



**T.C.
SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ GENEL MÜDÜRLÜĞÜ**

**BİLGİ GÜVENLİĞİ
POLİTİKALARI KILAVUZU**

Sürüm 2.1

2019

Bilgi Güvenliđi Politikaları Kılavuzu, Bakanlık Makamının 02/05/2018 tarihli ve 98813779.719.54 sayılı onayı ile yayımlanan Bilgi Güvenliđi Politikaları Yönergesi'nin eki olarak yayımlanmıştır.

Editörler:

Dr. M. Mahir ÜLGÜ
M. Fatih ULUÇAM
Dilek ŞEN KARAKAYA
Filiz AYDOĞDU
Burcu GÖKTÜRK
Erdal YILDIZ

Bakanlık Yayın No: 1108

ISBN No: 978-975-590-724-6

Yayın Tarihi: Temmuz 2019

Baskı ve Tasarım

Kuban Matbaacılık Yayıncılık
İvedik Organize San. Matbaacılar Sit. 1514. Sok.
No: 20 Yenimahalle/ANKARA
Tel: 0312 395 20 70 • Fax: 0312 395 37 23
www.kubanmatbaa.com

Bu Kılavuz'da yer alan yazı, fotoğraf ve sair içeriklerin, bireysel kullanım dışında izin alınmadan kısmen ya da tamamen kopyalanması, çoğaltılması, kullanılması, yayınlanması ve dağıtılması kesinlikle yasaktır. Bu yasađa uymayanlar hakkında 5846 sayılı Fikir ve Sanat Eserleri Kanunu uyarınca yasal işlem yapılacaktır. Ürünün tüm hakları saklıdır.



BİLGİ GÜVENLİĞİ POLİTİKALARI KILAVUZU

Sürüm 2.1

ÖNSÖZ	11
1. BİLGİ GÜVENLİĞİ POLİTİKALARI	15
1.1. Temel Prensipler.....	15
1.2. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu.....	16
1.3. Kurumsal BGYS Politikalarının Oluşturulması ve Uygulanması.....	18
2. BİLGİ GÜVENLİĞİ ORGANİZASYONU	23
2.1. Bakanlık Bilgi Güvenliği Yönetim Komisyonu	23
2.2. Sağlık Bakanlığı Sektörel SOME.....	24
2.3. Bilgi Güvenliği Alt Komisyonları	25
2.4. Bilgi Güvenliği Yetkilisi.....	26
2.5. Kurumsal SOME Ekip Lideri ve Kurumsal SOME'ler.....	26
2.6. Üst Yönetimlerin Sorumluluğu	27
3. İNSAN KAYNAKLARI VE SON KULLANICI GÜVENLİĞİ	29
3.1. İşe Alma Öncesinde Yapılacak Kontroller	29
3.2. Çalışma Esnasında Uygulanacak Kontroller.....	30
3.3. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri.....	31
3.4. Görev Değişikliği veya İşten Ayrılma İçin Uygulanacak Kontroller	32
3.5. Kullanıcıların Bilgi Güvenliği Sorumlulukları	33
3.6. Elektronik Posta Güvenliği	35
3.7. Sosyal Mühendislik ve Sosyal Medya Güvenliği	40
4. VARLIK YÖNETİMİ	43
4.1. BGYS Bakış Açısıyla Varlıklar	43
4.2. Varlık Envanterinin Tespiti.....	44
4.3. Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi.....	45
4.4. Taşınabilir Ortam Yönetimi.....	48
4.5. Ortamın Yok Edilmesi	50
5. RİSK YÖNETİMİ	55
5.1. Genel	55

5.2. Sorumluluklar.....	56
5.3. Risk Yönetimi.....	56
6. ERİŞİM KONTROLÜ	63
6.1. Erişim Kontrol Politikası.....	63
6.2. Kullanıcı Erişimlerinin Yönetimi	65
6.3. Parola Güvenliği.....	66
6.4. Sağlık Bakanlığı Uygulamalarına OGN.....	68
6.5. Merkezi Aktif Dizin ve E-Posta Sistemine Erişim.....	69
6.6. Veri Merkezi ve Sunucu Barındırma Hizmetlerine Erişim	70
6.7. Merkezi Veri Tabanı Yönetim Sistemine Erişim	71
6.8. Elektronik Belge Yönetim Sistemine Erişim	73
6.9. Kimlik Paylaşım Sistemine Erişim	74
6.10. e-Nabız, USS Bilgi Yönetim Sistemi ve KDS Raporlarına Erişim.....	75
6.11. Halk Sağlığı Yönetim Sistemine Erişim.....	79
6.12. Merkezi Web İçerik Yönetim Sistemine Erişim.....	80
6.13. Sağlık Bilişim Ağına Erişim.....	82
6.14. Uzaktan Çalışma ve Erişim	83
7. KRİPTOGRAFİK KONTROLLERİN KULLANIMI.....	89
7.1. Kriptografik Politikalar.....	89
7.2. Kriptografik Araç ve Yöntemler.....	90
8. FİZİKSEL VE ÇEVRESEL GÜVENLİK	95
8.1. Genel Hususlar	95
8.2. Güvenli Alanlar	96
8.3. Ekipman Güvenliği.....	98
9. İŞLETİM GÜVENLİĞİ	103
9.1. Yazılı İşletim Prosedürleri.....	103
9.2. Değişiklik Yönetimi	104
9.3. Kapasite Yönetimi	106

9.4. Geliştirme, Test ve İşletim Ortamlarının Ayrılması.....	107
9.5. Etki Alanı Kurulum ve Yönetimi	108
9.6. Sunucu ve Sistem Güvenliği	108
9.7. Ağ İşletim Güvenliği	113
9.8. Veri Tabanı Güvenliği.....	117
9.9. Yazılım Güvenliği	119
9.10. Sunucu/Sistem Odası Güvenliği.....	123
9.11. Tıbbi Cihaz Güvenliği.....	127
9.12. İz Kayıtları (Log) Yönetimi.....	130
9.13. Yedekleme Yönetimi	132
9.14. Teknik Açıklık Yönetimi	133
9.15. Sistem Güvenlik Testleri	135
10. HABERLEŞME GÜVENLİĞİ.....	139
10.1. Ağ Güvenliği	139
10.2. Uç Nokta (Yerel Alan Ağı) Ağ Güvenliği	140
10.3. Kablosuz Ağ Güvenliği	141
10.4. Veri Aktarımı Güvenliği.....	142
10.5. Gizlilik Sözleşmeleri	146
10.6. Veri Aktarım Anlaşmaları.....	148
11. TEDARİKÇİ İLİŞKİLERİ	151
11.1. Mal ve Hizmet Alımları Güvenliği.....	151
11.2. SBYS Firmaları ile İlişkilerde Dikkat Edilecek Hususlar	153
12. BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ	157
12.1. İhlal Bildirimi ve Olay Yönetimi	157
12.2. Kanıt Toplama	159
13. İŞ SÜREKLİLİĞİ YÖNETİMİ.....	163
13.1. İş Sürekliliği Genel Yaklaşımı	163
13.2. İş Sürekliliği Adımları.....	164

13.3. İş Sürekliliği Stratejisi Belirleme	169
13.4. İş Sürekliliği Planı Oluşturma	170
13.5. İş Sürekliliği Planlarını Tatbikatlar ile Test Etme	173
14. UYUM	175
14.1. Yasal Gereksinimlere Uyum.....	175
14.2. Lisanslama ve Fikri Mülkiyet Hakları.....	176
14.3. Kişisel Verilerin Korunması Mevzuatı	178
14.4. 5651 Sayılı Kanun ile Uyum	179
14.5. Bilgi Güvenliği Denetimleri.....	182
EKLER.....	185
KLVZ-EK-01 İşe Başlama Formu	186
KLVZ-EK-02 İşten Ayrılma Formu	187
KLVZ-EK-03 Kayıttan Düşme Teklif Ve Onay Tutanağı.....	188
KLVZ-EK-04 Disk İmha Formu.....	190
KLVZ-EK-05 Kurum Bilgi Varlıkları Envanter Çizelgesi.....	191
KLVZ-EK-06 Risk Hesaplama Faktörleri	192
KLVZ-EK-07 Risk İyileştirme Planı	195
KLVZ-EK-08 E-Posta Talep Formu / Gerçek Kişiler.....	196
KLVZ-EK-09 E-Posta Talep Formu / Tüzel Kişiler	197
KLVZ-EK-10 Sunucu Talep Formu.....	198
KLVZ-EK-11 Veri Tabanı / Kullanıcı Oluşturma Formu	199
KLVZ-EK-12 Personel Gizlilik Sözleşmesi	201
KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesi	206
KLVZ-EK-14 VT Kullanıcı İşlemleri ve Yetkilendirme Talep Formu	210
KLVZ-EK-15 Güvenli Yazılım Geliştirme Kontrol Listesi.....	212
KLVZ-EK-16 Yedekleme Kontrol Listesi	213

KLVZ-EK-17 Bilgi Güvenliđi Farkındalık Bildirgesi	214
KLVZ-EK-18 Olay Bildirim ve M¼dahale Formu	218
KLVZ-EK-19 İş Sürekliliđi Formları	219
KLVZ-EK-20 Yasal Mevzuat Uyumu İçin Takip Listesi	222

ÖNSÖZ

Bakanlığımızda bilgi güvenliđi çalıřmaları iki ana eksen üzerine oturtulmuřtur. Bunlardan ilki olan “**Bilgi Güvenliđi Politikaları Yönergesi**” ile hukuki ve idari alt yapı oluřturulmuř, Yönerge’den alınan yetki ile bilgi güvenliđine yönelik teknik ve yönetsel tedbirlerin yer aldıđı “**Bilgi Güvenliđi Politikaları Kılavuzu**” hazırlanmıřtır. Söz konusu dokümanların ilk sürümleri, eř zamanlı olarak 03 Mart 2014 tarihinde yayımlanarak yürürlüđe girmiřtir.

Yönerge ve Kılavuz, ilk sürümlerinin yayımından bugüne kadar geçen süreçte yařanan teknolojik geliřmeler, kullanıcılardan alınan geri bildirimler ve 1 sayılı Cumhurbaşkanlığı Kararnamesi ile deđiřen Bakanlık teřkilat yapısı dikkate alınarak güncellenmiřtir. Yönerge’nin en son sürümü 02 Mayıs 2018 tarihinde yayımlanmıřtır. Yönerge’nin ayrılmaz bir parçası olan Kılavuz ise Yönerge’nin yeni sürümü ile uyumlu olacak řekilde Eylül 2018 ayı içerisinde güncellenmiř, Temmuz 2019 ayı içerisinde (baskı iřlemleri öncesinde) yeniden gözden geçirilerek 2.1 sürümü olarak yayımlanmıřtır. Yönerge’ye Sađlık Bilgi Sistemleri Genel Müdürlüđünün (SBSGM) web sayfasından eriřim sađlanabilmektedir.

Bilgi teknolojilerindeki geliřmelerle birlikte, bilgi güvenliđinin sađlanmasına yönelik gereksinimler gittikçe daha karmařık ve kapsamlı hale gelmiřtir. Sınırlı bütçe ve personel kaynakları ile kapsamlı bir bilgi güvenliđi çalıřması yapılması için daha sistematik ve yönetsel sistemlerin uygulanması zorunluluk haline gelmiřtir. Kılavuz’un okumakta olduđunuz sürümü hazırlanırken teknik detaylardan mümkün olduđunca kaçınılmıř, ISO 27001 Bilgi Güvenliđi Yönetim Sistemi (BGYS) standardında belirtilen madde bařlıkları dikkate alınarak, güvenlik önlemlerinin kolay anlaşılabilir bir özeti sunulmuřtur.

Günümüzde bilgi güvenliđi ile birlikte sıkça anılan diđer iki önemli konu da “**siber güvenlik**” ve “**kiřisel verilerin korunması**” alanlarıdır. Kılavuz’da yer alan ve teknik personel tarafından özel yazılım, donanım ve araçlar kullanılmak suretiyle hayata geçirilen tedbirler, aslında birer siber güvenlik tedbidir. Etkin bir BGYS tesis edilmesi için siber güvenlik ile ilgili teknik tedbirlere ilave olarak yönetsel tedbirlerin de alınması, farkındalık eđitimleri ile kurum kültürünün deđiřtirilmesi ve tüm bu süreçlere üst yönetimlerin de etkin katılımı ve desteđi gerekir. Kılavuz’da yer alan konulara ek olarak Bakanlığımız bünyesinde siber güvenlik ve siber olaylara müdahale ile ilgili hususların iřleyiři, “**Kurumsal**

Siber Olaylara Müdahale Ekibi (SOME) Kurulum ve Yönetim Rehberi” ile düzenlenmiştir.

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

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

POLİTİKALAR

1. BİLGİ GÜVENLİĐİ POLİTİKALARI

1.1. Temel Prensipler

1.1.1. T.C. Sağlık Bakanlığı; anayasa, yasalar, yönetmelikler ve ilgili diđer mevzuat çerçevesinde yürütmekte olduđu 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.

1.1.2. Bakanlık, hizmet verdiđi vatandaşların kayıt altına aldığı her türlü bilgisini, kendisine emanet edilmiş bir değer olduđu vizyonu ile korumakla mükellef olduđunun bilinciyle hareket etmektedir.

1.1.3. Bakanlık, bilgi güvenliđi 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;

1.1.3.1. Bilgi güvenliđi standartlarının gerekliliklerini yerine getirmek,

1.1.3.2. Bilgi güvenliđi ile ilgili tüm yasal mevzuata uyum sağlamak,

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

1.1.3.4. Bilgi güvenliđi yönetim sistemini sürekli gözden geçirmek ve iyileştirmek,

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

1.1.4. Bilgi güvenliđi sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iş olduđu 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.

1.1.5. Bilgi güvenliđi 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.

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

1.1.7. Başarılı ve etkin işleyen bir bilgi güvenliđi 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.

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

1.2. Sağlık Bakanlığı Bilgi Güvenliđi Politikaları Kılavuzu

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

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 zararlar çıkılarak hizmet sürekliliğinin temininin esas alınması öncelikli şarttır.

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

1.2.4. Bu kapsamda önce 2013-2014 Eylem Planı yürürlüğe girmiş, zamanla artan güvenlik gereksinimleri nedeni ile güvenlik stratejilerinin güncellenmesi ihtiyacı

dođmuş ve “2016-2019 Ulusal Siber Güvenlik Stratejisi” ve “2016-2019 Ulusal Siber Güvenlik Eylem Planı” hazırlanmıştır. 2016-2019 Ulusal Siber Güvenlik Stratejisinde sađlık sektörü kritik altyapı barındıran sektörler arasında yer almakta ve bu bağlamda Bakanlıđımız da kritik altyapı işleyen kamu kurumları arasında yer almaktadır.

1.2.5. Ulaştırma, Denizcilik ve Haberleşme Bakanlıđı tarafından 21 Haziran 2017 tarihli 30103 sayılı resmi gazete ile “KamuNet Ađına Bağlanma ve KamuNet Ađının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliđ” yayımlanmıştır. Tebliđin amacı; “KamuNet’e dâhil edilecek kamu kurumlarının ađa bağlanan bilgi ve iletişim sistemlerine ilişkin olarak karşılama gereken asgari gereklilikler ile bu kurumların denetlenmesine ilişkin usul ve esaslar”ı belirlemek ve KamuNet’e bağlantı yapacak kamu kurumlarının kendi BGYS’lerini kurması, işletmesi ve kurulan BGYS için ISO 27001 standardına göre sertifikalandırılma zorunluluđu getirmektir.

1.2.6. SBSGM, 2014 yılından bu yana tüm faaliyetlerini kapsayacak şekilde kendi BGYS’ni kurmuş ve başarıyla uygulamaktadır. Tesis edilen sistemin ISO 27001 standardı ile uyumluluđu her yıl yapılan dış denetimler ile belgelenmekte ve güncelliđi sađlanmaktadır.

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

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

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

1.2.10. Bilgi güvenliđi önlemlerinin hukuksal dayanaklarına ilişkin en güncel gelişme, 6698 sayılı Kanun’un yürürlüđe girmesi ile olmuştur. Ülkemizde kişisel verilerin korunmasının sađlanması ve buna yönelik farkındalık oluşturarak bilinç düzeyinin geliştirilmesi görevi KVKK’ya verilmiştir.

1.2.11. KVKK tarafından, 6698 sayılı Kanun'un uygulanmasına yönelik birçok ikincil mevzuat ve açıklayıcı doküman hazırlanmış ve yayımlanmıştır. Kurul tarafından yayımlanan ikincil mevzuata ve ilgili diđer bilgi ve belgelere Kurulun <https://www.kvkk.gov.tr/> adresinden erişim sağlanabilmektedir.

1.2.12. KVKK tarafından yayımlanan mevzuata ilave olarak, kişisel sađlık verileri ile ilgili özel hususlar için Bakanlıđımızca "Kişisel Sađlık Verileri Hakkında Yönetmelik" yayımlanmış durumdadır.

1.2.13. Kılavuz hazırlanırken; 6698 sayılı Kanun, KVKK tarafından yayımlanan ikincil mevzuat ve Bakanlıđımız tarafından yayımlanmış olan Kişisel Sađlık Verileri Hakkında Yönetmelik'te yer alan ve doğrudan bilgi güvenliđi ile ilişkili olan hususların Kılavuz içerisine alınması için çaba gösterilmiştir. Bununla beraber;

1.2.13.1. Kılavuzda yer alan tedbirler gizlilik, bütünlük ve erişilebilirlik gibi güvenlik unsurlarının sağlanmasına yönelik rehberlik etmekte olup, kişisel verilerin mahremiyetinin sağlanması ve hukuka uygun bir şekilde işlenmesinin sağlanması için ayrıca KVKK mevzuatında yer alan diđer tedbirlerin de uygulanıyor olması gerekmektedir.

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

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

1.3. Kurumsal BGYS Politikalarının Oluşturulması ve Uygulanması

1.3.1. Sađlık Bakanlıđı merkez teşkilat birimleri, bađlı kuruluşlar ve İSM'ler Bakanlıđımız bilgi güvenliđi hedefleri doğrultusunda, kendi sorumluluk alanlarında bulunan ve bilgi işleme faaliyetlerinde kullanılan tüm unsurlar için (sistemler, süreçler, tesisler, insanlar vb.) kuralları tanımlanmış, planlı, etkileşimli ve sürekli iyileştirmeye dayanan bir BGYS kurmakla, aşağıda belirtilen esaslar çerçevesinde kendi kurumsal bilgi güvenliđi politikalarını oluşturmakla ve tesis edilen BGYS'yi etkin bir şekilde işletmekle yükümlüdür.

1.3.2. Tesis edilen BGYS'nin herhangi bir ulusal veya uluslararası standardı sıkı sıkıya esas alması ve bu standart doğrultusunda belgelendirilmesi (sertifikalandırılması) zorunluluđu bulunmamaktadır.

1.3.3. Kılavuzda yer alan hususlar, ilgili kurumlar tarafından hayata geçirilecek BGYS'lerde kullanılabilir temel bazı tedbirleri ve günümüz teknolojileri çerçevesinde var olan en iyi uygulama örneklerini içermektedir. Bilgi güvenliğinin tam olarak sağlanabilmesi için uygulayıcılar tarafından;

- Kendi kurumlarında kullanılan sistemler ve cihazlar, çalışan personelin eğitim durumu, bilgi işleme tesislerinin fiziki özellikleri, bölgesel ve coğrafi farklılıklar gibi hususlardan kaynaklanan kuruma özgü bilgi güvenliği risklerinin ayrıntılı olarak tespit edilmesi,
- Tespit edilen risklerin önlenmesi için Kılavuzda yer alan tedbirler başta olmak üzere gerekiyorsa ilave önlemlerin belirlenmesi,
- Alınacak önlemlerin yazılı hale getirilerek tüm kurum personeline duyurulması,
- Uygulamanın sürekli olarak takip edilerek varsa uygunsuzlukların ve yeni risklerin tespit edilmesi,
- Tespit edilen uygunsuzluklar ve yeni riskler için düzeltici faaliyetlerin hayata geçirilmesi,
- Sürekli iyileştirme için ihtiyaç duyulan çalışmaların yürütülmesi gerekmektedir.

1.3.4. Bilgi güvenliği politikası BGYS'nin en kritik ögesidir. Bir güvenlik politikası, verilerin ve kaynakların gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için bilgi kaynaklarına erişen herkesin uyması gereken asgari kuralları tanımlar. Ayrıca, kurumun bilgi güvenliği bakış açısını yansıtır, güvenlik sorumluluklarını tanımlar ve bilgi güvenliği olaylarına müdahale yaklaşımını ortaya koyar. Kurumsal bilgi güvenliği politikasının geliştirilmesi kurumsal hafızaya sahip çalışanlar, bilgi güvenliği uzmanları ve yönetimin ortak çalışması ile yapılır. Bilgi güvenliği politikasının bilgi güvenliği hedefleri, stratejik hedefler ve hizmet kapsamı ile uyumlu olması gerekir.

1.3.5. Bakanlığımıza bağlı kurum ve kuruluşlarda tesis edilen BGYS'ler için herhangi bir belgelendirme (sertifikasyon) zorunluluđu bulunmamaktadır. Ancak bir kurum veya kuruluş herhangi bir nedenle ISO 27001 veya benzeri bir standart kullanarak belgelendirme süreçlerine dâhil olmak istiyorsa, başta BGYS Politikası olmak üzere dokümantasyon işlemleri için ilgili standardın gereksinimlerine uygun olarak hareket eder.

1.3.6. İSM seviyesinde ilin tamamı için kullanılacak şekilde tek bir BGYS politikası hazırlanması ve İl Sağlık Müdürü tarafından imzalanarak yürürlüğe konulması yeterlidir. Hazırlanacak BGYS politikasının kısa, öz ve en az aşağıda sıralanan başlıkları içermesi gerekir.

