T.C.

ÇANKIRI VALİLİĞİ

ÇANKIRI SAĞLIK İL MÜDÜRLÜĞÜ

BİLGİ GÜVENLİĞİ POLİTİKALARI KILAVUZU

Sürüm 2.1

2019

Bu kılavuz çevre duyarlılığı kapsamında kâğıt ortamda basılmayarak; elektronik ortamda kullanıma sunulacak olup, değişikliklerin hızla gerçekleştirilmesine ve yayımlanmasına katkı sağlayacaktır.

Önsöz (1'inci Sürüm)

Günümüzde hızla gelişen bilim ve teknoloji insan hayatını oldukça kolaylaştırmaktadır. Bilgisayarlar, tabletler, akıllı cep telefonları vb. elektronik aletler günlük hayatımızda sürekli kullandığımız cihazlardır. İnternet teknolojisi ile bu cihazların kullanımı artmış, bilgiye ulaşmak kolaylaşmıştır. Bu küresel iletişim ağı bilimsel araştırmaların, üretkenliğin, kültürel değişmelerin, küresel ticaretin ve küresel eğitimin ana bilgi kaynağı olmuştur. Bu ağ dünyada yaşayan tüm insanlar arasında yazılı, sözlü ve görüntülü iletişim kurmak için küresel bir merkez oluşturmuştur. Dünyanın bir ucundaki kütüphanede bulunan bilgilere çok hızlı ve çok kolay bir şekilde ulaşabilmektedir. Artık kâğıt ortam yerini elektronik ortama bırakmış ve böylece bilgi akışı hızlanmış, bilgi ile belge saklama, depolama ve korumada büyük kolaylık sağlanmıştır. İstenilen bilgi, belge, doküman ve verilere ulaşımda zaman kazanılmış, maliyet azalmış ayrıca çevreyi koruma açısından önemli bir adım atılmıştır.

Günümüzde kurumlar, bilgilerinin büyük bir kısmını elektronik ortamda bulundurmakta ve bu bilgileri bilişim sistemleri altyapısı kullanarak işlemektedir. İş ve işlemlerin elektronik ortama taşınması, kamu hizmetlerinin etkinleştirilmesi, yasa dışı faaliyetlerin tespit edilebilmesi ve önlenmesine yönelik olarak kişisel bilgilerin de elektronik ortamda bulunması ve işlenmesi yoğun bir şekilde artmıştır. Ancak bu durum, kişisel bilgilerin sahiplerinin isteği dışında ilgisiz ve yetkisiz tarafların eline geçmesi, kişisel bilgi sahibini rahatsız edecek veya onlara zarar verecek şekilde yasa dışı olarak kullanılması ve kişi mahremiyetinin ihlali tehlikesini de doğurmaktadır. Dolayısı ile gelişen bilişim teknolojileri bilgi güvenliği olgusunu da beraberinde önce ihtiyaç sonra zorunluluk haline getirmiştir.

Sağlık sektöründe güncel teknolojinin hissedilir şekilde kullanılmasıyla birlikte teknolojinin taşıdığı bazı risklerle de yüz yüze gelinmiştir. Elektronik ortamdaki tüm veriler gibi, kişisel sağlık bilgilerini tehdit eden riskler için güvenlik önlemlerinin alınması zorunlu hale gelmiştir. Kişisel sağlık bilgileri, kişinin doğum öncesinden ölüm sonrasına kadar geçen süreyi kapsayan sağlık bilgilerinin tümüdür. Sağlık kayıtlarının sayısallaştırılması etkin sağlık hizmeti için yadsınamayan ciddi bir hamledir. Güncel teknolojilerin kişisel sağlık bilgilerinin gizlilik, bütünlük ve erişilebilirlik risklerini artırmasından dolayı sağlık bilgilerinin güvenliği zedelenmektedir. Kişisel sağlık bilgilerinin mahremiyeti esastır. Bu nedenle önlemlerin alınması, risklerin saptanıp indirgenmesi zorunlu hale gelmiştir.

Müdürlüğümüz olarak hazırlamış olduğumuz bu kılavuz sizlere yapılması gereken bilgi güvenliği çalışmalarında önderlik yapacaktır. Bir program dâhilinde ilerlemenizi sağlayacak, tüm yönetici ve son kullanıcıların bu kapsamda yapmaları gereken işler çerçevesinde bir rehber olarak hazırlanmıştır.

Önsöz (2'nci Sürüm)

Bakanlığımız tarafından 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 03.03.2014 tarihinde yayımlanarak yürürlüğe girmiştir.

Yönerge ve Kılavuz, ilk sürümlerinin yayımından bugüne kadar geçen süreçte yaşanan teknolojik gelişmeler, kullanıcılardan alınan geri bildirimler ve 694 sayılı KHK ile değişen Bakanlık merkez ve taşra teşkilatının yeni yapısı dikkate alınarak güncellenmiştir. Yönergenin ikinci sürümü 02.05.2018 tarihinde yayımlanmıştır. Yönergeye internet ortamında http://www.sbsgm.saglik.gov.tr/TR,13124/yonergeler.html adresinden erişim sağlanmaktadır.

Bilgi teknolojilerindeki gelişmelerle birlikte, bilgi güvenliğine yönelik gereksinimler gittikçe daha karmaşık ve kapsamlı hale gelmiştir. Sınırlı mali ve personel kaynakları ile kapsamlı bilgi güvenliği çalışmaları yapılması için daha sistematik ve yönetsel sistemlerin uygulanması zorunluluk haline gelmiştir. Kılavuzun ikinci sürümü hazırlanırken teknik detaylardan kasten kaçınılmış, TS ISO/IEC 27001:2017 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 başlık "**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 gerekmektedir. Kılavuzda yer alan konuların dışında, Bakanlığımız bünyesinde siber güvenlik ve siber olaylara müdahale ile ilgili hususların işleyişi, "**Kurumsal 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**" tarafından çıkarılan tüm mevzuata internet ortamında https://kvkk.gov.tr/ adresinden erişim sağlanabilmektedir. Kılavuz hazırlanırken Kişisel Verileri Koruma Kurulu tarafından hazırlanan mevzuat 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 İl Sağlık Müdürlükleri 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. Müdürlüğümüz, 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. Müdürlüğümüz, 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. Bilgi güvenliği yönetim sistemini sürekli gözden geçirmek ve iyileştirmek,

A.1.1.3.5. Bilgi güvenliği farkındalığını artırmak için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmek 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 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 Bakanlığımızın ve Müdürlüğümüzün güvenini ve itibarını sarsacak durumları bertaraf etmektir.

A.1.2. 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 bilgi ve iletişim sistemlerinin 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 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 sürekliliğin 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 20/10/2012 tarih ve 28447 sayılı Resmi Gazetede yayınlanan "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 21/06/2017 tarih, 30103 sayılı resmi gazete ile "Kamunet Ağına Bağlanma Ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkında Tebliğ" yayımlanmıştır. Amacı "KamuNet'e dâhil

edilecek ve dâhil olan kamu kurumlarının KamuNet'e bağlı bilgi ve iletişim sistemlerine ilişkin olarak karşılaması gereken asgari gereklilikler ile bu kurumların denetlenmesine ilişkin usul ve esasların belirlenmesi" olan tebliğ ile; KamuNet'e bağlantı yapacak kamu kurumlarının BGYS'ni kurması, işletmesi ve kurmuş olduğu BGYS için, TS ISO/IEC 27001 veya ISO/IEC 27001 standardına göre belgesini alması ve güncelliğini sağlaması gerekliliği hâsıl olmuştur.

A.1.2.6. Kılavuz başlıkları Bakanlığımız Sağlık Bilgi Sistemleri Genel Müdürlüğü'nün yayınladığı Bilgi Güvenliği Politikaları 2.versiyonundan alınmıştır. Bu başlıklar içerisinde tüm kullanıcıları kapsayan madde başlıkları olabildiği gibi sadece sistem ve veri tabanı yöneticilerini, hizmet sağlayıcıları, yöneticileri ilgilendiren müstakil konu başlıkları da yer almaktadır.

A.1.2.7. Bilgi güvenliği önlemlerinin hukuksal dayanaklarına ilişkin en güncel gelişme, 7 Nisan 2016 tarihinde 29677 sayılı Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanununun yürürlüğe girmesi ile olmuştur. Ülkemizde kişisel verilerin korunmasının sağlanması ve buna yönelik farkındalık oluşturarak bilinç düzeyinin geliştirilmesi görevi, 6698 sayılı kanun ile kurulan Kişisel Verileri Koruma Kurulu'na verilmiştir.

A.1.2.7.1. Kurul tarafından, 6698 sayılı kanunun uygulanmasına yönelik ikincil mevzuat (Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı vb.) hazırlanmış ve yayımlanmıştır. Kurul tarafından yayımlanan ikincil mevzuata ve ilgili diğer bilgi ve belgelere, Kurul'un https://www.kvkk.gov.tr adresinden erişim sağlanabilmektedir.

A.1.2.7.2. Kişisel Verileri Koruma Kurulu 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.1.2.7.3. Kılavuz hazırlanırken Kişisel Verileri Koruma Kurulu ve Bakanlığımız tarafından yayımlanmış olan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik yer alan ve doğrudan bilgi güvenliği ile ilişkili olan hususların Kılavuz içerisine alınması için çaba gösterilmiştir.

A.1.2.7.4. Bununla birlikte Kılavuzda yer alan bilgi güvenliği ile ilgili tüm tedbirlerin alınmış olması, kişisel verilerin mahremiyetinin sağlandığı ve hukuka uygun bir şekilde işlenmiş olacağını garanti etmemektedir.

A.1.2.7.5. ISO 27001 Bilgi Güvenliği Yönetim Sistemi 6698 Sayılı KVKK Süreçlerini de kapsayan bir çalışmadır ancak, KVKK incelendiğinde ISO 27001 BGYS'nin EK-A kontrolleri dediğimiz bazı maddelere atıfta bulunduğu gözlemlenmektedir. KVKK'nın maddeleri içerisinde yer alan veri sınıflaması, maskeleme, veri sızıntısını önleme, güvenli veri transferi, erişim kontrollerine ilişkin hükümlerin Bilgi Güvenliği Politikaları ile Prosedürlere ek olarak ayrıca düzenlenmesi gerektiği ortaya çıkmaktadır.

A.1.2.7.6. 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.2. BİLGİ GÜVENLİĞİ ORGANİZASYONU

A.2.1. Bilgi Güvenliği Yönetim Komisyonu

A.2.1.1. Müdürlüğümüz genelinde bilgi güvenliği ve siber olaylara müdahale ile ilgili konularda en üst düzeyde koordinasyon ve karar organı olarak görev yapmak üzere, Bilgi Güvenliği Alt Komisyonu kurulmuştur.
A.2.1.2. Müdürlüğümüz ve bağlı kurumlardaki Bilgi Güvenliği süreci, Bilgi Güvenliği İl **Yetkilisi** tarafından yürütülür. Bağlı Kurumlar bu süreç için personel ataması yapmazlar.

A.2.1.3. Komisyon, Destek Hizmetleri Başkanlığında, aşağıda belirtilen üyelerden oluşur.

Komisyondaki Görevi	Adı-Soyadı	Asli Görevi
Koordinatör	Gülay YURDCU	Destek Hizmetleri Bşk. Yrd. Bilgi Sistemleri Koordinatörü
Üye	Faruk GÜNGÖR	Bilgi Güvenliği Yetkilisi
Üye	İdris KÖRİSMAİLOĞLU	SOME Ekip Lideri
Üye	İsmail Tuğhan METİN	Bil. Sist. Çlş.

A.2.1.4. Alt Komisyonun görevleri şunlardır:

A.2.1.4.1. Yönerge ve Kılavuzda belirtilen hususlar çerçevesinde, kendi kurumları bünyesinde uygulanacak BGYS'ne yönelik çalışmaları koordine eder.

A.2.1.4.2. Bakanlık tarafından yayımlanan eylem planında yer alan hususların gerçekleştirilmesini sağlar.

A.2.1.4.3. Bilgi güvenliği yetkili/yetkililerini belirler ve görevlendirmesini yapar.

A.2.1.4.4. Bakanlık tarafından yayımlanan Kurumsal SOME Kurulum ve Yönetim Rehberinde belirtilen esaslar çerçevesinde Kurumsal SOME'sini kurar ve işletilmesini sağlar. Kurumsal SOME Ekip Lideri görevlendirmesini yapar.

A.2.5. Kurumsal 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 yönetim 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 organizasyonu 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 edilir (tarama yapılır).

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, devlet memurluğuna atanacak kişiler ile ilgili, 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 Kanununa 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 katılış 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 ile insan kaynakları birimi müştereken 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, EBYS, HBYS vb), bilgi güvenliği farkındalık eğitimi, oryantasyon eğitimi, gizlilik sözleşmesi imzalatılması gibi hususlar mutlaka yer alır. Örnek olarak kullanılabilecek bir işe başlama formu ekte (KLVZ-EK-01) sunulmuştur.

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 eğitim 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 (Türk Standartları Enstitüsü, Türkiye ve Orta Doğu Amme İdaresi Enstitüsü, 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 bile 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 bir işten ayrılma formu ekte (KLVZ-EK-02) sunulmuştur.

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 (varsa VPN hesapları) 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, Çankırı İl Sağlık Müdürlüğü Bilgi Güvenliği Politikaları Kılavuzunda yer alan koşullara uygun hareket eder. Burada yer alan hükümleri kişisel olarak ihlal etmesi halinde Müdürlüğümüze, 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. Müdürlüğümüz ve Bağlı Kuruluşlarda 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/Müdürlüğümüze/Kuruma 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 adı/parolayı hiç kimseyle paylaşmaz. Parolasının gizli kalması için alınması gereken tüm tedbirleri alır. Kurumdan ayrılması halinde kullanıcı adı/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/Sağlık Müdürlüğü 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. Müdürlüğümüz ve bağlı kurumlarda 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. Müdürlüğümüz ve bağlı kurumlarda görev yapan 657 sayılı Kanuna bağlı tüm kamu personeline, talep etmeleri halinde kurumsal e-posta hesabı açılır.

A.3.6.4. Çeşitli sözleşmeler kapsamında Müdürlüğümüz ve bağlı kurumlarda 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. Müdürlüğümüz ve bağlı kurumlarda 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. Bakanlık E-Posta Birimi tarafından uygulanan e-posta yönetimi ve güvenliği ile ilgili politikalar şu şekildedir.

A.3.6.7.1. Kullanıcıların e-posta hesaplarına tarayıcı programları, masaüstü istemci uygulaması (Office Outlook) ve cep telefonları üzerinden güvenli olarak erişebilmeleri için gerekli servisler sağlanır.

A.3.6.7.2. 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.3.6.7.3. Kullanıcı parolalarının Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen politikalar ile uyumlu olup olmadığı denetlenir.

A.3.6.7.4. E-Posta yönetim birimi tarafından oluşturulan ve sisteme ilk kez girişte kullanılan parolanın ilk kullanımdan sonra değiştirilmesi sağlanır.

A.3.6.7.5. Kullanıcıların son kullandığı üç parolayı kullanması engellenir.

A.3.6.7.6. Kullanıcılar, altı ayda bir parolalarını değiştirmeye zorlanır. Parola değiştirme süresine beş gün kala uyarı iletisi gönderilir.

A.3.6.7.7. Kullanıcılara e-posta hesabının parolasını değiştirmek için SMS 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.3.6.7.8. 657 sayılı Kanun kapsamı dışında istihdam edilmiş olan personel için e-posta hesabın 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.3.6.7.9. Bir yıl süre ile sisteme giriş yapmayan kullanıcıların hesapları geçici olarak kapatılır. Bu hesaplar aktif dizinde pasife çekilir.

A.3.6.7.10. Kullanıcılara e-posta hesabı ilk kez açıldığında bir (1) GB disk alanı tanımlanır. Kota artırımı E-Posta Birimi tarafından dinamik olarak veya E-Posta Birimine e-posta ile yapılan talepler doğrultusunda yapılır.

A.3.6.7.11. 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.3.6.7.12. Yüksek sayıda üye içeren dağıtım grupları, tüm kullanıcılar tarafından görülen genel adres defterinden gizlenir.

A.3.6.7.13. Bir e-postaya eklenebilecek en fazla alıcı sayısı 100 (yüz) e-posta adresi ile sınırlı tutulur.

A.3.6.7.14. Gönderilen e-posta boyutu 25 MB geçemez.

A.3.6.7.15. Dağıtım gruplarının kullanım durumları (e-posta akış trafiği) takip edilir ve bir yıl boyunca kullanılmayan gruplar tespit edilerek silinir.

A.3.6.7.16. E-posta erişim trafiği SSL ile şifrelenir.

A.3.6.7.17. E-posta iletimlerinde "exe" gibi çalıştırılabilir dosyaların gönderilmesi engellenir.

A.3.6.7.18. E-posta sistemlerinde fazla veri (data) boyutu oluşturması sebebi ile e-posta hesaplarına profil resmi eklenmesi engellenmiştir.

A.3.6.7.19. saglik.gov.tr uzantılı e-posta hesabından farklı uzantılı e-posta adreslerine gönderilen iletilerde E-Posta Yasal Uyarı (Disclaimer) metni gönderilmektedir.

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 resmi e-posta hesabı 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, eposta 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 çalıştırılması kaynaklı oluşabilecek 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 Müdürlüğümüz Bilgi İşlem Birimine haber verilir.

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 kırma 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. USB ya da harici bir disk 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 dosyası, barkodlar, gözlem formları vs.) 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. 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.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. Donanım Bilgi Varlıkları

- Sunucu ve bilgisayarlar (tablet, dizüstü bilgisayar, masaüstü bilgisayar, akıllı telefon vb.)
- Depolama ortamları (manyetik, optik, sabit disk, harici disk, disket, CD, DVD vb.)
- Haberleşme cihazları (telsiz, telefon, faks (belgegeçer), cep telefonu vb.)
- Ofis cihazları (yazıcı, tarayıcı, yansı cihazları, kameralar vb.)

A.4.1.4.2. Fiziksel Bilgi Varlıkları

Basılı doküman/belgeler (resmi yazışmalar, mektup, e posta, KEP, tasarım belgeleri, planlar, sözleşmeler, raporlar, hasta dosyaları, ihale dosyaları, kroki, fikri mülkiyet haklarına dair belgeler vb.)

A.4.1.4.3. Yazılım Bilgi Varlıkları

- Veri tabanları, veri dosyaları
- İz ve işlem kayıtları
- Yazılımlar (sistem, uygulama, geliştirme, kurumsal vb.)
- Yazılım kaynak kodları ve yazılım yan ürünleri (tasarım, algoritma vb.)

A.4.1.4.4. Proje ve Hizmet Bilgi Varlıkları

o İlgili kurumun görev alanına giren, herhangi bir başvuru gerektirmeyen ya da talep üzerine karşılanan tüm hizmet ve projeler.

o Bilgi İşlem ve Haberleşme Servisleri, SBSY'ler, Web servisleri, FTP servisleri vb.

A.4.1.4.5. İnsan Kaynakları

Kurumun BGYS kapsamı için tanımlanmış fiziksel alanlarda kuruma ait iş ve işlemleri yürüten 657 memurlar, yüklenici firma çalışanları, danışmanlar vb.

A.4.1.4.6. Altyapı ve Mekânlar

o Yapısal ve elektrik kablolama altyapısı, UPS, jeneratör, iklimlendirme, giriş / çıkış kontrol sistemleri, kamera sistemleri, yangın, duman uyarı sistemleri, yangın söndürme sistemleri, destek teçhizatı vb.

o 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.

A.4.2.2. 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 (ÇKYS, MKYS 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. Varlık sahipleri;

A.4.2.7.1. Varlıklarını envantere doğru olarak kaydettirmekten,

A.4.2.7.2. Varlıklarına uygun gizlilik derecesi ve varlık değeri atamaktan, varlıklarının uygun şekilde korunmasından,

A.4.2.7.3. Varlıklara erişecek kişi veya süreçleri için erişim izinlerini planlamaktan, bunlarla ilgili kararları vermekten,

A.4.2.7.4. Varlıkların silinmesi ya da imha edilmesinde uygun işlemlerin uygulanmasından sorumludur.

A.4.2.8. 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 yazılalar 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 kişiler) tarafından 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

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 süre 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. Kağıt 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 SBSYS verileri ve SBSYS yedeklerinin saklandığı medya ortamlarının mutlak surette envanter listesi oluşturulur, 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) bilgisayarlara bağlanamaz. 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 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 alınır. (Örneğin; ısı, nem ya da elektromanyetik alanlara maruz kalma gibi çevresel faktörlere karşı koruma)

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.

