasıtasıyla sunulan içerikten, sistemi işleten SBSGM değil ilgili web sitesine içeriği koyan kişi veya kurumlar sorumludur.

A.14.4.9. Yer Sağlayıcı, internet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.

A.14.4.10. Yer sağlayıcı;

A.14.4.10.1. Yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, Kanun ve ilgili mevzuat hükümlerine göre BTK, adli makamlar veya hakları ihlal edilen kişiler tarafından haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde, hukuka aykırı içeriği yayından kaldırmakla,

A.14.4.10.2. Yer sağlayıcı trafik bilgisini ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri iki yıl süre ile saklamakla sorumludur.

A.14.4.10.3. Yer sağlayıcı trafik bilgisi, internet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgilerdir.

A.14.4.11. Bakanlık merkez, bağlı kuruluşlar ve taşra teşkilatı birimlerine ait web sayfalarının ve uygulamaların sunumunda kullanılan yazılım ve donanımları işleten birimler “Yer Sağlayıcısı” konumundadır. Bu kapsamda;

A.14.4.11.1. Web siteleri, Merkezi Web İçerik Yönetim Sistemi vasıtasıyla sunuluyorsa yer sağlayıcısı SBSGM,

A.14.4.11.2. Web siteleri ve uygulamaları, kuruma ait sunucu/sistemler vasıtası ile sunuluyorsa yer sağlayıcısı ilgili kurumun kendisi,

A.14.4.11.3. Web siteleri barındırma hizmeti, hizmet alımı ile SBYS firmaları veya diğer üçüncü kişilerden alınıyorsa yer sağlayıcısı ilgili SBYS firması veya üçüncü kişiler olmaktadır.

A.14.4.12. Web siteleri barındırma hizmeti, hizmet alımı ile SBYS firmaları veya diğer üçüncü kişilerden alınıyorsa, A.14.4.10 maddesinde yer alan hususun ilgili firmalar tarafından yapılmasını temin etmek için hizmet sözleşmelerine konu ile ilgili maddelerin koyulması ve yapılacak firma denetimleri ile bu verilerin alındığının kontrol edilmesi gerekir.

A.14.4.13. İnternet Toplu Kullanım Sağlayıcılar, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişilerdir. Bakanlığımıza ait

kurum ve kuruluşlarda tesis edilen bilişim altyapısı kullanılmak suretiyle, son kullanıcılara internet ortamına erişim sağlanıyorsa, ilgili kurum ve kuruluşlar "İnternet Toplu Kullanım Sağlayıcı" konumundadır.

A.14.4.14. İnternet Toplu Kullanım Sağlayıcıları;

A.14.4.14.1. Erişim kayıtlarını ve bu kayıtların doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri 2 (iki) yıl süre ile saklamakla,

A.14.4.14.2. Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme (İnternet ortamında web adresi, alan adı, IP adresi, kelime ve benzeri ölçütlere göre erişimi engelleyen yazılımları ve donanımları) sistemini kullanmakla,

A.14.4.14.3. Kamuya açık alanlarda internet erişimi sağlayan toplu kullanım sağlayıcılar, SMS ve benzeri yöntemlerle kullanıcıları tanımlayacak sistemleri kurmakla sorumludur.

A.14.4.14.4. Erişim kaydı olarak kullanıcılara iç ağda dağıtılan IP adres bilgilerinin, IP adreslerinin kullanıma başlama ve bitiş zamanlarının ve bu IP adreslerini kullanan bilgisayarların MAC adreslerinin, hedef IP adreslerinin, bir veya birden fazla IP adresinin portlar aracılığı ile kullanıcılara paylaştırılması yöntemi ile sunulan internet erişim hizmetinde kullanıcılara tahsis edilen gerçek IP ve port bilgilerinin kayıt altına alınması gerekir.

A.14.4.15. İnternet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sisteminin yanı sıra, ilave tedbir olarak güvenli internet hizmeti de alabilirler.

A.14.5. Bilgi Güvenliği Denetimleri

A.14.5.1. Kılavuzda yer alan kontrol önlemlerinin Bakanlığımıza bağlı birimler tarafından uygulanma düzeyini tespit etmek, varsa aksaklıkları belirlemek ve düzeltici faaliyetlerde bulunmak amacıyla bilgi güvenliği denetimleri yapılır.

A.14.5.2. Bilgi güvenliği denetimleri "yerinde denetim" ve "sistem güvenlik testleri" şeklinde gerçekleştirilir.

A.14.5.3. Sistem güvenlik testleri ile ilgili hususlar, Kılavuzun A.9.15 (Sistem Güvenlik Testleri) maddesinde açıklanmıştır.

A.14.5.4. Yerinde denetimler, Kılavuzda yer alan konuların (tamamının veya seçilecek bazı maddelerin) uygulanma/gerçekleştirilme durumunun, Bakanlık tarafından görevlendirilecek denetçiler vasıtasıyla kontrol edilmesi suretiyle yapılır.

A.14.5.5. Yerinde denetimler, ilgili kurumların en üst düzey yöneticileri imzasıyla yapılacak talep veya yetkili makamlar (Bakan, Bakan Yardımcısı, SBSGM Genel Müdürü) tarafından verilecek talimatlara istinaden planlı olarak yapılır. Denetim için önceden hazırlanan yazılı kontrol formları/soru listeleri kullanılır.

A.14.5.6. Talep üzerine yapılacak denetimler için SBSGM'deki ilgili birimlerde görev yapan denetçi personelin iş yükü dikkate alınarak planlama yapılır.

A.14.5.7. Denetim; sorumlu personel ve son kullanıcılar ile yüz yüze görüşme yapılması, varsa kayıtların incelenmesi, gerekiyorsa ölçümlerin yapılması suretiyle gerçekleştirilir. İhtiyaç var ise A.9.15 (Sistem Güvenlik Denetimleri) maddesinde belirtilen teknik testler de yapılabilir.