- Amaç
- Kapsam
- Dayanak
- Tanım ve Kısaltmalar
- Bilgi Güvenliđi Organizasyonu
- Politika Metni
- Ekler

1.3.7. BGYS Politikasında yer almayan ve detaylandırılmaya ihtiyaç duyulan diğer hususlar için destek dokümanları hazırlanır. Destek dokümanları ihtiyaca göre politika, prosedür, talimat, yönerge, liste, form vb. detaylarda oluşturulabilir. Herhangi bir konuya ilişkin İSM'nin geneli için ortak olarak kullanılacak tek bir destek dokümanı hazırlanabileceđi gibi ilgili konunun hastanelerde uygulanmasında farklılıklar var ise kurumlara özgü ayrı destek dokümanlarının hazırlanması uygun olacaktır. Örneđin yedekleme ile ilgili hususlar merkezi olarak tek elden yapılıyor ise İSM tarafından bu konuyu açıklayan tek bir doküman hazırlanır ve il genelinde bu doküman kullanılabilir. Bununla birlikte yedekleme işlemi her hastanede farklı araç ve yöntemlerle yapılıyor ise her kurumun kendi yedekleme işlemi açıklayan bir prosedür veya talimat hazırlanması gerekir. Destek dokümanları hazırlanırken aşağıdaki hususları içerip içermediđi kontrol edilmelidir:

- Erişim kontrolü / mobil cihazlar ve uzaktan çalışma (Kılavuz Madde 6),
- Bilgi sınıflandırma (ve işleme) (Kılavuz Madde 4.3),
- Fiziksel ve çevresel güvenlik (Kılavuz Madde 8),
- Varlıkların kabul edilebilir kullanımı / temiz masa ve temiz ekran (Kılavuz Madde 4),
- Bilgi transferi, haberleşme güvenliđi (Kılavuz Madde 10),
- Yazılım kurulumu ve kullanımı ile ilgili kısıtlamalar (Kılavuz Madde 9),
- Yedekleme (Kılavuz Madde 9.13),
- Kötücül yazılımlardan koruma (Kılavuz Madde 9.6),
- Kriptografik kontrollerin kullanımı (Kılavuz Madde 7)

- Teknik açıklıkların yönetimi (Kılavuz Madde 9.14),
- Kişi tespit bilgisinin mahremiyeti ve korunması (Kılavuz Madde 12),
- Tedarikçi ilişkileri (Kılavuz Madde 11).

1.3.8. Bazı İSM'lerde bilgi güvenliđini doğrudan ilgilendiren birçok faaliyetin (tek etki alanı, ortak veri merkezi, merkezi HBYS kullanımı, merkezi virüs koruma, tek noktadan satın alma vb.) merkezi olarak yönetilmesi durumunda, bu konuları içerecek şekilde daha kapsamlı BGYS Politikalarının hazırlanmasında bir mahsur bulunmamaktadır.

1.3.9. İSM'ler tarafından örnek olarak kullanılabilir bir BGYS politikası ve diđer destek dokümanlarına ait örnekler, Bakanlık bilgi güvenliđi web sayfasında yayımlanır (<https://bilgiguvenligi.saglik.gov.tr/Home/Dokumantasyon>).

1.3.10. Hazırlanan BGYS Politikasının kurumun tüm çalışanları tarafından bilinmesi ve anlaşılması gerekir. Bu maksatla BGYS politikası tüm personele tebliđ edilir, farkındalık eğitimlerinde politika içinde yer alan konular hakkında kullanıcılara daha ayrıntılı bilgi verilir.

1.3.11. BGYS politikası (ve ilişkili diđer destek dokümanları) tüm çalışanlar tarafından gerektiğinde ulaşılabilecek şekilde, kurumun iç ađında kontrollü olarak yayımlanır.

1.3.12. Yukarıdaki hususlara ilave olarak Kurum BGYS vizyonunu açıklayan ve bu konuyla ilgili üst yönetim desteđini ve bađlılıđını ifade eden “Kurum Üst Yönetimi Bilgi Güvenliđi Taahhünamesi” başlıklı bir doküman, kurumun en üst düzey yöneticisi tarafından imzalanır ve kurum web sayfasının herkese açık bölümünde yayımlanmak suretiyle ilgili tüm iç ve dış taraflar ile paylaşılır.

1.3.13. İSM'lere bađlı hastaneler ve diđer sađlık tesisleri tarafından ayrıca BGYS Politikası hazırlanması ve yayımlanmasına gerek yoktur. Hastaneler ve diđer bađlı kuruluşlar İSM tarafından yayımlanan BGYS Politikasına uymakla mükelleftir. Bununla birlikte İSM tarafından yayımlanan BGYS politikasında yer almayan veya ilave açıklama gereken hususlar; Hastane kalite süreçleri kapsamında hazırlanan “bilgi yönetim sistemi politikaları” içerisinde veya ayrı destek dökümanları olarak açıklanır.

2. BİLGİ GÜVENLİĐİ ORGANİZASYONU

2.1. Bakanlık Bilgi Güvenliđi Yönetim Komisyonu

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

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

Komisyonadaki Görevi	Bağlı Olduđu Birim	Görevi
Başkan	SBSGM	Genel Müdür
Başkan Yrdc.	SBSGM	Genel Müdür Yardımcısı
Koordinatör	SBSGM	Sistem Yönetimi ve Bilgi Güvenliđi Dairesi Başkanı
Raportör	SBSGM	SOME Birim Sorumlusu
Raportör	SBSGM	BGYS Birim Sorumlusu
Üyeler	Türkiye İlaç ve Tıbbi Cihaz Kurumu Başkanlığı	Kılavuz'un 2.3 maddesi geređi bağlı bulunduđu Kurum/ Genel Müdürlük adına "Bilgi Sistemleri Koordinatörü" olarak görevlendirilen en az Daire Başkanı düzeyinde personel
	Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü	
	Kamu Hastaneleri Genel Müdürlüğü	
	Halk Sağlığı Genel Müdürlüğü	
	Sağlık Hizmetleri Genel Müdürlüğü	
	Acil Sağlık Hizmetleri Genel Müdürlüğü	
	Yönetim Hizmetleri Genel Müdürlüğü	
	Sağlığın Geliştirilmesi Genel Müdürlüğü	
	Sağlık Yatırımları Genel Müdürlüğü	
	Hukuk Hizmetleri Genel Müdürlüğü	
	Strateji Geliştirme Başkanlığı	
Teftiş Kurulu Başkanlığı		

2.1.3. Komisyona bađlı olarak alıřmak üzere sorumluluk sahası ile ilgili alıřma grupları oluřturulabilir. alıřma grupları oluřturulurken konunun zelliđi dikkate alınarak farklı disiplinlerden personel bulundurulur.

2.1.4. Komisyon, bařkanın ađırısı üzerine yılda en az bir kere toplanır. Gerekli grlen durumlarda bařkan komisyonu her zaman toplantıya ađırabilir.

2.1.5. Toplantıda kararlar oy okluđu ile alınır. Oyların eřitliđi halinde bařkanın kullanmıř olduđu oy esas alınır.

2.1.6. Komisyonun grevleri řunlardır:

2.1.6.1. Bakanlık genelinde uygulanacak bilgi gvenliđi ve siber olaylara mdahale ile ilgili st dzey politika ve stratejileri belirler.

2.1.6.2. Bakanlık Bilgi Gvenliđi Politikaları Ynergesi'nde yer alan konuları koordine eder.

2.1.6.3. Bilgi gvenliđi ve siber olaylara mdahale ile ilgili politika ve stratejilerin uygulanması iin eylem planları hazırlar ve yayımlar.

2.1.6.4. Eylem planlarının uygulanmasının etkinliđini ler, sonularını deđerlendirir ve iyileřtirme iin ihtiya duyulan tedbirleri alır.

2.1.6.5. Ulusal Siber Gvenlik Stratejisi ve Eylem Planı uyarınca, kritik sektrler arasında yer alan sađlık sektr ile ilgili siber gvenlik stratejilerinin, Bakanlık dıřındaki diđer paydařlar ile koordine edilmesi faaliyetlerini yrtr.

2.1.5.6. SBSGM bnyesinde grev yapan Bakanlık Sektrel SOME faaliyetleri, Komisyonun gzetiminde yrtlr.

2.2. Sađlık Bakanlıđı Sektrel SOME

2.2.1. Sađlık sektr alanındaki siber gvenlik alıřmalarının planlanması, koordinasyonu ve denetimi iin Bakanlık bnyesinde Sektrel SOME oluřturulur.

2.2.2. Sektrel SOME, sektr tecrbesine ve siber gvenlik uzmanlıđına (kayıt ynetimi, siber olay ynetimi ve bilgi gvenliđi ynetimi) sahip personelden oluřur.

2.2.3. Sektrel SOME, yıllık olarak hazırlayacađı Sektrel Siber Gvenlik Faaliyet Raporunu Bakanlık Bilgi Gvenliđi Ynetim Komisyonuna sunar.

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

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

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

2.3. Bilgi Güvenliđi Alt Komisyonları

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

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

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

2.3.4. Alt komisyonların görevleri şunlardır:

2.3.4.1. Yönerge ve Kılavuz'da belirtilen hususlar çerçevesinde, kendi kurumları bünyesinde uygulanacak BGYS'ye yönelik çalışmaları koordine eder.

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

2.3.4.3. Bilgi güvenliđi yetkili/yetkililerini belirler ve görevlendirmesini yapar.

2.3.4.4. Bakanlık tarafından yayımlanan Kurumsal SOME Kurulum ve Yönetim Rehberi'nde belirtilen esaslar çerçevesinde Kurumsal SOME'sini kurar ve işletilmesini sağlar. Kurumsal SOME Ekip Lideri görevlendirmesini yapar.

2.4. Bilgi Güvenliđi Yetkilisi

2.4.1. Bakanlık merkez, bađlı kuruluřlar ve il sađlık m¼d¼rl¼kleri b¼nyesinde bilgi güvenliđi faaliyetlerini y¼r¼tmek ve koordine etmek üzere “**bilgi güvenliđi yetkilisi**” g¼revlendirilir.

2.4.2. Hangi seviyede ve hangi alt kuruluřlarda “bilgi güvenliđi yetkilisi” g¼revlendirileceđi, ilgili alt komisyonlar tarafından karar altına alınır. Bu tespit yapılırken kurum bilgi iřleme tesisleri, personel sayısı, b¼lgesel özellikler, tespit edilen risklerin miktarı ve önem derecesi gibi ölç¼tler göz önüne alınarak, ölçek yaklaşımı çerçevesinde karar verilir ve g¼revlendirilen bilgi güvenliđi yetkilisinin sorumluluk kapsamı belirlenir.

2.4.3. Bilgi güvenliđi yetkilisi olarak; yönetim sistemleri konusunda tecrübeli, kurumda y¼r¼t¼len iř s¼reçlerine hâkim, kurum k¼lt¼r¼ne vakıf, tercihen bilgi sistemleri konusunda teknik eđitim almıř, alt komisyondan aldıđı yetkiye dayanarak bilgi güvenliđi ile ilgili faaliyetleri y¼r¼t¼rken kurumda g¼rev yapan t¼m personel ile uygun yöntemlerle iletiřim kurabilecek, gerektiđinde otorite kullanabilecek, m¼mk¼nse yönetici d¼zeyinde bir personel g¼revlendirilir.

2.4.4. Bilgi güvenliđi yetkilisinin ana iřlevi, bulunduđu kurumdaki bilgi güvenliđi faaliyetlerini alt komisyondan almıř olduđu yetkiye dayanarak SBSGM ile koordineli bir řekilde y¼r¼tmektir. Bu yön¼yle, bađlı buldukları alt komisyonun bilgi güvenliđi ile ilgili konulardaki icra organı olarak hareket ederler.

2.4.5. Bilgi güvenliđi yetkilisi olarak g¼revlendirilen personel, SBSGM tarafından ana ilkeler konusunda eđitilir ve yönlendirilir.

2.5. Kurumsal SOME Ekip Lideri ve Kurumsal SOME'ler

2.5.1. Kurumsal SOME'ler; Bakanlık bađlı kuruluřları, il sađlık m¼d¼rl¼kleri ve sekt¼rel SOME tarafından uygun gör¼len sađlık alanında faaliyet gösteren özel kuruluřların b¼nyelerinde kurulur.

2.5.2. Kurumsal SOME'ler, sekt¼rel SOME tarafından koordine edilir.

2.5.3. Kurumsal SOME'ler, siber olaya m¼dahale sonrası siber olay m¼dahale raporunu ve yıllık faaliyet raporunu Sekt¼rel SOME'ye iletir.

2.5.4. Kurumsal SOME'ler, temel sorumluluđu siber güvenlik olan bir ekip lideri koordinat¼rl¼đ¼nde faaliyet gösterir.

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

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

2.6. Üst Yönetimlerin Sorumluluđu

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

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

2.6.3. Üst yönetim, bilgi güvenliđi önlemlerinin uygun düzeye getirilmesi için gereken kararlılıđı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik yeterli kaynađı tahsis eder.

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

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

3. İNSAN KAYNAKLARI VE SON KULLANICI GÜVENLİĐİ

3.1. İŖe Alma Öncesinde Yapılacak Kontroller

3.1.1. Bilgi iŖleme tesislerine eriŖim izni verilecek tüm personel için (kamu personeli, tam zamanlı ya da yarı zamanlı olarak çalıŖan sözleşmeli personel, yüklenici firma çalıŖanları, iŖ ortaklarının çalıŖanları, destek alınan firmaların personeli vb.) iŖe alma öncesinde/alım yapılırken aŖağıdaki hususların dikkate alınması gerekir.

3.1.2. İŖe alma öncesinde yapılacak güvenlik kontrollerinin amacı, çalıŖanların kendilerinden beklenen sorumlulukları anlamalarını sađlamak ve düşünöldükleri roller için uygun olmalarını temin etmektir.

3.1.3. İŖe alınacak adaylar iŖ gereksinimleri, eriŖilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak eđitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilir (taranır).

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

3.1.5. İŖe alınacak kiŖilerin eđitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilmesi için aŖağıdaki yöntemlerden biri ya da birkaçı birlikte kullanılabilir.

3.1.5.1. KiŖi özgeçmiŖinin dođrulanması (belgelerin tamlıđı),

3.1.5.2. KiŖinin atanacađı görevle ilgili eđitim ve tecrübe açısından gerekli yeterliliđe sahip olmasının sađlanması,

3.1.5.3. Beyan edilen akademik ve iŖle ilgili niteliklerin dođrulanması (diplomaların, referans mektuplarının, bonservis belgelerinin dođru ve geçerli olduđunun teyit edilmesi),

3.1.5.4. 657 sayılı Kanun'un 48/8 maddesi geređi Yönetim Hizmetleri Genel Müdürlüđünce, devlet memurluđuna atanacak kiŖiler ile ilgili olarak 12 Nisan 2000 tarihli ve 24018 sayılı Resmi Gazetede yayımlanan "Güvenlik SoruŖturması ve ArŖiv AraŖtırması Yönetmeliđi" uyarınca "güvenlik soruŖturması ve/veya arŖiv araŖtırması" yaptırılması,

3.1.5.5. 657 sayılı Kanun'a bađlı olmayan diđer personel için bađlı oldukları yasal mevzuatta yer alan hükümler uyarınca güvenlik incelemelerinin yaptırılması,

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

3.1.6. Yüklenciciler ile yapılan sözleşmelerde, idare tarafından yüklencici personeli için tarama yapılacağı ve tarama sonuçlarının menfi olması durumunda alınacak önlemler (örneğin personelin deđiştirilmesi vb.) belirtilir.

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

3.1.8. Kuruluşun güvenlik ilkelerine uyulmaması durumunda, çalışanlar ve yüklenciciler için yürütülecek işlemler (disiplin kurallarının uygulanması, gerekiyorsa iş akitlerinin sonlandırılması, tedarik sözleşmesinin feshi vb.) önceden belirlenir ve taraflara duyurulur.

3.2. Çalışma Esnasında Uygulanacak Kontroller

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

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

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

3.2.4. İşe başlama formunda bilgi güvenliđi ile ilgili olarak personel giriş kartı çıkarılması ve bina/tesislere erişim için verilecek yetkiler, bilgi sistemlerine erişim için hesap açılması ve verilecek yetkiler (e-Posta, elektronik belge yönetim sistemi, hastane bilgi yönetim sistemi, insan kaynakları sistemi gibi), bilgi güvenliđi farkındalık eğitimi, oryantasyon eğitimi, gizlilik sözleşmesi imzalatılması gibi hususlar mutlaka yer alır. Örnek olarak kullanılabilir bir işe başlama formu KLVZ-EK-01’dir. Bu form kurumların ihtiyaçlarına bađlı olarak revize edilmek suretiyle kullanılır.

3.2.5. Üst yönetim, bilgi güvenliđi politikalarını, prosedürlerini ve kontrollerini desteklediđini her fırsatta örnek teşkil edecek şekilde gösterir. Bu suretle, diđer çalışanların bilgi güvenliđi ile ilgili motivasyonları üst düzeyde tutulur.

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

3.2.7. alıřanların kuruluşun bilgi güvenliđi politikasına uyumu izlenir.

3.2.8. Tüm alıřanlar ve yükleniciler için bilgi güvenliđi farkındalık eğitimi programları hazırlanır ve uygulanır.

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

3.2.10. Bilgi güvenliđi ihlali yapan personele uygulanan yaptırımlar (kiři kimlik bilgisi verilmeden) diđer alıřanlara duyurulur ve onlar için de örnek teşkil etmesi sağlanır.

3.3. Bilgi Güvenliđi Teknik ve Farkındalık Eğitimleri

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

3.3.2. Hazırlanan plan, kurumun bilgi güvenliđi alt komisyonu tarafından onaylanır.

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

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 eğitime yönelik hükümler eklenir.

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

3.3.6. Göreve başlama esnasında verilen eğitimlere ilave olarak her yıl tüm personele bilgi güvenliđi farkındalık eğitimi verilir. Eğitimin mümkün ise sınıf ortamında veya seminer/konferans tarzında yüz yüze verilmesi tercih edilir. Personel sayısı ve cođrafi lokasyon farklılıkları nedeni ile eğitim yüz yüze yapılamıyorsa, uzaktan eğitim teknolojilerinden de istifade edilebilir. Eğitim uzaktan yapılacak ise asgari düzeyde de olsa etkileşim sağlanması (örneğin eğitimin başlangıcında ve sonrasında ön test ve son test yapılması gibi) gerekir. Farkındalık eğitimlerinin

içeriđinin kişilere e-posta yoluyla iletilmesi veya web ortamında yayımlanan bir içeriđe kullanıcıların hiç bir etkileşim olmadan erişmelerinin sağlanması uygun yöntem olarak kabul edilmez.

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

3.3.7.1. Bilgi güvenliđi afişleri,

3.3.7.2. Bilgi güvenliđi broşür ve el kitapları, e-bültenler,

3.3.7.3. Bilgisayarların açılış ekranlarına merkezi olarak konulacak ara yüzler,

3.3.7.4. İnternet tabanlı eğitim gibi araçlar kullanılabilir.

3.3.8. Sunulan bilgi güvenliđi teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülür ve eğitim etkililiđi hususunda değerlendirme yapılır.

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

3.4. Görev Deđişikliđi veya İşten Ayrılma İçin Uygulanacak Kontroller

3.4.1. Görev deđişikliđi veya işten ayrılma ile ilgili güvenlik kontrollerinin amacı, ayrılma işlemleri esnasında yapılması gereken bilgi güvenliđi ile ilgili tedbirlerin ortaya konulması ve çalışanların görevleri sona erse dahi bilgi güvenliđi ile ilgili devam eden sorumlulukları hakkında bilgilendirilmesidir.

3.4.2. Kişi, görevi esnasında edinmiş olduđu bilgileri, görev yeri deđişmesi veya ayrılması durumunda dahi sır olarak saklamaktan ve hiçbir şekilde yetkisiz olarak ifşa etmemekten sorumludur. Sır saklama yükümlülüđü süresizdir.

3.4.3. İşten ayrılan veya görev deđişikliđi yapan personelin ayrılma işlemlerinin bilgi güvenliđi açısından eksiksiz olarak yapılmasını sağlamak için “işten ayrılma formu” hazırlanır ve uygulanır. Örnek olarak kullanılabilir form işten ayrılma formu KLVZ-EK-02’dir.

3.4.4. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bađlı bulunduđu birim yöneticisi ile insan kaynakları birimi müştereken sorumludur.

3.4.5. İřten ayrılan veya görev yeri deđiřen kiřinin eski görevi ile ilgili bilgisayar hesapları ve uzaktan eriřim için kullandıkları hesaplar kapatılır veya eriřim yetkileri yeni görev yerinin gereksinimlerine göre yeniden düzenlenir.

3.4.6. Kiřiye teslim edilmiř tüm bilgi varlıkları (bilgisayarlar, yazılı ortamda saklanan bilgi ve belgeler, bilgisayar ortamında tutulan dosyalar, lisans belgeleri, CD'ler vb.) sayım yapılarak iade alınır.

3.4.7. Ayrılan veya görev yeri deđiřen personel tarafından yürütölen faaliyetlerin aksamaması için birim sorumlusu tarafından gerekli tedbirler alınır.

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

3.4.9. Ayrılan kiřiden teslim alınan bilgisayarlar güvenli silme iřlemi yapılmadan bir bařka kullanıcıya teslim edilemez.

3.5. Kullanıcıların Bilgi Güvenliđi Sorumlulukları

3.5.1. Personel, T.C. Sađlık Bakanlıđı Bilgi Güvenliđi Politikaları Yönergesi ve Bilgi Güvenliđi Politikaları Kılavuzu'nda yer alan kořullara uygun hareket eder. Burada yer alan hükümleri kiřisel olarak ihlal etmesi halinde Bakanlıđa, görev yaptıđı kuruma ve üçüncü kiřilere vereceđi her türlü zarardan sorumludur.

3.5.2. Personel, görev yaptıđı kurum tarafından kendisine teslim edilmiř veya eriřim yetkisi verilmiř olan bilgileri, sadece görevi ile ilgili iřler için kullanır. Bu bilgileri kendi gizli bilgisi gibi korur ve bilmesi gereken yetkili kiřiler haricinde hiçbir kimse ile paylařmaz. Personel, bilgi paylařabileceđi kiřiler konusunda řüpheye düřerse, bilginin sahibi olan veya süreci yöneten birim ile irtibata geçerek veriyi kimlerle paylařabileceđini teyit eder.

3.5.3. Personel, özel olarak yetkilendirildiđi durumlar dıřında, hizmet verilen tarafların yetkilileri de dâhil olmak üzere yetkisi olmayan hiçbir kiři ile bilgi paylařımı yapmaz. Yetkisi olmadıđı halde bulunduđu görev ve makamı kullanarak kendisinden ısrarla bilgi talep eden kiřileri en yakın amirine bildirir.

3.5.4. Personel, görevi kapsamında kendisine teslim edilmiř olan bilgileri ilgili mevzuata uygun olarak korur, iřler ve aktarır. Görev yaptıđı kuruma ait bilgileri, yetkisi olmayan üçüncü kiřilerin yanında konuřmaz.

3.5.5. Personel, edindiđi bilgileri hiçbir kiři, grup, kurum veya kuruluřun menfaati için kullanamaz.

3.5.6. Bakanlıđımızda kullanılan bilgi sınıflandırması ile ilgili hususlar Kılavuz'un 4.3 (Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi) numaralı maddesinde açıklanmıştır. Bu kapsamda usulüne uygun olarak sınıflandırılmamış ve etiketlenmemiş olsa dahi; Bakanlıđa 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 diđer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduđu tüm işler gizlidir. Bunların, görevin gerektirdiđi durumlar haricinde kullanılması kesinlikle yasaktır.

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

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

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

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.