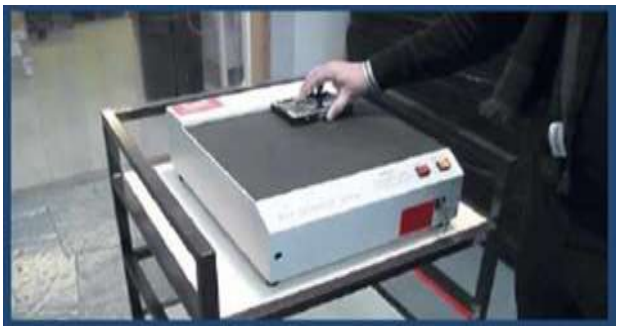
A.4.5.2. Kaydı silinen bilgi sistem cihazlarına ait veri depolama üniteleri, içerisinde gizlilik dereceli bilgi bulundurma ihtimali nedeniyle, usulüne uygun olarak imha edilir veya güvenli silme işlemi yapılır.

A.4.5.3. Kaydı silinen bilgisayarların sabit diskleri, bağlı kurumlarımızın bilgi işlem birimlerden destek alınmak suretiyle sökülür. Bilgi işlem birimi harici personel disklere müdahale edemez.

A.4.5.4. Sökülen sabit disklerden daha önce kurumun bilgi işlem birimi 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. İmha edilecek disklere ait Kayıttan Düşme Teklif ve Onay Tutanağı (KLVZ-EK-03) ve Disk İmha Formunun (KLVZ-EK-04 kullanılarak, 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, router 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. Kağıt 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 kağıt 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. Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

A.4.5.11.1. İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde veri depolama alanları sökülerek gönderilmelidir. yer alan verilerin Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

A.4.5.11.2. Cihazın veri depolama alanının sökülmesinin mümkün olmadığı durumlarda ise Kılavuzun A.4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle verilerin yok edilerek gönderilmesi gerekmektedir.

A.4.5.11.3. Kurumlarımız yukarıda anlatılan süreçler için, süreç yönetim algoritması geliştireceklerdir. Bilgi İşlem Birimi sorumlusunun onayı olmadan hassas verileri içeren hiçbir cihaz servise/bakıma gönderilemez.

A.4.5.11.4. 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. Risk yönetimi bir tehdidin gerçekleşme olasılığı ile gerçekleşmesi halinde yol açacağı sonucun şiddetinin birlikte ele alınmasıdır.

A.5.1.3. Kurumlarımızın üst yönetimlerince risk yönetimine ilişkin görev, yetki ve sorumlulukların tanımlanması, risklerin yönetimine ilişkin kuralların oluşturulması, görevlendirilen personel vasıtasıyla risklerin belirlenmesi ve analiz edilmesi gerekir.

A.5.1.4. Risk analizi, risklerin kapsamlı olarak anlaşılmasını sağlayan yöntemler ile risklerin belirlenmesi, risklerin oluşması halinde ortaya çıkabilecek zararın şiddetini ele alacak şekilde değerlendirilmesini ifade etmektedir.

A.5.1.5. 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.5.1.6. Risk analizlerinde bilhassa aşağıdaki hususlara yönelik riskler değerlendirilir:

A.5.1.6.1. Sistem, ağ ve kaynaklarına erişim kontrolünde güvenli kimlik doğrulama yöntemlerinin kullanılması,

A.5.1.6.2. Uygulama kullanıcısı, yönetici kullanıcı ve teknik kullanıcıların yetkilendirme ve erişim yöntemleri,

A.5.1.6.3. Kullanıcı ve sistem yöneticilerinin görev, sorumluluk yetkilerinin ayrılması,

A.5.1.6.4. Kullanılabilirlik, gizlilik ve bütünlük çerçevesinde varlıkların korunma dereceleri,

A.5.1.6.5. Sistem işletim süreçlerinde iz kayıtlarını tutma, izleme ve inkâr edememe gereksinimleri,

A.5.1.6.6. Veri sızıntısı algılama sistemleri veya kaydetme ve izleme gibi güvenlik kontrolleri,

A.5.1.6.7. 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 planın 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 yönetimin 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 anlatılmıştır.

A.5.3.1.3. Her bir varlığa, sorumluluk ve hesap verilebilirliği sağlamak üzere mutlaka "varlık sahibi" atanmış olması gerekir. Varlık sahibi, varlığın kullanımı, bakımı ve güvenliğinden sorumlu kişi veya birimdir.

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-05 Risk Hesaplama Faktörlerinde yer alan Varlık Değeri Tablosunda belirtilen kriterler kullanılmak suretiyle 1-4 arası 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 (ör. yetkisiz eylemler, fiziksel hasar, teknik arıza) ve kaynağına (ör. doğal kaynaklı, insan kaynaklı) 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 aynı değerlendirmek ve risk analiz tablosuna ayrıca işlemek gerekir.

A.5.3.3.5. Tehdit ve zafiyetlerin gerçekleşme olasılığı için KLVZ-EK-05 Risk Hesaplama Faktörlerinde yer alan Riskin Gerçekleşme Olasılığı tablosunda belirtilen kriterler kullanılmak suretiyle 1-5 arası 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-05 Risk Hesaplama Faktörlerinde yer alan Gizlilik Etki Değeri, Bütünlük Etki Değeri ve Erişilebilirlik Etki Değeri Tablolarında belirtilen kriterler kullanılmak suretiyle 1-5 arası 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 önceliklendirmesi için KLVZ-EK-05 Risk Hesaplama Faktörlerinde yer alan Risk Değeri Tablosu kullanılır.

A.5.3.6.3. Risk Değeri Tablosunda yer alan yüzdelerin anlamlandırılması ve risk önceliklendirmesi aşağıdaki tabloda olduğu gibidir.

Risk Puanı	Risk Seviyesi
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. Ör: 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 metodoloji uyarınca hazırlanmış, örnek bir Risk İyileştirme Planı KLVZ-EK-06'dadır.

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 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 yönetimi yöntemi kullanıldığına bakılmaksızın risk tanımlama formu ve risk analiz tablosu kayıtlarının oluşturulması, muhafazası ve güncellenmesi gerekir.

A.6. ERİŞİM POLİTİKASI

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

A.6.1.3. Erişim kontrol politikası / erişim yetki ve kontrol matrisleri hazırlanırken aşağıda sıralanan prensipler dikkate alınır.

A.6.1.4. 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.6.1.5. Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan erişim kontrol politikalarının sıkılaştırılması (zorlaştırılması) gerekir.

A.6.1.6. Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.

A.6.1.7. Bilgiye erişim talepleri ve ilgili makamlarca bu taleplere yapılan işlemlerin takip edilebilirliğini sağlamak üzere yazılı kurallar oluşturulur.

A.6.1.8. Erişim izinleri ile ilgili kayıtlar, varsa ilgili mevzuatta belirtilen sürelerce, yoksa varlığın sahibi tarafından belirlenecek süre boyunca saklanır.

A.6.1.9. Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.

A.6.1.10. "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.6.1.11. "Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.

A.6.1.12. Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Kullanılacak parolalar, kurumumuz bilgi güvenliği parola politikalarına uygun olmak zorundadır. 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.6.1.13. Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur. Erişim ile ilgili hangi kullanıcı hareketlerinin izleneceği hususu, varlık sahipleri tarafından belirlenir.

A.6.1.14. Sağlık Bilişim Ağı dışındaki ağlar güvensiz ağ olarak kabul edilir. Sağlık Bilişim Ağına dahil kurumlarımız kesinlikle harici bir internet erişim ağı(ADSL, 3G Modem vb.) kullanamaz. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.

A.6.1.15. Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya sanal ağlar(vlan) ile ayrılmalıdır. Veri tabanı yönetim sistemi sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.

A.6.1.16. Bilgi varlıklarına fiziksel olarak yapılacak erişimler için bu yönergenin A.8 maddesinde belirtilen önlemler alınır.

A.6.1.17. **Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için Kişisel Verileri Koruma Kurulu'nun 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.**

A.6.2. Kullanıcı Erişimlerinin Yönetimi

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

A.6.2.2. Müdürlüğümüz Bilgi güvenliği Politika kılavuzunu tebellüğ etmeyen ve personel gizlilik sözleşmesi/Bilgi Güvenliği Farkındalık Bildirgesi imzalamayan personele **kesinlikle erişim yetkisi verilmez.**

A.6.2.3. Başta kişisel sağlık verilerinin işlendiği bilgi sistemleri olmak üzere erişim kontrolüne 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, Müdürlüğümüz "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. Hizmet veya sistemlerin sahiplerince erişim hakları 3 ayda bir düzenli olarak tesislerimiz tarafından oluşturulan komisyon tarafından incelenir. Bilmesi gereken prensibi uyarınca, gereksiz olarak verilmiş yetkiler raporlanarak kaldırılması sağlanır.

A.6.2.4. Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilir.

A.6.2.5. **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.

A.6.2.6. 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.6.2.7. Ayrıcalıklı erişim hakkı süreci talepte bulunan kullanıcının ayrıcalıklı erişim formunu Bilgi Güvenliği Alt Komisyonuna teslim etmesiyle başlar. Bu formda, erişim istenilen sistem adı, ip bilgisi, erişim düzeyi ve gerekçesi detaylı olarak bildirilir. Bilgi güvenliği Politika kılavuzunu tebellüğ etmeyen ve personel gizlilik sözleşmesi imzalamayan personele **kesinlikle erişim yetkisi verilmez.**

A.6.2.8. 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.6.2.9. Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanır ve sıkı bir şekilde kontrol edilir.

A.6.2.10. 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. Müdürlüğümüz Parola politikaları gereği, müdürlüğümüz ve bağlı kurumlarda hizmet veren sistem ve uygulamaların kullanıcılarının asgari olarak aşağıdaki kurallara uygun parola kullanmaları sağlanır.

A.6.3.1.1. Parolalar en az 8 (sekiz) karakterden oluşur. Root, administrator gibi sistem yönetim işlemlerinde kullanılan parolaların en az 12 karakterden oluşur.

A.6.3.1.2. İçerisinde en az 1 (bir) tane büyük ve en az 1(bir) tane küçük harf bulunur.

A.6.3.1.3. İçerisinde en az 1 (bir) tane rakam bulunur.

A.6.3.1.4. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !,?,A,+,$,#,&,/,{,*,-,],=,...)

A.6.3.1.5. Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab...)

A.6.3.1.6. Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf,1234,zxcvb...)

A.6.3.1.7. Kişisel bilgiler veya klavye kombinasyonları ile basitçe üretilebilecek karakter dizilerinin kullanılması engellenir. (Örneğin 12345678, qwerty, doğum tarihi, çocuğun adı, soyadı gibi)

A.6.3.1.8. Sözlükte bulunabilen kelimelerin kullanılması engellenir.

A.6.3.1.9. Kullanıcının son 3 parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir.

A.6.3.1.10. Sistem ve uygulamalarda oturum (session) kontrolü yapılarak bir kullanıcı adı ve parolasının aynı anda birden çok bilgisayarda kullanılması engellenir.

A.6.3.3. Veri tabanı yönetim sistemi, aktif dizin sunucusu, uygulama sunucusu, ağ cihazları gibi sistem hesaplarına ait parolalar (root, administrator, vs.) en geç 3 (üç) ayda bir değiştirilir.

A.6.3.4. Kullanıcı hesaplarına ait parolalar (örnek: HBYS, e-posta, web, masaüstü bilgisayar vs.) en geç 4 (dört) 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 konfigüre edilmesi gerekir.

A.6.3.11. Yazılım uygulaması, kullanıcı parolasının oluşturulması için aktivasyon özelliğini barındırmıyorsa, kullanıcı için oluşturulan parola yukarıda yer alan hususlar çerçevesinde kullanıcıya tebliğ edilir.

A.6.4. Uzaktan Çalışma ve Erişim

A.6.4.1. Uzaktan çalışma, 4857 sayılı İş Kanununun 14'ncü 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.6.4.2. Uzaktan çalışma; ağırlıklı olarak yükleniciler, tedarikçiler, iş ortakları çalışanları gibi müdürlüğümüz ile geçici olarak iş ilişkisi olan kişiler tarafından yapılır. Ancak acil durumlarda Müdürlüğümüz çalışanları için de söz konusu olabilir.

A.6.4.3. **Uzaktan erişim ile ilgili yöntem/mimari belirlenirken aşağıda belirtilen esaslar doğrultusunda hareket edilir.**

A.6.4.3.1. Firmaların/yüklenicilerin uzaktan erişim talebinde bulunmaları için ihale dökümanlarında mutlaka bu husus ile ilgili maddeler yer almalıdır. İhale dökümanında sadece yerinde destek ile ilgili ibareler var ise, desteğin yerinde alınması sağlanmalıdır.
A.6.4.3.2. Kurumlarımız ya da müdürlüğümüz ile "Kurumsal Gizlilik Sözleşmesi" imzalamamış olan yüklenici/firmalara **kesinlikle uzaktan erişim yetkisi verilemez.**
A.6.4.3.3. Bağlanılacak bilgisayar (hedef bilgisayar) kurumun iç ağında yer alıyorsa, bağlantı müdürlüğümüz Bilgi Sistemleri Birimi tarafından oluşturulan SSL VPN yöntemiyle yapılır.
A.6.4.3.4. İç ağda yer alan kaynaklara, VPN kullanılmadan bağlantı yapılmasına hiçbir şekilde izin verilmez.

A.6.4.3.5. VPN işlemi (bu maksatla kullanılan ayrı bir yazılım ve/veya donanım yoksa) İl SBA Bulutu girişinde bulunan güvenlik duvarı üzerinden yapılır.

A.6.4.3.6. Erişim kontrollerinin uygulanabilmesi maksadıyla, hedef bilgisayara sabit IP adresi verilir. Birden fazla bilgisayara erişim yapılacak ise bu bilgisayarlar tek bir VLAN üzerinde toplanır. Yapılacak erişim "erişim yapacak kişi, hedef bilgisayar IP adresi (VLAN adresi) ve kullanılacak port/uygulama" bazında sınırlandırılır.

A.6.4.3.7. VPN bağlantılarına ilişkin iz kayıtları tutulur ve söz konusu iz kayıtları en az iki yıl süre ile saklanır.

A.6.4.3.8. Uzak bağlantı yapılacak uygulamalara/kaynaklara erişimin daha kontrollü olarak yapılması gerekiyorsa, bağlantılar bu amaçla ayrılan bir terminal / vekil sunucu üzerinden de yapılabilir. Gerekiyorsa vekil cihaz üzerindeki oturum kayıt altına alınır.

A.6.4.3.9. Uzak bağlantı yapacak istemci bilgisayarların IP adresleri/blokları biliniyorsa, hedef bilgisayara sadece belirtilen IP adreslerinden erişim yapılması için gerekli ayarlar yapılır.

A.6.4.3.10. Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

A.6.4.3.10.1. Bağlantı yapan kişinin, hedef bilgisayarda oturum açma izni olan bir kullanıcı olması gerekir.

A.6.4.3.10.2. Hedef bilgisayara kullanıcı adı ve parola girilerek oturum açılır. Anonim girişlere izin verilmez.

A.6.4.3.10.3. Hedef bilgisayar kullanıcı adı ve parola yönetimi etki alanı sunucusu tarafından yönetilir. Eğer yetki alanına dahil değil ise, müdürlüğümüz Parola Politikalarına uygun parola kullandırılması gerekir.

A.6.4.3.10.4. 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.6.4.3.10.5. Bağlantı yapan kullanıcının hedef bilgisayardaki oturum açma, oturum kapatma gibi kullanıcı hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az bir yıl süre ile saklanır.

A.6.4.3.10.6. Hedef bilgisayar üzerinden bir başka sunucuya bağlantı yapılacak ise (örneğin SBYS yazılımı kullanılacak ise) ilgili kullanıcının söz konusu sunucuda yaptığı işlemlere ait iz kayıtları de kayıt altına alınır.

A.6.4.3.10.7. Uzak bağlantı yazılımı olarak mümkün ise "Microsoft Uzak Bağlantı Programı" kullanılır.

A.6.4.3.10.8. 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.6.4.4. Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmış olması gerekir.

A.6.4.4.1. Uzaktan çalışma yapacak kişi eğer müdürlüğümüz ya da bağlı kurum çalışanı ise Uzaktan çalışma için, kurum dışında, kullanıcının bağlantı için kullanacağı istemci cihaz ve personel aşağıda yer alan hususları sağlamalıdır:

A.6.4.4.1.1. Bilgisayar, Müdürlüğümüz ya da Kurumlarımız etki alanı içerisinde yer almalıdır.

A.6.4.4.1.2. Uzaktan çalışma yapacak personel, bilgi güvenliği politikaları kılavuzunu Tebellüğ etmiş ve kurumu ile bilgi güvenliği farkındalık bildirgesi/gizlilik sözleşmesi İmzalamış olmalı ve ayrıca Müdürlüğümüz tarafından hazırlanan "Uzaktan Erişim Yetki Formunu" müdürlüğümüze teslim etmiş olmalıdır.

A.6.4.4.1.3. Cihazın işletim sistemi güncel olmalı, Güvenlik duvarı aktif olmalı ve cihazda kurumumuz adına lisanslı antivirüs yazılımı yüklü olmalıdır.

A.6.4.4.1.4 . Cihazın aktif dizin Grup ilke politikalarını (GPO) sorunsuz yüklediğinden emin olunmalıdır.

A.6.4.4.2. Kurumumuz içerisinde yer alan ve uzaktan bağlantı/çalışma hedef bilgisayarında aşağıda yer alan hususlar asgari olarak karşılanmalıdır.

A.6.4.4.3. Öncelikle bu amaçla kullanılan cihazların envanteri oluşturulmalıdır.

A.6.4.4.4. Müdürlüğümüz tarafından oluşturulan "Uzaktan Erişim Yetki Formu"nda hedef cihaz olarak belirtilen cihaz mutlaka oluşturulan envanterde kayıtlı cihaz listesinde olmalıdır.

A.6.4.4.5. Cihaz mümkünse kurum etki alanına dahil edilmelidir.

A.6.4.4.6. Cihazlara kişisel güvenlik duvarı kurulu ve aktif hale getirildiğinden emin olunmalıdır.

A.6.4.4.7. İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanmalıdır.

A.6.4.4.8. Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir koruma yazılımı tedarik ettirilir. Yazılımın kendisi ve imza dosyaları güncel halde tutulması sağlanmalıdır.

A.6.4.4.9. Cihaz üzerinde uzaktan çalışma için kullanılmak üzere mümkün olan asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.

A.6.4.4.10. Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.

A.6.4.4.11. Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise dizüstü bilgisayar kilidi kullanılmak suretiyle çalınmaya karşı cihazın emniyeti alınır

A.6.4.4.12. Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (bluetooth vs.) pasif hale getirilir.

A.6.4.4.13. 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.6.4.4.14. Uzaktan çalışma ve uzaktan erişim için kullanılacak cihazlara çok faktörlü kimlik doğrulama (parola, PIN vb. bilgilere ilave olarak parmak izi, avuç içi veya retina kontrolü) yapılarak giriş yapılması tercih edilir. Yapılacak risk değerlendirmesine bağlı olarak gerekiyorsa bu maksatla kullanılmak üzere yan donanımlar tedarik edilerek, asıl cihazlar ile birlikte kullanılır.

A.6.4.4.15. Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.

A.6.4.4.16. Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.

A.6.4.4.17. Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.

A.6.4.4.18. Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için “jailbreak” veya “rootlama” işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.

A.6.4.4.19. Android işletim sistemine sahip mobil cihazlara (telefon/tablet) mutlaka lisanslı anti-virüs yazılımı kurulması gerekir.

A.6.4.4.20. Kullanılan her türlü mobil cihaz için, mutlaka üreticinin sağladığı işletim sistemi güncelleştirmeleri ve yazılım güncelleştirmeleri 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, FTP 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 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. Özetleme (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. Sayısal sertifikalar, kişi veya cihazların elektronik ortamdaki kimlik kartları gibidir. Bilgisayar ortamında yapılacak işlemler tarafların sayısal sertifikaları ile yapılıyor ise ilgili kişilerin kimlikleri kesin olarak doğrulanabilir.

A.7.1.7. Elektronik imza (e-imza) 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-imza 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 ve ECC (Elliptic Curve Cryptography) algoritmalarından birisi kullanılır.

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

- ECC (Elliptic Curve Cryptography) algoritması kullanılacaksa n değeri olarak en az 224 bit seçilir.