A.14.5.8. Bilgi güvenliği denetimi yapacak personelin (denetçiler) denetim yapma tekniği ve denetlenecek konular hakkında eğitim almış personel olması gerekir.

A.14.5.9. Denetimler, Bakanlık personeli tarafından (SBSGM personeli, bağlı kuruluşlar ve il sağlık müdürlükleri bünyesinde görev yapan personelden Bakanlık tarafından bilgi güvenliği denetimi yapmak üzere seçilen ve denetçi eğitimi almış kişiler) yapılır.

A.14.5.10. Denetimlerin çeşitli nedenlerle, Bakanlık personeli tarafından yapılamaması durumunda, Bakanlık tarafından yetkin görülen ve onaylanan yetkili denetim kurumları tarafından da denetim yapılabilir.

A.14.5.11. Talep edilmesi halinde, Sağlık Bakanlığı Denetim Hizmetleri Başkanlığı tarafından Denetim Hizmetleri Yönergesinin 6 (1)(b) maddesi uyarınca yapılacak "bilgi teknolojileri" denetimleri için uzman personel görevlendirilir.

A.14.5.12. Sağlıkta Kalite ve Akreditasyon Daire Başkanlığı tarafından yapılan kalite denetimleri içinde yer alan bilgi yönetimi/bilgi güvenliği ile ilgili ölçümler, bilgi güvenliği denetimlerinin bir parçası olarak değerlendirilir.

EKLER

NUMARASI	ADI
KLVZ-EK-01	İŞE BAŞLAMA FORMU
KLVZ-EK-02	İŞTEN AYRILMA FORMU
KLVZ-EK-03	KAYITTAN DÜŞME TEKLİF VE ONAY TUTANAĞI
KLVZ-EK-04	DİSK İMHA FORMU
KLVZ-EK-05	KURUM BİLGİ VARLIKLARI ENVANTER ÇİZELGESİ
KLVZ-EK-06	RİSK HESAPLAMA FAKTÖRLERİ
KLVZ-EK-07	RİSK İYİLEŞTİRME PLANI
KLVZ-EK-08	E-POSTA TALEP FORMU / GERÇEK KİŞİLER
KLVZ-EK-09	E-POSTA TALEP FORMU / TÜZEL KİŞİLER
KLVZ-EK-10	SUNUCU TALEP FORMU
KLVZ-EK-11	VERİ TABANI / KULLANICI OLUŞTURMA FORMU
KLVZ-EK-12	PERSONEL GİZLİLİK SÖZLEŞMESİ
KLVZ-EK-13	KURUMSAL GİZLİLİK TAAHÜTNAMESİ
KLVZ-EK-14	VT KULLANICI İŞLEMLERİ VE YETKİLENDİRME TALEP FORMU
KLVZ-EK-15	AİLE HEKİMLERİ İÇİN E-NABIZ ERİŞİM İŞ AKIŞI
KLVZ-EK-16	SAĞLIK TESİSİ HEKİMLERİ İÇİN E-NABIZ ERİŞİM İŞ AKIŞI
KLVZ-EK-17	GÜVENLİ YAZILIM GELİŞTİRME KONTROL LİSTESİ
KLVZ-EK-18	YEDEKLEME PLANI
KLVZ-EK-19	YEDEKLEME KONTROL LİSTESİ
KLVZ-EK-20	BİLGİ GÜVENLİĞİ FARKINDALIK BİLDİRGESİ
KLVZ-EK-21	OLAY BİLDİRİM VE MÜDAHALE FORMU
KLVZ-EK-22	İŞ SÜREKLİLİĞİ FORMLARI
KLVZ-EK-23	YASAL MEVZUAT UYUMU İÇİN TAKİP LİSTESİ

Eklerin içeriklerinin güncek ihtiyaçlara göre sık sık değişmesi nedeniyle, son hallerine https://bilgiguvenligi.saglik.gov.tr/Home/Mevzuat adresinden erişim sağlanacaktır.

KATKIDA BULUNANLAR

Adı Soyadı	Unvanı	Birimi
Ahmet ALTUNTAŞ	Birim sorumlusu	SBSGM
Ahmet Esad BERKTAŞ	Birim sorumlusu	SBSGM
Alper ÖZCAN	Birim sorumlusu	SBSGM
Buket ERDOĞAN	Birim sorumlusu	SBSGM
Ayşe GÜL ÇETİN	Birim sorumlusu	SBSGM
Ceyhan VARDAR	Birim sorumlusu	SBSGM
Deniz Tugay YANGI	Birim sorumlusu	SBSGM
Dilek GENÇER ÖZTEKİN	Birim sorumlusu	SBSGM
Dilek KAVAK	Birim sorumlusu	SBSGM
Fatih KARAKÖSE	Birim sorumlusu	SBSGM
Gamze CİMİLLİ	Birim sorumlusu	SBSGM
Gamze KARAKÖSE	Birim sorumlusu	SBSGM
Gizem YILDIZ	Birim personeli	SBSGM
Halil İbrahim ÖZDER	Birim sorumlusu	SBSGM
Mehmet CAVLAMAZ	Birim sorumlusu	SBSGM
Nuran ERDEM	Uzman	Kırklareli İl Sağlık Müdürlüğü
Nurullah ÇAKIR	Birim sorumlusu	SBSGM
Ruhi YİYİT	Birim sorumlusu	SBSGM
Tamer ERDOĞAN	Birim sorumlusu	SBSGM
Ümit MADEN	Birim personeli	SBSGM

(Alfabetik sıraya göre listelenmiştir)