3.5.11. Personel, bilgi sistemlerinde kullanılan/yer alan programları, verileri veya diđer unsurları hukuka aykırı olarak ele geçirme, deđiştirme, silme girişiminde bulunamaz ve bunları nakledemez veya çođaltamaz.

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

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

3.5.14. Personel, görev yaptıđı kurum tarafından kendisine verilen ya da tanımlanan kullanıcı adını/parolayı hiç kimseye paylaşmaz. Parolasının gizli kalması için alınması gereken tüm tedbirleri alır. Kurumdan ayrılması halinde

kullanıcı adını/parolayı iptal ettirir. Kullandığı bilgisayar ve/veya diđer elektronik veri depolama cihazlarında oluřturduđu veri, bilgi ve belgeler dâhil tüm belgeleri, cihazları ve ofis malzemelerini eksiksiz olarak ilgisine teslim eder ve bunların hiçbir kopyasını alamaz.

3.5.15. Personel, görev yaptıđı kuruma ait sunucular üzerinden kendisine tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP adresini kullanarak gerçekteřtirdiđi her türlü etkinlikten, Kurum biliřim kaynakları kullanılarak oluřturduđu ve/veya kendisine tahsis edilen Kurum biliřim kaynađı üzerinde bulunduđu her türlü içerikten (kayıt, doküman, yazılım vb.) sorumludur.

3.5.16. Personel, 5651 sayılı Kanun geređi tutulması gereken kayıtlara ilave olarak; Bakanlık ve görev yaptıđı kurum tarafından uygun görülen diđer sistemlerin, uygulamaların, kullanıcı iřlemlerinin ve bilgi sistem ađındaki veri akıřının iz kayıtlarının hukuki süreçlere kaynak teřkil etmesi ve sistemlerin güvenli bir řekilde iřletilmesi amacıyla toplanabileceđini kabul eder.

3.5.17. Kiřinin kendi kusuru nedeniyle parolasının ifřa olması durumunda, bařkası tarafından yapılmıř olsa dahi personele teslim edilen kullanıcı adı ve parolalar ile yapılan iř ve iřlemlerden ilgili personel řahsen sorumludur.

3.6. Elektronik Posta Güvenliđi

3.6.1. Bakanlıđımızda görev yapan personel tarafından görevleri geređi yürütölen kurumsal iř ve iřlemlerde, *@saglik.gov.tr uzantılı kurumsal veya tüzel e-Posta hesabı kullanılır. Kurumsal iř ve iřlemler, kiřilerin özel iřleri için (Gmail, Hotmail gibi) internet hizmet sađlayıcılarından alınan hesaplar üzerinden yürütölmez.

3.6.2. KVKK tarafından 6698 sayılı Kanun'da yer alan bazı hususların açıklanması amacıyla alınan 2018/10 sayılı karar geređi, e-Posta ile aktarılacak verilerin özel nitelikli kiřisel veri statüsünde olması durumunda aktarma iřlemlerinin kurumsal e-Posta veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak yapılması yasal zorunluluktur.

3.6.3. Bakanlıđımızda görev yapan tüm kamu personeline, talep etmeleri halinde kurumsal e-Posta hesabı açılır.

3.6.4. Çeřitli sözleşmeler kapsamında Bakanlıđımızda görev yapan ve yaptıkları iř geređi e-Posta hesabı olması gereken personele, sıralı yöneticileri tarafından onay verilmesi halinde kurumsal e-Posta hesabı açılır.

3.6.5. Kurumsal e-Posta adresi isimlendirme politikası, istisnai durumlar dıřında “ad.soyad@saglik.gov.tr” řekindedir. Yeni bir kullanıcı oluřturulurken o kullanıcının adı ve soyadı ile daha önce bir hesap açılmıř ise “ad.soyad” kombinasyonunun ardına her seferinde bir artacak řekilde sıradaki sayı eklenir. (yılmaz.demir2, yılmaz.demir3 gibi).

3.6.6. Bakanlıđımız merkez ve tařra teřkilatında yer alan birimler için ihtiyaç olması halinde, tüzel e-Posta hesapları açılır. Tüzel e-Posta hesapları, ilgili birimin adı veya yürüttüđü iřlev ile alakalı olarak belirlenir. (bilgiguvenligi@saglik.gov.tr, some@saglik.gov.tr gibi).

3.6.7. Kurumsal ve tüzel e-Posta hesabı açılması için bařvuru usulleri ve ilgililerince yapılacak iřlemler Kılavuz’un 6.5 (Merkezi Aktif Dizin ve E-Posta Sistemine Eriřim) maddesinde belirtilmiřtir.

3.6.8. Kurumsal ve tüzel e-Posta kullanım kayıtları Bakanlıkça tutulur. Bu kayıtlar 6698 sayılı Kanun’un 28’inci maddesinin birinci ve ikinci fıkralarında yer alan řartlar kapsamında; yalnızca yetkili kiři, kurum ve kuruluřlar tarafından, yine aynı Kanunun 4’üncü maddesinde yer alan genel ilkelere uymak kaydıyla incelenebilir.

3.6.9. Bakanlık tarafından uygulanan e-Posta yönetimi ve güvenliđi ile ilgili politikalar řu řekildedir:

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

3.6.9.2. e-Posta hesabı ilk kez açıldıđında kullanıcılara “Bakanlık e-Posta Kullanım Politikası ve e-Posta Kullanımında Dikkat Edilmesi Gereken Hususlar/Kullanıcı Sorumluluklarını Bildiren Bilgilendirme Yazısı” e-Posta ekinde gönderilir.

3.6.9.3. Kullanıcı parolalarının Kılavuz’un 6.3 (Parola Güvenliđi) maddesinde belirtilen politikalar ile uyumlu olup olmadıđı denetlenir.

3.6.9.4. Bakanlık e-Posta sistemi tarafından oluřturulan ve sisteme ilk kez giriřte kullanılan parolanın ilk kullanımdan sonra deđiřtirilmesi sađlanır.

3.6.9.5. Kullanıcıların son kullandıđı üç parolayı kullanması engellenir.

3.6.9.6. Kullanıcılar, altı ayda bir parolalarını deđiřtirmeye zorlanır. Parola deđiřtirme süresine beř (5) gün kala uyarı iletisi gönderilir.

3.6.9.7. Kullanıcılara e-Posta hesabının parolasını deđiřtirmek için kısa mesaj

servisi (SMS) ile onay kodu gönderilir veya alternatif e-Posta aracılığı ile parola deđişimi sađlanır. SMS onayı kullanıcıyı yeni oluşturacağı parola ekranına yönlendirir. Kullanıcıların daha önce sisteme kaydettiđi alternatif e-Posta adresi üzerinden parola yenilenmesi tercih edilmişse, sistem tarafından parola deđişikliđi linki gönderilir.

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

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

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

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

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

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

3.6.9.14. Gönderilen e-Posta boyutu 25 MB’yi geçemez.

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

3.6.9.16. e-Posta iletimlerinde “exe” gibi çalıştırılabilir dosyaların gönderilmesi engellenir.

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

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

Yasal Uyarı: Bu e-Postanın içerdiği bilgiler (ekleri de dâhil olmak üzere) gizlidir. T.C. Sağlık Bakanlığı onayı olmadan içeriđi kopyalanamaz, üçüncü kişilere açıklanamaz veya iletilemez. Bu mesajın gönderilmek istendiđi 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 doğruluđu veya eksiksiz olduđu konusunda bir garanti vermemektedir. Bu nedenle, bilgilerin ne şekilde olursa olsun içeriđinden, iletilmesinden, alınmasından ve saklanmasından T.C. Sağlık Bakanlığı sorumlu değildir. Bu mesajın içeriđi 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.

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

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

3.6.10.2. Kullanıcılar, parolalarını Kılavuz'un 6.3 (Parola Güvenliđi) maddesinde belirtilen parola politikaları uyarınca oluşturur ve kullanır.

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

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 kullanıcıasına aittir.

3.6.10.5. Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-Posta hesapları

kullanılmaz. Aksine durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.

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

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

3.6.10.8. İnternet haber gruplarına üyelik için kurumun sağladığı e-Posta hesapları kullanılmaz. Ancak iş geređi üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak kurumun sağladığı resmi e-Posta adresi kullanılabilir.

3.6.10.9. Kullanıcılar, e-Posta hesaplarında hukuki açıdan suç teşkil edecek materyal ve belgeleri bulduramaz. Kullanıcılar, kendi kullanıcı hesaplarında barındırdıkları içeriklerden ve gerçekleştirilen tüm elektronik posta işlemlerinden sorumludur.

3.6.10.10. Kurumsal e-Posta vasıtasıyla gizlilik dereceli veri aktarımı için Kılavuz'un 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.

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

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

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

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

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

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

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

3.7. Sosyal Mühendislik ve Sosyal Medya Güvenliđi

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

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.

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

3.7.3.1. Taşıdığımız ve işlediğimiz verilerin öneminin bilincinde olunuz.

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

3.7.3.3. Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.

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

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

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

3.7.3.7. Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.

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

3.7.3.9. Çok acele bilgi istendiđi zaman istenen bilginin niteliđine göre teyit mekanizması kullanınız.

3.7.3.10. Bilgisayarınızı yabancı bir kiřiye kullandırmayınız. Bu kiřiler tarafından bilgisayarınıza takılacak olan USB depolama aygıtları ya da harici disklerden bilgisayarınıza zararlı yazılım bulařtırabilir.

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

3.7.4. Hastanelerde sosyal mühendislik alanında alınacak bazı önlemler řu řekilde sıralanabilir:

3.7.4.1. Kiřisel sađlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kiřisel veri kategorisinde olduđu ve 6698 sayılı Kanun ile özel koruma uygulanması gerektiđi her zaman dikkate alınır.

3.7.4.2. Telefon ile hasta hakkında bilgi almak isteyen kiřilere, hastanın kiřisel bilgileri ile ilgili açıklama yapılmaz.

3.7.4.3. Hasta dosyaları, hastanın tedavi sürecine dâhil olan sađlık profesyonelleri/ çalışanları dışında kimseyle paylaşılmaz. Kolay ulařılır yerlere konulmaz.

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

3.7.5. Kiřisel Sosyal Medya Güvenliđi

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

3.7.5.2. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.

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

3.7.5.4. Eğitimlerde sosyal medya güvenliđi ile ilgili hususlara yer verilir.

4. VARLIK YÖNETİMİ

4.1. BGYS Bakış Açısıyla Varlıklar

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

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

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 işlendiđi ortamlar “varlık” olarak değerlendirilir.

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

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

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

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

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

4.1.4.5. İnsan Kaynakları: Çalışanlar

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

4.4.1.7. Mekânlar: Yönetim ve hizmet odaları, sunucu odaları, arşiv odaları, tıbbi kayıt saklama odaları vb.

4.2. Varlık Envanterinin Tespiti

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

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

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

4.2.4. Varlık envanteri, sadece fiziksel varlıklar veya bilgi sistem teçhizatından oluşmaz. Varlıklar belirlenirken, başta hassas bilgilerin işlendiđi kritik iş süreçleri olmak üzere, bu süreçlere konu olan tüm kurumsal bilgi varlıklarının ortaya çıkarılması gerekir. (Örneđin 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.)

4.2.5. Envanterde yer alan her bir varlık için “varlık sahibi” belirlenir. Varlık sahibi gerçek bir kişi olabileceđi gibi, bir birim ya da kurum da olabilir.

4.2.6. Varlık sahiplerince Kılavuz'un 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 deđeri nedeniyle daha sıkı güvenlik tedbirleri uygulanır.

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

4.2.8. Varlık sahipleri;

4.2.8.1. Varlıklarını envantere dođru olarak kaydettirmekten,

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

4.2.8.3. Varlıklara eriřecek kiři veya süreçleri için eriřim izinlerini planlamaktan, bunlarla ilgili kararları vermekten,

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

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

4.3. Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi

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.

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

4.3.2.1. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda kiři güvenliđi veya milli güvenlik açısından saygınlık ve çıkarlarımıza **hayati derecede** zararlar verebilecek, yabancı bir devlet için faydalar temin edebilecek ve güvenlik bakımından **olađanüstü** sonuçlar doğurabilecek bilgiler “**çok gizli**”;

4.3.2.2. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kiři güvenliđi veya milli güvenlik açısından, saygınlık ve çıkarlarımıza **büyük zarar** verebilecek, yabancı bir devlet için faydalar temin edebilecek özellikler taşıyan bilgiler “**gizli**”;

4.3.2.3. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kiři güvenliđi veya milli güvenlik açısından saygınlık ve menfaatlere zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek bilgiler “**özel**”;

4.3.2.4. İerdiği bilgi itibarıyla OK 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.

4.3.2.5. ok 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, elik masa veya diđer tipte elik dolaplar içinde muhafaza edilir.

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

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

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.

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 Yönergesi’nde belirtilen kurallar uygulanır.

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 Yönetmelik’te belirtilen kurallar uygulanır.

4.3.2.11. Resmi yazı şeklinde olmayan ancak içerdikleri bilgilerin hassasiyeti açısından sınıflandırılmaya ihtiyaç duyulan diđer bilgi varlıklarının sınıflandırılması için de yukarıda belirtilen gizlilik dereceleri kullanılır. Bu varlıkların korunması ve erişim haklarının düzenlenmesi için alınacak tedbirler, yapılacak olan risk analiz neticesine göre belirlenir ve bu Kılavuz’un 6.1 (Erişim Kontrol Politikası) maddesi geređi hazırlanacak kurum erişim kontrol politika/prosedürü içerisinde ayrıntılı olarak açıklanır.

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

- 4.3.3.1.** Bilgiye eriřimin kayıt ve kontrol altına alınması,
- 4.3.3.2.** İzinsiz kopyalamanın önlenmesi,
- 4.3.3.3.** Elektronik veya basılı olarak depolama süresi ve koşullarının tanımlanması,
- 4.3.3.4.** İletim hassasiyetinin belirlenmesi,
- 4.3.3.5.** Gerektiğinde kanıt olarak kullanılmak üzere bütünlüğünün sağlanması,
- 4.3.3.6.** İhtiyacın sonlanması durumunda imha edilmesi süreçlerinin tanımlanması için uygun Őekil ve yöntemlerle etiketlenmesi gerekir.
- 4.3.3.7.** Tasnif dıŐı bilgiler için etiketleme yapılmasına gerek yoktur.
- 4.3.4.** Resmi yazı Őeklinde olan belgelerin etiketlenmesi için yürürlükteki Resmi YazıŐmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te belirtilen esaslar dođrultusunda hareket edilir.
- 4.3.5.** Bu kapsamda;
- 4.3.5.1.** Her sayfaya gizlilik dereceleri yazılır ve damgalanır.
- 4.3.5.2.** Ekler de yazı ile aynı gizlilik derecesini taşıır.
- 4.3.5.3.** Gizlilik dereceli bütün yazılar, zaman zaman gizlilik derecelerinin yeniden deđerlendirilmesi bakımından gözden geçirilir.
- 4.3.5.4.** Gizlilik derecelerinin indirilip yükseltilmesi yazıyı yazan makamlarca yapıldığı gibi alan makamlarca da bu hususta teklif yapılabilir.
- 4.3.5.5.** Gizlilik dereceli ve bilhassa kontrollü yazılarda kullanılan müsveddeler, karbon kâğıtları ve yanlış yazılar muhakkak imha edilir.
- 4.3.5.6.** Gizlilik dereceli evrak, kâğıt sepetine bütün olarak atılmaz. Kâğıt kırpa makinaları kullanılmak suretiyle imha edilir.
- 4.3.5.7.** Gizli ve özel gizlilik derecesini haiz evrak ve belgeler izinsiz olarak çođaltılamaz.
- 4.3.5.8.** Gizlilik derecesi taşıyan bilgileri veya belgeleri görevi dıŐında elde eden veya belgeleri görenler, bu bilgiyi ve belge içeriğini resmi görevlerinin gerektirdiđi haller dıŐında açıklayamaz, çođaltamaz 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.

4.3.6. İlgili mevzuat tarafından verilen yetkiye dayanılarak Bakanlıđımıza bađlı sađlık hizmet sunucuları tarafından iřlenen kiřisel sađlık verileri; verinin ait olduđu kiři, ne maksatla istendiđi vb. özel durumlar da dikkate alınmak suretiyle yukarıda tanımlanan gizlilik derecelerinden en az “ÖZEL” gizlilik derecesi ile etiketlenir.

4.3.7. Sađlık verilerinin korunmasına yönelik risk analizi yapılırken, kiřisel verilerin hassasiyeti ve kanuna aykırı bir řekilde ifřası halinde uygulanacak ađır idari ve cezai yaptırımlar nedeniyle en üst düzeyde özen gösterilir.

4.4. Tařınabilir Ortam Yönetimi

4.4.1. Kaybolma, kolayca çođaltma vb. nedenlerden dolayı özellikle elektronik medya (CD/DVD, USB giriřli hafif tařınabilir bellekler, tařınabilir diskler, hafıza kartları, teyp kartuřları vb.) ve basılı evraklar (yazılar, dosya klasörleri, etüdüler, çizimler, krokiler, proje evrakları vb.) olmak üzere tařınabilir ortamlarda saklanan her türlü bilginin korunması ve yetkisiz kiřilerin eline geçmemesi için özel önlemler alınır.

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

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

4.4.2.2. Kuruma ait medyalar varlık envanteri içinde listelenir ve kimler tarafından kullanıldıđı kayıt altına alınır. Görev devir teslimlerinde veya iřten ayrılıřlarda, kiřilere teslim edilmiř olan medyaların iade edilmesi istenir veya ne řekilde sarf edildiđi bilgisi sorgulanır.

4.4.2.3. Özellikle eski SBYS verileri ve SBYS yedeklerinin saklandıđı medya ortamlarının mutlak surette envanter listesi oluřturulur, 6 (altı) aydan az olmayacak řekilde belirlenecek sürelerde sayım iřlemleri yapılır ve sayım sonuçları kayıt altına alınır.

4.4.2.4. ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL veriler, tařınabilir ortamda saklanamaz. Özellikle bu tür ortamlarda saklama zorunluluđu var ise bu Kılavuz’un 7.2.5 (Sabit Ortamdaki Verilerin řifrelenmesi) maddesinde belirtilen řekilde řifreli olarak saklanır.

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.

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.

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

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

4.4.3. Taşınabilir ortamda yer alan verilerin bütünlüğünün (deđişmediđinin) garanti edilmesi özel önem arz ediyor ise Kılavuz'un 7.2.1.3 (Özetleme İşlemleri) maddesinde belirtilen standartta uygun bir özetleme (hash) algoritması kullanılmak suretiyle verilerin bir özeti (parmak izi) alınır. Alınan özet, kullanılan algoritma ve anahtar ile birlikte bir tutanak ile kayıt altına alınır ve taşınabilir ortam ile birlikte muhafaza edilir. İhtiyaç duyulan durumlarda verinin tekrar özeti alınarak herhangi bir deđişiklik olup olmadığı kontrol edilir.

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.

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

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

4.4.5.2. Yönetim tarafından yetkili kurye listeleri oluşturulur.

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

4.4.5.4. Ortamın içeriđini tanımlayan kayıtlar ile birlikte kaç kez transfer edildiđi, transfer sorumluları ve alıcı tarafından alındığının kayıtları tutulur.

4.5. Ortamın Yok Edilmesi¹

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

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.

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

4.5.4. Sökülen sabit disklerden daha önce ilgili teknik birimler tarafından “onarımı mümkün değil” şeklinde rapor verilenler ile sağlam olmakla birlikte “yeniden kullanımı düşünülmemeyen” cihazlar aşağıda belirtilen yöntemlerden biri ya da birkaçı birlikte kullanılmak suretiyle imha edilir:

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

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

¹ Kılavuz’un ortamın yok edilmesi ile ilgili bölümünde yer alan yöntemler, KVKK tarafından hazırlanan “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi” dikkate alınarak hazırlanmıştır.

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

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

4.5.6. Bilgisayarların sabit diskleri dışında hassas veri bulundurma ihtimali olan diđer depolama ortamları, ortam türüne bađlı olarak ařađıda yer alan yöntemlerden biri kullanılarak yok edilir.

4.5.6.1. Ağ cihazları (anahtarlama cihazı, yönlendirici vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çođu zaman silme komutuna sahiptir ama yok etme özelliđi bulunmamaktadır. Kılavuz’un 4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

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 Kılavuz'un 4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

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.

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.

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. Kılavuz'un 4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

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.

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 Kılavuz'un 4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

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. Kılavuz'un 4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

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

4.5.8. Orijinal kâğıt formattan tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre Kılavuz'un 4.5.4 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

4.5.9. Yeniden kullanılması planlanan disklerle, ilerinde yer alan bilgilerin yetkisiz kiřilerin eline gemesini engellemek maksadıyla ‘güvenli sil’ (üzerine yazma) iřlemi yapılır.

4.5.10. Güvenli silme iřlemi, manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1’lerden oluřan rastgele veriler yazarak eski verinin kurtarılmasının önüne geilmesi iřlemidir. Bu iř için uygun bir yazılım (DBAN, Kill Disk, Eraser, Disk Wipe, HDS shredder gibi) veya donanım kullanılır.

4.5.11. Bulut ortamındaki sistemlerde yer alan hassas verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle řifrenmesi ve kiřisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözüümü için ayrı ayrı řifreleme anahtarları kullanılması gerekir. Bulut biliřim hizmet iliřkisi sona erdiđinde; kiřisel verileri kullanılamaz hale getirmek için gerekli řifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

4.5.12. Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi iřlemleri ise ařađıdaki řekilde gerekleřtirilir:

4.5.12.1. İlgili cihazların bakım, onarım iřlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan verilerin güvenli silme iřlemine tabi tutulması,

4.5.12.2. Güvenli silme iřleminin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diđer paraların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

4.5.12.3. Dıřarıdan bakım, onarım gibi amalarla gelen personelin, hassas verileri kopyalayarak kurum dıřına ıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

5. RISK YÖNETİMİ

5.1. Genel

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

5.1.2. Kılavuz'un bu bölümünde anlatılan risk deđerlendirme yöntemi ISO/IEC 27005 ve TS ISO 31000 standartları referans alınarak hazırlanmış olup kurumsal bilgi varlıklarının güvenliğine ilişkin bilgi güvenliği risk yaklaşımını özetlemektedir. Anlatılan yöntem örnek niteliğinde olup kurumun kapsam ve hedeflerine bađlı olarak farklı risk yönetimi yaklaşımları da uygulanabilir.

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

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

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

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

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

5.1.8. Risk analizlerinde bilhassa aşağıdaki hususlara yönelik riskler deđerlendirilir:

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

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

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

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

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

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

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

5.1.9. Risk yönetimi; riskin belirlenmesi, riskin analiz edilmesi ve kurumsal risk kıstaslarını sağlamak için risk iyileştirme yoluyla riskin değıştirilip değıştirilemeyeceğinin değerlendirilmesi aşamalarını içerir.