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

A.7.2.1.3. Özetleme (hash) işlemlerinde;

- Özetleme algoritması olarak blok boyu en az 256 olacak şekilde SHA2 veya SHA3 algoritması 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, IKE veya Elliptic Curve Diffie-Hellman (ECDH) algoritmalarından birisi seçilir.

o Anahtar üretim ve değişim öncesinde uç noktaların birbirlerini doğrulamaları gerekir.

o Doğrulama için taraflara ait açık anahtarlar kullanılır.

o Kimlik doğrulama için kullanılan sunuculara (örneğin; RADIUS veya TACACS sunucuları) bilinen güvenilir bir sertifika otoritesi tarafından imzalanmış geçerli bir sayısal sertifika yüklenir.

o 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 KamuSM'den alınır.
- Bakanlık tarafından geliştirilen/kullanılan uygulamalarda, sertifikaların geçerliliğini kontrol etmek için OCSP (Online Certificate Status Protocol) veya CRL (Certificate Revocation List) metotlarından biri ya da her ikisi birlikte kullanılır.

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. Herkesin erişimine açık ve https kullanan web sitelerinde "genişletilmiş onaylama (Extended Validation – EV) Sertifikası" tercih edilir.

A.7.2.2.4. Web trafiğinin korunması için HTTPS protokolü kullanılır.

A.7.2.2.5. HTTPS protokolü TLS 1.1 veya üstü bir protokol ile birlikte kullanılır. Tüm web sunucularında SSL servisleri kapatılır.

A.7.2.2.6. HTTPS trafiğinin şifrelenmesinde anahtar boyu en az 128 bit olacak şekilde AES algoritması kullanılır. RC4 algoritması kullanıma kapatılır.

A.7.2.2.7. Oturum anahtarlarının güvenliği için "Perfect Forward Secrecy (PFS)" özelliği aktive edilir.

A.7.2.2.8. Sunucunun özel anahtarını korumak için mümkün olan en üst düzey önlemler alınır.

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 (SSH FTP Ver.2) veya FTPS (TLS/SSL üzerinden FTP) protokollerinden birisi kullanılır.

A.7.2.3.3. SFTP/FTPS protokolleri kullanılırken için 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 tercihan 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. Uzak sistemlerin ve cihazların yönetim işlemleri, SSH Sürüm 2 veya daha yüksek sürümünü kullanarak, komut satırı üzerinden veya söz konusu protokolü destekleyen yazılımlar kullanılarak yapılır.

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.7.2.5.Sabit Ortamdaki Verilerin Şifrelenmesi:

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

- Bitlocker kullanılır.
- Bitlocker "hibernate" ile gelişmiş modda kurulur.
- Şifreleme anahtarının saklandığı TPM yonga setine erişimin kısıtlamak için kullanıcıların BIOS 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.7.2.6. Dosya ve klasör şifreleme işlemleri için;

o 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.

o 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 tedbir 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 hizmet 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 görüldüğüne 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 erişimin 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 dahil) 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) 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 sadece kurumsal amaçlarla kullanımı için Müdürlüğümüz bilgi güvenliği alt komisyonu tarafından yetkilendirme yapılması gerekir.

A.8.3.7.2. Kişisel cihazların(tablet, telefon, pc vb.) kurumlarımız sistemlerine bağlanması **kesinlikle yasaktır.** Kişilerin bu hususta ısrarcı olmaları durumunda kurum bilgi işlem sorumluları ivedilikle durumu Müdürlüğümüz Bilgi Güvenliği İl Yetkilisine bildirmekle yükümlüdür.

A.8.3.7.3. Bu şekilde kullanılan ekipmanların ve kullanıcıların listesi oluşturulur ve takip edilir.

A.8.3.7.4. Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenir.

A.8.3.7.5. 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.8.3.7.6. Tesis dışına çıkarılan ekipmanın gözetimsiz bırakılmamasına ve seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilir.

A.8.3.7.7. 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 cihazların 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. Sunucu ve Sistem Güvenliği Politikası

A.9.1.1. İş sürekliliği ve acil durum planlanması 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.9.1.2. 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.9.1.3. 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 sıkılıkla ihtiyaç duyulan bilgiler yer alır.

A.9.1.4. Sunuculara ve uygulamalara erişim sağlayan kullanıcıların erişim hakları, erişimlerin iptal edilmesi veya erişim yetkisinin değiştirilmesi gibi kuralların tanımlandığı bir "erişim matrisi" oluşturulur.

A.9.1.5. Yönetici yetkisi olan kullanıcılar, sunucularda zorunlu kalmadıkça 'administrator' ve 'root' gibi genel sistem hesaplarını kullanmamalıdır.

A.9.1.6. Sunuculara yapılan erişimlerin raporlanması, mesai saati dışındaki erişimlerin işaretlenmesi gibi detaylar gözlenir. Kullanıcılara olması gerekenden fazla yetki tanımlanmaz.

A.9.1.7. Sunucularda açılan oturumlar için kurallar tanımlanır. Sunuculara ve uygulamalara yapılan başarılı ve başarısız girişimlerin kayıtları tutulur. Kaba kuvvet ataklarına engel olmak maksadıyla sunuculara beş başarısız oturum açma denemesi yapıldığında ilgili hesap belirlenecek bir süre boyunca askıya alınır.

A.9.1.8. Sunucularda oturum açmış kullanıcı hesapları ile herhangi bir işlem yapılmadığı takdirde 10 dakika sonra ekran kilitlenir ve ilgili kullanıcının oturum açma ekranına düşmesi sağlanır. Bir saat boyunca işlem yapılmadığı takdirde, ilgili kullanıcının oturumu otomatik olarak sonlandırılır.

A.9.1.9. Sistem hesaplarına ait parolalar için Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen yönetici hesaplarına ilişkin kurallar dikkate alınır.

A.9.1.10. 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.9.1.11. Sunucuların güvenliğini sağlayabilmek için kullanılmayan uygulamalar veya servisler kapatılır. Gerekli servis ve hizmetler dışında başka bir servis çalıştırılmaz.

A.9.1.12. Sunuculara güvenli bağlantı yapılabilmesi için SSL sertifikası yüklenir. Sunuculara SSH bağlantısı yapılacak ise kullanılan anahtarlar belirli aralıklarla değiştirilir.

A.9.1.13. Sertifika kullanım süresi, son kullanım süresi yaklaşan sertifikaların takibi gibi işlemler hazırlanacak bir sertifika takip listesi vasıtasıyla takip edilir.

A.9.1.14. 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.9.1.15. Sunucuda depolanan veriler, işletim sisteminin çalıştığı disk bölümünden (varsayılan C:) farklı bir disk bölümünde tutulur.

A.9.1.16. Sunucuların arka planda çalışan servisleri ile birlikte o servislerinde kullandığı portlar kontrol edilir. Gereksiz portlar kapatılır. Mümkün olduğu surette uygulamaların varsayılan portları değiştirilir.

A.9.1.17. 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.9.1.18. Sunucu işletim sistemleri, güvenlik açıklarına karşı güncel tutulur.

A.9.1.19. 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.9.1.20. Mutlaka zorunlu değil ise sunucuların internete erişimleri kapatılır.

A.9.1.21. Sistem kaynakların uygun seviyede planlanması, sürdürülebilmesi ve etkin kullanılabilmesi için 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.9.1.22. Her etki alanı için NTP (Ağ Zaman Protokolü) sunucusu kurularak sistemdeki tüm aktif cihazların bu servis üzerinden tarih ve saat eşleştirmesi yapması sağlanır. Bu bağlamda müdürlüğümüz tarafından belirlenen ntp sunucularının kullanması gerekmektedir.

A.9.1.23. Kullanıcıların bilgisayarlarının saat ve tarih ayarlarını değiştirmesi engellenir.

A.9.1.24. Virüs vb. zararlı yazılımlardan korunmak ve kurumsal bilgilerin kurum dışına sızmasını engellemek amacıyla gerekiyorsa USB bellek gibi taşınabilir cihazların kullanımı engellenir.

A.9.1.25. Kullanıcıların ".exe/.bat" gibi çalıştırabilir dosyaları çalıştırmaları engellenir.

A.9.1.26. Kullanıcıların kısayolu 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.9.1.27. Kullanıcıların bilgisayar ayarlarını değiştirmelerini önlemek amacıyla denetim masasına ve C dizinine erişimleri engellenir.

A.9.1.28. Kullanıcıların DNS adreslerini değiştirmeleri engellenir.

A.9.1.29. Sunuculara yapılacak uzak masa üstü bağlantılarında Kılavuzun A.6.112 (A.6.12. Uzaktan Çalışma ve Erişim) maddesinde belirtilen hususlara dikkat edilir.

A.9.1.30. 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.9.1.31. 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.9.1.32. 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.9.1.33. 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.9.1.34. 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.9.1.35. Tüm bilgisayarlar lisanslı anti-virüs yazılımı ile korunur. Anti-virüs yazılımının virüs veritabanı güncel tutulur.

A.9.1.36. Özellikle Bakanlık merkez teşkilat 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.9.1.37. 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.9.1.38. 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. Müdürlüğümüz tarafından Hata ve çözümlerinin bulunduğu web tabanlı merkezi bir havuz oluşturulur.

A.9.1.39. 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.9.1.40. Sunucular üzerinde yapılacak değişiklikler 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, değişikliklerinden meydana gelebilecek olan güvenlik açıkları veya sistem problemlerini önceden belirleyerek önlem almak gibi amaçlarla kayda dayalı değişiklik yönetimi uygulanır.

A.9.1.41. 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.9.1.42. 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 Güvenliği

A.9.7.1. İş sürekliliği ve acil durum planlanması süreçlerinde ilgili otoritelerle iletişim yöntemleri tanımlanır ve yazılı hale getirilir. Acil durumlarda erişilmesi gereken kişilerin irtibat numaraları personelin kolayca ulaşabileceği bir şekilde bulundurulur.

A.9.7.2. 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.9.7.3. Kullanıcılara erişim hakkı tanımlanmadan önce gizlilik sözleşmesi olduğu kontrol edilir. Bilgi Güvenliği Politika Kılavuzumuzu tebellüğ etmeyen ve Bilgi güvenliği Gizlilik sözleşmesi imzalamayan personele erişim verilmez. Güvenlik cihazları ve ağ yönetiminde ayrıcalıklı erişim hakkı verilen kullanıcıların sisteme erişimi onay mekanizmasından geçerek tamamlanır. Erişim talepleri, resmi yazı veya kurumsal eposta ile bildirilir. Ayrıcalıklı erişim hakkı elde eden personelin yer ve görev değişikliği olması durumunda, erişimleri düzenleyen birime bilgi verilmesi sağlanır.

A.9.7.4. 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.9.7.5. Güvenlik ve ağ cihazlarına yapılacak uzaktan erişimler için yönergenin A.6.11 maddesinde belirtilen hususlara dikkat edilir.

A.9.7.6. Uzaktan erişim verilen kullanıcılara bağlantı zamanı ve süresi ile ilgili kısıtlamalar getirilir. Kurumdaki görevi gereği kullanıcıların bağlantı süreleri farklı olabilir.

A.9.7.7. Güvenlik ve ağ cihazları üzerinde var olan yerel kullanıcılar silinir. Güvenlik duvarları, ana omurga cihazları gibi kritik sistemlere yapılacak erişimler için ikincil bir kimlik doğrulaması yapılması tavsiye edilir.

A.9.7.8. 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.9.7.9. 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.9.7.10. Güvenlik ve ağ cihazlarının kurulumu, yapılandırmasını ve sistemde karşılaşılan hataları gidermek için izlenilen yöntemleri anlatan kılavuz dokümanları hazırlanır. Bu kılavuzlardan bilgi havuzu oluşturulur.

A.9.7.11. Yedekleme politikası uyarınca güvenlik ve ağ cihazlarının konfigürasyon yedekleri düzenli aralıklarla alınır.

A.9.7.12. Sistemi etkileyecek bir çalışma yapılması gerekiyorsa mesai saati dışında yapılır. Bu çalışmadan etkilenecek kurum/firma ya da kişilere bilgi verilir..

A.9.7.13. 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.9.7.14. Kablosuz ağlar üzerinde sisteme 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 kurum BGYS politikaları uyarınca, ağa dâhil olan tüm kullanıcılar kaydedilir ve bu bilgiler belirlenen süreler boyunca saklanır.

A.9.7.15. Telnet gibi güvensiz bağlantılara izin verilmez. SSH protokolünu kullanan bağlantılarda kullanılan sürümün güvenli olup olmadığı kontrol edilir.

A.9.7.16. İhtiyaç olmayan tüm portlar Bilgi Güvenliği İl Yetkilisi tarafından 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.9.7.17. Güvenlik duvarı ve ağ cihazları için kontrol listeleri (ACL, güvenlik ürünleri erişim kısıtlaması vb.) tanımlanır.

A.9.7.18. Güvenlik ve ağ cihazlarının fiziksel güvenliğini sağlamak için gerekli tedbirler alınır.

A.9.7.19. 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 esaslara göre oluşturur.

A.9.7.20. Güvenlik ve ağ cihazları üzerindeki gereksiz ve kullanılmayan tüm servisler kaldırılır.

A.9.7.21. Cihazları kaba kuvvet saldırılarından korumak için beş yanlış deneme sonrasında oturum belirli bir süre kilitlenecek şekilde ayarlama yapılır.

A.9.7.22. 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.9.7.23. 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.9.7.24. Dış ağdan sunucular üzerindeki servislere, sunucu yönetim protokolleri (RDP, SSH) ile erişim engellenir. Sunucular, iç ağda kendi aralarında servis ve yönetim yapılması maksadıyla belirli portlardan erişim sağlayacak şekilde yapılandırılır.

A.9.7.25. Kurum bünyesinde barındırılan ve hizmet veren uygulamalara, HTTPS üzerinden bağlanılır.

A.9.7.26. Güncel atak metotlarından korunma için saldırı tespit ve önleme sistemleri, ağ hizmetlerine erişim ilkelerinin belirlenmesi için Güvenlik Duvarı kullanılır.

A.9.7.27. 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. Bu sebeple müdürlüğümüz ve bağlı kuruluşlarda aşağıdaki erişim faaliyetleri kapatılmıştır.

A.9.7.27.1. Basın yayın organlarını takip ederek idareye raporlamakla sorumlu personel haricindeki tüm personelin dizi, film ve TV erişimleri,

A.9.7.27.2. Kurum sosyal medya hesaplarını yönetmekle sorumlu personel dışındaki tüm personelin Facebook, Twitter, İnstagram vb. uygulamalara erişimlerin engellenmesi veya bant genişliği sınırlaması yapılması,

A.9.7.27.3. Youtube, Vimeo, Dailymotion gibi platformlarda erişimlerle ilgili olarak sadece ihtiyaç duyan personele izin verilmesi

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. Veri tabanında kullanıcı hesabı oluşturma ve kullanıcılara erişim yetkisi tanımlama talepleri resmi yazı ile yapılır. Talep eden kullanıcının Kurumumuz Bilgi Güvenliği Politika Kılavuzunu tebellüğ etmiş olması ve görev yaptığı kurumu ile Bilgi Güvenliği Gizlilik Sözleşmesi /Farkındalık Bildirgesi imzalamış olması gerekmektedir.

A.9.8.3. 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.9.8.4. 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 tanımlanması yapılır.

A.9.8.5. 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.9.8.6. 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.9.8.7. Veri tabanına erişen ortak kullanıcı hesaplarına izin verilmez.

A.9.8.8. Uygulama sunucuları üzerinden gelen veri tabanı kullanıcılarının, sadece ilgili uygulama sunuculardan bağlantı sağlaması ve okuma, yazma, silme ve değiştirme yetkileri olması; yeni tablo/nesne oluşturma, şema değişikliği yapmak gibi yetkilerinin kaldırılması gerekir.

A.9.8.9. 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.9.8.10. Veri tabanına son girilen başarılı ve başarısız oturum bilgilerinin giriş kayıtları tutulur.

A.9.8.11. 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.9.8.12. "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.9.8.13. Veri tabanında "sysdba, sysoper, admin" yetkisine sahip olan kullanıcı hesaplarının kontrolleri yapılır. En yetkili kullanıcıların veritabanında yaptığı işlemler kayıt altına alınır.

A.9.8.14. SQL Server kurulumu ile gelen varsayılan "SA" kullanıcısı pasife alınır.

A.9.8.15. 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.9.8.16. "Yedek alabilme" hakkına sahip kullanıcı hesapları, kurum erişim kontrol politikasında belirtilen aralıklarla kontrol edilir.

A.9.8.17. 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.9.8.18. Güvenlik paketleri ve yamalar, kontrollü olarak uygulanır. Sistemde hangi yamaların uygulanıp uygulanmadığı kontrol edilir.

A.9.8.19. Veri tabanı güncelleştirmeleri takip edilir. Sistem üzerinde kod çalıştırabilen ve yetki yükseltilebilen zafiyetlerin giderilmesine öncelik verilir.

A.9.8.20. Yama ve güncelleme çalışmaları yapılmadan önce tüm ilgili kişi ve kurumlara bildirimde bulunulur ve sonrasında ilgili uygulama kontrolleri gerçekleştirilir.

A.9.8.21. Veri tabanı kullanıcısının kaynakları, limit parametreleri belirli aralıklarla kontrol edilir.

A.9.8.22. Veri tabanına yapılan erişimlerde kaba kuvvet saldırılarına karşı, kullanıcı hesabının kitlenmesi için giriş kontrolü yapılır (5 yanlış deneme sonrası kullanıcı hesabının kilitlenmesi gibi).

A.9.8.23. İstemci, veri tabanı ve uygulama sunucuları arasındaki ağ trafiği şifrelenir. Veri tabanı sunucularına internet üzerinden erişimlerde, VPN gibi güvenli bağlantılar kullanılır.

A.9.8.24. 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.9.8.25. Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılarak uygun yedekleme politikaları oluşturulur. Yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli olarak alınması kontrol altında tutulur.

A.9.8.26. 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.9.8.27. Veri tabanında parola politikasında kullanılan parametrelerin tanımları ve varsayılan değerleri değiştirilir. Veri tabanı üzerinde oluşturulan her kullanıcı profili için parola parametrelerinin tanımlanması gerekir.

A.9.8.28. Veri tabanı kullanıcı profillerine göre tanımlanması gereken diğer parola parametreleri ve önerilen değerleri şu şekildedir:

A.9.8.28.1. Kullanıcı hesabının kilitlenmesi için gerekli maksimum başarısız oturum açma girişim sayısı 5,

A.9.8.28.2. Parolanın geçerli sayılacağı maksimum gün sayısı 90 gün,

A.9.8.28.3. Kullanıcı parola süresi dolmadan önce kullanıcıya parolasını değiştirmesi için hatırlatma gönderme süresi 7 gün,

A.9.8.28.4. Parolanın tekrar kullanılabilmesi için tanımlanması gereken minimum farklı parola sayısı 3,

A.9.8.28.5. Parolanın tekrar kullanılabilmesi için geçmesi gereken minimum süre 90 gün,

A.9.8.28.6. Maksimum sayıdaki başarısız oturum açma girişimlerinden sonra, hesabın ne kadar süreyle kilitli kalacağı süre 10 dk.

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. Erişim talep eden kullanıcı Müdürlüğümüz Bilgi Güvenliği Politikaları Kılavuzunu tebellüğ etmiş olmalı ve kurumu ile Bilgi Güvenliği Farkındalık Bildirgesi imzalamış olmalıdır.

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. Yetkilendirme sunucu tarafında yapılır. Sadece istemci tarafında yetkilendirme kontrolü yapılmamalıdır.

A.9.9.9. 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.9.9.10. Geliştirme ve test işlemlerinin, kullanıma aktarılmadan önce belirli kuralları kapsadığı yazılı bir dokümanı hazırlanır. Geliştirme ve test ortamları esas çalışma ortamından ayrılır. Yazılım projelerinde yapılan değişiklikler öncelikle test ortamında kontrol edilir, gerekli test aşamaları tamamlandıktan sonra canlı ortama yapılan düzenlemeler aktarılır. Test işlemlerinde gerçek kişisel veriler kullanılmaz. Bütün yazılım projeleri için test senaryoları hazırlanır ve testlerde çıkan hataların kontrolü yazılı olarak tutulur.

A.9.9.11. 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.9.9.12. İş sürekliliğini sağlamak adına uygulamaların hata kayıtlarını ve çözümlerini içeren bir hata havuzu oluşturulur.

A.9.9.13. Yedekleme politikası uyarınca bilgi ve yazılımlar yedeklenir. Yedekler belirlenen kurallar doğrultusunda test edilir.

A.9.9.14. Uygulama yazılımları, kullanıcıların parolasını parola politikasına göre oluşturması yönünde zorlayıcı şekilde tasarlanır. Yazılımlar kullanıcıya parolasını değiştirecek yetkilendirmeyi verecek şekilde yapılandırılır.

A.9.9.15. 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.9.9.16. Kullanıcılara tanımlanan geçici parola, güçlü parola politikasına göre ve sınırlı geçerlilik süresine göre verilir.

A.9.9.17. Kurumda kullanılan uygulamalarda tanımlı süre boyunca aktif olmayan oturumlar otomatik olarak kapatılır ve yazılım projeleri türüne göre oturum süreleri belirlenir.

A.9.9.18. Kullanıcı sayısının fazla olduğu ve yoğun olarak kullanılan sistemlerde kimlik yönetim servislerinin yük dengeli (load-balancer) olarak çalıştırılması öngörülür.

A.9.9.19. Uygulama yazılımları başka kaynaklara bağlanırken erişim için kullandığı parolaları şifrelenmiş (encrypted) bir halde saklanır (veri tabanına bağlanırken). 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.9.9.20. Yazılım projelerinde teknik açıkla ilgili kontroller sağlanır. Zafiyetlerin yayınları takip edilir. Uygulama projelerinde güvenliği sağlamak için yazılımı yayına almadan önce KLVZ-EK-13 Güvenli Yazılım Geliştirme Kontrol Listesi ile kontrol edilir.

A.9.9.21. Oturum açılması gereken uygulamalarda belirli sayıda yanlış kimlik doğrulama denemesinden sonra captcha uygulaması ile kullanıcıdan doğrulama talep edilir. Müdürlüğümüz tarafından Google captcha servisi kullanılmaktadır.

A.9.9.22. Son kullanıcı ile uygulama sunucusu arasındaki trafik şifrelenir. SSL protokolünün güncellenmiş son sürümü kullanılır.

A.9.9.23. Uygulama yazılımlarında kullanıcıya dönen hata sayfalarında, kullanıcıya sistem hakkında bilgi verilmemesi ve hata kontrolü yapılması (versiyon bilgisi gibi) için tedbir alınır.

A.9.9.24. 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.9.9.25. Kullanıcı ve yönetici hesap hareketlerinin iz kayıtları tutulur. İz kayıtları yetkisiz kişiler tarafından değiştirilmeye karşı korunur.

A.9.9.26. KVKK'nın 2018/10 sayılı kararı uyarınca özel nitelikli kişisel verilerin işlendiği yazılımlarda;

A.9.9.26.1. Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

A.9.9.26.2. Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

A.9.9.26.3. Veriler üzerinde gerçekleştirilen tüm hareketlerin iz kayıtlarının bir başka ortamda güvenli olarak saklanması,

A.9.9.26.4. 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.9.9.26.5. 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.9.9.26.6. Verilere uzaktan erişim gerekiyorsa en az 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 kriterlere 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 70º'dir. Bu ısıya ulaşan sunucular, üzerlerindeki sensörler aracılığıyla kendilerini kapatırlar. Hizmet sürekliliği için ortam sıcaklığının 18º ila 22ºC arası olması kabul edilir. Sistem odasının birkaç noktasına, e-posta, SMS ya da telefon çağrısı aracılığıyla bilgilendirme yapan ısı sensörleri konumlandırılabilir. Ayrıca, hava sirkülasyonunu doğru sağlamak 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 detektörü konumlandırılmalıdır. Detektör – alarm düzeneği iki basamaklı olup, birinci düzeyde (daha alçakta) suyu fark edip alarmı çalıştıracak bir detektör, ikinci düzeyde (daha yüksekte) ise elektriği kesecek ve bilgisayar sistemlerinin elektrik bağlantısını sonlandıracak bir detektör 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'e 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 ve 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 cihaz alımı yapılırken teknik /idari şartnamelerde Bilgi Güvenliği ile ilgili hususların beraber hazırlanması gerekir.

A.9.11.1.2. Tıbbi cihazlara fiziksel erişim sadece yetkili kişiler ile sınırlandırılır. Cihazların çalınmasını, kurcalanmasını engelleyebilmek için düzenli olarak güvenlik kontrolleri yapılır.

A.9.11.1.3. Tıbbi cihaz envanteri çıkarılır. Cihazlara ait temel bilgiler tespit edilerek kullanıldığı yer ile birlikte kayıt altına alınır. Temel bilgiler bağlantı yöntemini(LAN, RS232 vb.) kullandığını, hangi servislerin çalıştığını, hangi protokollerin kullanıldığını, hangi servisler/ip ile haberleştiğini kapsamalıdır.

A.9.11.1.4. Cihaz ve terminal bilgisayarında işletim sistemi katmanında sıkılaştırma yöntemleri kullanılır. (Güvenlik duvarı, antivirüs yazılımı, ACL tanımlama vb.)

A.9.11.1.5. Tedarik safhasında bilgi güvenliği yapılandırma imkânı sağlayan cihazlar tercih edilir ve bu husus hazırlanacak tıbbi cihaz tedarik şartnamelerine konulur.

A.9.11.1.6. Cihaz yaşam döngüsü boyunca bilgi teknolojileri ile ilgili cihaz yapılandırma ihtiyaçları için üretici firma desteği alınır.

A.9.11.1.7. 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.9.11.1.8. 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.9.11.1.9. 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.9.11.1.10.İz kaydı üretme imkânı olan tıbbi cihazların iz kayıtları sadece yerel cihazda değil merkezi bir iz kaydı saklama sunucusuna da aktarılmak suretiyle saklanır.

A.9.11.1.11. Tıbbi cihazlar tarafından üretilen iz kayıtları, (varsa) SİEM (İz Kaydı Görüntüleme ve Analiz Sistemleri) vasıtasıyla diğer sistemler tarafından üretilen iz kayıtları ile ilişkilendirilir ve gerekli analizler yapılır.

A.9.11.1.12. Tıbbi cihazların düzgün bir şekilde yapılandırıldıklarından emin olmak ve güncelliğini yitirmiş yazılımlardan kaynaklanan tehlikelerin hedefi haline gelmeyeceklerine garanti altına alabilmek için düzenli olarak zafiyet taramaları yapılır. Tespit edilen açıklıklar üretici firmalardan da destek alınmak suretiyle giderilir.

A.9.11.1.13.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.9.11.1.14. 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.9.11.1.15. Cihazlara hesap kilitleme ilkesi uygulanır. Ardı ardına üç defadan fazla hatalı giriş halinde, hesaplar kilitlenir veya belirlenecek bir süre için askıya alınır.

A.9.11.1.16. Cihazlar, verilerin sadece güvenli bir format ve SSH gibi güvenli iletişim protokolleri aracılığı ile gönderilmesini mümkün kılacak şekilde yapılandırılır. Telnet veya http gibi güvenli olmayan iletişim protokolleri yerine https protokolü kullanılır. Güvenli olmayan ağ protokolleri devre dışı bırakılır.

A.9.11.1.17. Cihazın bellenimi (firmware) ve önemli konfigürasyon bilgileri harici olarak yedeklenir.

A.9.11.1.18. Cihazın belleğindeki veriler mümkün ise şifreli olarak muhafaza edilir.

A.9.11.1.19. Yönetici hesabı ve kullanıcı hesapları ayrılır. Mümkün ise ağ üzerinden yönetici hesabı ile cihaza erişim yapılması engellenir.

A.9.11.1.20. Güncelleme mekanizmaları oluşturulur. İşletim sistemleri de dâhil cihaz üzerindeki yazılımlar güncel halde tutulur.

A.9.11.1.21. Cihaz üzerindeki kullanılmayan arayüzler, yazılımsal veya mümkün olmuyorsa donanımsal olarak kapatılır.

A.9.11.1.22. Tıbbi cihazlara uzaktan erişim yapmaya yetkili personelin kimlikleri belirlenir, bu personel ile kişisel gizlik sözleşmesi imzalanır. Uzak bağlantılar Kılavuzun A.6.112 (Uzaktan Çalışma ve Erişim) maddesinde belirtilen tedbirler alınmak suretiyle yapılır.

A.9.11.1.23. Tıbbi cihazlara uzaktan müdahalede bulunan firma çalışanlarına 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 yönetilmesinden sorumlu kişiler ismen belirlenir.

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 kayıtlarının saklanma süresi belirlenirken yasal zorunluluklar, iz kayıtlarından sağlanacak fayda, saklama maliyeti ve ilgili iz kaydının kritikliği göz önünde bulundurulur. Başkaca bir yasal zorunluluk yoksa elektronik olarak üretilen tüm iz kayıtlarının en az iki yıl süre ile saklanır.

A.9.12.5. Güvenlik kameraları tarafından alınan görüntülerin en az üç ay geriye dönecek şekilde saklanması için gerekli tedbirler 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. Teknik olarak mümkün olması durumunda, iz kayıtlarını üreten sistemlerin çalışanlarının yönetici yetkisine sahip olsalar dahi üretilen iz kayıtlarına erişimleri engellenir. İz kayıtlarına, sadece özel olarak erişim yetkisi verilen kişilerin ulaşması sağlanır.

A.9.12.9. Kurumların iz kayıtlarının yönetimi (iz kayıtlarının üretilmesi, aktarılması, depolanması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi gibi süreçler) bağımsız bir birim tarafından yapılır.

A.9.12.10. Teknik olarak mümkün olması durumunda, iz kayıtları gizlilik ve hassasiyet seviyelerine göre sınıflandırılarak, ilgili kullanıcıların sadece verilen yetkiler çerçevesinde iz kayıtlarına bakmaları sağlanır.

A.9.12.11. Bütün sistemlerin zamanlarının aynı olması için Ağ Zaman Protokolü (NTP-NetworkTime 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, güvenlik duvarları, antivirüs yazılımları, saldırı tespit/önleme sistemleri, yönlendiriciler ve anahtarlama cihazları, sunucular, diğer iş uygulamaları (kritik kurumsal projeler), veri tabanları, VPN iz kayıtları.

A.9.12.15.4. Tutulması gereken asgari iz kayıtları;

A.9.12.15.4.1. Kaydı oluşturan sistem

A.9.12.15.4.2. Kaydın oluşturulma zamanı (tarih, saat, zaman dilimi)

A.9.12.15.4.3. Kaydı oluşturan olay

A.9.12.15.4.4. Kaydın ilişkili olduğu kişi (IP-Port bilgisi, MAC adresi, işlemi yapan tekil kullanıcı adı veya sistemin adı)

A.9.12.15.5. 5651 sayılı kanun ve bu kanuna dayanarak yayınlanan ikincil mevzuat ile kurumun tutmak zorunda olduğu iz kayıtları Kılavuzun A.14.4 maddesinde ayrıntılı olarak açıklanmıştır.

A.9.13. YEDEKLEME POLİTİKASI

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. Müdürlüğümüz Yedekleme Politikası sadece veri yedeklenmesini içermemektedir. Bu politikanın amacı, iş sürekliliği açısından hem verinin hem de verinin barındırıldığı ve erişim sağlandığı uygulama ve işletim sistemi katmanında yedekleme sağlanmasıdır. Müdürlüğümüz ve bağlı kurumlarda yedekleme politikası kapsamında asgari olarak aşağıda yer belirtilen sistem ve verilerin yedeklenmesi gerekmektedir:

1. SBYS Uygulama Sunucuları (Sanal ya da fiziksel olabilir. SBYS uygulamaları HBYS, PACS,LBYS vb. uygulamaları kapsamaktadır.),
2. SBYS Veritabanı Sunucuları(Sanal ya da fiziksel),
3. SBYS veritabanı verileri,
4. PACS Dicom verileri,
5. Güvenlik Duvarı konfigürasyon dosyası,
6. Network cihazları konfigürasyon dosyaları,
7. Aktif Dizin Sunucuları (Sanal ya da fiziksel),
8. Müdürlüğümüz tarafından geliştirilen İş Kritik uygulamaları.

A.9.13.1.3. Müdürlüğümüz ve bağlı kurumlarda oluşturulacak olan Yedekleme Planı aşağıda belirtilen asgari alt başlıkları kapsayacak şekilde tanımlanmıştır.

1. Yedeklenen Sistemin tanımı (Veri Tabanı,Sanal Sunucu,Pacs,File Server,Aktif Dizin vb.),
2. Yedekleme Türü(Full yedek,Değişen yedek,Artırımlı yedek, Log yedek,)
3. Yedekleme periyodu,
4. Yedekleme Süresi,
5. Saklama 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. Buna göre müdürlüğümüz ve bağlı kurumlarda kategoriler şu şekildedir:

1. Fiziksel Sunucular,
2. Sanal Sunucular,
3. Veritabanları,
4. Dosyalar,
5. Güvenlik Duvarı,
6. Ağ ve Güvenlik Cihazları iz kayıtları,
7. Sistem erişimi iz kayıtları

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 husustur. Bunun için 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. Müdürlüğümüz ve bağlı kurumlarda, 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.9.13.3.2. Yedeklenecek veriler bilgi işleme süreci içerisinde değişiklik gösterebileceğinden yedekleme listesi en az yılda 2 (iki) kez gözden geçirilmeli ve güncellenmelidir.

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-14'da 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. Bu ortam bir NAS cihazı ya da storage olabilir.

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 günlük olarak kontrol edilmeli ve Yedekleme Kontrol Listesi ile kayıt altına alınmalıdır. Örnek bir Yedekleme Kontrol Listesi KLVZ-EK-15'de verilmiştir. Yedekleme kontrol listesinde kurumlarımız bilgi işlem birim sorumluları ile kurum yöneticilerinin mutlaka ıslak imzası olmalıdır.

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 usullerce şifrelenir.

A.9.13.5.6. Yedekleme medyaları 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. Müdürlüğümüz Yedekleme Politikaları kapsamında, müdürlüğümüz ve bağlı kurumlarda yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için yılda en az 2 defa geri dönüş testlerinin yapılması gerekir.

A.9.13.6.2. Geri dönüş testi tutanakla kayıt altına alınır. Tutanakta; asgari olarak sunucu adı, test tarihi, önceki test tarihi, yedek türü, ne zaman başladığı, ne zaman sona erdiği ve durumu (başarılı/başarısız) ile kimler tarafından yapıldığı (en az 1 yüklenici personel ile kurum yetkilisinin bilgileri) yer almalıdır.

A.9.13.6.3. SBYS yazılımları geri dönüş testi için, tutanağın ekinde kurumlarımızın bilgi işlem sorumlusu ve idari mali hizmetler müdürü tarafından hazırlanan en az 100 adet soru içeren "Geri Dönüş Testi Kontrol Listesi" hazırlanmalıdır. Kontrol listesi soruları geçmiş yıl verilerini de kapsamalıdır. Kontrol listesi soru seti asgari olarak radyoloji, laboratuvar, ayaktan hasta, yatan hasta, ameliyathane faturalama hizmetleri, personel hizmetleri vb. gibi modülleri kapsamalıdır. Geri dönüş testinin başarılı sayılması için, soru setinin tamamına yanıt vermelidir.

A.9.13.6.4. Yedekten geri yükleme testlerinin, başarısız olması nedeniyle veri kaybı olabileceği durumu gözönüne alınarak, canlı ortamda değil gerçek ortamın aynısı olan test ortamında yapılması gerekmektedir.

A.10. HABERLEŞME GÜVENLİĞİ

A.10.1. Uç Nokta (Yerel Alan Ağı) Ağ Güvenliği

A.10.1.1. SBA'ya veya herhangi bir geniş alan ağına bağlı olsun veya olmasın, bir yerel alan ağında ağ güvenliği ile ilgili uygulanması gereken tedbirler takip eden maddelerde sıralanmıştır.

A.10.1.2. Ağa bağlanacak bilgisayarların ağ yöneticileri tarafından belirlenecek kriterleri taşıyan, kimliği tanımlanmış ve doğrulanmış olması gerekir. Bu maksatla mümkünse ağ tabanlı erişim kontrol sistemleri (NAC) kullanılır. NAC tabanlı çözümlerin olmaması durumunda, anahtarlama cihazında mac-port eşleştirilmesi yöntemi kullanılabilir.

A.10.1.3. Yerel alan ağlarında, port kısıtlaması yapılamayan, yönetim yeteneği olmayan ağ dağıtım kutuları (hub) veya eski nesil kenar anahtarlar kullanılmaz.

A.10.1.4. NAC tabanlı çözümlerin olmaması durumunda, kullanılmayan uçlar için kenar anahtar ile dağıtım paneli arasına ara bağlantı kablosu takılmaz.

A.10.1.5. Yerel alan ağları performans, güvenlik ve ölçeklenebilirlik avantajlarını kullanmak üzere VLAN'lara bölünerek yönetilir.

A.10.1.6. 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.10.1.7. 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.) kesinle yasaktır.

A.10.1.8. Müdürlüğümüz yazılı onayı alınmaksızın yukarıda belirtilen şekilde ağ bağlantılarının yapıldığının tespit edilmesi halinde, ilgililer hakkında idari ve yasal işlemler yapılır.

A.10.1.9. Yerel alan ağlarının SBA'ya bağlandığı noktalarda sınır güvenliğinin sağlanması için asgari tedbir olarak bir adet güvenlik duvarı kurulur.

A.10.1.10. Bu noktalarda tesis edilen güvenlik duvarlarının yönetimi, uç noktalardaki bilgi işlem yöneticileri tarafından yapılır.

A.10.1.11. 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 noktaları WPA3 metodunu desteklemeyen cihazlar için Müdürlüğümüz yazılı onayı alınmadan kullanılamaz.

A.10.3.2. Kablosuz erişim noktası olarak kullanılan cihazların yönetimi için kullanılan parolalar değiştirilir. Kurum parola politikasına uygun olarak karmaşık parola verilir.

A.10.3.3. Cihazların varsayılan yayın adı (SSID değeri) değiştirilir, mümkünse gizlenir.

A.10.3.4. Bağlantı ayarları için şifreleme etkinleştirilir. Şifreleme seçeneği etkinleştirirken ağa erişim için kullanılmak üzere üçüncü taraflar tarafından tahmin edilemeyecek karmaşık bir parola belirlenir. Şifreleme yöntemi olarak;

A.10.3.5. Öncelikle WPA3 modu kullanılır.

A.10.3.6. WPA3 modunu desteklemeyen cihazlarda, KRACK ataklarını engellemek için cihazların yazılım güncellemeleri yapılarak WPA2 modu kullanılır.

A.10.3.7. Uyumluluk, güvenilirlik, performans ve güvenlik ile ilgili nedenlerle WEP ve WPA1 kullanımı uygun değildir.

A.10.3.8. Kablosuz ağa bağlanacak kullanıcı sayısı kısıtlı ise ilave güvenlik önlemi olarak ağa bağlanacak cihazların MAC adresleri, kablosuz erişim cihazı üzerinde tanımlanır.

A.10.3.9. 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, "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 verinin sahibi makamlardan 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 Müdürlüğümüz 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 Müdürlüğümüz 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 Kişisel Verileri Koruma Kurulu'nun 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 kullanmak 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 kriterler (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. Müdürlüğümüz 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.10.4.20. 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 (validation) mekanizmasından geçirilir. XML 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. Müdürlüğümüze ait gizli kalması gereken bilgilerin korunması maksadıyla, Müdürlüğümüz ve 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 ya da farkındalık bildirgesi, 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-11 Personel Gizlilik Sözleşmesi,

A.10.5.6.2. Firmalar ve diğer kurum ve kuruluşlar için KLVZ-EK-12 Kurumsal Gizlilik Taahhütnamesi,

A.10.5.6.3. 657 sayılı Devlet Memurları Kanununa bağlı personel için KLVZ-EK-16 Bilgi Güvenliği Farkındalık Bildirgesi kullanılır.

A.10.5.7. Bağlı her kurumumuz kendi ihtiyaçlarına özgü olarak söz konusu dokümanları güncellemelidirler.

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. Dış kurumlara veya dış kurumlardan veri aktarımı yapılırken aşağıda belirtilen hususlar göz önünde bulundurulur;

A.10.6.2. Müdürlüğümüzden veya müdürlüğümüze ya da bağlı kuruluşlara veri aktarımının değerlendirilmesinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'na, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğe ve ilgili diğer mevzuata uyum aranır.

A.10.6.3. Müdürlüğümüzden ya da müdürlüğümüze ya da bağlı kuruluşlara 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 Kişisel Verilerin Korunması Kanunu'nda yer alan ilkelere uygun olarak yapılır.

A.10.6.5. Veri aktarımları bir Protokol çerçevesinde gerçekleşir.