5.2. Sorumluluklar

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

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

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

5.3. Risk Yönetimi

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

5.3.1. Varlıkların Tanımlanması

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

5.3.1.2. BGYS bakış açısıyla varlıkların tanımlanması, Kılavuz'un 4 (Varlık Yönetimi) numaralı bölümünde ayrıntılı olarak açıklanmıştır.

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

5.3.2. Varlıkların Deđerinin Belirlenmesi

5.3.2.1. Varlığın kullanılmakta olduđu iş süreci, etkilediđi süreçler, mali kıymeti gibi unsurlar dikkate alınarak varlık sahibi tarafından varlığa bir deđer atanır. Varlık deđerinin belirlenmesi risk yönetim sürecinin en önemli parçasıdır. Sonraki aşamalar bu aşama üzerine kurulur.

5.3.2.2. Üst Yönetim varlık deđerinin belirlenmesi için etkin ve kolay kullanılabilir 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 deđerlerinin en yüksek olanının alınmasıdır.

5.3.2.3. Varlık deđerini olarak KLVZ-EK-06 Risk Hesaplama Faktörlerinde yer alan Varlık Deđerini Tablosunda belirtilen ölçütler kullanılmak suretiyle bir deđer atanır.

5.3.3. Tehdit ve Zafiyetlerin Gerçekleşme Olasılıklarının Belirlenmesi

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

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

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 deđerini belirlenir. Olasılık deđerini, bilgi güvenliđi olayının gerçekleşme olasılıđını ifade eder.

5.3.3.4. Bir tehdit birden fazla etkiye neden olabilir. Yani farklı bilgi güvenliđi olaylarına neden olabilir. Bu nedenle her bir tehdit senaryosunun ve etkisinin olasılıđını ayrı ayrı deđerlendirmek ve risk analiz tablosuna ayrıca işlemek gerekir.

5.3.3.5. Tehdit ve zafiyetlerin gerekleŖme olasılıđı iin KLVZ-EK-06 Risk Hesaplama Faktörlerinde yer alan Riskin GerekleŖme Olasılıđı tablosunda belirtilen ölçütler kullanılmak suretiyle bir deđer atanır.

5.3.4. İŖe Etki Deđerlerinin Belirlenmesi

5.3.4.1. Varlık sahibi tarafından; riskin gerekleŖmesi durumunda, varlıđın kullanıldıđı ve bađımlı olduđu iŖ süreçlerine yapacađı etkiler gizlilik, bütünlük ve erişilebilirlik aısından incelenir ve her birine ayrı bir puan verilir.

5.3.4.2. İŖe etki deđerinin belirlenmesinde gizlilik, bütünlük ve erişilebilirlik deđerlerinin ortalamasının alınması ya da en yüksek deđerin kullanılması gibi farklı yöntemler kullanılabilir.

5.3.4.3. İŖe etki deđeri olarak KLVZ-EK-06 Risk Hesaplama Faktörlerinde yer alan Gizlilik Etki Deđer, Bütünlük Etki Deđer ve EriŖilebilirlik Etki Deđer Tablolarda belirtilen ölçütler kullanılmak suretiyle bir deđer atanır.

5.3.4.4. Risk puanı hesaplanırken gizlilik, bütünlük ve erişilebilirlik iin belirlenen etki deđerlerinden en yüksek deđer dikkate alınır. (Örneđin seilen bir varlık iin gizlilik etki deđer 3, bütünlük etki deđer 4, erişilebilirlik etki deđer 5 olarak belirlenmiŖse, iŖe etki deđer 5 olarak alınır)

5.3.5. Risk Puanı Hesaplama

5.3.5.1. Risk deđerlendirme ve iŖleme iin risk seviyesinin hesaplanması gerekir.

5.3.5.2. Risk puanı hesaplamak iin birok yöntem kullanılabilir. Örnek bir risk deđer hesaplama yöntemi aŖađıdaki gibidir:

$$\text{Risk Deđer} = \text{Varlık Mutlak Deđer} (\text{Varlık Deđer} \times \text{İŖe Etki Deđer}) \times \text{Olasılık Deđer}$$

5.3.6. Risk Önceliklendirme

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

5.3.6.2. Risklerin anlamlandırılması ve önceliklendirilmesi aŖađıdaki tabloya göre yapılır.

Risk Deđeri	Risk Önceliđi
1-25	Düşük
26-50	Orta
51-75	Yüksek
76-100	Çok Yüksek

5.3.7. Risk Kararı

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

5.3.7.2. “Kabul edilebilir” risk seviyesi, yasal yükümlülöklere ve kurumsal politikalara uygun, kurumsal itibar zedelenmesi veya hizmeti yerine getirmeye engel olabilecek herhangi bir durum oluřturmayacak risk seviyesini ifade eder.

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

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 řu şekildedir:

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

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

5.3.7.4.3. Risk Transfer: Riski azaltmak için yapılacak eylemler bu işi daha profesyonel şekilde yönetebilecek bir dış paydařa sözleşme ile transfer edilebilir.

Riski transfer etmek, riskin gerekleşmesi durumunda oluşacak etkidenden doğacak tüm zararı transfer etmek anlamına gelmediđi için transfer edilen risk sürekli izlenmeli ve kontroller denetlenmelidir.

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

5.3.8. Risk İşleme

5.3.8.1. Risk İyileştirme Planlarının Hazırlanması

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

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

5.3.8.2. Risk Analizi İletişimi ve İstişaresi

5.3.8.2.1. Bilgi güvenliđi 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 gerekleştirir.

5.3.8.3. Bilgi Güvenliđi Risklerinin İzlenmesi ve Gözden Geçirilmesi

5.3.8.3.1. Riskler statik deđildir. Tehditler, zayıf noktalar, olasılıklar veya sonuçlar varlık yaşam döngüsü boyunca deđişiklik gösterir. Riskler ve faktörlerini (varlıkların deđeri, etkileri, tehditleri, zayıflıkları, risklerin ortaya çıkma ihtimalleri), iç ve dış bağlam deđişikliklerini izlemek, olası deđişiklikleri erken belirlemek için riskler sürekli izlenmeli ve gözden geçirilmelidir.

5.3.9. Raporlama ve Kayıtlar

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

5.3.9.2. Üst Yönetim tarafından risk deđerlendirme 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.

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

6. ERİŐİM KONTROLÜ

6.1. EriŐim Kontrol Politikası

6.1.1. EriŐim kontrolünün amacı, bilgi ve bilgi iŐleme tesislerine yapılacak olan eriŐimlerin kısıtlanması, sadece yetki verilen kiŐilerin kontrollü ve kayıt altına alınarak bilgiye eriŐmesine imkân verecek bir sistemin tesis edilmesidir.

6.1.2. EriŐim kontrolü ile ilgili hususları açıklamak üzere, kurumun BGYS politikası ile uyumlu olacak Őekilde “EriŐim Kontrol Politikası” dokümanı hazırlanır. 6698 sayılı Kanun kapsamında çıkarılan ikincil mevzuat uyarınca, kiŐisel verilere eriŐim için yapılan düzenlemeler söz konusu doküman içinde ayrı bir baŐlık/bölüm olarak ayrıntılı bir Őekilde açıklanır.

6.1.3. EriŐim kontrol politikası, kurumun bilgi güvenliđi yetkilisi tarafından hazırlanır ve bilgi güvenliđi alt komisyonu tarafından onaylanarak yayımlanır.

6.1.4. EriŐim kontrol politikasının ayrılmaz bir parçası olarak “eriŐim yetki ve kontrol matrisi” oluşturulur. EriŐim yetki ve kontrol matrisinde kimin, hangi bilgiye, hangi yetkilerle eriŐeceđi ve eriŐimin kontrolü için kullanılacak yöntemler yer alır.

6.1.5. EriŐim yetki ve kontrol matrisi gerekiyorsa “daha genel hususlardan daha özele olacak Őekilde” birden fazla kademe Őeklinde de hazırlanabilir.

6.1.6. EriŐim kontrol politikası/eriŐim yetki ve kontrol matrisleri hazırlanırken aŐađıda sıralanan prensipler dikkate alınır:

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

6.1.6.2. Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan eriŐim kontrol politikalarının sıkılaŐtırılması (zorlaŐtırılması) gerekir.

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

6.1.6.4. Bilgiye eriŐim talepleri ve ilgili makamlarca bu taleplere yapılan iŐlemlerin takip edilebilirliđini sađlamak üzere yazılı kurallar oluşturulur.

6.1.6.5. Eriřim izinleri ile ilgili kayıtlar, varsa ilgili mevzuatta belirtilen sürelerce, yoksa varlıđın sahibi tarafından belirlenecek süre boyunca saklanır.

6.1.6.6. Eriřim izinleri verilirken, “görevlerin ayrılıđı” ve “bilmesi gereken” prensiplerine göre hareket edilir.

6.1.6.7. “Görevlerin ayrılıđı” prensibi uyarınca; kritik iř süreçlerinin gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye eriřim için aşamalı yetkilendirme yapılarak bir kiřinin kendi başına tüm bilgi varlıklarına eriřimi engellenir. Teknik nedenlerle görev ayırımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır. Gerekiyorsa idari kontrol mekanizmaları oluşturulur.

6.1.6.8. “Bilmesi gereken” prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına eriřirken, kendilerine atanmış görevlerini gerçekleřtirmelerine yetecek kadar yetki verilir.

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

6.1.6.10. Bilgi varlıklarına yapılan eriřimler için iz kayıtları oluşturulur. Eriřim ile ilgili hangi kullanıcı hareketlerinin izleneceđi hususu varlık sahipleri tarafından belirlenir.

6.1.6.11. Sađlık Biliřim Ađı (SBA) dıřındaki ađlar güvensiz ađ olarak kabul edilir. Yetkisiz eriřimler de dâhil olmak üzere iç ađı dıř tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.

6.1.6.12. Kullanıcı ve sunucuların bulunduđu ađlar, güvenlik duvarları ve/veya ađ cihazları eriřim kontrol listeleri vasıtasıyla ayrılır. VTYS sunucularının bulunduđu ađ kesimlerine, normal kullanıcı eriřimleri engellenir.

6.1.6.13. Bilgi varlıklarına fiziksel olarak yapılacak eriřimler için Kılavuz’un 8. (Fiziksel ve Çevresel Güvenlik) maddesinde belirtilen önlemler alınır.

6.1.6.14. Özel nitelikli kiřisel verilere (kiřisel sađlık verileri) eriřim için KVKK’nın 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.

6.2. Kullanıcı Eriřimlerinin Yönetimi

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

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

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

6.2.3.1. Hizmet veya sisteme erişim için nasıl müracaat edileceđi,

6.2.3.2. Müracaat esnasında hangi bilgilerin isteneceđi,

6.2.3.3. Kullanıcıların yetkilendirilmesinde kullanılan roller ve haklarının neler olduđu,

6.2.3.4. Yetki deđişiklik taleplerinin hangi koşullarda ve nasıl yapılacađı,

6.2.3.5. Ayrıcalıklı erişim taleplerinin nasıl deđerlendirileceđi,

6.2.3.6. Kullanıcı erişimlerinin izlenmesi için alınmış olan tedbirler,

6.2.3.7. Kullanıcı hesaplarının kapatılması/silinmesi için yapılacak işlemler.

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

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

6.2.6. Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların deđiřtirilmesi veya görev yeri deđişiklikleri sonrasında gözden geçirilir.

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

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

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

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

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

6.2.12. Programların kaynak kodları ve ilgili öğelere (tasarımlar, özellikler, doğrulama planları ve geçirme planları gibi) erişim (yetkisiz işlevsellik girişini ve istenmeyen deđişiklikleri önlemenin yanı sıra deđerli fikri mülkiyet haklarının gizliliđini sağlamak için) sıkı bir şekilde kontrol edilir.

6.3. Parola Güvenliđi

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

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

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

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

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

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

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

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

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

6.3.2.8. Sözlükte bulunabilen kelimelerin kullanılması engellenir.

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

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

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

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

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

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

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

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

6.3.9. İnternet tarayıcısı ve diđer parola hatırlatma özelliđi olan uygulamadaki “parola hatırlama” seçeneđi kullanılması bilgi güvenliđi açısından sakıncalı olup kullanıcılara farkındalık eđitimlerinde bu hususun önemi iletilir.

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

6.4. Sağlık Bakanlığı Uygulamalarına OGN

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

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

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

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

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

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

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

6.4.3.5. e-Devlet ile giriş işlemi için; e-Devlet giriş seçeneđi seçilerek gelen ekrandan “e-Devlet Girişini için Tıklayınız” butonuna tıklanarak kullanıcı e-Devlet

giriş ekranına yönlendirilir. e-Devlet üzerinden başarılı giriş yapıldığı takdirde sistem kullanıcıya OGN’de tanımlı Bakanlık uygulamalarını listeler. Kullanıcı tercih ettiği uygulamayı seçerek işlemlerine devam eder.

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

6.5. Merkezi Aktif Dizin ve E-Posta Sistemine Erişim

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.5.6. Kullanıcı hesaplarının ve posta kutularının yönetimi

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

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

6.6. Veri Merkezi ve Sunucu Barındırma Hizmetlerine Eriřim

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

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

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

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

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

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

6.7. Merkezi Veri Tabanı Yönetim Sistemine Erişim

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.8. Elektronik Belge Yönetim Sistemine Erişim

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

6.8.2. Evrakın EBYS üzerinden hazırlanması ve yayımlanması ile ilgili usul ve esaslar, EBYS Yönergesi'nde açıklanmıştır. Yönerge'ye SBSGM web sayfasında bulunan "Mevzuat" bađlantısından erişim sağlanmaktadır.

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

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

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

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

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

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

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

6.8.7. Kullanıcı tanımlama işlemleri için “kullanıcının kimlik numarası, adı ve soyadı, *@sađlık.gov.tr uzantılı e-Posta adresi, birimi, unvanı” bilgilerinin bildirilmiş olması gerekir.

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

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

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

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

6.9. Kimlik Paylaşım Sistemine Erişim

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

6.9.2. KPS’nin kuruluş amacı, çalışma ve yetkilendirme esasları, gizlilik ve kullanıcı sorumlulukları “KPS Usul ve Esasları Hakkında Yönerge”de açıklanmıştır. Yönerge’ye BSGM web sayfasında bulunan “Mevzuat” bağlantısından erişim sağlanmaktadır.

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

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

6.9.5. KPS mimarisi geređince, her kuruma (il sađlık m¼d¼rl¼kleri, hastaneler, aile hekimlikleri vb.) bir kullanıcı tanımlanmakta ve kimlik dođrulmaya ihtiyaç duyan kiřiler, kuruma tanımlanan kullanıcı ¼zerinden sorgulama yapmaktadır.

6.9.6. Kurumlara tanımlanan kullanıcının, belli bir IP adresi ¼zerinden sorgulama yapması gerekmektedir.

6.9.7. KPS’de web servis kullanıcısı oluřturma, yetkilendirme, silme gibi iřlemler tařra teřkilatı iin il sađlık m¼d¼rl¼klerinde bulunan KPS il y¼neticileri tarafından, Bakanlık merkez teřkilatı iin KPS Birimi tarafından yapılmaktadır.

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

6.9.9. KPS kullanacak kurum veya kiřilerin, yetki ve sorumlulukları řu řekildedir:

6.9.9.1. Alınan bilgiler, tanımlanmıř hizmetlerin yerine getirilmesi amacı dıřında bařka hibir amala kullanılmaz ve ilgilisi dıřında kimse ile paylařılmaz.

6.9.9.2. Bilgilerin hukuka aykırı olarak iřlenmesini ve eriřilmesini ¼nlemek, bilgilerin muhafazasını sađlamak amacıyla uygun guvenlik tedbirleri alınır.

6.9.9.3. KPS web servisleri sadece dođrulama amalı kullanılır. Bu servislerden elde edilen bilgiler ¼nc¼ řahıřlar ile paylařılmaz.

6.9.9.4. Yapılan iř ve iřlemlerde, 6698 sayılı Kanun dikkate alınır.

6.9.10. KPS ile ilgili her t¼rl¼ iletiřim kps@saglik.gov.tr adresine e-Posta atılarak veya <https://yazilimdestek.saglik.gov.tr/> adresi ¼zerinden talep aılarak sađlanır.

6.10. e-Nabız, USS Bilgi Y¼netim Sistemi ve KDS Raporlarına Eriřim

6.10.1. Ulusal Sađlık Sistemi (USS); 6698 sayılı Kanun ve 1 sayılı Cumhurbaşkanlıđı Kararnamesi ile Sađlık Bakanlıđına verilen g¼revler çerevesinde kamu sađlıđının korunması, koruyucu hekimlik, tıbbi teřhis, tedavi ve bakım hizmetlerinin y¼r¼t¼lmesi, sađlık hizmetleri ile finansmanının planlanması ve y¼netimi amacıyla; Bakanlıđımız birimleri tarafından ulusal ¼lekte tesis edilen ve birbiri ile entegre olarak alıřan muhtelif veri kayıt ve bilgi sistemlerinin tamamı iin kullanılan genel bir ifadedir.

6.10.2. e-Nabız Projesi ¼lke genelinde birinci, ikinci ve ¼nc¼ basamakta faaliyet g¼steren ve sađlık hizmeti sunmakta olan b¼t¼n sađlık tesisleri tarafından iřlenen kiřisel sađlık verilerinin **merkezi bir veri kayıt sisteminde toplanması** ve

toplanan verilerin çeşitli uygulamalar ve raporlar aracılığı ile verinin sahibi olan vatandaşlara ve yetkilendirilen Sağlık Bakanlığı çalışanlarına sunulması amacıyla gerçekleştirilmektedir. USS'yi oluşturan diğer bilgi sistemleri de Kılavuz'un 6.10.1 maddesinde belirtilen amaçlar doğrultusunda, merkezi veri kayıt sistemine veri gönderir.

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

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

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

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

6.10.4. e-Nabız Kişisel Sağlık Sistemine Erişim:

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

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

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

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

- **Hiçbir Hekim Verilerimi Görmesin:** Kiři e-Nabız sisteminde bu seçeneđi işaretlediye Sağlık Bakanlıđında bulunan hiçbir hekim SMS ile doğrulama yapmadan hastanın sağlık verilerine erişim yetkisine sahip değildir.
- **Aile Hekimim Verilerimi Görsün:** Kiři e-Nabız sisteminde bu seçeneđi işaretlediye hastanın aile hekimliđi birimine atanmış (asaleten, vekâleten, geçici) aile hekimleri ilgili hastanın sağlık verilerine erişme yetkisine sahiptir.
- **Muayene Olduđum Hekim Verilerimi Görsün:** Kiři e-Nabız sisteminde bu seçeneđi işaretlediye sadece hastanın son 24 saat içerisinde muayene olduđu hekim sağlık verilerine erişme yetkisine sahiptir.
- **Muayene Olduđum Hastanedeki Tüm Hekimler Verilerimi Görsün:** Kiři e-nabız sisteminde bu seçeneđi işaretlediye hastanın son 24 saat içerisinde muayene olduđu sağlık tesisindeki tüm hekimler hastanın sağlık verilerine erişme yetkisine sahiptir.
- **Sađlık Bakanlıđındaki Tüm Hekimler Verilerimi Görsün:** Kiři e-Nabız sisteminde bu seçeneđi işaretlediye Sağlık Bakanlıđında bulunan tüm hekimler hastanın sağlık verilerine erişim yetkisine sahiptir.

6.10.5. USS Bilgi Yönetim Sistemine Erişim:

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

6.10.5.2. Kullanıcılar USS Bilgi Yönetim Sistemine erişirken sisteme;

- Yönetici yetkisine sahip kullanıcılar tarafından tanımlanan kullanıcı adı ve parola,
- Kurumsal (*@saglik.gov.tr) e-Posta ve parola,
- e-Devlet Kapısı (T.C. Kimlik No ve e-Devlet şifresi) (OGN üzerinden girişlerde),
- e-İmza kullanmak suretiyle giriş yaparlar.

6.10.5.3. Kullanıcıların sisteme tanıtılması, yetkilerinin verilmesi, yetkilerinin izlenmesi, gereksiz yetkilerin kaldırılması ve kullanıcı hesaplarının kapatılması/pasife alınması işlemleri “Merkez, İSM veya Toplum Sađlığı Merkezi (TSM) Yöneticileri” tarafından yapılır.

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

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

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

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

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

6.10.6. KDS Raporlarına Erişim

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

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

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

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

6.10.6.5. SİNA raporlarına erişim sina.saglik.gov.tr adresinden veya Bakanlık

OGN (ortak giriş noktası) <https://giris.saglik.gov.tr/> üzerinden erişim sağlanabilir.

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

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

6.11. Halk Sağlığı Yönetim Sistemine Erişim

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

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

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

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

6.11.5. Kullanıcılar HSYS'ye erişirken kendilerini sisteme;

6.11.5.1. HSYS tarafından tanımlanan kullanıcı adı ve parola,

6.11.5.2. Kurumsal (*[@saglik.gov.tr](mailto:***@saglik.gov.tr)) e-Posta ve parola,

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

6.11.5.4. e-İmza kullanmak suretiyle tanıtılabilir.

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

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

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

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

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

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

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

6.12. Merkezi Web İçerik Yönetim Sistemine Erişim

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.13. Sağlık Bilişim Ağına Erişim

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

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

6.13.3. SBA projesinin işletme ve yönetim faaliyetleri SBSGM tarafından yerine getirilir.

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

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

6.13.6. İl Bulut sorumlularınca;

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

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

6.13.6.3. SBA projesi kapsamında kurulumları Türk Telekom tarafından yapılan

cihazların sürekli alıřır kalması, yüklenicinin taahhütlerinin ölçülmesi açısından önem arz etmektedir. Bu nedenle enerji sorunu bulunan yerlerde gerekli tedbirler alınarak cihazların 7/24 esasına göre alıřtırılması sağlanır.

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

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

6.14. Uzaktan alıřma ve Eriřim

6.14.1. Uzaktan alıřma, 4857 sayılı İş Kanun'unun 14'üncü maddesine göre; “alıřanların, işveren tarafından oluşturulan iş organizasyonu kapsamında, iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisi” olarak tanımlanmaktadır.

6.14.2. Uzaktan alıřma; ağırlıklı olarak yükleniciler, tedarikiler, iş ortakları alıřanları gibi Bakanlıđımız ile geçici olarak iş ilişkisi olan kişiler tarafından yapılır. Ancak acil durumlarda Bakanlıđımız alıřanları için de söz konusu olabilir.

6.14.3. Uzaktan alıřma ile ilgili esaslar belirlenirken, uzaktan alıřmanın ne tür fiziki ortamlarda yapılacağı göz önüne alınır. Muhtemel uzak alıřma ortamları ařađıda sıralanmıřtır.