A.10.6.6. Hangi verilerin, hangi amaç veya amaçlarla, ne şekilde ve ne süreyle 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, Kişisel Verileri Koruma Kurulu 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, Kişisel Verileri Koruma Kurulu tarafından yayımlanan alt düzelmeye tamamen 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.

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 gerçekleştirilmesi 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, Müdürlüğümüz Bilgi Güvenliği politikalarına uymak zorundadır.

A.11.1.2.2. Müdürlüğümüz 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 birincil 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. Yukarıdaki metne, satın alma faaliyetine konu işin mahiyetine göre, bilgi güvenliği ile ilgili ilave maddeler eklenir.

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 kriterleri, personel istihdam edilecekse ilgili personel kriterleri 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 bitmesinde 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 oluşturulmadığından emin olunması için test edilmesi gerekir. Satın alınacak ürün; işlevsellik, yönetim ve bakım destek hizmetleri açısından da bilgi güvenliği açısından değerlendirilmelidir

A.11.2. SBSY 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. SBSY üreticisi firmalar, Bakanlık tarafından talep edilen geliştirme 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. 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.11.2.6. İlgili mevzuat kapsamında SBYS yazılım üreticilerine eksikliklerini gidermeleri için süre verilir. Bu süre içerisinde eksikliklerini gideren SBYS yazılım üreticileri aktif listeye alınır.

A.11.2.7. Kullanılmasına karar verilen sağlık bilişimi standartları ve veri gönderiminde dikkat edilecek hususlar Sağlık Bilgi Sistemleri Genel Müdürlüğü web sayfasında (www.sbsgm.saglik.gov.tr) yayımlanır ve güncellenir.

A.11.2.8. Sağlık hizmeti sunucularınca SBYS yazılım üreticilerinden, ürettiği SBYS yazılımının minimum şartlara uyum sağladığını gösteren "KTS Yetki Belgesi" istenir. KTS yetki belgesinin geçerliliği KTS web sayfası üzerinden sorgulanır.

A.11.2.9. 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.11.2.10. Sağlık kuruluşları ile SBYS yazılım üreticisi arasında yaşanabilecek uyuşmazlıklarda uygulanacak cezai şartların SBYS yazılım üreticisi ile yapılacak sözleşmelerde yer alması sağlanır.

A.11.2.11. Sağlık kuruluşları ve aile hekimleri, SBYS yazılım üreticisi ve bayileriyle ayrıca gizlilik sözleşmesi imzalamalıdır. Sağlık tesisleri ve aile hekimleri bu maksatla KLVZ-EK-12 Kurumsal Gizlilik Taahhütnamesini kullanabilecekleri gibi, kendileri de sözleşme metinlerini oluşturabilirler.

A.11.2.12. İlk kurulum esnasında uzaktan destek ile kurulum talepleri kabul edilmez.

A.11.2.13. SBYS yazılım üreticisi, ilk kurulum esnasında çalıştıracağı personel ile ilgili planlamayı kurulum ve proje planında detaylı olarak açıklamak zorundadır.

A.11.2.14. 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.11.2.15. Sağlık kuruluşları, HBYS tedarikçilerinden altı ayda biri geçmemek üzere kendilerine verilen son yedek üzerinden veri kurtarma testi yapmasını istemeli ve gerekli kontrolleri yapmalıdır.

A.11.2.16. Herhangi bir sebeple mevcut SBYS yazılımının kullanımına son verilirse, verilerin tamamı orijinal veri tabanı formatında, kolay ve sorunsuz okunabilir bir medya ortamında, üç kopya halinde sağlık kuruluşuna teslim edilmek zorundadır.

A.11.2.17. Kritik alanlardaki değiştirme ve silme işlemlerinin, ancak yetki ölçüsünde yapılması gerekir. Değişikliklere sonradan erişim ve geri düzeltme için mutlaka iz

kaydıdosyaları detayları olarak tutulmalı veya Veri Tabanı Yönetim Sistemi katmanındaki denetleme (audit) uygulama yazılımından da desteklenir olmalıdır.

A.11.2.18. 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.11.2.19. 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.11.2.20. Çeşitli yetki düzeyleri ve grupları tanımlanabilmeli, yetki değişimi SBYS Yöneticisi tarafından yapılabilmelidir. Verilere erişim bu tanımlamalar çerçevesinde yapılmalıdır.

A.11.2.21. Kullanıcılar için saat bazında sisteme giriş sınırlandırması yapılabilmelidir.

A.11.2.22. Kullanıcıların otomasyona giriş-çıkış zamanları ve geçersiz giriş denemeleri istenildiğinde raporlanabilmelidir.

A.11.2.23. Poliklinik, Klinik, Laboratuvar bazında yetkilendirmeler yapılabilmelidir. Kullanıcının yetki verilmeyen bir poliklinikteki hasta listesine erişimi engellenmelidir.

A.11.2.24. SBYS yazılımlarında Kılavuzun A.6.3 (Parola Güvenliği) maddesinde belirtilen parola kriterleri tanımlanabilmeli ve bu kurala uymayan parolalar kabul edilmemelidir.

A.11.2.25. Sağlık kuruluşu ile ilişiği kalıcı olarak kesilen tüm personelin erişim yetkisi tamamen ve otomatik olarak iptal edilmelidir.

A.11.2.26. Geçici olarak sağlık kuruluşunda bulunmayan (izin-rapor-geçici görev kurs-eğitim vb.) personelin SBYS'ye girişi otomatik olarak engellenmelidir.

A.11.2.27. 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. Müdürlüğümüz ve bağlı kuruluş çalışanları ve vatandaşlar tarafından tespit edilen, Sağlık Bakanlığı ile ilgili her türlü bilgi güvenliği ihlal olayı, https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir adresinde yer alan merkezi ihlal bildirim sistemine girilir.

A.12.1.2. 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.12.1.3. Merkezi ihlal bildirim sistemine girilen olaylar, Sağlık Bilgi Sistemleri Genel Müdürlüğü 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-17 Olay Bildirim ve Müdahale Formunun 1'nci Bölümünü (Olay Bildirimi) doldurur ve kurumsal ihlal bildirimi hafızası oluşturmak üzere saklar.

A.12.1.4. Küçük çaplı, yalnızca kendi kurumunu ilgilendiren ve bilgi güvenliği yetkilisi ya da kurumsal SOME tarafından kendi imkânları ile yerel olarak çözülebilecek olaylara gerekli müdahale yapılır. KLVZ-EK-17'nin 2'nci Bölümünü (Olay Müdahale) doldurularak e-posta ile bilgiguvenligi@saglik.gov.tr adresine gönderir.

A.12.1.5. İhlal olayı 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-17'nin 2'nci Bölümünü (Olay Müdahale) doldurarak bilgiguvenligi@saglik.gov.tr adresine gönderir.

A.12.1.6. 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-17'nin 2'nci Bölümü (Olay Müdahale) doldurularak kayıt altına alınır.

A.12.1.7. Merkezi ihlal bildirim sisteminde yer alan olay türleri ve açıklamaları şu şekildedir:

A.12.1.7.1. **Servis Dışı Bırakma Saldırısı (DoS/DDoS) :** Saldırının amacı hedef alınan sistemi hizmet veremeyecek hale getiricek yöntemlerle, ilgili servisi hizmet dışı bırakmaktır. Kullanılan temel yöntem, ilgili hizmet servisine olağan dışı miktarda çok paket gönderip, engellemektir.

A.12.1.7.2. **Bilgi Sızdırma (Data Leakage):** Kurumun ürettiği, kullandığı ya da işlediği verileri bilinçli veya bilinçsiz olarak yanlış hedefe gönderilmesi, çalınması ve/veya sızdırılmasıdır.

A.12.1.7.3. **Zararlı Yazılım (Malware):** Her türlü bilgi işleme yapabilen sistemlere zarar vermek, veri çalmak ve/veya yok etmek için üretilen yazılımlardır.

A.12.1.7.4. **Sahtecilik (Fraud):** Daha çok finansal sistemlerinde karşılaşılan, aldatma amacı ile yapılan kasıtlı eylemlerdir.

A.12.1.7.5. **Port Tarama:** Herhangi bir hizmet veren sunucu bilgisayarlarında çalışan servislerin varlığını tespit etmek, bilgi toplamak ve tespit edilecek zafiyetler ile zararlı bir işlem yapma amacı ile gerçekleştirilen eylemlerdir.

A.12.1.7.6. **Veri Tabanı Saldırısı:** Veri Tabanı yazılımlarının kullanımından oluşabilecek zafiyetlerden veri tabanının ele geçirilmesi, yönetilmesi, veri sızdırılması ve/veya yetki yükseltilmesi şeklindeki saldırılardır. SQL Injection saldırısı da buna bir örnektir.

A.12.1.7.7. **Web Uygulamaları Güvenlik İhlalleri:** Bu ihlallere örnek olarak, XXS Saldırıları, Kötü amaçlı dosya çalıştırılması, güvenli olmayan direk nesne referanslama, Sunucu taraflı çapraz kod çalıştırma (CSRF), Bilgi sızdırma ve uygun olmayan hata kontrolü, İhlal edilmiş kimlik doğrulama ve oturum yönetimi, Güvensiz İletişimler gibi ihlaller bu madde altında değerlendirilir.

A.12.1.7.8. **Sosyal Mühendislik:** Kişilerin zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye yönelik teknikler içerir.

A.12.1.7.9. **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. durumlarda yaşanan durumları ifade eder.

A.12.1.7.10. **Zararlı Elektronik Posta (SPAM):** İsteğiniz olmadan, size gönderilen ticari içerikli ya da politik bir görüşün propagandasını yapmak ya da bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileridir.

A.12.1.7.11. **Parola Ele Geçirme:** Depolanmaması gereken bir yerde depolanan parolaların tespiti ya da sızması durumudur. Ya da herhangi bir saldırı yöntemi ile parolaların ele geçirilmesidir.

A.12.1.7.12. **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.12.1.7.13. **Kimlik Taklidi:** Kişilerin fiziksel, telefon ya da dijital ortamda olmadığı bir kişi gibi davranıp, onun yetkilerini bilgisi dışında kullanmasıdır.

A.12.1.7.14. **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.12.1.7.15. **Kişisel Bilgilerin Kötüye Kullanımı**: Kişisel verilerin işlenmesine ilişkin süreçlerde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan usul ve esaslara uygunluk sağlanmalıdır. Kişisel verilerin işlenmesinde, 6698 sayılı Kanun'da 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 iyi bir şekilde 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. UYUM

A.13.1. Yasal Gereksinimlere Uyum

A.13.1.1. 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.13.1.2. 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.13.1.3. 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.13.1.4. 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.13.1.5. 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-19 Yasal Mevzuat Uyumu İçin Takip Listesinde yer almaktadır.

A.13.1.6. 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 bab 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.13.1.7. 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, Telekomünikasyon Kurumu (TİB) 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.13.2. Lisanslama ve Fikri Mülkiyet Hakları

A.13.2.1. 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.13.2.2. Fikri mülkiyet, sınai mülkiyet hakları ve telif hakları olmak üzere iki ana başlık altında incelenir.

A.13.2.3. 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.13.2.4. 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, TC. Kültür ve Turizm Bakanlığı Telif Hakları Genel Müdürlüğü tarafından yürütülür.

A.13.2.5. Müdürlüğümüze bağlı tüm birimlerce/kurumlarca yapılan her türlü iş ve işlemlerde, fikri mülkiyet haklarına saygılı davranılır. Bu hakların korunması için gerekli tedbirleri alınır.

A.13.2.6. Çeşitli maksatlar için tedarik edilen yazılımlar, kurumların taşınır kayıt birimleri tarafından envantere alınmak suretiyle kayıt altına alınır. Ayrıca xxxx bölümde belirtilen Kurum Bilgi Varlıkları Envanterine işlenir.

A.13.2.7. Yazılımlara ait lisans belgeleri, CD/DVD ve benzeri materyal, USB dongle vb. anahtarlar, ilgili projenin yürütüldüğü birimde muhafaza edilir.

A.13.2.8. 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.13.2.9. Müdürlüğümüze ait hiçbir cihazda, üreticisi tarafından açıklanmış lisanslama politikasına aykırı bir şekilde (lisanslama/kullanım anahtarının kırılması, yazılımın izinsiz olarak kopyalanması vb.) yazılım kullanılamaz.

A.13.2.10. Lisans çerçevesinde izin verilen kullanıcı sayısının aşılmaması için gerekli tedbirler alınır.

A.13.2.11. Çeşitli isimler altında (open source, freeware, shareware) ücretsiz olarak dağıtılan yazılımlar, zararlı öğeler barındırma ihtimaline karşı test edilmeden kuruma ait bilgisayarlara kurulmaz.

A.13.2.12. Müdürlüğümüz 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, Müdürlüğümüze aittir. Müdürlüğümüz söz konusu varlıkları, ilgili mevzuat uyarınca kendi adına tescil ettirebilir. Kişiler, söz konusu varlıklar üzerine kişisel bir hak iddia edemezler.

A.13.2.13. Aksi kararlaştırılmadıkça, tedarik sözleşmeleri kapsamında yüklenici firmalar tarafından yapılan/yaptırılan tasarım, geliştirme ve/veya eklemelere ilişkin ortaya çıkan fikri mülkiyet hakları Müdürlüğümüze 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 üzerine kişisel/kurumsal bir hak iddia edemezler. Müdürlük, söz konusu fikri mülkiyet haklarından Yükleniciyi bir lisans sözleşmesi çerçevesinde (bedeli mukabili veya bedelsiz olarak) faydalandırabilir.

A.13.2.14. Yüklenici firmalar, sözleşmeler kapsamında Müdürlüğümüz için yaptıkları iş ve işlemlerde üçüncü taraflara ait herhangi bir fikri mülkiyet hakkını ihlal edemezler. Bu husus sözleşmelere konulmak suretiyle garanti altına alınır.

A.13.2.15. Telif hakları kapsamında korunan kitaplar, makaleler, raporlar ve diğer belgeler hiçbir şekilde kopyalanamaz, çoğaltılmaz ve dağıtılamaz.

A.13.2.16. Fikri mülkiyet haklarının ihlal edilmesi ile ilgili şikâyetler www.bilgiguvenligi.saglik.gov.tr adresinde yer alan Olay Bildirim Uygulaması vasıtasıyla Bakanlığa iletilir.

A.13.3. Kişisel Verilerin Korunması Mevzuatı

A.13.3.1. Anayasa'nın 20 nci maddesinin, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ve Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması

Hakkında Yönetmeliğin, kişisel verilerin korunmasına ilişkin hükümlerine azami düzeyde hassasiyet gösterilir.

A.13.3.2. Kişisel verilerin ve kişisel sağlık verilerinin işlenmesinde, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 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.13.3.3. Kişisel verilerin ve kişisel sağlık verilerinin aktarılmasında, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 8 inci ve 9 uncu maddesinde yer alan hükümlere riayet edilir.

A.13.3.4. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesinin birinci fıkrası uyarınca veri sorumlusu (İdare); 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.13.3.5. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 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.13.3.6. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesinin üçüncü fıkrası uyarınca veri sorumlusu (İdare), 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 (İdare), veri işleyeni (HBYS işletimi hizmeti veren yüklenici) denetleyebilir.

A.13.3.7. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesinin dördüncü fıkrası uyarınca veri sorumlusu (İdare) 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.13.3.8. Kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.

A.13.3.9. 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümlerine uygunsuzluk nedeniyle Kişisel Verileri Koruma Kurulu 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.13.4. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi

A.13.4.1. Bilişim denilince bunun en önemli ayaklarından bir tanesini de internet oluşturmaktadır. 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.13.4.2. 5651 sayılı kanun ile temel olarak aşağıdaki hususlarda düzenlemeler yapılmıştır:

A.13.4.2.1. İnternet aktörlerinin (içerik sağlayıcı, yer ve erişim sağlayıcı, toplu kullanım sağlayıcı) tanımı yapılmış ve bu aktörlerin hak ve sorumlulukları belirlenmiştir.

A.13.4.2.2. Yasada suçlar bakımından erişimin engellenmesi usul ve esasları düzenlenmiştir.

A.13.4.2.3. İnternet ortamında yayınlanan içerik nedeniyle haklarının ihlal edildiğini iddia eden kişilere ilişkin; içeriğin yayından çıkarılmasını sağlama ve cevap hakkı uygulamalarına ilişkin usul ve esaslara yer verilmiştir.

A.13.4.2.4. Konusu suç teşkil eden (ve/veya küçükler için zararlı olan) içerik kapsamında filtreleme usulü öngörülmüştür.

A.13.4.2.5. Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen katalog suçlara ilişkin şikâyetlerin yapılabileceği internet bilgi ihbar merkezi (ihbarweb.org.tr) kurulmuştur.

A.13.4.3. 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.13.4.4. "Erişim sağlayıcı" kuruluşlar, abonelerine ticari olarak internet erişimi sağlayan telekomünikasyon firmaları olup Bakanlığımıza bağlı hiçbir kurum bu kategoriye girmemektedir.

A.13.4.5. İçerik Sağlayıcı, İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir. Bakanlık merkez, bağlı kuruluşlar ve taşra teşkilatı birimleri web sayfaları vasıtası ile kullanıcılara içerik sundukları için "İçerik Sağlayıcı" konumundadır.

A.13.4.6. İçerik Sağlayıcı;

A.3.4.6.1. İnternet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

A.3.4.6.2. 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.3.4.6.3. 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 yayınlama ile ilgili usul ve esaslar belirlenmeli, yazılı hale getirilmeli ve titizlikle uygulanmalıdır.

A.13.4.7 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.13.4.8 İnternet Toplu Kullanım Sağlayıcıları;

1. Erişim kayıtlarını (kendi iç ağlarında dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş zamanını ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri, hedef IP adresi, bir veya birden fazla IP adresinin portlar aracılığı ile kullanıcılara paylaştırılması yöntemi ile sunulan internet erişim hizmetinde kullanıcıya tahsis edilen gerçek IP ve port bilgilerini) elektronik ortamda kendi sistemlerine kaydetmek ve iki yıl süre ile saklamakla,
2. Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme (İnternet ortamında web adresi, alan adı, IP adresi, kelime ve benzeri kriterlere göre erişimi engelleyen yazılımları ve donanımları,) sistemini kullanmakla,
3. Kamuya açık alanlarda internet erişimi sağlayan toplu kullanım sağlayıcılar, kısa mesaj servisi (SMS) ve benzeri yöntemlerle kullanıcıları tanımlayacak sistemleri kurmakla sorumludur.

EKLER

KLVZ-EK-01 İŞE BAŞLAMA FORMU

Adı Soyadı			
Unvan/ Yüklenici Firma			
Birimi			
Başlama Tarihi	……./……./20……		
Tamamlanması Gereken Başlıklar	**İlgili Birim / Kişi**	**Kurum Çalışanı Adı Soyadı / İmza**	**İşe Başlayan Kişi Adı Soyadı / İmza**
Kimlik - Giriş Kartının Çıkarılması	İnsan Kaynakları Birimi		
Oryantasyon Eğitimi	Eğitim Birimi		
E-posta Hesabının Açılması	Bilgi İşlem Birimi		
Bilgi Güvenliği Farkındalık Eğitimi	Bilgi Güvenliği İl Yetkilisi / SOME Birimi		
EBYS Açılması	Bilgi İşlem Birimi		
EBYS Eğitimi	Bilgi İşlem Birimi		
Zimmet Oluşturulması	Taşınır Kayıt Kontrol Birimi		
Bilgi Güvenliği Farkındalık Bildirgesi İmzalatılması	Birim Sorumlusu		
Banka Hesabı Açma	Maaş Birimi		

Formun Doldurulma Tarihi: …… /….. / 20……

Formun Doldurulma Tarihi: …… /….. / 20……

KLVZ-EK-02 İŞTEN AYRILMA FORMU

Adı Soyadı			
Unvanı/ Yüklenici Firma			
Birimi			
İşten Ayrılma Tarihi	……./……./20……		
Tamamlanması Gereken Başlıklar	**İlgili Birim / Kişi**	**Kurum Çalışanı İsim/Soy isim İmza**	**İşten Ayrılan Kişi İsim/Soy isim İmza**
Yaptığı İş ve İşlemlerle İlgili Dokümantasyon ve Bilgilendirme Devri Yapılması	Birim Sorumlusu		
VPN Hesaplarının Kapatılması	Bilgi Güvenliği İl Yetkilisi /SOME Birimi		
E-posta Hesabının Kapatılması /E-posta Gruplarından Çıkartılması	Bilgi İşlem Birimi		
EBYS Kapatılması	Bilgi İşlem Birimi		
Zimmet Devri	Taşınır Kayıt Kontrol Birimi		
Kimlik Kartının İade Edilmesi	İnsan Kaynakları Birimi		
Uygulama ve Veri Tabanı Kullanıcılarının Kapatılması (HBYS-ÖBS-HSYS-MBYS vb.)	Bilgi İşlem Birimi		
Banka Hesabı İşlemleri	Maaş Birimi		
Lojman İşlemleri	Lojman İşleri Birimi		

Formun Doldurulma Tarihi: …… /….. / 20……

KLVZ-EK-03 KAYITTAN DÜŞME TEKLİF VE ONAY TUTANAĞI

TUTANAK SIRA NO :

HARCAMA BİRİMİ : FEN EDEBİYAT FAKÜLTESİ **KODU:** 38 08 04 32/432

BÖLÜMÜN ADI :

T A Ş I N I R I N

ZİMMET NO	KODU / SİCİL NO	ADI	HANGİ YILA AİT OLDUĞU	MİKTAR/ADET	BİRİM FİYATI	TUTARI

Yukarıda kodu, adı ve özellikleri, miktarı ve kayıtlı değeri belirtilen toplam .....kalem ve .....adetten oluşan taşınırların;

1 Kullanım sonucu yıpranmış ve hurdalaşmış olduğundan,

2 Kullanım süresi dolmuş olduğundan, (2)

3 Kullanıcısı tarafından kırılıp, bozulmuş ve tamir imkanı olmadığından,

4 Canlı taşınır öldüğünden, **5** .....nedeniyle,

a) Hurdaya ayrılarak teknik, sağlık, güvenlik vb. nedenlerle imha edilmek,

b) Hurdaya ayrılarak, madeni ve ahşap olarak ayrı ayrı satılmak,

c) Taşınırın kırılıp bozulmasında kasıt, kusur veya ihmali görülen sorumludan rayiç bedeli üzerinden tahsil edilmek,

d) .....