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

6.14.3.2. alıřanların evleri veya (tedarikiler, iş ortakları için) ofisleri,

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

6.14.3.4. Bakanlıđımıza bağlı birimlerin fiziki ortamını kullanan ancak kurum ađına (SBA'ya) doğrudan bağlanma izni verilmeyen durumlar (örneğin; kurum tesislerinde alıřan yüklenici personeli, kendi cihazları ile kurumun misafir ađına bağlanan alıřanlar).

6.14.4. Uzaktan alıřma işlemi, yapısı itibarı ile güvensiz olarak kabul edilir ve bilgi güvenliđini sağlamak için ek önlemler alınması gerekir.

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

6.14.5.1. Uzak çalışma ortamlarının fiziki güvenliđindeki yetersizlikler,

6.14.5.2. Uzak bađlantının güvenli olmayan ađ ortamları (çođunlukla internet) üzerinden yapılması,

6.14.5.3. Kurum güvenlik politikaları uygulanmamıř güvenilir olmayan cihazların i ađa bađlanması,

6.14.5.4. İ ađdaki kaynaklara dıřarıdan eriřim.

6.14.6. Günümüzde teknolojinin bizlere sađlamıř olduđu yetenekler kullanılmak suretiyle, farklı yöntemler kullanılarak uzak bađlantı yapılması mümkündür.

6.14.7. Uzaktan eriřim iin en uygun yöntemin belirlenmesi amacıyla, her ihtiyacın kendine özgü řartları ve risklerinin ayrıntılı olarak deđerlendirilmesi gerekir.

6.14.8. Uzaktan eriřim yöntemi olarak ařađıda açıklamaları verilen tünelleme, uygulama portalleri, uzak masaüstü eriřim veya dođrudan uygulama eriřimi yöntemlerinin biri veya birkaçı birlikte kullanılabilir.

6.14.8.1. Tünelleme yöntemi, uzaktan çalışmada kullanılan bilgisayar ile i ađın kriptolojik yöntemler kullanılmak suretiyle oluşturulan güvenli bir tünel vasıtasıyla birbirine bađlanmasıdır. Tünelleme iřlemi, ađırlıklı olarak sanal özel ađ (VPN: Virtual Private Network) teknolojileri vasıtasıyla yapılır. VPN iřlemi IP güvenliđi (IPsec: IP Security), taşıma katmanı güvenliđi (TLS: Transport Layer Security) veya güvenli kabuk (SSH: Secure Shell) protokolleri kullanılmak suretiyle yapılabilir.

6.14.8.2. Uzak masaüstü eriřim çözümleri, uzaktan çalışan kullanıcıların kurumun i ađında yer alan bir sunucu veya istemci bilgisayarın karřısındaymiř gibi kullanılmasını sađlar. Bu yöntemde, uzak kullanıcılar bađlanılan bilgisayarın klavye ve fare kontrollerini uzaktan yapar hale gelirler. Uzak masaüstü eriřim yöntemleri kendi ilerinde birok kısma ayrılır. Bazı eriřim modellerinde vekil/terminal sunucu vasıtasıyla iřlem yapılırken, bazı eriřim modellerinde arada bir vekil/terminal sunucu olmadan da bađlantı kurulur.

6.14.8.3. Dođrudan uygulama eriřimlerinde, eriřilecek uygulamalara ait sunucular kurumun halka açık sunucuların konumlandırıldıđı “arındırılmıř bölgeye (DMZ:De-Militarized Zone) yerleřtirilir. Bu mimaride kullanıcılar genellikle web arayüzleri üzerinden dođrudan ilgili uygulama sunucusuna bađlanarak iřlemlerini gerekleřtirirler. Dođrudan uygulama eriřimleri genellikle daha az

kritik uygulamalar için kullanılır. Bakanlıđımızın güvenli metin aktarma iletiřim protokolü (HTTPS: Secure Hyper Text Transfer Protocol) kullanılarak eriřilebilen e-Posta (<https://eposta.saglik.gov.tr>) ve EBYS (<https://www.ebys.saglik.gov.tr>) sistemleri, yine hastanelerde laboratuvar tahlil sonuçlarının vatandaşlar tarafından doğrudan internet üzerinden sorgulanmasını sađlayan sistemler bu mimariye örnek olarak verilebilir.

6.14.8.4. Portal uygulamaları, bir veya daha fazla uygulamanın genellikle web teknolojileri kullanılan tek bir arayüz üzerinden merkezi ve güvenli olarak sunulmasını sađlar. Portal çözümlerinde; portal sunucuları kurumun halka açık sunucuların konumlandırıldıđı DMZ bölgesinde, uygulamalara ve veri tabanlarına ait sunucular ise iç ađa yerleřtirilir. Bu řekilde uzaktan eriřim yapacak kullanıcıların, uygulamalara ve verilere güvenli olarak eriřmeleri sađlanır. Portal uygulamaları, doğrudan uygulama eriřimlerinin özel bir türüdür.

6.14.9. Uzak çalıřma için hangi uzak eriřim yönteminin veya yöntemlerinin kullanılacađına, yapılacak risk deđerlendirmesine bađlı olarak kurumların bilgi güvenliđi alt komisyonları tarafından karar verilir ve kurumun Eriřim Kontrol Politikası içerisinde (veya ayrı bir politika olarak) yazılı olarak belirtilir.

6.14.10. Uzaktan eriřim ile ilgili yöntem/mimari belirlenirken ařađıda belirtilen esaslar doğrultusunda hareket edilir:

6.14.10.1. Bakanlıđımızda genel bir politika olarak uzak masaüstü iřlemleri VPN bađlantısı üzerinden yapılır. VPN bađlantısı yapılmadan doğrudan uzak masaüstü bađlantısı yapılmasına hiçbir řekilde izin verilmez.

6.14.10.2. 6698 sayılı Kanun'un açıklanması amacıyla KVKK tarafından yayımlanan 2018/10 sayılı karar uyarınca, özel nitelikli verilerin iřlendiđi, muhafaza edildiđi elektronik ortamlara uzaktan eriřim yapılırken, en az iki kademeli kimlik dođrulama sistemi kullanılması yasal bir zorunluluktur. Diđer sistemler için de çok faktörlü kimlik dođrulama yapılması tercih edilir.

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

6.14.10.4. Eriřim kontrollerinin uygulanabilmesi maksadıyla, hedef bilgisayarlara sabit IP adresi verilir. Yapılacak eriřim "eriřim yapacak kiři, hedef bilgisayar IP adresi (VLAN adresi) ve kullanılacak port/uygulama" bazında sınırlandırılır.

6.14.10.5. VPN bađlantılarına iliřkin iz kayıtları tutulur ve söz konusu iz kayıtları en az iki yıl süre ile saklanır.

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

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

6.14.10.8. Uzak erişim için yapılan bađlantıda bořta kalma süresi (herhangi bir işlem yapılmadıđı takdirde connection time out süresi) kurumun ihtiyacına göre sınırlanır. Bu süre 1 (bir) saati geçemez.

6.14.10.9. Uzak bađlantı, masaüstü erişim amaçlı olarak yapılıyorsa;

6.14.10.9.1. Bađlantı VPN üzerinden yapılır.

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

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

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

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

6.14.10.9.6. Hedef bilgisayar üzerinden bir başka sunucuya bađlantı yapılacak ise (örneğin SBYS yazılımı kullanılacak ise) ilgili kullanıcının söz konusu sunucuda yaptıđı işlemlere ait iz kayıtları da kayıt altına alınır.

6.14.10.9.7. Uzak bađlantı yazılımı olarak mümkün ise “Microsoft Uzak Bađlantı Programı” kullanılır.

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

6.14.11. Uzaktan çalışma için kullanılacak cihazlar belirlenirken ařađıda belirtilen esaslar dođrultusunda hareket edilir:

6.14.11.1. Uzaktan çalışma prensip olarak Bakanlıđımız birimlerine ait cihazlar ile yapılır.

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

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

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

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

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

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

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

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

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

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

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

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

6.14.12.8. Disk şifreleme vb. araçlarla bilgisayarlarda tutulan verilerin şifreli olarak saklanması sağlanır. Disk şifreleme işlemleri için <https://bilgiguvenligi.saglik.gov.tr/> adresinde yayımlanan sürücü şifreleme el kitaplarından yararlanılır.

6.14.12.9. Uzaktan çalışma için kullanılan bilgisayarların yerel disklerinde yer alan kurumsal verilerin yedeklenmesi için gerekli tedbirler alınır. Alınacak bu yedekler sadece şifreli ortamlarda ve/veya şifreli yedeklenmiş olarak tutulabilir.

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

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

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

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

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

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

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

7. KRİPTOGRAFİK KONTROLLERİN KULLANIMI

7.1. Kriptografik Politikalar

7.1.1. Elektronik ortamda yer alan bilgiler;

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

7.1.1.2. Kaybı halinde yasal olarak yaptırımlara uğranması riski varsa,

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

7.1.1.4. Herkesin kolayca erişebileceđi web sayfaları vb. yerlerde tutuluyorsa,

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

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.

7.1.2. Sadece taşınabilir cihazlar deđil 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 kullanımını göz önünde bulundurulur.

7.1.3. Kriptografik kontroller;

7.1.3.1. Bilgilerin gizliliđini sağlamak,

7.1.3.2. Bütünlüğünü korumak,

7.1.3.3. Gönderici ve alıcının kimliklerini doğrulamak,

7.1.3.4. Yapılan işlemlerin hiçbir şekilde inkâr edilmemesini ve

7.1.3.5. Özgünlük ve güvenilirliđi garanti etmek amacıyla kullanılır.

7.1.4. Şifreleme, bilgilerin gizliliđini sađlamak amacıyla yapılır. Şifrelenmiş bir bilgi, kötü niyetli bir kişinin eline geçse dahi okunamayacağı, erişilemeyeceđi için önemli bir koruma sađlar.

7.1.5. Veri özeti (hash), bütünlüğü korunacak bilginin sabit boyutta bir parmak izinin (özetinin) çıkarılmasını sađlar. Bilginin bir harfinin (veya bir bitinin) bile deđişmesi durumunda, yeni çıkarılacak özet, aslından farklı olacağı için bilginin deđişmediđi garanti edilmiş olur.

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

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

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

7.2. Kriptografik Araç ve Yöntemler

7.2.1. Algoritma ve Anahtar Uzunlukları:

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

- RSA (Ron Rivest, Adi Shamir ve Leonard Adleman) ve eliptik eğri kriptolojisi (ECC:Elliptic Curve Cryptography) algoritmalarından birisi kullanılır.
- RSA algoritması kullanılacaksa anahtar uzunluğu en az 1024 bit, tercihen 2048 bit olarak seçilir.
- ECC algoritması kullanılacaksa “n” deđeri olarak en az 224 bit seçilir.

7.2.1.2. Blok (simetrik) Őifreleme iŐlemlerinde, geliŐmiŐ Őifreleme standardı (AES:Advanced Encryption Standard) kullanılır ve anahtar boyu en az 256 bit olur.

7.2.1.3. Veri özeti (hash) iŐlemlerinde;

- Özetleme algoritması olarak blok boyu en az 256 olacak Őekilde güvenli özetleme algoritmasının (SHA: secure hash algorithm) ikinci veya üçüncü sürümü (SHA2 veya SHA3) kullanılır.
- SHA2 algoritmasını kullanan sistem ve uygulamaların, SHA3'e yükseltilmesine gerek yoktur.

7.2.1.4. Anahtar deđiŐimi ve dođrulama (authentication) iŐlemlerinde;

- Diffie-Hellman (DH) , internet anahtar deđiŐim (IKE: İnternet Key Exchange) veya eliptik eđri kullanan DH (ECDH: Elliptic Curve Diffie-Hellman) algoritmalarından birisi seçilir. Anahtar boyutu olarak 2048 bit anahtar kullanılır.
- Anahtar üretim ve deđiŐim öncesinde uç noktaların birbirlerini dođrulamaları gerekir. Dođrulama için tarafların X.509 Ver3 standardında üretilen sertifikalar kullanılır.
- Kimlik dođrulama için kullanılan sunuculara bilinen güvenilir bir sertifika otoritesi tarafından imzalanmıŐ geçerli bir sayısal sertifika yüklenir.
- SSL veya TLS kullanan tüm sunucular ve uygulamaların, bilinen güvenilir bir sertifika otoritesi tarafından imzalanmıŐ geçerli bir sayısal sertifikası olması gerekir.

7.2.1.5. Sunucu ve istemci dođrulama iŐlemlerinde kullanılacak sayısal sertifikalar:

- X.509 Ver3 standardında olmalıdır.
- Son kullanıcı sertifikaları Kamu Sertifikasyon Merkezinden alınır.
- Bakanlık tarafından geliŐtirilen/kullanılan uygulamalarda, sertifikaların geçerliliđini kontrol etmek için çevrimiçi sertifika durumu protokolü (OCSP:Online Certificate Status Protocol) veya sertifika iptal listesi (CRL: Certificate Revocation List) metotlarından biri ya da her ikisi birlikte kullanılır.

- Sertifika geçerlilik kontrolünde kullanılan SİL ve OCSP'lerin farklı durumlara göre birbirlerine üstünlükleri vardır. CRL'ler belirli aralıklarla yayınlandıkları için bazı kontrollerde bazı sertifikaların geçerlilik durumları doğru anlaşılammaktadır. Bu yüzden eđer bir internet bağlantısı varsa öncelikle OCSP kullanılması gerekir.
- Sertifika geçerlilik kontrolünün sık yapıldığı durumlarda, CRL dosyalarının her sertifika kontrolü için yeniden indirilip içerisinden kontrol yapılması kurum için birçok yük getirecektir. Bu yüzden Sertifika Deposu dediğimiz depolama yönteminin kullanılması kurum için çok büyük kolaylık getirecektir. Sertifika Deposunda, geçerlilik kontrolü yapılan her sertifika için kontrol sırasında gerekli olan tüm kök sertifikalar, çekilen CRL'ler ya da OCSP cevapları güvenliđi sağlanmış bir veri tabanı gibi bir depo içerisine kaydedilir. Aynı sertifika için tekrar geçerlilik kontrolü yapılmak istendiğinde gerekli olan tüm bilgiler depoda bulunmaktadır ve bu bilgileri tekrar internette çekmeye gerek yoktur.

7.2.2. Web Trafıđi Güvenliđi:

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.

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.

7.2.2.3. Web trafiđinin korunması için HTTPS kullanılır.

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

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

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

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

7.2.2.8. Oturum anahtarlarının güvenliđi için kusursuz iletme gizliliđi (PFS: Perfect Forward Secrecy) özelliđi aktive edilir.

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

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

7.2.3. FTP İşlemleri Güvenliđi:

7.2.3.1. Standart FTP hizmeti, doğası geređi güvensiz olduđu için hiçbir şekilde kullanılmaz.

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

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

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

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

7.2.4. Uzaktan Yönetim Faaliyetleri:

7.2.4.1. Kimlik doğrulaması için temelde iki bağlanma yöntemi mevcuttur. Bunlardan birincisi kullanıcı adı ve şifre ile oturum sağlanan yöntem, ikincisi ise SSH key (SSH açık/gizli anahtar) yardımı ile oturumun sağlandığı yöntemdir. İlk yöntemin yeni kullanıcılar için anlaşılması kolaydır. Ancak kötü niyetli kullanıcılar genellikle art arda şifre denemeleri ile güvenlik tavizlerine yol açabilir. Bu yöntem yerine SSH anahtarı yardımı ile oturum sağlanması daha güvenlidir.

7.2.4.2. SSH Protokolü içerisinde şifreleme algoritması olarak AES-256 kullanılır.

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

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

7.2.5. Sabit Ortamdaki Verilerin Şifrelenmesi:

7.2.5.1. Windows tabanlı sistemlerde tam disk şifreleme işlemleri için;

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

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

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

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

7.2.6. Dosya ve klasör şifreleme işlemleri için;

- Güvenilir bir kaynak tarafından yayımlanmış ve AES-256 algoritmasını destekleyen herhangi bir yazılım (Winrar (5.0 veya üstü), Winzip (9.0 veya üstü) veya 7-zip) kullanılabilir.
- Microsoft Office (Word, Excel, PowerPoint) tarafından sağlanan şifre koyma yeteneđi, AES-128 algoritmasını kullandığı için özellikle zayıf bir parola seçilmesi durumunda şifrenin kırılması ihtimaline karşı yeterince güvenli olarak kabul edilmez.

8. FİZİKSEL VE ÇEVRESEL GÜVENLİK

8.1. Genel Hususlar

8.1.1. Günümüzde bilgiler büyük oranda bilgi sistemleri vasıtasıyla işlenmekte ve sayısal ortamlarda saklanmaktadır. Bu nedenle bilgi güvenliđi 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 edildiđi bilişim sistemleri ve ağlarının güvenliđi için fiziksel ve çevresel önlemlerin alınması kaçınılmazdır.

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

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

8.1.2.2. İş Sağliđı ve Güvenliđi Hizmetleri Yönetmeliđi (Resmî Gazete, Tarih/Sayı: 29.12.2012-28545),

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

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

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

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

8.1.2.7. Sağliđıkta Kalite Standartları –Hastane/ADSH.

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 diđer mevzuat da dikkate alınmıştır. Kılavuz’da yer alan kontrollerin uygulanması esnasında yürürlükteki diđer mevzuat ile çelişen bir husus ile karşılaşılmaması durumunda, normlar hiyerarşisi dikkate alınarak üst seviye norm dikkate alınır. Yine de tereddütte kalınması halinde kurumun bilgi güvenliđi alt komisyonunda deđerlendirilerek karar verilir.

8.2. Güvenli Alanlar

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.

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

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

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

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.

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.

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.

8.2.8. Giriş kontrolleri, korunacak tesis veya varlığa göre deđişir.

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

8.2.8.2. Bakanlık merkez yerleşke, bađlı kuruluşlar, il sağlık müdürlükleri gibi sağlık hizmeti sunumu yapılmayan ancak sağlık hizmetinin sunumu için destek hizmetlerinin verildiđi bina ve yerleşkelerde, en dış güvenlik sınırında yer alan

geçiş noktalarında sadece yetkili personele erişim izni verilmesini temin edecek giriş kontrolleri yapılır.

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.

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

8.2.11. Özel bir gereksinim yoksa bu tür tesis ve odalara ne şekilde erişileceđini gösteren işaretlerin konulmasından sakınılır.

8.2.12. Kapsam ve yöntemi idarelerce belirlenmek suretiyle tüm personel ve ziyaretçilerin güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartları (veya kurum giriş kartları) hazırlanır ve kullanılır.

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

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

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

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

8.2.17. Güvenli alanların yerlerini belirten krokiler ve dâhili telefon rehberleri herkes tarafından kolayca erişilebilir yerlere konulmaz.

8.2.18. İçerisinde fiilen personel çalışmayan/gözetimsiz güvenli alanlar fiziksel olarak kilitlenir ve periyodik olarak gözden geçirilir.

8.2.19. Yetki verilmediđi sürece, fotoğraf, video, ses ve diđer kayıt cihazları ve mobil cihazlardaki kameralara izin verilmez.

8.2.20. Yetkisiz kiřilerin teslimat ve ykleme iřlemleri iin güvenli alanlara giriř yapmasını engellemek zere güvenli alan dıřında olacak řekilde teslimat ve ykleme alanları oluřturulur.

8.2.21. Postacı, kurye personeli, dađıtıcı gibi kiřilerin tesis ilerine kontrolsz olarak girmesi engellenir. Teslimat ile ilgili kurallar oluřturulur. Teslimat iřlemlerinin kurum iinde belirlenecek noktalarda yapılması iin tedbir alınır.

8.2.22. Personel güvenliđi ve sađlıđı iin ilgili ynetmelikler uygulanır.

8.2.23. Yangın, sel, deprem, patlama ve diđer dođal afetler veya toplumsal kargařa sonucu oluřabilecek hasara karřı fiziksel koruma tedbirleri alınır ve uygulanır.

8.2.24. Giriř/ıkıř yapılan yerler ve ortak kullanım alanları güvenlik kameraları ile kayıt altına alınır.

8.3. Ekipman Gvenliđi

8.3.1. Masalarda ya da alıřma ortamlarında korumasız bırakılmıř bilgiler yetkisiz kiřilerin eriřimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle btnlđnn bozulmalarına ya da yok olmalarına sebep olabilir. Tm bu veya daha fazla tehditleri yok edebilmek iin ařađıda yer alan belli bařlı temiz masa kurallarına alıřanlar tarafından uyulması sađlanır.

8.3.2. Belli bařlı temiz masa kuralları

8.3.2.1. Hassas bilgiler ieren bilgi, belge ve evraklar masa zerlerinde ya da kolayca ulařılabilir yerlerde aıkta bulundurulmaz. Bu gibi bilgi ve belgeler kilitli dolap, elik kasa ya da arřiv odası gibi fiziki koruması olan güvenli alanlarda muhafaza edilir.

8.3.2.2. Yetkisiz kiřilerin eriřiminin engellenmesi iin bilgisayar bařından ayrılma durumunda ekran kilitlemesi yapılır. Otomatik ekran kilitlemesi devreye alınır.

8.3.2.3. Sistemlerde kullanılan parola, telefon numarası ve T.C. kimlik numarası gibi bilgiler ekran stlerinde veya masa stnde bulundurulmaz.

8.3.2.4. Kullanım mr sona eren, artık ihtiya duyulmadıđına karar verilen bilgiler Kılavuz'un 4.5. (Ortamın Yok Edilmesi) maddesinde belirtilen yntemler ile imha edilir.

8.3.2.5. Faks makinelerine gelen yazılar srekli kontrol edilir ve makinede yazı bırakılmaması iin tedbir alınır.

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

8.3.2.7. Fotokopi ve diđer çođaltma teknolojilerinin yetkisiz kullanımını önlemek için uygun idari ve teknik tedbirler alınır.

8.3.3. Ekipman Yerleşimi ve Koruması

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

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

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

8.3.3.4. Özel koruma gerektiren ekipmanlar izole edilmiş şekilde kullanılır.

8.3.3.5. Nem ve sıcaklık gibi parametreler izlenir.

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

8.3.3.7. Paratoner kullanılır.

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

8.3.4. Destek Hizmetleri

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

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

8.3.4.3. Kritik sistemlerde hizmet kesintisi yaşanmaması için kesintisiz güç kaynađı kullanılır.

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

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

8.3.5. Kablolama Güvenliđi

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

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

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

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

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

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

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

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

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

8.3.6. Ekipman Bakımı

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

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

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

8.3.6.4. Bakım kayıtları düzenli olarak tutulur.

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.

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

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

8.3.7. Kurum Dışındaki Ekipmanın Güvenliđi

8.3.7.1. Kuruma ait bilgisayarların kurum dışına çıkarılması ya da kişisel/yüklenici firmalara ait bilgisayarların işyerlerine getirilerek kurumsal amaçlarla kullanımı için kurum yöneticisi tarafından yetkilendirme yapılması gerekir.