.....

üzere kayıtlardan düşülmesi; hususu olurlarınıza sunulur.
...../...../.....

Taşınır Kayıt ve Kontrol Yetkilisi (3)
Adı, soyadı :.....
Unvanı :.....
İmza :.....

KOMİSYON BAŞKANI	**ÜYE (Taşınır Kayıt ve Kontrol Yetkilisi)**	**ÜYE (Uzman)**
Adı, soyadı :.....	Adı, soyadı :.....	Adı, soyadı :.....
Unvanı :.....	Unvanı :.....	Unvanı :.....
İmza :.....	İmza :.....	İmza :.....

UYGUNDUR / UYGUN GÖRÜŞLE SUNULUR
...../...../.....

HARCAMA YETKİLİSİ
Adı, soyadı :.....
Unvanı :.....
İmza :.....

UYGUNDUR
...../...../.....

ÜST YÖNETİCİ
Adı, soyadı :.....
Unvanı :.....
İmza :.....

T.M.Y. Örnek No:10

KAYITTAN DÜŞME TEKLİF VE ONAY TUTANAĞINA İLİŞKİN AÇIKLAMALAR

Bu tutanak, çalınma veya kaybolma nedeniyle yok olan, yıpranma, kırılma ve bozulma nedeniyle kullanılamaz hale gelen ve hurdaya ayrılan taşınırlar ile canlı taşınırların ölümü gibi nedenlerle taşınırların kayıtlardan düşülmesi amacıyla üç nüsha olarak düzenlenir. Harcama yetkilisi veya üst yönetici tarafından onaylanan tutanağın bir nüshası, çıkış kaydına esas olmak üzere düzenlenen Taşınır İşlem Fişi ekine bağlanır. Bir nüshası, Taşınır İşlem Fişi ekinde muhasebe birimine gönderilir. Diğer nüshası ise dosyasında muhafaza edilir.

(1) Tüketim malzemelerinin kayıttan çıkarılmasında taşınır kodu, dayanıklı taşınırın kayıtlardan çıkarılmasında ise taşınır sicil numarası yazılır.

(2) Gıda, ilaç ve kimyasal maddeler gibi kullanım süresi dolduğunda kullanılması sakıncalı ve zararlı olan tüketim malzemeleri için doldurulacaktır.

(3) Bu bölüm komisyon kurulmasına gerek görülmeyen hallerde imzalanacaktır.

KLVZ-EK-04 DİSK İMHA FORMU

VERİ DEPOLAMA ÜNİTESİ BULUNAN TAŞINIRIN				
Sıra No	Marka	Model	Seri No	HDD Seri No
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

İmha edilmesini talep ettiğim/ettiğimiz diskin/disklerin çerisindeki veriler nedeniyle ileride gündeme gelebilecek adli ve idari soruşturmalarda sorumluluğun şahsıma/şahsımıza ait olduğunu kabul ve beyan ederim/ederiz. …/.../20…..

Disk İçinde Bulunan Verilerin
Sahibi Kişi(ler)

Dayanıklı taşınır kayıtlarında bulunan ve ……. tarih ve …… sayılı onay ile oluşturulan komisyon üyelerinin değerlendirmesi sonucunda, ekonomik ömrünü tamamladığı, teknik ve fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dışı bırakılması gerektiği ‘‘**Kayıttan Düşme Teklif ve Onay Tutanağı**’’ ile tespit edilen taşınırların veri depolama üniteleri HEK komisyonda bulunan üyelerin gözetiminde imha edilmiştir. …/.../20…

Teknik Uzman Üye T.K.K.Y Komisyon Başkanı

KLVZ-EK-05 RİSK HESAPLAMA FAKTÖRLERİ

	Varlık Değeri Tablosu			
Güvenlik Hedefi	**Düşük (1)**	**Orta (2)**	**Yüksek (3)**	**Çok Yüksek (4)**
Gizlilik	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkiler. Söz konusu bilgi sadece kurum içerisindeki personelin bilmesi gereken bilgidir. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Söz konusu bilgi kuruma ve kişiye ait gizli bilgilerdir (program, uygulama yazılımları, EBYS, ÇKYS vb, bilgisayar şifre ve /veya parolaları, kişisel bilgiler, sözleşme bilgileri, ihale bilgileri, personel bilgileri, hasta bilgileri).	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. Kuruma ait çok gizli bilgiler (sistem, sunucular, network cihazları, veritabanları erişimleri sağlayan şifre ve /veya parolalar, kurum stratejileri vb.) yetkisiz kişilerin eline geçmesi durumunda Sağlık Bakanlığına büyük ölçüde zarar verecek her türlü bilgi.
Bütünlük	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler. Elektronik imzanın kullanılmadığı, kontrol kayıtlarının tutulmadığı bilgi varlıkları.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Elektronik imza / kayıt onay mekanizmasının kullanıldığı bilgi varlıkları.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Her kayıt için onay sürecinin olduğu, değişiklik kayıtlarının tutulduğu bilgi varlıkları.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. Zaman damgalı elektronik imzanın kullanıldığı, onay kayıt sürecinin her adımda işlendiği bilgi varlıkları.
Erişilebilirlik / Kullanılabilirlik	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler. Uzun süreli kesintilerde iç ve dış hizmetleri aksatmayan bilgi varlıkları.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Kurumda verilen hizmetlerde her hangi bir kesinti/aksama durumunda tolere edilebilinecek süre 3 saat olup, bu süre içinde erişilebilir hale getirilmesi gereken bilgi varlıkları(AD, Exchange vb)	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. Kurumda verilen hizmetlerde her hangi bir kesinti/aksama durumunda tolere edilebilinecek süre 1 saat olup, bu süre içinde erişilebilir hale getirilmesi gereken bilgi varlıkları (IIS-Uygulama sunucuları – veritabanı - FW)	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.Kurumda verilen hizmetlerde her hangi bir kesinti/aksamaya tahammül bulunmamaktadır.

Riskin Gerçekleşme Olasılığı	
Düşük (1)	Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali %1 ile %10 arasındadır.
Düşük (2)	Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali 11% ile %39 arasındadır.
Orta (3)	Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali 40% ile %69 arasındadır.
Yüksek (4)	Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali 70% ile %80 arasındadır.
Çok Yüksek (5)	Bilgi Güvenliği İhlali, saldırı, olumsuz bir olayın olma ihtimali en az 81% ve üzeridir.

GİZLİLİK ETKİ DEĞERİ	
Düşük (1 - 2)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin gizliliğe etkisi düşük olur.Kurum imajı etkilenmez, zarar çok kısa vadede telafi edilebilir, iş süreci aksamaz.
Orta (3)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin gizliliğe etkisi orta derecede olur. Kurum imajı belirli oranda zarar görür. İtibar kaybı ve yasal yükümlülük açısından zarara yol açmaz.
Yüksek (4)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin gizliliğe etkisi yüksek şiddette olur. Medyada yayınlanacak şekilde kurum imajı zedelenir. Zarar orta vadede telafi olunur. Yüksek ek maliyetler doğar ya da çalışanların motivasyonu üzerinde ciddi olumsuz etkiye yol açar.
Çok Yüksek (5)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin gizliliğe etkisi çok yüksek şiddette olur. Yıkıcı / felaket düzeyinde etki gerçekleşir. Kurum çok ciddi itibar kaybına uğrar. Yasal yükümlülükler doğurur, çok yüksek ek maliyetler doğar.

BÜTÜNLÜK ETKİ DEĞERİ	
Düşük (1- 2)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin bütünlüğe etkisi düşük olur. Bütünlük ihlali kurum imajını etkilemez. Sistem ve işleyişte performans sorunu gerçekleşmez.
Orta (3)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin bütünlüğe etkisi orta derecede olur. Bütünlüğü kaybedilen bilgi kurum imajına zarar verir. Ek iş maliyetlerinin doğmasına neden olur.
Yüksek (4)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin bütünlüğe etkisi yüksek şiddette olur. Kritik iş süreçlerinin zarar görmesi kuruma kritik derecede zarar verir.
Çok Yüksek (5)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin bütünlüğe etkisi çok yüksek şiddette olur. Bütünlüğün sağlanamaması felaket düzeyde etkiye neden olur. Yasal yükümlülükler doğrurur, çok yüksek ek maliyetler doğar.

ERİŞİLEBİLİRLİK ETKİ DEĞERİ	
Düşük (1- 2)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin erişilebilirliğe etkisi düşük olur. Risk kurum dışına yansıyacak düzeyde değildir. İş süreçlerinin aksamasına neden olmaz.
Orta (3)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin erişilebilirliğe etkisi orta derecede olur. Belirli bir hizmette yavaşlama ya da küçük çapta iş kesintileri oluşur. Erişlemeyen bilgi orta vadede yerine koyulabilir.
Yüksek (4)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin erişilebilirliğe etkisi yüksek şiddette olur. Olumsuzluk kurum dışına yansır. İş kaybı oluşur, yüksek maliyetler doğar.
Çok Yüksek (5)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliği olayının sonucunda riskin erişilebilirliğe etkisi çok yüksek şiddette olur. Kurum çok ciddi iş kaybına uğrar. Etki yıkıcı / felaket düzeyinde olur. Yasal yükümlülükler doğar. Zarar telafi edilemez / uzun vadede telafi edilebilir.

KLVZ-EK-06 RİSK İYİLEŞTİRME PLANI

RİSKE KONU OLAN VARLIK BİLGİLERİNİN TANIMLANMASI					RİSKE KONU OLAN VARLIĞIN DEĞERİNİN TANIMLANMASI				RİSKE KONU OLAN VARLIK İLE İLGİLİ TEHDİT ve ZAFİYETLER			RİSK TANIMI ve DETAYLARI					RİSK DEĞERLEME (İLK DÖNEM)							RİSK İYİLEŞTİRME PLANI (İLK DÖNEM)			BİR SONRAKİ DÖNEM RİSK GÖZDEN GEÇİRME ve YENİDEN DEĞERLEME							
Risk No	Varlık Grubu / Hizmet	Varlık Adı	Varlık Sahibi	Varlık Yeri	Varlığın Gizlilik Değeri	Varlığın Bütünlük Değeri	Varlığın Erişilebilirlik Değeri	Varlık Değeri Maks (GBE)	Tehdit	Zafiyet	Mühtemel Sonuçlar	Risk Tanımı	Mevcut Durum	Etkilenecek Varlıklar	Risken Sahibi	Riskin Oluştuğuşu Yil	Riskin Olasılığının Ölçümü	İşin Etki	Varlık Değeri	Riskin Olasılığının Ölçümü X Varlık Değeri	Risk Seviyesi	Risk Kararı	Planlanan Faaliyetler	Kaynak/ Finansman	Bir sonraki gözden geçirme tarihi	Gözden Geçirme Tarihi	Sonuçların Değerlendirilmesi	Yeni Olasılık	Yeni Etki	Yeni Risk Puanı	Yeni Risk Kararı	Planlanan Faaliyetler	Kaynak/ Finansman	Bir sonraki gözden geçirme tarihi

KLVZ-EK-07 E-POSTA TALEP FORMU / GERÇEK KİŞİLER

	HİZMETE ÖZEL			
	E-POSTA TALEP FORMU - GERÇEK KİŞİLER İÇİN			
Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.FR.18	10.1.2013	12.12.2016	1	1

Bu Sütunlarda Türkçe Harf Kullanmayınız. Tanımlanacak "SİSTEM ADI" sütunları (AD nokta SOYAD olmalıdır)
Tanımlanacak "SİSTEM ADI" sütunları 20 karakteri geçemez

SIRA	T.C. Kimlik Numarası	Yazışmalarda Görünmesi Tercih Edilen İsim	Sistem Adının Noktadan Önceki Kısmı	Sistem Adının Noktadan Sonraki Kısmı	SİSTEM ADI	Mevcut Yaptığı Görevi	Bağlı İlk Yöneticisi epostası (@saglik.gov.tr mail olmalı)	DAİRE BAŞKANLIĞI veya DENGİ BİRİMİ (dtvt id olan)	Bağlı Olunan KURUM	Adres (Kurum Adresi)	İlçe	Şehir	Sabit Telefon	Cep Telefonu
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														

KLVZ-EK-08 E-POSTA TALEP FORMU / TÜZEL KİŞİLER

HİZMETE ÖZEL

E-POSTA TALEP FORMU - TÜZEL (BİRİM) KİŞİLER İÇİN

Kodu	Yayınlama tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.FR.19	10.1.2013	12.12.2016	1	1

Bu Sütunlarda Türkçe Harf Kullanmayınız. Tanımlanacak "SİSTEM ADI" sütunları 20 karakteri geçemez

						Mail adresinin kullanıldığı Daire Başkanlığı / Koordinatörlük sorumlusu						
Sıra	Yazışmalarda Görünmesi Tercih Edilen İsim	Sistem Adının Noktadan Önceki Kısmı	Sistem Adının Noktadan Sonraki Kısmı	Sistem Adı	Kullanım Yeri	Bağlı Yöneticisi epostası (@saglik.gov.tr olmalıdır)	Başkanlık / Bölüm / Birim	KURUM	ADRES	İLÇE	ŞEHİR	TELEFON
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												

KLVZ-EK-09 SUNUCU TALEP FORMU

Sunucu Talep Eden			
Genel Müdürlük/Daire Başkanlığı/Birim			
Proje Adı			
Adı / Soyadı			
Kurum Telefon No		Cep Telefon	
E-Posta Adresi	……..@saglik.gov.tr		
Kullanım Türü	Gerçek Zamanlı Sunucu	Test Sunucusu	
Kullanıma Başlama Tarihi			
Kullanım Bitiş Tarihi			
Sunucuya Erişim Yetkisi Verilecek Diğer Kullanıcılar	Adı, Soyadı, E-posta Adresi, Görevi, Tlf.Nu.		
Yedekleme İhtiyacı	Evet	Hayır	
DNS Kaydı İsteniyor mu	Evet	Hayır	
DNS Adı	……saglik.gov.tr		
Veri Tabanı İhtiyacı Var mı	Evet	Hayır	
Sistem Gereksinimleri	**Talep Edilen**	**Sağlanan**	
İşlemci			
Bellek			
Disk Alanı			
İşletim Sistemi			
Sunucu Rolü			
Load Balencer İhtiyacı			
Uygulama Bilgileri			
IIS, SQL, PHP vb			
Ağ Gereksinimleri			
Talep Edilen Portlar			
Kullanım Amacı			

Sunucu Talep Yapan Kişinin Görev ve Sorumlulukları

- Sunucudaki bilgilerin ve içeriklerin sorumluluğu sunucu sahibine aittir.
- Sunucuya ait erişim bilgileri sadece yetkili kullanıcıya verilir. Tanımlanan bu yetkili hesaplar devredilemez veya değiştirilemez.
- Sunucuya ait erişim bilgileri yetkili dışında kimse ile paylaşılamaz. Sorumluluk yetki tanımlanmış olan kullanıcıya aittir.
- Sunucu sahibi, sunucu üzerindeki aykırı işlemler sonucu doğabilecek tüm hukuki ve cezai sorumluluğu kabul etmektedir.

KLVZ-EK-10 VERİ TABANI OLUŞTURMA / KULLANICI YETKİLENDİRME FORMU

1. ORTAK BÖLÜM:

TALEPTE BULUNAN ORGANİZASYON	
KURUM / KURULUŞ / GENEL MÜDÜRLÜK	
BAŞKANLIK / DAİRE BAŞKANLIĞI	
BİRİM / ŞUBE VEYA EŞİTİ	
TALEP İLE İLGİLİ TEMAS PERSONELİ	
ADI VE SOYADI	
GÖREVİ VE ÜNVANI	
TELEFON NUMARASI	
E-POSTA ADRESİ	

OLUŞTURULACAK VERİ TABANI İLE İLGİLİ BİLGİLER					
UYGULAMA ADI					
UYGULAMA İLE İLGİLİ ÖZET BİLGİ					
ENTEGRASYON İHTİYACI OLAN DİĞER UYGULAMALAR					
KULLANILACAK VERİ TABANI YÖNETİM SİSTEMİ	ORACLE	MS SQL	POSTGRE SQL	MONGO DB	DİĞER
VERİ TABANI ADI					
KULLANICI / ŞEMA ADI					
TAHMİNİ VERİ TABANI BOYUTU (BİR YIL SONRASI İÇİN) (GB)					

BİRİM SORUMLUSU
ADI / SOYADI/ İMZA

DAİRE BAŞKANI
ADI / SOYADI/ İMZA

3. KULLANICI YETKİLENDİRME TALEPLERİ İÇİN DOLDURULACAK BÖLÜM:

YETKİLENDİRME YAPILACAK VERİ TABANI BİLGİLERİ	
UYGULAMA ADI	
VERİ TABANI ADI	

YETKİLENDİRME TALEPLERİ						
S.Nu.	Adı Soyadı	Telefon	E-Posta	Schema Adı	Tablo/Object Adı	Yetki/Açıklama

BİRİM SORUMLUSU
ADI / SOYADI/ İMZA

DAİRE BAŞKANI
ADI / SOYADI/ İMZA

FORMUN KULLANIMI İLE İLGİLİ HUSUSLAR:

1. İlk defa veri tabanı oluşturma işlemi için 1, 2 ve 3'ncü bölümler birlikte doldurulur.
2. Mevcut bir veri tabanı için yeni kullanıcı ekleme, silme, kullanıcılara yetki verme işlemleri için 1 ve 3'ncü bölümler doldurulur.
3. Sistem Yönetim Daire Başkanlığınca (gerekiyorsa) 1'inci bölümde ismi yazan temas personeli (telefon veya eposta) ile aranılarak taleple ilgili detay bilgiler alınır.
4. İlk defa veri tabanı oluşturma işlemi sonrasında, oluşturulan veri tabanı ile ilgili bilgiler (sunucu adı, IP adresi, port numarası, kullanıcı adı, kullanıcı erişim bilgileri vb.) resmi yazı ile talep makamına, parola bilgileri ilgili kişilerin SMS adreslerine gönderilir.
5. Yetkilendirme işlemlerinde, işlemin gerçekleştirildiği bilgisi, temas personeline e-posta ile bildirilir.

KLVZ-EK-11 PERSONEL GİZLİLİK SÖZLEŞMESİ

Bu sözleşme... / ... / 20... tarihinde, aşağıda yer alan hükümler çerçevesinde, Çankırı Sağlık İl Müdürlüğü ile aşağıda kimlik bilgileri yazılı kişi (Personel) arasında akdedilmiştir.

1. TANIMLAR:

Kuruma Ait Gizli Kalması Gereken Bilgiler:

- Kurum tarafından işlenen (24.3.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan) kişisel veriler ile (20.10.2016 tarih ve 29863 sayılı Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik ile tanımlanan) kişisel sağlık verileri.