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

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

8.3.7.4. Bu şekilde kullanılan ekipmanlar Kılavuz'un 4.4 (Taşınabilir Ortam Yönetimi) maddesinde belirtilen tedbirler alınmak suretiyle kullanılır. Bu ekipmanların içinde yer alan bilgilerin gizliliđi için ilgili cihazlar Kılavuz'un 7.2.5 (Sabit Ortamdaki Verilerin Şifrelenmesi) maddesinde belirtilen şekilde şifrelenir.

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

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

8.3.8. Ekipmanın Güvenli İmhası

8.3.8.1. Üzerlerinde kalıcı olarak veri barındıran ekipmanlar (sunucu, masaüstü veya dizüstü bilgisayarın, merkezi veri depolama birimlerinin ve benzeri bilgi sistem cihazlarının sabit diskleri ile USB flaş sürücüsü, USB hafıza ünitesi, flash disk ya da USB hafıza olarak bilinen taşınabilir veri depolama ortamları) Kılavuz'un 4.5 (Ortamın Yok Edilmesi) maddesinde belirtilen yöntemler kullanılarak imha edilir.

8.3.9. Fiziksel ortamların taşınması

8.3.9.1. Güvenilir taşıma şekli ve kuryeler kullanılır.

8.3.9.2. Yönetim tarafından yetkili bir kurye listesi belirlenir.

8.3.9.3. Kuryelerin kimliğini kontrol eden süreçler geliştirilir.

8.3.9.4. Paketleme, içeriğın fiziksel hasarlardan yeterince korunmasını sağlayacak şekilde yapılır.

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

9. İŞLETİM GÜVENLİĐİ

9.1. Yazılı İşletim Prosedürleri

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

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

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

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

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

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

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

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

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

9.2. Deđişiklik Yönetimi

9.2.1. Bilgi teknolojilerindeki deđişiklikler ile birlikte sistem, sunucu veya yazılım deđişiklikleri veya güncellemeleri de kaçınılmazdır. Ancak bu deđişikliklerin kontrolsüz bir şekilde yapılması, bilgi güvenliđi açısından riskleri de beraberinde getirir. İş sürekliliđine ilişkin açıklamalar Kılavuz'un 13 (İş Sürekliliđi) numaralı bölümünde açıklanmıştır. Deđişikliklerin yönetimsel bir süreci takip etmemesi iş sürekliliđini tehdit eden bir unsurdur.

9.2.2. Deđişiklik yönetiminin amacı, süreç ve yöntemi tanımlanmış olan bilgi sistemleri deđişikliklerinin bilgi güvenliđi prensipleri çerçevesinde gerçekleştirilmesini sağlamaktır. Bunun için en iyi yol, takip edilmesi gereken adımları tanımlayan yazılı işletim prosedürleri mantığıyla hazırlanan deđişiklik yönetimi dokümanının oluşturulmasıdır.

9.2.3. Deđişiklik Türleri

9.2.3.1. Yazılım Deđişiklikleri

9.2.3.1.1. Kurumsal yazılım geliştirme yaşam döngüsü boyunca ele alınan deđişikliklerdir.

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

9.2.3.2. Donanım ve Altyapı Deđişiklikleri

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

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

9.2.3.3. Veri Tabanı Deđişiklikleri

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

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

9.2.4.1. Deđişiklik nedeninin yazılı olarak tanımlanması: Her deđişiklik, deđişiklik talep eden personel ya da uygulama sahibi tarafından deđişim isteđi talep yazısı veya varsa kullanılan standart form ile başlatılır.

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

9.2.4.3. Deđişiklik onay süreci: Sorumlu personel tarafından yapılan deđişiklik analiz çalışması yönetici onayına sunulur. Yönetici deđişikliđi onaylayabilir, reddedebilir ya da ek bilgi talep edebilir. Etkileşimde olan diđer sistem sorumlularının, kendi sorumlulukları dâhilinde olan sistemler için gerekli önlemleri alması ve yazılı olarak önlemleri aldığı bildirilmesi beklenir. Deđişiklik onayı yöneticiden alındıktan sonra deđişiklik çalışmalarına başlanır.

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

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

9.2.4.6. Uygulama sonrası inceleme: Deđişikliđin istenen hedeflere ulaşıp ulaşımadıđını sađlamak için uygulama sonrası gözden geçirme yapılır. Uygulama sonrası eylemler, deđişikliđi kabul etmeye, deđiştirmeye veya geri almaya karar vermeyi içerir.

9.2.5. Aşağıdaki deđişiklikler, operasyonel bir süreç gerektirmekle birlikte deđişim yönetimi süreci gerekliliklerine dâhil deđildir:

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

9.2.5.2. Acil durum olađanüstü durum kurtarma

9.2.5.3. Sistem yapılandırmasında gerek duyulmadan yapılan masaüstü deđişiklikleri.

9.3. Kapasite Yönetimi

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

9.3.2. Kapasite yönetimi ile ayakta kalabilirlik/kullanılabilirlik (uyarılar ile hataların proaktif olarak düzeltilmesi ve iş sürekliliđinin sađlanması) ve ölçeklenebilirlik (yürütölen iş sürecinin veri hacmi büyüdükçe veri merkezinin ölçeklendirilmesi için gerekli kaynakların öngörülebilmesi) sađlanır.

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

9.3.4. Sistem izleme, bilgi teknolojileri altyapısı ile ilgili kritik iş uygulamalarının çalışır olmasını, performansının optimize edilmesini ve sistem güvenliđini sađlamak için gereklidir. Temel amaç, çeşitli ana bilgisayarların, ađ sistemlerinin ve depo ünitelerinin sorunsuz çalışmasını ve her sistem ve bileşenin ne kadar yüklü olduđunu ve ne kadar verimli kullanıldıđını, darbođaza yol açan kullanımların sistem güvenliđini tehdit edip etmediđini bilmektir. Sistemlerin kapasitesinin izlenmesi bilgi güvenliđinin sađlanması ve iş sürekliliđinin sađlanması için girdi oluşturun.

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

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

9.3.7. Gelecekteki sistem ihtiyaçları ve ileriye yönelik planlanan yeni iş uygulamaları mevcut kapasite göz önüne alınarak değerlendirilir. Mevcut kapasitenin optimizasyonu için disk alanından saklanma süresi dolan verinin silinmesi, uygulama mantıđının ya da veri tabanı sorgularının optimize edilmesi, kaynak tüketen hizmetlerden kritik olmayanlar için reddetme ya da bant genişliđi sınırlaması gibi çözüm yöntemleri uygulanabilir.

9.4. Geliştirme, Test ve İşletim Ortamlarının Ayrılması

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

9.4.2. Bu ortamlar aşıđıdaki hususlar dikkate alınarak değerlendirilir;

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

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

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

9.4.2.4. Geliřtirme, iřletim ve test sistemi için farklı kullanıcı profilleri ve kimlik dođrulama anahtarları kullanılır.

9.4.2.5. Test ortamında gerek veriler kullanılmaz.

9.4.2.6. Hassas verilerin, gerek ortamla eřdeđer bir test ortamında kontrol edilmeden iřletime alınmaması gerekir.

9.5. Etki Alanı Kurulum ve Yönetimi

9.5.1. Yönetilebilirlik, öleklenebilirlik, genişletilebilirlik, güvenlik entegrasyonu, diđer etki alanları ile birlikte alıřabilme, güvenli kimlik dođrulama ve yetkilendirme, grup politikaları ile yönetim, DNS ve DHCP gibi servislerle birlikte alıřabilme gibi avantajları nedeniyle etki alanları kurulur ve iřletilir.

9.5.2. Merkez teřkilata bađlı birimlerin etki alanı hizmetleri SBSGM tarafından iřletilen merkezi etki alanı vasıtasıyla sađlanır.

9.5.3. SBSGM tarafından sunulan merkezi etki alanı ve veri merkezi/sunucu barındırma ile ilgili hususlar, Kılavuz'un 6.5 (Merkezi Aktif Dizin ve e-Posta Sistemine Eriřim) ve 6.6 (Veri Merkezi ve Sunucu Barındırma Hizmetlerine Eriřim) numaralı maddelerinde açıklanmıřtır.

9.5.4. Bakanlık bađlı kuruluşları ve il sađlık müdürlüklerinin her birinin müstakil birer etki alanı ile yönetilmesi hedeflenir. Gemiş dönemlerde eřitli nedenlerle birden fazla etki alanı kuran ve alıřtıran birimlerce, söz konusu etki alanlarının birleřtirilmesi, birleřtirilemiyorsa birlikte alıřması için gerekli önlemler alınır.

9.6. Sunucu ve Sistem Güvenliđi

9.6.1. Sunucuların ve sistemin güvenliđini sađlamak için gerekli güvenlik kořullarının tanımlandıđı, güvenlik ilkelerinin belirlendiđi “Sistem Güvenlik Politikası” oluřturulur.

9.6.2. İř sürekliliđi ve acil durum planlaması için ilgili otoritelerle iletiřim yöntemleri tanımlanır ve yazılı hale getirilir. Acil durumlarda eriřilmesi gereken kiřilerin irtibat numaraları ilgili personelin kolayca ulařabileceđi bir Őekilde bulundurulur.

9.6.3. Yeni teknolojileri, uygulamaları, tehdit veya açıklıkları takip etmek için dernek, forum siteleri, e-Posta grupları gibi özel ilgi grupları belirlenir ve ilgili personel tarafından takip edilir. USOM tarafından yayımlanan <https://www.usom.gov.tr/tehdit.html> adresinden yaygın kullanılan yazılım ve donanımlarla ilgili

güvenlik bildirimleri takip edilebilir. Aynı şekilde Bakanlıđımız BGYS ve SOME birimleri tarafından yayımlanan <https://bilgiguvenligi.saglik.gov.tr> ve <https://some.saglik.gov.tr> adreslerinden güvenlik haberleri takip edilebilir.

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

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

9.6.6. Sunuculara ve uygulamalara erişim sağlayan kullanıcıların erişim hakları, erişimlerin iptal edilmesi veya erişim yetkisinin deđiştirilmesi gibi kuralların tanımlandığı erişim yetki ve kontrol matrisleri oluşturulur.

9.6.7. Sunucularda zorunlu kalmadıkça “administrator” ve “root” gibi genel sistem hesapları kullanılmaz.

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

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

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

9.6.11. Sistem hesaplarına ait parolalar için Kılavuz’un 6.3 (Parola Güvenliđi) maddesinde belirtilen yönetici hesaplarına ilişkin kurallar dikkate alınır.

9.6.12. Sunucuda varsayılan yönetici adı (administrator) deđiştirilir. 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 deđiştirilir. Açılmış fakat kullanılmayan kullanıcı hesapları kapalı duruma (disabled) getirilir veya silinir.

9.6.13. Sunucuların güvenliđini sađlayabilmek için kullanılmayan uygulamalar veya servisler kapatılır. Gerekli servis ve hizmetler dışında başka bir servis çalıştırılmaz.

9.6.14. Sunuculara güvenli bağlantı yapılabilmesi için SSL sertifikası yüklenir. Sunuculara SSH bağlantısı yapılacak ise kullanılan anahtarlar belirli aralıklarla deđiştirilir. Sertifika ve anahtar yönetimi ve kriptografik işlemler için Kılavuz'un 7.2 (Kriptografik Araç ve Yöntemler) maddesinde belirtilen hususlara dikkat edilir.

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

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

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

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

9.6.19. Kılavuz'un 9.15 (Sistem Güvenlik Testleri) maddesinde belirtilen güvenlik testleri yapılarak sunucular ve sistem ile ilgili açıklıklar tespit edilir. Tespit edilen açıklıkların kapatılması sađlanır. (Sunucuda Windows işletim sistemi kullanıyor ise "Netstat -an", Linux işletim sistemi kullanıyor ise "Netstat -tulp" komutu ile açık veya kullanılan portlar listelenerek kontrol edilebilir.)

9.6.20. Sunucu işletim sistemleri, güvenlik açıklarına karşı güncel tutulur. Güncellemelerde deđişiklik yapılacak ise bu deđişiklikler Kılavuz'un 9.2 (Deđişiklik Yönetimi) maddesinde belirtilen deđişiklik yönetimi kuralları çerçevesinde, onay ve uygulama sahipleri tarafından test mekanizmasından geçirildikten sonra uygulanır.

9.6.21. Etki alanındaki sunucu ve istemci bilgisayarların yama yönetiminin merkezi bir sunucu üzerinden otomatik olarak yapılması için gerekli olan sistem tesis edilir. Bu amaçla üreticiler tarafından yayımlanan yamalar merkezi bir sunucuya çekilir ve bu sunucu vasıtası ile diđer bilgisayarlara dağıtımı yapılır.

9.6.22. Mutlaka zorunlu deđil ise sunucuların internete erişimleri kapatılır.

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

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

9.6.25. Kullanıcıların bilgisayarlarının saat ve tarih ayarlarını deđiştirmesi engellenir.

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

9.6.27. Kullanıcıların “.exe/.bat” gibi çalıştırabilir dosyaları çalıştırmaları engellenir.

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

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

9.6.30. Kullanıcıların DNS adreslerini deđiştirmeleri engellenir.

9.6.31. Sunuculara yapılacak uzak masa üstü bağlantılarında Kılavuz'un 6.14 (Uzaktan Çalıřma ve Eriřim) maddesinde belirtilen hususlara dikkat edilir.

9.6.32. Sunucuda paylařıma açılmıř klasörlerde izin verilen kullanıcı ve gruplar kontrol edilir. Kullanıcılara, gruplara verilen izinler ve kullanıcıların baskın izin seçeneđini nereden aldıđı incelenir. Herkes (everyone) isimli kullanıcı grubuna izin atanmaz. İzinler kullanıcılardan ziyade gruplara verilir. Kullanıcıların bilgisayarlarını günlük işlerini yapmalarını sağlayacak seviyede en az yetki ile

çalıştırmaları sağlanır. Aynı izinlere sahip olması gereken kullanıcılar bir grupta toplanır. (Satın Alma, İnsan Kaynakları gibi)

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

9.6.34. Kurumda işletilen sistemler için Kılavuz'un 9.13 (Yedekleme Yönetimi) maddesinde belirtildiđi şekilde yedekleme politikası hazırlanır. Kurumun yedekleme politikasında belirtilen kurallara göre yedekleme işlemi yapılır.

9.6.35. Sunucularda yapılan işlemlerin iz kayıtlarına erişmek için olay günlükleri (event logs) tutulur. İz kayıtları, Kılavuz'un 9.12 (İz Kayıtları Yönetimi) maddesinde belirtildiđi şekilde saklanır.

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

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

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

9.6.39. Sunucuların fiziksel güvenliđini sağlamaya yönelik tedbirler alınır. Sunucu/sistem odalarında alınması gereken tedbirler bu Kılavuz'un 9.10 (Sunucu/Sistem Odası Güvenliđi) maddesinde olduđu gibidir. Sunucu odası dışında sunucu bulundurulmaz. Sunucu/Sistem odalarına yapılan giriş çıkışlar kontrol edilir, giriş-çıkışların kayıtları tutulur.

9.6.40. Sistemde hata ile karşılaşıldığında hataları gidermek adına izlenen yöntemler, aynı hata ile tekrar karşılaşıldığında hızlı aksiyon alınabilmesi ve iş sürekliliđinin sağlanabilmesi için yazılı hale getirilir. Hata ve çözümlerinin bulunduđu merkezi bir havuz oluşturulur.

9.6.41. Sunucu kurulumları ve sunucu üzerinde yapılan konfigürasyonlardan oluşan bir sistem bilgi bankası oluşturulur. Hazırlanmış olan bilgi bankasında

yapılan işlemler takip edilebilir ve yeni bir yapılandırma işleminde bu bilgi bankası kullanılabilir.

9.6.42. Sunucular üzerinde yapılacak deđişiklikler bu Kılavuz'un 9.2 (Deđişiklik Yönetimi) maddesinde belirtilen deđişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanır. Önemli sistem ayarlarının yetkisiz kişiler tarafından deđiştirilmesini engellemek, yetkili kullanıcılar tarafından yapılan deđişiklikleri izlemek, deđişikliklerden meydana gelebilecek olan güvenlik açıkları veya sistem problemlerini önceden belirleyerek önlem almak gibi amaçlarla kayda dayalı deđişiklik yönetimi uygulanır.

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

9.6.44. Sunucuların erişilebilirlik (availability) seviyesini artırmak için herhangi bir sunucunun çalışmaması durumunda diđer bir sunucunun onun yerine amaçlanan şekilde çalışmasını sağlayacak kümelenmiş (cluster) mimari yapıda yapılandırılması gerekir. Yüksek maliyet ya da yönetsel zorluklar nedeni ile sunucular kümelenmiş yapıda tesis edilemiyorsa en azından disklerin kümelenmiş olarak yapılandırılması tavsiye edilir.

9.7. Ağ İşletim Güvenliđi

9.7.1. Ağ mimarisi ve aktif ağ cihazlarının yönetimi, güvenlik ilke ve kuralları, erişim haklarının yazılı olduđu "Ağ Güvenliđi Politikası" oluşturulur.

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

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

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

9.7.5. Güvenlik ve ađ cihazlarına eriřim sađlayan kullanıcılar için cihazlara giriř yapmadan önce bilgilendirme sayfası açılması gerekir. Açılacak bu sayfada sadece yetki verilen kişiler tarafından erişilebilecek bir cihaz olduđu, izinsiz erişimlerde kanuni işlem yapılacağı gibi hususları bildiren bir sorumluluk metni oluşturulur.

9.7.6. Kullanıcılara erişim hakkı tanımlanmadan önce gizlilik sözleşmesi olduđu kontrol edilir. Güvenlik cihazları ve ađ yönetiminde ayrıcalıklı erişim hakkı verilen kullanıcıların sisteme erişimi onay mekanizmasından geçerek tamamlanır. Eriřim talepleri, resmi yazı veya kurumsal e-Posta ile bildirilir. Ayrıcalıklı erişim hakkı elde eden personelin yer ve görev deđişikliđi olması durumunda erişimleri düzenleyen birime bilgi verilmesi sađlanır.

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

9.7.8. Güvenlik ve ađ cihazlarına yapılacak uzaktan erişimler için Kılavuz'un 6.14 (Uzaktan Çalışma ve Eriřim) maddesinde belirtilen hususlara dikkat edilir.

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

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

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

9.7.12. Güvenlik ve ađ cihazlarının gösterildiđi "ađ mimarisi kroki" hazırlanır. Hazırlanan kroki, sadece ilgili personelin görebileceđi bir şekilde saklanır. Güvenlik ve ađ mimarisinde deđişiklik yapıldıđı zaman kroki de güncellenir.

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

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

9.7.15. Sistemi etkileyecek bir alıřma yapılması gerekiyorsa mesai saati dıřında yapılır. Bu alıřmadan etkilenecek kurum/firma ya da kiřilere bilgi verilir.

9.7.16. Aktif ađ cihazlarından bilgi toplamak iin kullanılan SNMP protokolünün (Simple Network Management Protocol) v2 veya v3 surm kullanılır. SNMP v2 protokol kullanılacak ise SNMP protokol topluluk anahtarı (community string) ile sorgulama yapar ve varsayılan olarak “public” ve “private” olarak gelen “snmp community” deđerleri deđiřtirilir. Deđiřtirilen “snmp community” deđeri aık (clear-text) bir řekilde gnderildiđi iin mmkn ise daha gvenli bir versiyon olan SNMPv3 tercih edilir.

9.7.17. Kablosuz ađlara giriř yapan tm kullanıcılar sisteme kimlik tanımlı olarak kaydedilmelidir. Kimlik dođrulamasında bađlantı yapacak kullanıcının kimlik bilgileri ve ne kadar sre ađda kalacađı gibi bilgiler alınır. 5651 sayılı Kanun ve Bakanlık BGYS politikaları uyarınca, ađa dhil olan tm kullanıcılar kaydedilir ve bu bilgiler belirlenen sreler boyunca saklanır.

9.7.18. Telnet gibi gvensiz bađlantılara izin verilmez. SSH protokoln kullanan bađlantılarda SSH Ver2 kullanılır.

9.7.19. İhtiya olmayan tm portlar kapatılır. Dıřarıdan tarama yapıldıđında portların durumunun aık olarak grlmemesi iin gerekli tedbirler alınır. Kurum web sayfaları, laboratuvar sonu sorgulama sayfası gibi uygulamalarca kullanılan 80 ve 443 dıřındaki portlar kullanıma kapatılır.

9.7.20. Gvenlik duvarı ve ađ cihazları iin kontrol listeleri (ACL, gvenlik rnleri eriřim kısıtlaması vb.) tanımlanır.

9.7.21. Gvenlik ve ađ cihazlarının fiziksel gvenliđini sađlamak iin gerekli tedbirler alınır.

9.7.22. Gvenlik ve ađ cihazlarının yazılım gvenliđini sađlamaya ynelik tedbirler alınır. Cihazlar ilk kurulduđunda varsayılan olarak atanmıř olan kullanıcı adı ve parolalar deđiřtirilir. Parolalar, Kılavuz’un 6.3 (Parola Gvenliđi) maddesinde yer alan sunucular iin gl parola ilkeleri esaslarına gre oluřturur.

9.7.23. Gvenlik ve ađ cihazları zerindeki gereksiz ve kullanılmayan tm servisler kaldırılır.

9.7.24. Cihazları kaba kuvvet saldırılarından korumak iin 5 (beř) yanlıř deneme sonrasında oturum belirli bir sre kilitlenecek řekilde ayarlama yapılır.

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

9.7.26. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Kanunu uyarınca tutulması gereken trafik bilgileri (iz kayıtları) ile ilgili hususlar Kılavuz'un 14.4 (5651 Sayılı Kanun İle Uyum) numaralı maddesinde detaylı olarak açıklanmıştır.

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

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

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

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

9.7.31. Güncel atak metotlarından korunmak için saldırı tespit ve önleme sistemleri, ağ hizmetlerine erişim ilkelerinin belirlenmesi için güvenlik duvarı kullanılır.

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

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

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

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

9.8. Veri Tabanı Güvenliđi

9.8.1. Kılavuz'un 6.1 (Eriřim Kontrol Politikası) maddesi geređi, kurumda kullanılan veri tabanına yapılacak eriřim ile ilgili hususları aıklayan bir eriřim kontrol dokümanı oluşturulur. Söz konusu dokümanda; veri tabanına eriřim sađlayan roller, veri tabanında hesap oluřturma/yetki deđiřikliđi/hesap kapatma gibi kullanıcı iřlemleri için takip edilmesi gereken süreçler, kullanıcı hesaplarının izlenmesi ve denetimi için yapılması gereken faaliyetler yer veriler. Kullanıcılara verilen eriřim yetkileri, eriřim kontrol dokümanında belirtilen aralıklarla kontrol edilir.

9.8.2. SBSGM tarafından merkezi bir hizmet olarak sunulan veri tabanı hizmetlerinden yararlanmak için yapılması gereken iřlemler Kılavuz'un 6.7 (Merkezi VTYS'ye Eriřim) maddesinde aıklanmıřtır.

9.8.3. SBYS yazılımlarının iřletimi bařta olmak üzere bađlı kuruluşlar, il sađlık müdürlükleri ve sađlık hizmet sunucuları tarafından tesis edilen VTYS'ler için de Kılavuz'un 6.7 (Merkezi VTYS'ye Eriřim) maddesinde belirtilen süreçlere benzer süreçler oluřturulur.

9.8.4. Veri tabanında kullanıcı hesabı oluřturma ve kullanıcılara eriřim yetkisi tanımlama talepleri resmi izin süreçleri oluřturulur. Bu süreçler, kurum eriřim kontrol dokümanında ayrıntılı olarak aıklanır.

9.8.5. Kurumun veri tabanına eriřen kullanıcılar (veri tabanı yöneticileri, uygulama geliřtiriciler, yedekleme operatörleri vb.) ile mutlaka gizlilik sözleşmesi imzalanır ve eriřim hakkı edindikten sonra almıř olduđu sorumluluklar kullanıcıya bildirilir.

9.8.6. Zaman içerisinde deđiřen kullanıcı eriřim yetkileri, audit (izleme/denetim) kurallarıyla takip edilir.

9.8.7. Veri tabanına eriřen ortak kullanıcı hesaplarına izin verilmez.

9.8.8. Veri tabanında yer alan tüm kullanıcı hesaplarının durumlarına bakılır. Veri tabanında oluřturulmuř isimsiz hesaplar, gemiřte aılmıř fakat kullanılmayan hesaplar özellikle kontrol edilir. Kurumdan ayrılan alıřanlara ait veri tabanı hesapları kilitlenir veya silinir.

9.8.9. Veri tabanına son girilen bařarılı ve bařarısız oturum bilgilerinin giriř kayıtları tutulur.

9.8.10. Veri tabanında kritik rollere (admin) sahip kullanıcıların yetkileri ve görevleri, kurum eriřim kontrol dokümanında belirtilen aralıklarla düzenli olarak kontrol edilir. Varsa geređinden fazla verilmiř olan yetkilerin kaldırılması sađlanır.

- 9.8.11.** SQL Server kurulumu ile gelen varsayılan “SA” kullanıcısı pasife alınır.
- 9.8.12.** Veri tabanında sahip olduđu yetkileri bir başka kullanıcıya (“with admin option” ya da “with grant option” gibi seçeneklerle) devretme yetkisi olan kullanıcı hesapları kontrol edilir. Mutlak zorunluluk yok ise kullanıcılara bu tür yetkiler verilmez.
- 9.8.13.** 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 erişim kontrol prosedüründe belirtilen aralıklarla kontrol edilir.
- 9.8.14.** Güvenlik yamaları kontrollü olarak uygulanır. Sistemde hangi yamaların uygulanıp uygulanmadığı kontrol edilir.
- 9.8.15.** Veri tabanı güncelleştirmeleri takip edilir. Sistem üzerinde kod çalıştırabilen ve yetki yükseltilebilen zafiyetlerin giderilmesine öncelik verilir.
- 9.8.16.** Yama ve güncelleme çalışmaları yapılmadan önce tüm ilgili kişi ve kurumlara bildirimde bulunulur ve sonrasında ilgili uygulama kontrolleri gerçekleştirilir.
- 9.8.17.** Veri tabanı kullanıcısının kaynakları, limit parametreleri belirli aralıklarla kontrol edilir.
- 9.8.18.** Veri tabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar kullanılır.
- 9.8.19.** 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.
- 9.8.20.** Veri tabanına dinamik içerikli web sitelerinden gelen istekler için Kılavuz’un 9.9 (Yazılım Güvenliđi) maddesinde belirtilen güvenlik tedbirleri alınır.
- 9.8.21.** Kurum yedekleme politikası uyarınca veri tabanının yedekleri alınır. Alınan yedeklerin başarılı olarak alındığı iz kayıtları üzerinden kontrol edilir. Kurum yedekleme politikasında aksine bir hüküm yok ise yılda en az iki kez olacak şekilde geri dönüş testleri yapılır.
- 9.8.22.** Veri tabanında parola politikasında kullanılan parametrelerin tanımları ve varsayılan değerleri değiştirilir. Veri tabanı üzerinde oluşturulan her kullanıcı profili için parola parametrelerinin tanımlanması gerekir.

9.8.23. Veri tabanı kullanıcı profillerine göre tanımlanması gereken diđer parola parametreleri ve önerilen deđerleri Őu Őekildedir:

9.8.23.1. Kullanıcı hesabının kilitlenmesi iin gerekli maksimum baŐarisız oturum ama giriŐim sayısı 5 (beŐ),

9.8.23.2. Parolanın geerli sayılacađı maksimum gn sayısı 90 gn,

9.8.23.3. Kullanıcı parola sresi dolmadan nce kullanıcıya parolasını deđiŐtirmesi iin hatırlatma gnderme sresi 7 (yedi) gn,

9.8.23.4. Parolanın tekrar kullanılabilmesi iin tanımlanması gereken minimum farklı parola sayısı 3 (),

9.8.23.5. Parolanın tekrar kullanılabilmesi iin gemesi gereken minimum sre 90 gn,

9.8.23.6. Maksimum sayıdaki baŐarisız oturum ama giriŐimlerinden sonra, hesabın ne kadar sreyle kilitli kalacađı sre 10 (on) dakika.

9.8.24. Veri tabanı kullanıcıları ilk kez tanımlanan hesaplarıyla oturum atıklarında parola deđiŐtirmeye zorlanır.

9.8.25. Kullanılan uygulamaların kurulumu ve yapılandırmasının anlatıldıđı kılavuz dokmanları hazırlanır. (Oracle Kurulum, SQL Kurulum, bađlantı dokmanları gibi)

9.8.26. Veri tabanı sunucusu zerindeki gereksiz olan servisler kapatılır.

9.8.27. Veri tabanı ynetim sistemlerinin, alanında uzman ve eđitim almıŐ personel tarafından ynetilmesi sađlanır.

9.8.28. Veri tabanında “any” yetkileri, sistem yetkileri verilip verilmediđi kontrol edilir. rneđin “alter system”, “select any table”, “select any dictionary”, “drop any table” Őeklindeki yetkiler verildiyse alınır.

9.8.29. Veritabanında Public kullanıcılarına veritabanı nesnelere eriŐim yetkisi verilip verilmediđi kontrol edilir. Bu Őekilde yetkiler verilmiŐse geri alınır.

9.9. Yazılım Gvenliđi

9.9.1. Uygulama yazılımlarına eriŐen kullanıcıların eriŐim yetkileri ve rol ynetimi yazılı olarak tanımlanır. Kullanıcı eriŐim talepleri onay mekanizmasından geirilir.

9.9.2. Uygulama yazılımlarına erişim sağlayan kullanıcıların aldıkları erişim hakları, erişimlerin iptal edilmesi veya erişim yetkisinin deđiştirilmesi gibi kurallar yazılı hale getirilir. İşten ayrılma veya görev deđişikliği olması durumunda kullanıcı hesapları iptal edilir ve tanımlanan yetkiler görev deđişikliği dođrultusunda güncellenir.

9.9.3. Uygulamalarda yönetici ve kullanıcı hesap yetkilerinin tanımlanması, her proje için yazılı kurallar dođrultusunda yapılır. Yetki tanımlanan kullanıcıların yetki kısıtlamaları belirli aralıklarla takip edilir.

9.9.4. Uygulama yazılımlarında roller oluşturularak erişim kontrol (yetkilendirme) matrisi oluşturulur. Rol tabanlı yetkilendirmeler yapılır. Kullanıcıların sadece yetkilendirildiđi rol kapsamındaki verilere erişim sağlayacak şekilde düzenleme yapılır.

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

9.9.6. Kurulumla birlikte gelen varsayılan (default) kullanıcı hesapları ve rolleri silinir veya pasif hale getirilir.

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.

9.9.8. Program kaynak kütüphaneleri işletimdeki sistemler dışında ayrıca farklı bir yerde saklanır. Kaynak kodlara erişim yapan hesaplar yazılı olarak tanımlanır ve bu hesapların hareketleri izlenir. Program kaynak kütüphanelerine erişim yapan kullanıcıların tüm erişimlerinin iz kayıtları tutulur.

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

9.9.10. Yazılım paketlerinde yapılacak deđişiklik öncesi test hazırlık sürecinde roller ve sorumluluklar belirlenir. Deđişiklik talepleri alındıktan sonra onay

merciinden geirilir. Orijinal yazılımda deđiřiklik gerekli ise yazılımın orijinal hali saklanır. Versiyon deđiřiklikleri (minor ve major deđiřiklik gibi) kayıt altına alınır ve deđiřikliklerde risk deđerlendirmesi nceden yapılır.

9.9.11. İř srekliliđini sađlamak adına uygulamaların hata kayıtlarını ve zmlerini ieren bir hata havuzu oluřturulur.

9.9.12. Yedekleme politikası uyarınca bilgi ve yazılımlar yedeklenir. Yedekler belirlenen kurallar dođrultusunda test edilir.

9.9.13. Uygulama yazılımları, kullanıcıların parolasını parola politikasına gre oluřturması ynnde zorlayıcı Őekilde tasarlanır. Yazılımlar kullanıcıya parolasını deđiřtirme yetkisi verecek Őekilde yapılandırılır.

9.9.14. Uygulama yazılımları kullanıcıya parola kurtarma seeneđi ile kullanıcının yeniden parola oluřturmasına olanak sađlayacak Őekilde tasarlanır. Kurtarma parolası kullanıcı tarafından sisteme tanımlanmış olan kurumsal e-Posta adresine veya cep telefonuna gnderilecek parolayı sıfırlama gibi bir fonksiyon sunulur.

9.9.15. Kullanıcılara tanımlanan geici parola, gl parola politikasına gre ve sınırlı geerlilik sresine gre verilir.

9.9.16. Kurumda kullanılan uygulamalarda tanımlı sre boyunca aktif olmayan oturumlar otomatik olarak kapatılır ve yazılım projeleri trne gre oturum sreleri belirlenir.

9.9.17. Kullanıcı sayısının fazla olduđu ve yođun olarak kullanılan sistemlerde kimlik ynetim servislerinin yk dengeli (load-balancer) olarak alıřtırılması tavsiye edilir.

9.9.18. Uygulama yazılımları bařka kaynaklara bađlanırken (veri tabanı vb.) eriřim iin kullandıđı parolalar Őifrelenmiş (encrypted) bir halde saklanır. Parolaların Őifrelerini zmek iin gereken anahtarlar, yetkisiz eriřimden korunur. Parolalar hibir durumda uygulamanın kaynak kodu iinde saklanmaz. Son kullanıcıların ya da istemci durumundaki uygulama servislerini kullanan diđer sistemlerin kimliklerini dođrulamak iin kullandıđı parolalar kriptografik zet halinde (hash) saklanır.

9.9.19. Yazılım projelerinde teknik aıkla ilgili kontroller sađlanır. Zafiyetlerin yayınları takip edilir. Uygulama projelerinde gvenliđi sađlamak iin yazılımlar KLVZ-EK-15 Gvenli Yazılım Geliřtirme Kontrol Listesi ile kontrol edilir.

9.9.20. Oturum açılması gereken uygulamalarda belirli sayıda yanlış kimlik doğrulama denemesinden sonra captcha uygulaması ile kullanıcıdan doğrulama talep edilir. Belirli sayıda hatalı kimlik doğrulama denemesinin ardından hesap geçici olarak kilitlenir. (Örneđin 5 yanlış deneme)

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

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

9.9.23. Uygulama yazılımları kullanıcıya az bilgi ile geri bildirim yapacak şekilde tasarlanır. Kullanıcıya dönen hata sayfalarında “kullanıcı adı yanlış” gibi hatanın nerden kaynaklı olduğunu söyleyen bilgiler değil de “kullanıcı adı veya parola yanlış” gibi hata kaynađını göstermeyen bilgiler verilir.

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

9.9.25. KVKK'nın 2018/10 sayılı kararı uyarınca özel nitelikli kişisel verilerin işlendiđi yazılımlarda;

9.9.25.1. Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

9.9.25.2. Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

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

9.9.25.4. Verilerin bulunduđu ortamlara (örneğin VTYS sunucuları) ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin (sızma testleri) düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

9.9.25.5. Verilere bir yazılım aracılıđı 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,

9.9.25.6. Verilere uzaktan erişim gerekiyorsa en az 2 (iki) kademeli kimlik doğrulama sisteminin sağlanması gerekir.

9.10. Sunucu/Sistem Odası Güvenliđi

9.10.1. Hizmet sunumunun sürekliliđinin sađlanması için kesintisiz ve sürekli çalıřan 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 edilmiř, yetkisiz personelin giriřinin engellendiđi, sıcaklık ve nemin kontrol edildiđi, elektrik kaynađının stabilize edildiđi, özel şekilde iklimlendirilmiř ve güvenliđi sađlanmış sunucu/sistem odasında konumlandırılması gerekir. Sistem odalarındaki donanımların hizmet sürekliliđinin sađlanması için yedekli bir güç kaynađı sistemi, yedekli haberleřme bađlantıları, ısı, nem gibi çevre deđiřkenlerinin kontrolü için iklimlendirme cihazları ve güvenlik cihazları yer alır.

9.10.2. Bir sistem odasının en temel özellikleri;

9.10.2.1. 7×24 kesintisiz çalıřabilirlik,

9.10.2.2. Güç yönetimi ve ađ bađlantılarında farklı kanallardan yedeklilik,

9.10.2.3. Ađ güvenliđi, fiziksel eriřimlerde yetkilendirme ve görüntülü gözetleme,

9.10.2.4. Çevre şartlarının kontrol altında tutulması,

9.10.2.5. Yangına karřı duman algılama gibi erken uyarı sistemleridir.

9.10.3. Sistem odasının kesintisiz çalıřmasına; sıcaklıđın normal aralıđın dıřına çıkması, yangın, su baskını, deprem, yetkisiz kiřilerin sistem odasına girmesi, odadaki herhangi bir cihazın arızalanması engel olabilir. Tüm bu olumsuz durumların yařanmasının önlenmesi ve hizmetlerin sađlıklı çalıřabilmesi için standartlara (ANSI/TIA/EIA-942 standardı gibi) uygun bir sistem odası oluřturulması ve ana bilgisayar, sunucu ve diđer hizmet sürecindeki bileřenlerin güvenli olarak bu alanlarda konumlandırılması gerekir. Bahse konu “ANSI/TIA-942 Standardı”, veri merkezlerinin sınıflandırılabil-diđi 4 (dört) tip katman içerir. Her ařama kendisinden bir önceki ařamada bulunması gereken kořulları sađlamalıdır. Bu katmanlar řunlardır;

9.10.3.1. Katman-1 Temel Altyapı (Tier-1) : Tek bir kapasiteye sahip bileřenlere ve bilgisayar ekipmanına hizmet veren tek, yedeksiz bir dađıtım yoluna sahip bir veri merkezidir. Fiziksel olaylara karřı sınırlı korumaya sahiptir.

9.10.3.2. Katman-2 Yedek Kapasite Bileřen Altyapı (Tier-2): Yedek kapasite bileřenlerine ve bilgisayar ekipmanına hizmet veren tek, yedeksiz bir dađıtım yoluna sahip bir veri merkezidir. Fiziksel olaylara karřı geliřmiř koruma sađlar.

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 olduđu yeteneklerini son kullanıcıya zarar vermeden planlı bir şekilde çıkarılabileceđi/deđiştirilebileceđi/servis edilebileceđi anlamına gelir. Çođu fiziksel olaylara karşı korumaya sahiptir.

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.

9.10.4. Sistem odası ile ilgili aşığıdaki ölçütlere dikkat edilmesi gerekir;

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, eđer mümkünse orta katlarda ya da 2.katında konumlandırılmalıdır. Sistem odasının yeri iklimlendirme açısından da deđerlendirilerek, sistem odasından bina çıkışıdaki klimanın dış ünitesine giden borunun mesafesi düşünülerek seçilmelidir. Mümkün olduđunca sistem odasında cam pencere ve duvarlar olmamalıdır. Sistem odasının bulunduđu binada yıldırımlara karşı paratoner kurulmalı ve kabloları sistem odasından uzakta olmalıdır. Manyetik alan oluşturabilecek enerji ve elektrik hatlarından izole olmalı, telefon santrali ve benzeri dış unsurlar kesinlikle sistem odasına alınmamalıdır, kullanılması gerekiyorsa kafes yapmak gibi ek güvenlik önlemi alınmalıdır.

9.10.4.2. Sistem Odasının İnşaat Özellikleri: Kesintisiz güç kaynakları ve elektrik dağıtım panoları; aktif cihazlar ve sunucuların yerleştirildiđi alandan ayrı bir bölüm olarak tasarlanabilir. Odanın dış duvarları, yangına ve sızdırmazlığa karşı gaz beton tuđla veya iki tarafı alçı ile kaplanmış -50° ile $+650^{\circ}$ arasındaki sıcaklıklara dayanıklı bir malzeme olan taş yünü ile örülmelidir. İç duvarlar pasif yangın koruması sağlayacak epoksi boya ile kaplanmalıdır. Sistem odalarındaki kablo yoğunluđu ve diđer iletim hatları yükseltilmiş taban ve asma tavanların içinden geçirilerek sistem odası içerisinde oluşabilecek karmaşı önlenmelidir. Yangın ve su baskını durumunda cihazların etkilenme riskini azaltma, gerektiğinde hızlı ve kolay müdahale edebilme, sođuk 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

bađlantıları ve sistem odasına yerleřtirilen algılayıcılara ait iletim kablolarının yerleřtirilebilmesi için asma tavan uygulanmalıdır. Asma tavan, neme ve yangına dayanım standartlara sahip özellikle plakalardan oluřmalıdır.

9.10.4.3. Giriř – Çıkıř Kontrolü: Sistem odasına giriř ve çıkıřlar kart okuyucu, avuç içi damar okuyucu veya řifreli giriř ile kontrol altına alınmalı ve giriř/çıkıřlara ait iz kayıtları tutulmalıdır. IP kamera ile izleme sistemi kurulmalı, odanın durumu, giriř çıkıřları ve yapılan iřlemler kameralarla kayıt altına alınmalıdır.

9.10.4.4. Isı Kontrolü: Birçok iřlemci için üreticisi tarafından belirtilen en yüksek sıcaklık derecesi ortalama 70 °C'dir. Bu ısıya ulařan sunucular, üzerlerindeki sensörler aracılıđıyla kendilerini kapatırlar. Hizmet sürekliliđi için ortam sıcaklıđının 18 °C ile 22 °C arası olması kabul edilir. Sistem odasının birkaç noktasına, e-Posta, SMS ya da telefon çağırısı aracılıđıyla bilgilendirme yapan ısı sensörleri konumlandırılabilir. Ayrıca, hava dolařımının uygun bir řekilde sađlanması için sunucuların ön yüzleri birbirine bakacak řekilde konumlandırılmalı, yükseltilmiř zemin yardımıyla sođuk havanın sunuculara ön yüzden ulařması sađlanmalı, dıřarıya verilen sıcak havanın ise sođutma tesisatının giriřine ulařacak řekilde olması sađlanmalıdır.

9.10.4.5. Nem Kontrolü: Nem sadece sunucular ve bilgisayar sistemleri için deđil üzerinde elektronik devre elemanları bulunduran tüm cihazlar için bir risk oluřturur. Ortamdaki nem oranının eřik deđerlerinin altına dıřmesi elektronik devre elemanlarının statik elektrikle yüklenmesine, üstüne çıkması ise sıvı oluřumlarına neden olur ki bu da cihazlarınızın kullanabileceđinden fazla elektrik tařıması ya da kısa devre nedeniyle bozulmasına sebep olacaktır. Bu nedenle sistem odasının e-Posta, SMS ya da telefon çağırısı aracılıđıyla bilgilendirme yapan nem sensörleri ile izlenmesi ve uygun kořullarda tutulması gerekmektedir. Bunun için en uygun nem aralıđı %45 ile %70 arasındır.

9.10.4.6. Toz kontrolü–Temizlik: Tozlu ortamlar elektronik sistemlerin ařırı ısınmasına yol açaabilmektedir. Bundan dolayı sistem odasının tozdan arındırılmıř olması, kabinetler ve sistemlerde filtreler kullanılması gerekmektedir. Tozların temizliđi dıřa üfleme ve içe emmeli kompresör ile yapılmalı, böcek ilaç ve tabletleri ile sistem odasında örümcek, sinek gibi böceklerin varlıđı engellenmelidir.

9.10.4.7. Yangın Kontrolü: Sistem odasının dıřında çıkabilecek yangınlara karřı, odanın dıř kısımları su püskürtmeli yangın sistemi ile koruma altına alınmalıdır. Sistem odasının kapısı yangına dayanıklı, ısıyı ve dumanı diđer tarafa geçirmeyen, standartlara (TS EN 1634-1:2014+A1) uygun özel üretim bir kapı olmalıdır. Yükseltilmiř 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 kilitlemelidir. Herhangi bir yangın tehlikesi durumunda sistem odasının elektriđi kesilerek yangına müdahale edilmelidir.

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

9.10.4.9. Enerji Kontrolü: Enerjinin sürekliliđi ve yedekliliđi, iletimi, izlenmesi ve topraklama hassasiyetle üzerinde durulması gereken konulardır. Sistem odasındaki cihazların çektiđi 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 kalınlıđı seçilmeli, enerji kabloları kablo kanalı ile korunmalıdır. Kablo ısınması ya da sigorta atması ve benzeri sonuçların engellenmesi için tüm cihazların kullandığı enerji miktarı sayısal deđer olarak izlenmelidir. Sistem odası kuruluş aşamasında topraklama yapılmalı, ölçümleri düzenli olarak izlenmeli ve ölçüm sonuçlarına göre önlemlerin yeterliliđi deđerlendirilmelidir. Topraklama sistemleri ‘Elektrik Tesislerinde Topraklama Yönetmeliđi’ne uygun olarak yapılmalıdır.

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

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.

9.10.4.12. Kabin Düzeni: Kabinlere cihazlar yerleştirilirken yerel ağ ve DMZ bölgesine hizmet eden sunucuları ve anahtarlama cihazlarını (switchleri) ayrı konumlandırmak, veri depolama, yedekleme, ağ bağlantısı ve güvenlik cihazlarını kolay erişilebilir bir kabine yerleştirmek planlı büyüme için kolaylık sağlayacaktır.