- T.C. Sağlık Bakanlığının 24.4.2013 tarih ve 18805 sayılı oluru ile yürürlüğe giren Elektronik Belge Yönetim Sistemi (EBYS) Yönergesi Md. 11 kapsamında tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belge.

- Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belge.

2. YÜKÜMLÜLÜKLER:

- Personel, görevi kapsamında edineceği bilgilerin gizliliğini ve güvenliğini sağlamak için aşağıdaki kurallara uyacağının beyanı olarak bu sözleşmeyi imzalar.

- Personel, T.C. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ile Çankırı Sağlık İl Müdürlüğü tarafından hazırlanan Bilgi Güvenliği Politikaları Kılavuzunda yer alan koşullara uygun hareket eder.

- Personel, bu sözleşme hükümlerine uygun davranmaktan, ihlâli halinde ise kurumumuza ve üçüncü kişilere vereceği her türlü zarardan sorumludur. Sözleşmenin ihlal edilmesi sonucu doğacak tüm hukuki ve cezai sorumlukları peşinen kabul eder.

- Personel, Müdürlüğümüz Bilgi Güvenliği Yönetim Sistemi kapsamında yayımlanmış her türlü politika, prosedür, süreç ve sözleşmelere uygun davranır. Bahse konu dokümanlarda belirtilen sorumlulukları eksiksiz olarak yerine getirir.

- Personel, kurumumuz 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 İdare ile irtibata geçerek veriyi kimlerle paylaşabileceğini teyit eder.

- 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.

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

- Personel, edindiği bilgileri hiçbir kişi, grup, kurum veya kuruluşun menfaati için kullanmaz.

- Gizli kalması gereken bilgiler bu sözleşmenin tanımlar maddesinde açıklanmıştır. Tanımda belirtilen hususlara ilave olarak Kurumumuza ve/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 proje kapsamında çalışma süresi içerisinde yapmış olduğu tüm işler gizlidir. Bunların, görevin gerektirdiği durumlar haricinde kullanılması kesinlikle yasaktır.

- 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. Bu yükümlülük, personelin kurum ile ilişkisinin sona ermesi halinde de devam eder.

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

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

- 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.

- Personel, başkasına zarar vermek ya da kendisine veya başkasına haksız yarar sağlamak maksadıyla yahut herhangi bir maksat gütmeksizin, proje ile ilgili bilgi sistemlerini veya verileri ya da diğer herhangi bir unsuru kısmen veya tamamen tahrip etmek, değiştirmek, silmek, sistemin işlemesine engel olmak veya yanlış biçimde işlemesini sağlamak gibi davranışlarda bulunamaz.

- Personel, Müdürlüğümüzün bilgisi veya onayı dışında, projede kullanılan veriler ve sistemler üzerinde görevin gerektirdiği iş ve işlemler dışında değişiklik yapamaz.

- Personel, hangi amaçla olursa olsun görevi kapsamında kurumumuzdan edindiği bilgileri, projede kullanılan çeşitli şekillerde (basılı, manyetik vb.) bulunabilecek olan verileri, yetkisiz ve izinsiz olarak kullanamaz, kopyalayamaz, taşıyamaz ve aktaramaz.

- Personel, Müdürlüğümüz tarafından kendisine verilen yâda tanımlanan kullanıcı adı/parolayı hiç kimseyle paylaşmaz. Parolasının gizli kalması için alınması gereken tüm tedbirleri alır. Kurumdan/Birlikten ayrılması halinde kullanıcı adı/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.

- Personel, Kurumumuz ve Bakanlığımız sunucuları 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 (belge, doküman, yazılım vb.) sorumludur.

- Personel, 5651 sayılı kanun gereği tutulması gereken kayıtlara ilave olarak; Müdürlük/kurumumuz 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 peşinen kabul eder.

- Personel, sosyal medya hesaplarını kullanırken görevinin gerektirdiği dikkat ve özeni gösterir. Kuruma ait gizli kalması gereken bilgiler, sosyal medya platformlarında paylaşılmaz.

- 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.

- İşbu sözleşme üç nüsha olarak imzalanır, bir nüshası İnsan Kaynakları biriminde, bir nüshası Birim Sorumlusunda saklanır. Diğer nüshası ise personelin kendisine verilir.

- Yukarıda sayılan kurallardan biri ya da birkaçının ihlâlinin tespit edilmesi halinde, güvenlik ihlâline yol açan personel hakkında idari ve yasal işlem başlatılır. Bu kapsamda; 657 Sayılı Devlet Memurları Kanununa tabi olanlar aynı kanunun 125 maddesinde sayılan hükümlere göre, 657 Sayılı Devlet Memurları Kanununun dışında kalan çalışanlar ile ilgili olarak (Danışmanlar, Firma Personeli vb.) sözleşmelerinde belirtilen özel hükümlere göre, yoksa genel hükümlere göre hareket edilir.

Yukarıda sıralanan yükümlülüklere uygun davranacağımı, bu yükümlülüklerden bir veya birkaçına herhangi bir şekilde uygun davranmamam halinde, doğabilecek her türlü idari, mali, hukuki ve cezai yaptırımların uygulanabileceğini kabul ve beyan ederim.

<table>
<tr><td colspan="2">İLGİLİ PERSONELİN</td><td rowspan="5">Firma Yetkilisi
İmza</td></tr>
<tr><td>T.C. Kimlik No</td><td></td></tr>
<tr><td>Adı, Soyadı</td><td></td></tr>
<tr><td>Cep Telefonu</td><td></td></tr>
<tr><td>İkametgâh Adresi</td><td></td></tr>
<tr><td>E-posta Adresi</td><td></td><td></td></tr>
<tr><td>Çalıştığı Firma & Kurum</td><td></td><td rowspan="4">Kurum İdari Amiri/Başkanı/Müdürü
İmza</td></tr>
<tr><td>Çalıştığı Proje & Birim</td><td></td></tr>
<tr><td>Proje & Sözleşme Bitiş Tarihi
Gizlilik Sözleşmesinin Bitiş Tarihi</td><td></td></tr>
<tr><td>İmza</td><td></td></tr>
</table>

KLVZ-EK-12 KURUMSAL GİZLİLİK TAAHÜTNAMESİ

Genel Şartlar

Bir taraftan Cumhuriyet Mahallesi, Namık Kemal Parıltı Cad. No:22, 18100 Çankırı adresinde faaliyet gösteren Çankırı Sağlık İl Müdürlüğü ile diğer taraftan ..... adresinde faaliyet gösteren ..... arasında (a) da yapılan iş tanımı ile ilgili olarak birbirlerine ilişkin edindiği veya edineceği aşağıda detayları belirtilen bilgilerin gizli tutulacağını ve aşağıda belirlenen kurallara uyulacağını kabul beyan ve taahhüt etmişlerdir. İş bu sözleşme birbirinin aynı 2(iki) asıl kopya olarak tanzim edilmiş olup her biri taraflardan birine saklanmak üzere teslim edilmiş olacaktır.

a- İşin Tanımı :

.....

b- Erişim Yeri, Şekli ve Süresi :

.....

2. Tanımlar:

İdare: Çankırı Sağlık İl Müdürlüğü

Taraf: Çankırı Sağlık İl Müdürlüğü ve Hizmet Sunan

Yazılım: İş bu sözleşme kapsamında üretilen ve üretim sürecindeki her türlü yazılım

VTYS: Veri Tabanı Yönetim Sistemi

Veri Öznesi: Kişisel sağlık verilerinin sahibi olan birey

SGK: Sosyal Güvenlik Kurumu

Kişisel Veri: Kişiyi belirli veya belirlenebilir kılan her türlü veri ya da veri kümesidir.

Bilgi Güvenliği Yönergesi: T.C. Sağlık Bakanlığının Bilgi Güvenliği Politikaları Yönergesi.

Kılavuz: Çankırı Sağlık İl Müdürlüğü Bilgi Güvenliği Politikaları Kılavuzu

Kişisel Sağlık Verisi: Kimliği belirli veya belirlenebilir bir kişinin fiziksel, ruhsal, sosyal sağlığına veya veri öznesinin aldığı sağlık hizmetine ilişkin olan, elektronik, kâğıt veya benzeri yollarla üretilen, taşınan veya saklanan sağlıkla ilgili her türlü verisidir. Bu kapsama sağlık hizmeti almak isteyen bireylere ilişkin kayıt bilgileri, ödeme bilgileri, sağlık gerekçeleriyle bireyi teşhis edebilmek amacıyla ilgili kişiye tahsis edilen numara, takma ad, sembol veya diğer herhangi bir özellik veya tanıtıcı, veri öznesine sağlık hizmeti sağlayan kişinin (örneğin; sağlık personeli) kimlik bilgileri gibi bilgiler de girmektedir.

Veri İşleme: Otomatik olarak yapılıp yapılmadığına bakılmaksızın kişisel veriler üzerinde gerçekleştirilen herhangi bir işlem veya işlem dizisidir. Veri işleme; kişisel verilerin toplanmasını, kaydedilmesini, organize edilmesini, depolanmasını, uyarlanmasını veya değiştirilmesini, geri erişimini, konsültasyonunu, kullanılmasını, iletim yoluyla açıklanmasını, yayılmasını veya diğer herhangi bir şekilde kullanılır halde bulundurulmasını, sıralanmasını veya kombinasyonunu, bloke edilmesini, silinmesini veya yok edilmesini ifade eder.

3. Amaç

Sözleşme kapsamında yapılacak çalışmalar dolayısıyla Hizmet sunana vereceği ya da Hizmet sunan tarafından herhangi bir şekilde öğrenilecek gizli bilgiler ile Hizmet sunandan alınacak olan gizli bilgilerin işbu sözleşmede belirtilen şartlar ve taahhütler dâhilinde gizli tutulmasıdır.

4. Gizli Bilgi

4.1. Bu gizlilik sözleşmesi ile aşağıdaki bilgiler kesinlikle "Gizli Bilgi" olarak kabul edilecektir:

- İşbu Sözleşmenin imzalanmasından önce veya sonra Tarafların birbirinden, temsilcilerinden, çalışanlarından, yardımcılarından ve ilgili diğer üçüncü taraflardan yazılı veya sözlü olarak edindikleri, gizli olduğu açıkça ifade edilen veya edilmeyen, İş'le ve Taraflarla ilgili ticari olup olmadığına bakılmaksızın her türlü gizli bilgi,
- İş'in yapılması sırasında elde edilen her türlü gizli bilgi, yazışmalar, yazılımlar ve yazılımlara ait ticari sır niteliği taşıyan bilgiler,
- Veri öznelerine ait kişisel sağlık verileri başta olmak üzere her türlü kişisel veri,
- Yazılıma kaydedilen ve özel ve hassas niteliği olan veri/bilgi,
- Yürürlükteki mevzuat ve iç düzenlemeler uyarınca kullanıcılar tarafından gizli tutulması gereken elektronik ortamdaki veya kâğıt ortamdaki resmi ya da özel kişisel bilgi, belge, veri ve kayıtlar,
- İş bu sözleşme kapsamında doğrudan ya da dolaylı, sözlü veya yazılı şekilde elde edilen veyahut elektronik ortamda bulunan resmi ya da özel, teknik, mali, hukuki, idari her türlü kişisel ve hassas niteliği olan veri bilgi, belge ve kayıtlar,
- İdareye ait tüm ihale verileri ve dokümanları,
- Sözleşmeler, taahhütnameler ve saire her türlü hukuki evrak,
- Bunun yanında sözlü, yazılı, grafiksel veya bilgisayar ortamında okunabilecek türde fakat henüz yayımlanmamış, kamuya duyurulmamış yönetsel kararlar ya da gizli tutulan her türlü belirleme, tasarım, planlama, çizim, bilgi, buluş, araştırma, oluşum, metot, süreç, prosedür, geliştirme, know-how, araştırma, iş planı, strateji, finansal bilgi.
- Herhangi bir şüpheye mahal bırakmaksızın, işbu Sözleşme kapsamında Gizli Bilgi; İdare ve İdare tarafından yaptırılan diğer proje yüklenicilerinin çalışanları da dâhil ve bunlarla sınırlı olmamak üzere İdare için doğrudan ya da dolaylı hizmet eden tüm personeli, danışmanları ve diğer yetkilileri tarafından Hizmet Alana temin edilen bilgileri de kapsar.

4.2. Aşağıdaki bilgiler ise gizli olarak addedilmeyecektir:

- Kişisel ve kurum bilgileri haricinde, İfşa edilme tarihinde kamuya genel olarak duyurulmuş olan veya duyurulan bilgiler.
- Herhangi bir anlaşmaya veya gizlilik yükümlülüğü getiren bir göreve tabi olmayan bir kaynak tarafından gizliliğe tabi olmayan bir şekilde verilen bilgiler.

5.Kişisel Sağlık Verilerinin Gizlilik, Güvenlik, Bütünlük, Erişilebilirlik ve Mahremiyetinin Sağlanmasına Dair Genel Şartlar

- İş bu sözleşmenin tarafları aralarında yürütecekleri iş ve işlemleri Bilgi Güvenliği Yönergesi ve Kılavuz hükümleri çerçevesinde yürütecektir.
- Tüm yazılımların Müdürlüğümüz bilgi güvenliği politikalarına ve kişisel sağlık verilerinin mahremiyetinin korunması ile ilgili mevzuata uygun olması şarttır.

- Kişisel sağlık verileri özel niteliği olan veri kategorisinde yer almaktadır. Bu nedenle SGK, kişilerin özel sigorta şirketleri ile yapmış oldukları sözleşme kapsamı ile sınırlı olmak üzere bu şirketler, Sağlık Bakanlığı veya Bakanlığa bağlı İl Sağlık Müdürlüklerinde bulunan veri tabanı dışında hiçbir veri tabanı yönetim sistemine kişisel sağlık verileri başta olmak üzere hiçbir veri, idarenin bilgisi dışında (otomatik olup olmadığına bakılmaksızın) gönderilmez ve kaydedilemez.
- Yazılımı üzerinde, İdare ile arasında hukuki bir bağ olanlar dışında hiç kimseye doğrudan veya dolaylı olarak kişisel sağlık verilerine erişim hakkı verilmez. Yazılım üzerinde, sağlık hizmeti sunumuna katılan personele sadece hizmet sunumu gereği kadar veri ve bilgiye erişebileceği düzenlemeler yapılmış olmalıdır.
- Yazılım ile toplanan kişisel sağlık verileri, veri öznesi, SGK, kişilerin özel sigorta şirketleri ile yapmış oldukları sözleşme kapsamı ile sınırlı olmak üzere bu şirketler, Sağlık Bakanlığı ve İl Sağlık Müdürlükleri dışında hiçbir surette üçüncü taraflarla paylaşılamaz. Yasalarla öngörülen istisnalar saklıdır.
- İdarece belirlenen bilgisayar, donanım, yazılım ve bilgi teknolojileri ile ilgili asgari şartlara uyulur.
- Yazılımda, vatandaşlara ait veriler dahil tüm verilerinin gizlilik, bütünlük, güvenlik, erişilebilirlik ve mahremiyetini sağlamak amacıyla yazılım üreticisi gerçek ya da tüzel kişi Anayasa, Yasalar, Yönetmelikler, Yönerge, Tebliğ, Genelge ve diğer alt mevzuat ile Genel Toplumsal değerlere, dürüstlük ilkelerine aykırı hiçbir işlem tesis edemez.
- Yazılım, web servisleri, web siteleri, e-posta, Sabit Diskler, Taşınabilir Diskler, kağıda yazdırılmış veri ve bilgiler vb aracılığıyla ya da sözlü olarak SGK, kişilerin özel sigorta şirketleri ile yapmış oldukları sözleşme kapsamı ile sınırlı olmak üzere bu şirketler, İdare ve/veya İl Sağlık Müdürlüğünün sağlamış olduğu sunucu bilgisayarlar haricinde başka sunucu bilgisayarlardaki veri tabanı yönetim sistemlerine, görevi gereği bu verilere erişim hakkı bulunan gerçek ya da tüzel kişiler haricindeki diğer kişilere ait sistemlere kimlik ve kişisel sağlık verilerinin aktarılması ve/veya kaydedilmesi yasaktır.
- Herhangi bir vatandaşa ait kişisel verileri ile kişisel sağlık verilerinin SGK, kişilerin özel sigorta şirketleri ile yapmış oldukları sözleşme kapsamı ile sınırlı olmak üzere bu şirketler, İdarenin sunucuları haricindeki sunucu bilgisayarlara kaydedildiğinin bağımsız ve yetkili, en az üç kişiden oluşan bir teknik ekip tarafından tespit edilmesi halinde, hukuki ve tazminat süreci başlatılır. En kısa süre içerisinde ihlal şartları ortadan kaldırılarak bu yazılımın kullanımına son verilir.
- Mevzuata aykırı davrandığı tespit edilenler ile kişisel sağlık verilerini hukuka aykırı olarak işleyenler (otomatik olup olmadığına bakılmaksızın, kişisel verilerin ve kişisel sağlık verilerinin toplanması, kaydedilmesi, organize edilmesi, depolanması, uyarlanması veya değiştirilmesi, geri erişimi, konsültasyonu, kullanılması, iletim yoluyla açıklanması, yayılması veya diğer herhangi bir şekilde kullanılır halde

bulundurulması, sıralanması veya kombinasyonu, bloke edilmesi, silinmesi veya yok edilmesi)hakkında yasal işlem başlatılır.

- İdare söz konusu yazılımın kullanımdan kaldırılması için her tür haber verme ve duyuru yolunu kullanabilir.
- İdare, bilgi güvenliği ihlali halinde en kısa zamanda gizlilik, güvenlik, bütünlük ve mahremiyetin korunması şartlarını ve İdarece yayımlanan mevzuat gereklerini sağlayan başka bir yazılım edinir ve önceki tedarikçi için idari işlemler başlatılır.
- Yazılım ekranlarında hiçbir surette gerçek ya da tüzel kişi, ürün ya da hizmete dair reklam nitelikli unsurlara yer verilemez, hiçbir ürün ya da hizmetin satışı, satışının teşviki, ürün ya da hizmete doğrudan ya da dolaylı yönlendirme yapılamaz.

- Hizmet Alan veri tabanında yer alan hiçbir kayıt üzerinde hak iddia edemez. Yazılım kullanım sözleşmesi herhangi bir nedenle sona erdirildiğinde idarenin kendi sunucu ve kullanıcı bilgisayarlarında tutulan tüm veriler bir başka yazılıma, (kapsamı idare tarafından belirlenmek üzere) aktarılabilecek bir formatta, veri miktarına uygun bir medya ile ve bir tutanak ile idareye Teslim edilir.
- Yazılım bakım, güncelleme ve teknik destek hizmetleri, (Varsa) öncelikle destek elemanları aracılığıyla karşılanmaya çalışılır. Sistemi tümüyle çalışmaz hale getiren bir arıza gibi zorunluluk halinde İdarenin vereceği tek kullanımlık şifre ile belirli bir süre zarfında yani geçici süreli olarak erişim hakkı verilebilir.
- İdare, yazılım tedarikçisi tarafından kendisine sağlanan yazılımı ve bu yazılıma ait ticari sır niteliğindeki hiçbir bilgiyi üçüncü taraflarla paylaşamaz.
- Yazılımı içerisinde, sağlık hizmeti sunumu amacını aşan ve bilimsel literatür haricinde kalan hiçbir veri/bilgi otomatik şekilde işlenemez.
- Hizmet Alan&Sunan tarafından Resmi Yazı, Resmi yazı faksı ve iş bu sözleşmede belirtilen kurumsal e-posta hesabı üzerinden gelen taleplere karşılık Genel Müdürlük tarafından sunulan hizmetler ve bu hizmetler kapsamında elde edilen her türlü hak, imtiyaz, erişim ve veri için de iş bu sözleşme ile belirlenen hükümler geçerlidir.

6. İstisnalar

Hizmet Alan&sunan, İdareden alacağı bilginin;

- İşbu sözleşmenin hükümlerini ihlal etmeyen ve kamuoyuna mal olmuş ya da olacak türden olması durumunda,
- Açıklanması İdare tarafından kesin yazılı onay ile mümkün kılınmış olan bilgi olması halinde,
- Yüklenici tarafından gerekliliğinin önceden idareye yazılı olarak bildirilmesi ve onayının alınması sonucunda bütünüyle işbirliğinin sağlanmış olması halinde,
- Herhangi bir kanuna, mahkeme kararına ya da hükmüne dayanılarak açıklanmak zorunda kalınan bilgi olması halinde ancak belirtilen mahkeme kararı ile sınırlı olmak kaydıyla, öğrendiği bilgiyi, belgeyi, veriyi, kaydı gizli tutmak zorunda değildir.

7. Mülkiyet Hakkı

İdare tarafından Hizmet Alana sağlanan bilgiyi Hizmet Alan, kullanma izni çerçevesinde veya başka suretle herhangi bir lisans, marka, patent ya da buna benzer bir fikri mülkiyet hakkı tesisine konu edemez. Söz konusu bilgi üzerinde mutlak mülkiyet hakkı İdareye aittir. Dolayısıyla, İdare tarafından Gizli Bilgi'nin Hizmet Alana sağlanması, hiçbir surette Hizmet Alana böyle bir hak sağlamayacaktır.

8. Yükümlülükler

- Taraflar, yazılı veya sözlü olarak aldıkları gizli bilgilerle ilgili olarak aşağıdakileri kabul etmektedir ve bünyeleri altında faaliyet gösteren diğer tüm personelin ("Temsilciler") de aşağıdaki yükümlülüklere uymasını sağlayacaktır:
- Taraflardan her biri, gizli bilgileri yalnızca sağlık hizmet sunumu ve hizmetin kapsam ve niteliğinin geliştirilmesi amacı için kullanacaktır. Taraflardan her biri, gizli bilgileri başka herhangi bir amaçla, özellikle de bir diğer Taraf aleyhine doğrudan veya dolaylı zarar verecek herhangi bir şekilde kullanmayacaktır.
- Taraflardan her biri, gizli bilgileri tamamen ve titizlikle gizli tutacak ve iş amacıyla bu bilgilere ihtiyaç duyan temsilcileri dışında herhangi bir şahsa kısmen veya tamamen ifşa etmeyeceklerdir.

Temsilcilerine, gizli bilgilerin gizlilik niteliğini ve işbu Sözleşme gereği bu bilgilerin gizli tutulmasından sorumlu olduklarını bildirecekler ve Temsilcileri de akdi olarak bu bilgilerin gizli tutulması ile yükümlü kılacaklardır.

- Gizli bilgilerin bütün asılları İş'in sonunda derhal ilgili tarafa iade edilecek, iade edilemeyen bütün kopyalar ilgili tarafça onaylanacak şekilde yok edilecektir.
- Taraflardan herhangi biri gizli bilgilerin gizlilik niteliği ve bu gizli bilgilerin kullanılabileceği amaçlar hakkında açıkça bilgi vermeyi; bu kişilerin kendilerinin işbu sözleşme ile taahhüt edilen yükümlülüklere tabi imişler gibi sorumluluklarına riayet etmelerinden mesul olmayı kabul eder.
- Taraflar göstereceği asgari özenin kendisine ait bilgileri koruma hususunda gösterdiği özenden aşağı olmayacağını kabul eder.

9. Süre

- İş bu sözleşme, imzalandığı tarihte yürürlüğe girecek ve İş'in tamamlanmasından sonra da süre sınırı olmaksızın geçerliliğini koruyacaktır.
- İdarenin yeni bir Gizlilik Sözleşmesi yayınlaması ve yayınlanan yeni Gizlilik Sözleşmesinin Taraflarca imza altına alınması durumunda iş bu sözleşme hükümleri ortadan kalkacak ve yeni Gizlilik Sözleşmesi hükümleri geçerli olacaktır.
- İş bu sözleşme 2(iki) orijinal metin olarak tanzim edilmiş olup her biri taraflardan birine saklanmak üzere teslim edilmiş olacaktır.

10.Tazminat ve Mahkeme

İş bu sözleşme kapsamındaki yükümlülüklerin ihlal edilmesi ve ihlalin tespiti halinde, ihlal eden taraf diğer Taraf'ın bu yüzden uğrayacağı zararları ilk yazılı talep üzerine nakden ve defaten tazmin edecektir. İş bu Sözleşmeden doğacak uyuşmazlıklarda Çankırı Mahkeme ve İcra Daireleri yetkili olacaktır.

11. Vergi Resim Harçlar

Bu sözleşmenin imzalanmasıyla doğacak olan her türlü vergi, resim harç vb resmi giderler Yükleniciye ait olacaktır.

İmza tarihi: …../…../……

<table>
<tr><td colspan="2">Hizmet Sunan</td><td rowspan="6">Yetkili Onayı
(İdare Yetkilisi kaşe & imza)</td></tr>
<tr><td>Firma Ünvanı</td><td></td></tr>
<tr><td>Ticaret Sicil No</td><td></td></tr>
<tr><td>Vergi Dairesi ve No</td><td></td></tr>
<tr><td>Firma Adresi</td><td></td></tr>
<tr><td>Firma Kaşe Yetkili İmza</td><td></td></tr>
</table>

KLVZ-EK-13 GÜVENLİ YAZILIM GELİŞTİRME KONTROL LİSTESİ

TÜBİTAK BİLGEM tarafından yayımlanan dokümana Kurumun internet sitesinden https://egitim.sge.gov.tr/pluginfile.php/6115/mod_page/content/20/SGE-KLV-GuvenliYazilimGelistirmeKilavuzu_Rev1.0.pdf adresinden erişim sağlanabilmektedir.

KLVZ-EK-14 YEDEKLEME PLANI

HİZMETE ÖZEL

YEDEKLEME PLANI

Birim Adı	Sunucu Adı	IP	Tip	Yedek Tipi	Periyod	Yedekleme Süresi	Yedekleme Sistemi

KLVZ-EK-15 YEDEKLEME KONTROL LİSTESİ

HİZMETE ÖZEL

YEDEKLEME KONTROL LİSTESİ

Kontrol Tarihi	Sunucu Adı	Yedek Periyodu	Durum	Son Başarılı Yedek Tarihi

KLVZ-EK-16 BİLGİ GÜVENLİĞİ FARKINDALIK BİLDİRGESİ

AMAÇ:

Bu bildirge; İl Sağlık Müdürlüğü bünyesinde görev yapan 657 Sayılı Devlet Memurları Kanununa Tabi personel ile kadroya alınan 4857 Sayılı İş Kanununa tabi personelin, hizmetin ifası esnasında veya herhangi bir gerekçeyle vâkıf oldukları, kuruma ait gizli kalması gereken bilgilerin, gizliliğinin sağlanması ve ifşa edilmemesi için uyulması gereken kuralları tanımlar.

2. KAPSAM:

Bu bildirge, Kurum bünyesinde görev yapan 657 Sayılı Devlet Memurları Kanunu ve kadroya alınan 4857 Sayılı İş Kanununa tabi personel için hazırlanmıştır. Kuruma ait gizli bilgilere erişim ihtiyacı olan diğer personel (danışman, firma personeli vb.) için Çankırı Sağlık İl Müdürlüğü tarafından yayımlanmış "Personel Gizlilik Sözleşmesi" hükümleri uygulanır.

3. YASAL DAYANAK:

Bu bildirge, 657 Sayılı Devlet Memurları Kanununun Gizli Bilgileri açıklama yasağı başlıklı 31'nci maddesine ve 31.12.2015 tarihli Sağlık Bakanlığı Bilgi Güvenliği Yönergesine istinaden hazırlanmıştır.

4. TANIMLAR:

Bu bildirgede geçen;

KURUM: Çankırı Sağlık İl Müdürlüğü(Bağlı Birimler, Bağlı kurumlar)

KURUMA AİT GİZLİ KALMASI GEREKEN BİLGİLER:

1) Kurum tarafından işlenen (24.3.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Tanımlanan) kişisel veriler ile (20.10.2016 tarih ve 29863 sayılı Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkındaki Yönetmelik ile tanımlanan) kişisel sağlık verilerini,

2) T.C. Sağlık Bakanlığının 24.4.2013 tarih ve 18805 sayılı oluru ile yürürlüğe giren EBYS Yönergesi Md. 11 kapsamında tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belgeyi,

3) Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya Kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belgeyi, İfade eder.

5. PERSONELİN YÜKÜMLÜLÜKLERİ:

- Kuruma ait gizli kalması gereken bilgileri, yasal zorunluluklar ve Kurum tarafından resmi olarak izin verilmesi halleri dışında süresiz olarak koruyacağımı; Kurum tarafından aksi belirtilmedikçe, hiç bir şekilde söz konusu bilgileri doğrudan veya dolaylı olarak kullanmayacağımı; başka bir yere aktarmayacağımı, yayınlamayacağımı, açıklamayacağımı, kişisel kopyalarını almayacağımı,

- Kuruma ait gizli kalması gereken her türlü bilgiyi sır olarak saklamak, bunları üçüncü kişilere inceletmemek, söylememek, iletmemek ve açıklamamakla yükümlü olduğumu; öğrendiğim sırları veya bilgileri ve bunlara ilişkin belgeleri yetkileri olmayan kişilere ve makamlara açıklamayacağımı; bu yükümlülüğümün Kurum ile ilişkimin sona ermesi halinde de devam ettiğinin bilincinde olduğumu,

- Sosyal medya hesaplarımı kullanırken görevimin gerektirdiği dikkat ve özeni göstereceğimi, kuruma ait gizli kalması gereken bilgileri, hastalara ilişkin kişisel bilgileri (hasta görüntüleri vb.) sosyal medya platformlarında paylaşmayacağımı.

- Kurum tarafından uygun görülen 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,

- Tarafıma verilen "kullanıcı adı" ve "parola"yı bir başkası ile paylaşmayacağımı ve bir başkasına kullandırmayacağımı, Kurumdan ayrılmam halinde şahsıma tahsis edilen kullanıcı adı ve parolayı iptal ettireceğimi; kullandığım bilgisayar ve/veya diğer elektronik veri depolama cihazlarında oluşturduğum veri, bilgi ve belgeler dâhil tüm dosyaları, cihazları ve ofis malzemelerini eksiksiz olarak kurum yetkilisine teslim edeceğimi ve hiçbir kopyasını almayacağımı,

- Bilgisayarımda tarafıma tahsis edilen "kullanıcı adı" ve "parola" ile oturum açacağımı; çalışmam bitince, oturumu veya bilgisayarımı kapatarak bilgisayarıma başkalarının fiziksel erişimine fırsat vermeyeceğimi, bilgisayarımın başından kısa süreli ayrılmalarımda bilgisayar oturumunu kilitleyeceğimi,

- Kurum tarafından sağlanan İnternet üzerinden girilen ve girilemeyen tüm siteler ve adreslerin, sistem tarafından gerekli olduğunda kullanılmak üzere kayıt altına alındığını; bu kapsamda 5651 sayılı "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun" gereği bana tahsis edilen kullanıcı adı ve parola kullanılmak suretiyle usulüne uygun olarak kayıt altına alınan işlemlerden yasal olarak sorumlu tutulacağımı bildiğimi,

- Kurum sunucuları üzerinde bana tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP (Internet Protokol) adresini kullanarak gerçekleştirdiğim her türlü etkinlikten, Kurum bilişim kaynaklarını kullanarak oluşturduğum ve/veya bana tahsis edilen Kurum bilişim kaynağı üzerinde bulundurduğum her türlü kaynağın (belge, doküman, yazılım vb.) içeriğinden sorumlu olduğumu,

- Şahsıma teslim edilen kullanıcı adı ve parolanın gizli kalmasını sağlamakla yükümlü olduğumu, şahsi kusurum nedeniyle kullanıcı adı ve parolamın başkaları tarafından öğrenilmesi halinde, bu bilgiler kullanılarak yapılan iş ve işlemlerden şahsen sorumlu tutulabileceğimi bildiğimi,

- İşin gerektirdiği haller dışında kurumsal e-posta hesabımı kullanmayacağımı, Kurum içindeki diğer kullanıcılara iş ile ilgili olmayan toplu ve/veya kişisel e-posta göndermeyeceğimi; Kurum içine veya Kurum dışına göndermiş olduğum tüm e-postalardan kişisel olarak sorumlu olduğumu ve ilgili tüm yasal sorumlulukların tarafıma ait olduğunu,

- Tarafıma teslim edilmiş elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gereç üzerinde kurum bilgisi dışında hiçbir mekanik ya da yazılımsal yapılandırma değişikliği yapmayacağımı,

- Bilgisayarıma Kurum tarafından yüklenmiş işletim sistemi ve uygulama yazılımları dışında herhangi bir işletim sistemi veya lisanssız yazılım yüklemeyeceğimi, Kurum tarafından yüklenmemiş yazılımlardan doğacak her türlü hukuki sorumluluğun tarafıma ait olduğunu, taahhüt eder, bu taahhütlerimi yerine getirmemem veya kasıtlı olarak taahhütlerimi ihlal etmem hâlinde; Kurum açısından oluşacak zararı karşılayacağımı, mali, cezai ve hukuki tüm sorumlulukların bana ait olduğunu beyan ve kabul ederim.

İsim **İmza** **tarih**

6. İLGİLİ DOKÜMANLAR

4857 Sayılı iş kanunu

KLVZ.EK.17 OLAY BİLDİRİM VE MÜDAHALE FORMU

OLAY BİLDİRİM BÖLÜMÜ

1. Bildirimi yapan birim:

2. Bildirimi yapan personelin

Ad, Soyadı :
Unvan/Birim :
Telefon :
E-posta :

3. Olay türü:

□ Servis Dışı Bırakma Saldırısı (DoS/DDoS)
□ Bilgi Sızdırma (Data Leakage)
□ Zararlı Yazılım (Malware)
□ Dolandırıcılık (Fraud)
□ Port Tarama
□ Veritabanı Saldırısı
□ Diğer (Lütfen açıklayınız):

□ Web Uygulamaları Güvenlik İhlalleri
□ Sosyal Mühendislik
□ Veri Kaybı/ Veri İfşası
□ Zararlı Elektronik Posta(Spam)
□ Parola Ele Geçirme
□ Taşınır Cihaz Kaybı
□ Kimlik Taklidi
□ Oltalama (Phishing)
□ Kişisel Bilgilerin Kötüye Kullanımı

4. Olay sistem kesintisine sebep oldu mu? □ Evet □ Hayır

5. Olayın:

Tahmini başlangıç zamanı
Tarih : …….. Saat : ……..

Tespit edildiği zaman
Tarih : …….. Saat : ……..

6. Eklemek istedikleriniz:

OLAY MÜDAHALE BÖLÜMÜ
Dikkat: Bu kısım Bilgi Güvenliği /SOME Olay Müdahale Ekibi tarafından doldurulur.
7. Siber olaylara ait iz (log) kayıtları tespit edildi mi? □ Hayır □ Evet Kaynak IP :_____ Hedef IP :_____ Port : _____ Diğer : _____
8. Olayın etkisini azaltıcı ilk önlemler:
9. Olayın muhtemel sebepleri:
10. Olayın tekrarlanmaması için alınan önlemler:
11. Tahmini Olay Maliyeti
12. Eklemek istedikleriniz:

KLVZ-EK-18 İŞ SÜREKLİLİĞİ FORMLARI

KRİTİK SÜREÇLER / VARLIKLAR LİSTESİ			
No	PROJE/SÜREÇ/HİZMET ADI	AÇIKLAMA	SAHİBİ
1	HBYS	Hastane Bilgi Yönetim Sistemi	HBYS Yazılımı Üreten Özel Sektör Firması

KAYNAK İHTİYAÇ LİSTESİ				
Kaynak / Detay	Miktar	24 saat	72 saat	1 hafta
Masaüstü ve dizüstü bilgisayarlar (yazılımla birlikte), bağlantılı yazıcılar; kablosuz cihazlar (e-posta erişimine sahip)				
Önemli kayıtlar, veriler, yedekler				

KRİTİK VARLIK / SÜREÇ ANALİZ FORMU	
Kritik iş süreci adı	HBYS
Hizmetin sunulması için gerekli bilgi sistemlerini idare etmek kimin sorumluluğunda?	Hastane yönetimi (Hastane Bilgi İşlem Birimi)
Hizmeti sunmak kimin sorumluluğunda?	Hizmet veren firma
Hizmetin kullanıcısı kimler? Kim bu hizmetten faydalanıyor / ihtiyaç duyuyor?	Hastane çalışanları ve hastalar
Hizmet sunum şekli nasıl?	Yazılım aracılığıyla
Tolere Edilebilecek Maksimum Kesinti Süresi Nedir?	30 dk
Kritik İş Sürecinin En Fazla Kaç Saatlik Veri Kaybına Tahammülü Vardır?	8 saat
Destekleyen Varlıklar	
Donanım:	1 adet uygulama sunucusu,1 adet VTYS sunucusu
Yazılım:	XXX sunucu işletim sistemi ve yazılımları

Hizmetin sunulmasını destekleyen uygulamalar:	HBYS yazılımı
Kullanıcı tarafındaki uygulamalar:	HBYS Doktor ve hemşire ekranları
İnsan Kaynağı:	HBYS Firması destek personeli
Veri Tabanı:	XXX veri tabanı
Tesisler:	Sistem odası
Tedarikçiler:	XXX firması
Veri tabanı Yedek alma stratejisi:	Tam Yedekleme / değişen kısımların yedeğinin alınması / İşlem log kayıtları
Veri tabanı Yedek alma sıklığı:	Günde 3 kez
Sunucu Yedeklilik Durumu:	yok

İŞ KURTARMA PLANI						
Kritik İş Hizmeti Adı:			**Ölüm Bildirim Sistemi**			
	Çok Acil (3 saat içerisinde)		Acil (Aynı gün içerisinde)		Normal (Bir hafta içerisinde)	
	Yapılması Gerekenler	Sorumlu Personel	Yapılması Gerekenler	Sorumlu Personel	Yapılması Gerekenler	Sorumlu Personel
Kritik sunucunun hizmet dışı kalması						
Kritik sanal sunucunun hizmet dışı kalması						
Kritik sunuculara geniş çaplı virüs saldırısı gerçekleşmesi						
Hacker saldırısı						

Tedarikçinin süreçten ayrılması (iflas vb.)						
Bilgi sızıntısı						

TATBİKAT TEST UYGULAMA FORMU					
Kritik İş Hizmeti Adı:		**Ölüm Bildirim Sistemi**			
	Sorumlu personel / tedarikçi	Beklenen sonuç	Elde edilen sonuç	Tatbikat tarihi	Onaylayan
Kritik sunucunun hizmet dışı kalması					
Kritik sanal sunucunun hizmet dışı kalması					
Kritik sunuculara geniş çaplı virüs saldırısı gerçekleşmesi					
Hacker saldırısı					
Tedarikçinin süreçten ayrılması (iflas vb.)					

KLVZ-EK-19 YASAL MEVZUAT UYUMU İÇİN TAKİP LİSTESİ

No	Mevzuatlar	Sayı	Yayın Tarihi	Değişim Tarihi	Kaynak
1	663 sayılı Sağlık Bakanlığı ve Bağlı kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname	Madde 2-11-47	11.10.2011	29.10.2016	http://www.mevzuat.gov.tr
2	5070 sayılı Elektronik İmza kanunu	25355	23.1.2004	09.08.2016	http://www.mevzuat.gov.tr
3	5809 Elektronik Haberleşme Kanunu	27050	10.11.2008	24.11.2016	http://www.mevzuat.gov.tr
4	Elektronik Tebligat Yönetmeliği	28533	19.01.2013		http://www.mevzuat.gov.tr
5	5651 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	26530	23.05.2007	15.08.2016	http://www.mevzuat.gov.tr
6	Bilgi Edinme Hakkı Kanunu	4982	24.10.2003	16.07.2015	http://www.mevzuat.gov.tr
7	Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik	25445	27.04.2004	10.11.2005	http://www.mevzuat.gov.tr
8	Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik	25692	06.01.2005		Kamu Sertifikasyon Merkezi
9	Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ	28544	30.01.2013		Kamu Sertifikasyon Merkezi
10	Kamu Kurum ve Kuruşları İçin IPV6'ya Geçiş Planı Genelge	27779	08.12.2010		http://www.mevzuat.gov.tr
11	İnternet Alan Adları Yönetmeliği	27752	07.11.2010		http://www.mevzuat.gov.tr

12	Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik	28036	25.08.2011		http://www.mevzuat.gov.tr
13	TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı	2013V	01.12.2013		https://www.tse.org.tr
14	TS ISO/IEC 15504 SPICE Standardı		25.12.2008		https://www.tse.org.tr
15	Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında KHK Değiştirilerek Kabulü Hakkında Kanun	3473	04.10.1988		http://www.resmigazete.gov.tr
16	Kamu Kurumları İnternet Siteleri Kılavuzu	26416	27.01.2007		http://kamis.gov.tr/
17	Lisanslı Yazılım Kullanılması Genelge	26938	16.07.2008		http://www.resmigazete.gov.tr

EDİTÖRLER :

Faruk GÜNGÖR
İdris KÖRİSMAİLOĞLU

2019