9.10.4.13. İzleme: Cihazların hata ya da alarmlarını manuel olarak kontrol etmek yerine Basit Ağ Yönetim Protokolü (SNMP) destekli cihazları bir izleme yazılımı üzerinden kontrol etmek için arıza durumunda e-Posta yoluyla bilgilendirme yapacak bir sistem oluşturulmalıdır. Bu iş için mevcut sunucuların üreticisinin

izleme için özel ürünlerini kullanmak bir yöntem olabilir ya da bakım anlaşması ve garanti kapsamındaki cihazlar için donanım arızası durumunda otomatik çağrı açılması ve arızalı parçanın deđişim sürecinin otomatik olarak başlatılması sağlanabilir.

9.11. Tıbbi Cihaz Güvenliđi

9.11.1. Hastanelerin Bilgi İşlem/Biyomedikal Birimleri Tarafından Takip Edilmesi Gereken Hususlar²

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

9.11.1.2. Tıbbi cihaz envanteri çıkarılır. Cihazlara ait temel bilgiler tespit edilerek kullanıldığı yer ile birlikte kayıt altına alınır.

9.11.1.3. Tedarik safhasında bilgi güvenliđi yapılandırma imkânı sağlayan cihazlar tercih edilir ve bu husus hazırlanacak tıbbi cihaz tedarik şartnamelerine konulur.

9.11.1.4. Cihaz yaşam döngüsü boyunca bilgi teknolojileri ile ilgili cihaz yapılandırma ihtiyaçları için üretici firma desteđi alınır.

9.11.1.5. Tıbbi cihazlar mümkün olduđu takdirde güvenlik duvarı vasıtasıyla oluşturulan DMZ bölgelerine konumlandırılarak cihazlara dış ağdan yapılacak erişimler engellenir veya asgari düzeye indirilir.

9.11.1.6. Sağlık hizmet sunucusunun sınır güvenliđini 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.

9.11.1.7. Yerel alan ağının VLAN'lara bölünerek yönetilmesi, VLAN'lar için ACL'ler oluşturularak trafiğin yönetilmesi tıbbi cihazlar için iç ağdan kaynaklanabilecek (bilinçli veya bilinçsiz) tehlikeleri önemli ölçüde azaltır.

9.11.1.8. İz kaydı üretme imkânı olan tıbbi cihazların iz kayıtları sadece yerel cihazda deđil merkezi bir iz kaydı saklama sunucusuna da aktarılmak suretiyle saklanır

² Bu başlık altında yazılı olan gereksinimler Open Web Application Security Program (OWASP) tarafından yayınlanmış "Secure Medical Device Deployment Standart" isimli doküman esas alınarak hazırlanmıştır. Söz konusu dokümanın İngilizce ve Türkçe Sürümlerine https://www.owasp.org/index.php/OWASP_Secure_Medical_Device_Deployment_Standard adresinden erişim sağlanabilmektedir.

9.11.1.9. Tıbbi cihazlar tarafından üretilen iz kayıtları, (varsa) Merkezi Kayıt ve Olay Yönetim Sistemi (SIEM) vasıtasıyla diđer sistemler tarafından üretilen iz kayıtları ile ilişkilendirilir ve gerekli analizler yapılır.

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

9.11.1.11. Tıbbi cihazlar genellikle en fazla bir ya da birkaç tane bilgisayar ile haberleşme ihtiyacı duyarlar. Sahte DNS ile ilgili ataklardan korunmak amacıyla, bağlanılacak sunucu ve/veya terminalerin isim ve IP adresleri tıbbi cihazların “host” dosyalarına yazılarak cihazın DNS bağlantıları kesilir.

9.11.1.12. Cihazın ağ bağlantısı yapılmadan önce mutlaka varsayılan deđer bilgileri (device host name, admin, user, supervisor vb.) deđiştirilir. Parola vb. bilgileri cihazların yazılımları içine deđiştirilemez bir şekilde gömülü cihazlar kesinlikle kullanılmaz.

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

9.11.1.14. Cihazlar, verilerin sadece güvenli bir format ve en güncel SSH gibi güvenli iletişim protokolleri aracılıđı ile gönderilmesini mümkün kılacak şekilde yapılandırılır. FTP, Telnet veya http gibi güvenli olmayan iletişim protokolleri yerine HTTPS veya sFTP protokolleri kullanılır. Güvenli olmayan ağ protokolleri devre dışı bırakılır.

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

9.11.1.16. Cihazın belleđindeki veriler mümkün ise şifreli olarak muhafaza edilir.

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

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

9.11.1.19. Cihaz üzerindeki kullanılmayan servisler (portlar) ve ara yüzler, yazılımsal veya mümkün oluyorsa donanımsal olarak kapatılır.

9.11.1.20. Tıbbi cihazlara uzaktan erişim yapmaya yetkili personelin kimlikleri belirlenir, bu personel ile kişisel gizlik sözleşmesi imzalanır. Uzak bağlantılar Kılavuz'un 6.14 (Uzaktan Çalışma ve Erişim) maddesinde belirtilen tedbirler alınmak suretiyle yapılır.

9.11.1.21. Tıbbi cihazlara uzaktan müdahalede bulunan firma çalışanları ile gizlilik sözleşmesi yapılır.

9.11.2. Tıbbi Cihaz Tedarik Planlaması Yapan Birimler Tarafından Dikkat Edilmesi Gereken Hususlar:

9.11.2.1. Mevcut tıbbi cihazlar, siber güvenlik yetenekleri yönüyle incelenir ve iyileştirmek için bir strateji uygulanır.

9.11.2.2. Tıbbi cihazlardaki yazılım ve donanım güncelleme işlemleri için üretici firma veya yetkili temsilcilerinin desteđi alınır.

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 güvenliđi politikalarının uygulanamayacağı cihazlar tedarik edilmez.

9.11.2.4. Envanterde yer alan ve siber güvenlik tedbirleri uygulanamayan cihazların yenilenmesi veya ağ bağlantısı ihtiyacı olmayan yerlerde kullanılması için planlama yapılır.

9.11.2.5. Yeni yapılacak tıbbi cihaz bakım ve onarım sözleşmelerine; yazılım/donanım güncellemelerinin yapılması, sıkılaştırma işlemleri ile ilgili hususlar da eklenir.

9.11.2.6. Tıbbi cihazlarda siber güvenliđin 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.

9.11.2.7. Tıbbi cihazlar, üreticilerinin öngördüğü kullanım amacı ve varsa kullanım kılavuzunda belirtilen öneriler dikkate alınarak kullanılır.

9.11.2.8. Tıbbi cihazların güvenli kullanımını sağlamak için üreticinin öngördüğü hususlar dikkate alınarak gerekli eğitimler yapılır.

9.12. İz Kayıtları (Log) Yönetimi

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

9.12.2. Kurumun iz kayıtları politikası yazılı hale getirilir. İz kayıtlarının tutulması ve yönetilmesi (iz kayıtlarının üretilmesi, aktarılması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi gibi süreçler) sadece erişim yetkisi verilen bir birim/kişiler tarafından yapılır. Bu yetkilerin tercihen Kurumsal SOME'lere verilmesi uygundur.

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.

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

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

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

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

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

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

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

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

9.12.12. İz kayıtları periyodik olarak yedeklenir ve yedeklerin uygun şekilde muhafaza edilmesi sağlanır.

9.12.13. Merkezi iz kaydı sunucusu sadece yeni iz kayıtlarının saklanması için fonksiyonlar içerir. Bu sunucuda iz kayıtlarının silinmesi/deđiştirilmesi amaçlı erişimlere izin verilmez.

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

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

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

9.12.15.2. Sanal ortam kayıtları,

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

9.12.15.4. Güvenlik duvarları,

9.12.15.5. Antivirüs yazılımları,

9.12.15.6. Saldırı tespit/önleme sistemleri,

9.12.15.7. Yönlendiriciler ve anahtarlama cihazları,

9.12.15.8. Sunucular,

9.12.15.9. Diđer iş uygulamaları (kritik kurumsal projeler),

9.12.15.10. Veri tabanları,

9.12.15.11. VPN iz kayıtları.

9.12.16. Tutulması gereken asgari iz kayıtları;

9.12.16.1. Kaydı oluřturan sistem,

9.12.16.2. Kaydın oluřturulma zamanı (tarih, saat, zaman dilimi),

9.12.16.3. Kaydı oluřturan olay,

9.12.16.4. Kaydın iliřkili olduđu kiři (IP/Port bilgisi, MAC adresi, iřlemi yapan tekil kullanıcı adı veya sistemin adı).

9.12.17. 5651 sayılı Kanun ve bu Kanun'a dayanarak yayımlanan ikincil mevzuat ile kurumun tutmak zorunda olduđu iz kayıtları Kılavuz'un 14.4 (5651 Sayılı Kanun ile Uyum) maddesinde ayrıntılı olarak açıklanmıřtır.

9.13. Yedekleme Yönetimi

9.13.1. Kurumsal verilerin yedeklenmesi, iř sürekliliđinin en temel prensipleri arasında yer alır. Donanım arızaları, yazılım hataları, kullanıcıdan kaynaklanan sorunlar ya da dođal tehditler gibi nedenlerle veri kayıpları yařanabilir. Bařarılı bir yedekleme iřlemi ve yedeklenen verinin ihtiyaç anında veri kaybı olmadan kurtarılabilmesi, veri yedekleme sistemlerinin en temel iki bileřenidir.

9.13.2. Yedekleme iřlemlerinin sađlıklı bir řekilde yapılabilmesi için kurum ihtiyaçlarına cevap verecek, etkin bir yedekleme sisteminin var olması gerekir. Yedekleme sistemi kurulumu için yedeklenecek veri miktarı, yedekleme sıklıđı, yedeklenen verinin zaman içerisinde deđiřme oranı, kabul edilebilir maksimum veri kaybı gibi parametreler dikkate alınır. Mümkün olması halinde insan faktörünü en aza indirecek řekilde otomatik araçlar tarafından yapılan bir sistem tesis edilmesi tercih edilir.

9.13.3. Yedeklerin kurumun gereksinimleri dikkate alınarak hazırlanmıř, yönetimin konuya bakıř açısını yansıtan bir yedekleme politikası dođrultusunda alınması, güvenliđinin sađlanması, saklanması ve belirli sıklıkta geri dönüř testlerinin yapılması gerekir.

9.13.4. Yedekleme politikası oluřturulmasının ilk ve en önemli safhası analiz çalıřmasının yapılmasıdır.

9.13.5. Analiz çalıřmasında, öncelikle hangi sistemlerin yedeđinin alınacađı belirlenir. Kurum için kıymet ifade eden ve kaybedilmesi halinde iř sürekliliđini etkileyecek tüm sistemlerin yedeklerinin alınması gerekir. Bu kapsamda; bařta SBYS verileri olmak üzere kurumda kullanılan kritik uygulamalara ait veriler, ortak dosya sunucusu üzerinde saklanan kullanıcı verileri, sunucuların tekrar hizmete alınması için ihtiyaç duyulan veriler, güvenlik ve ađ cihazlarının yapılandırma dosyaları ve

iřletme esnasında cihazlarda tanımlanmış kural setlerinin saklandıđı veri tabanları, iz bilgilerinin saklandıđı sunucular mutlaka dikkate alınır.

9.13.6. Yedekleme yöntemleri belirlenirken kaynakların etkin olarak kullanılması için gerekli özen gösterilir. Her seferinde tüm verilerin yedeđinin alınması yerine, artırımı yedekleme yapılarak hem sistemlerin geređinden fazla meřgul edilmesi önlenir, hem de depolama alanlarından tasarruf edilebilir.

9.13.7. Yedekleme politikası dođrultusunda yapılan yedekleme iřlemleri düzenli olarak kontrol edilir ve sonuçları kayıt altına alınır. Bu amaçla kurumda kullanılan yedekleme sisteminin rapor ekranları kullanılabilir veya örneđi KLVZ-EK-16’da verilen bir Yedekleme Kontrol Listesi oluşturulabilir.

9.13.8. Yedeklerin alındıđı medyalar, herhangi bir felaket (yangın, sel, su basması vb.) anında etkilenmeyecek şekilde bilgi iřlem odalarından farklı odalarda veya binalarda muhafaza edilir.

9.13.9. Özel nitelikli kişisel veri kategorisinde bulunan sađlık kayıtlarının yer aldıđı yedekleme ortamları, Kılavuz’un 7 (Kriptoloji) maddesinde yer alan usullere göre şifrelenir.

9.13.10. Yedeklenen verilerin orijinal verileri yansıtmaması ve başarılı bir şekilde yedeklenip yedeklenmediđinden emin olunması için yılda en az 2 (iki) kez geri dönüş testi yapılarak test sonuçları tutanak ile kayıt altına alınır. Tutanakta; sunucu adı, test tarihi, önceki test tarihi, yedek türü ve yedek durumu, geri yükleme testlerinin kimler tarafından ne zaman yapıldıđı, başarılı olup olmadıđı gibi asgari bilgiler yer almalıdır.

9.13.11. Yedekten geri yükleme testlerinin, başarısız olması nedeniyle veri kaybı olabileceđi durumu göz önüne alınarak, canlı ortamda deđil gerçek ortamın aynısı olan test ortamında yapılması gerekir.

9.14. Teknik Açıklık Yönetimi

9.14.1. “Teknik açıklık” bir bilgi güvenliđi terimidir. Kelime anlamı olarak “bir varlık veya kontrolde bulunan ve potansiyel olarak bir ya da daha fazla tehdit unsuru tarafından istismar edilebilecek herhangi bir kontrol zafiyetidir”. Aynı şekilde “tehdit” de “bir sisteme ya da organizasyona zarar verebilecek herhangi bir istenmeyen olayın potansiyel nedeni” olarak tanımlanabilir.

9.14.2. Teknik açıklıklar; bir varlık veya kontrolün tasarımı, uygulanması, konfigürasyonu veya çalışması sırasında dikkatsizlik nedeniyle veya kasıtlı olarak yaratılan kusurlardır.

9.14.3. Teknik açıklıkların tespiti bazen herhangi bir masraf yapmadan çok kolay şekilde olabilir. Bilhassa ürünün tasarımından kaynaklanan açıklıklar üreticiler tarafından yayımlanan yamalar ile düzeltilir. Envanterde yer alan bir yazılım veya işletim sisteminin yamalarının yapılarak en güncel sürümünün kullanılması, ilave bir çaba göstermeden olası pek çok teknik açıklığı önler. Sunucu ve sistem güvenliği kapsamında, yama yönetimi yapılması ile ilgili hususlar Kılavuz'un 9.6 (Sunucu ve Sistem Güvenliği) maddesinde açıklanmıştır.

9.14.4. Bununla birlikte yanlış uygulama ve konfigürasyonlardan kaynaklanan hataların giderilmesi, genellikle daha zor ve masraflıdır. Bu tür açıklıkların tespiti için teknik uzmanlardan yararlanılması, açıklık taramalarının yapılması veya bu Kılavuz'un 9.15 (Güvenlik Testleri) maddesinde belirtilen güvenlik testlerinin yapılması gerekir.

9.14.5. Teknik açıklıkların önlenmesi, tespiti ve giderilmesi için aşağıda sıralanan faaliyetler yapılır:

9.14.5.1. Olası teknik açıklıklar; başta Bakanlık Sektörel SOME, istihbarat sağlayan kurum ve kuruluşlar tarafından e-Posta ve resmi yazı ile yapılan bildirimler, üretici firmalar tarafından yayımlanan duyurular, forumlar ve özel ilgi grupları vasıtasıyla takip edilir.

9.14.5.2. Alınan tüm önlemlere rağmen çeşitli nedenlerle oluşabilecek açıklıkların tespit edilmesi için işletilen sistemler ticari veya ücretsiz açık kaynak kodlu güvenlik açığı tarama yazılımları ile taramaya tabi tutulur. Bu amaçla ağa bağlanan cihazlar üzerindeki açıklıkların tespiti için OpenVas, MetaSploit Framework, Nessus, Nexpose; web uygulamaları için Wapiti, Arachni, w3af, Acunetix, Netsparker gibi yazılımlar kullanılır.

9.14.5.3. Bakanlık Sektörel SOME ya da kurumların aldığı hizmet veya Kurumsal SOME'ler tarafından kurumların bilgi sistemleri yukarıda belirtilen araçlarla açıklık tarama işlemine tabi tutulur ve tespit edilen eksiklikler ilgili kurumlara yazılı ve elektronik olarak gönderilir.

9.14.5.4. Teknik açıklıkların önlenmesi ve giderilmesi için takip edilen kaynaklarda belirtilen/tavsiye edilen önlemler alınır. Bu amaçla yama ve güncelleştirmeler yapılır, cihaz/sistem konfigürasyonları önerilen şekilde ayarlanır. Çok sayıda açıklık tespit edilmesi durumunda öncelikle çok yüksek ve yüksek risk oluşturan açıklıkların giderilmesi hedeflenir.

9.14.5.5. Açıklıkların kapatılması sonrasında aynı araçlar ile tekrar tarama yapılarak alınan önlemlerin yeterlilik durumunun doğrulanması gerekir.

9.14.5.6. Teknik açıklıkların yönetiminde kullanılan yazılımların lisanssız ya da güvenlik açığı yaratabilecek korsan yazılım olmamasına dikkat edilir.

9.15. Sistem Güvenlik Testleri

9.15.1. Sistem güvenlik testleri, açıklık tarama araçları tarafından ve manuel olarak tespit edilen teknik eksikliklerin özel yazılım ve tekniklerle istismar edilmesi ve sistemlere erişim sağlanması amacıyla yapılır. Bu testler yaygın kullanımıyla “sızma testi” veya “penetrasyon testi” olarak da bilinir.

9.15.2. Bakanlığımıza bađlı tüm merkez ve taşra birimleri tarafından geliştirilen veya kaynak kodları ile birlikte tedarik edilen yazılımların “kaynak kod analiz” işlemleri de sistem güvenlik testlerinin bir parçası olarak gerçekleştirilir.

9.15.3. KVKK'nın özel nitelikli kişisel verilerin güvenliđi için alınması gereken tedbirler kapsamında yayımlanan 2018/10 sayılı kararı uyarınca bu veriler elektronik ortamlarda saklanıyor ise;

9.15.3.1. Verilerin bulunduğu ortamlara (örneğin VTYS sunucuları) ait güvenlik güncellemelerinin sürekli takip edilmesi, **gerekli güvenlik testlerinin (sızma testleri) düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,**

9.15.3.2. Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, **bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması (sızma testleri, kaynak kod analizleri), test sonuçlarının kayıt altına alınması** kanuni bir zorunluluktur.

9.15.4. Bakanlık merkez ve taşra teşkilatı ile bađlı kuruluşlara bađlı birimlerde yapılacak sistem güvenlik testleri, önceden makam onayı almak ve ilgili birimlere bilgi vermek şartıyla, Bakanlık Sektörel SOME vasıtasıyla gerçekleştirilir. Sektörel SOME tarafından yapılacak güvenlik testleri (USOM veya Bakanlık ihlal olayları bildirim sistemi vasıtası ile bildirilen olayların çözülmesi, Bakanlık Üst Yönetim tarafından verilen direktifler vb.) özel ihtiyaçlara binaen istisnai olarak yapılır.

9.15.5. Bakanlık bađlı kuruluşlar ile taşra teşkilatları, önceden kendi üst yönetimlerinden onay almak ve ilgili birimlere bilgi vermek şartıyla, kurumsal SOME'leri vasıtasıyla kendilerine bađlı birimlerde sistem güvenlik testi yapar veya yaptırabilir.

9.15.6. Güvenlik testi için hizmet alımı yapılması halinde, ilgili firma ve personeli ile mutlaka gizlilik sözleşmesi yapılır.

9.15.7. Yapılacak kontrol ve testler, “TSE 13638 Sızma Testi Yapan Personel ve Firmalar İçin Şartlar” standardına bađlı kalınarak yürütülür.

9.15.8. Testler, TS 13638’de tanımlandığı şekilde aşağıda belirtilen uzman/sertifikalı personel tarafından yapılır.

9.15.8.1. Stajyer Sızma Testi Uzmanı

9.15.8.2. Kayıtlı Sızma Testi Uzmanı

9.15.8.3. Sertifikalı Sızma Testi Uzmanı

9.15.8.4. Kıdemli Sızma Testi Uzmanı

9.15.9. Güvenlik testleri iç ađdan (internal) ve dış ađdan (external) olacak şekilde ayrı ayrı yapılır ve en az aşağıdaki hususların test edilmesi gerekir.

9.15.9.1. Ađ ve sistem altyapısı sızma testi,

9.15.9.1.1. Yerel ađ sızma testleri ađ sızma testi,

9.15.9.1.2. İnternet üzerinden sızma testleri,

9.15.9.1.3. Güvenlik sistemleri (antivirüs, IPS/IDS, güvenlik duvarı vb.) sızma testi,

9.15.9.1.4. İşletim sistemleri sızma testi,

9.15.9.1.5. Kablosuz ađ sızma testi.

9.15.9.2. Mobil uygulama sızma testi,

9.15.9.3. Veri tabanı testleri,

9.15.9.4. Hizmet aksatma saldırı (DoS/DDoS) testleri,

9.15.9.5. Endüstriyel kontrol sistemi (SCADA) sızma testi,

9.15.9.6. Sosyal mühendislik testleri,

9.15.9.7. Web uygulama sızma testleri ve yazılım kaynak kod analizleri (kaynak kodları olan yazılımlar için).

9.15.10. Kaynak kod analizlerinin sadece otomatik kod analiz araçları ile yapılması yeterli bir işlem olarak kabul edilmez. Kodların yetkin personel tarafından manuel olarak gözden geçirilmesi gerekir. Bu amaçla TÜBİTAK'ın yayımlamış olduđu güncel Güvenli Yazılım Geliştirme Kılavuzu veya KLVZ-EK-15 Güvenli Yazılım Geliştirme Kontrol Listesinde yer alan ölçütler kullanılır.

9.15.11. Yapılan testler sonucunda ortaya çıkan sonuçlar, önem derecesine göre raporlanır. Bu raporların oluşturulmasında TSE 13638 standart raporlama örneđi temel alınır. Raporla en az aşağıda belirtilen hususların yer alması gerekir.

9.15.11.1. Kapak Sayfası (testlerin yapıldığı zaman dilimini içerir),

9.15.11.2. Yönetici Özeti (Kısa bir okuma ile rapordaki önemli bilgilere ulaşmak isteyen okuyuculara (özellikle yöneticilere) yönelik bir bölümdür),

9.15.11.3. Genel Bilgiler,

9.15.11.4. Test Ekibi,

9.15.11.5. Kapsam ve IP Adresleri,

9.15.11.6. Genel Deđerlendirme,

9.15.11.7. Genel Test Metodolojisi,

9.15.11.8. Risk Derecelendirmesi (Sayısal olarak veya farklı renklendirme şeklinde, TSE 13638 Standartlarına göre (Acil, Kritik, Yüksek, Orta, Düşük) yapılarak kurumun risklerin giderilmesinde önceliklendirme yapılmasına imkân vermek üzere hazırlanır),

9.15.11.9. Genel Bulgular,

9.15.11.10. Teknik Bilgiler (Raporun teknik detaylarının verildiđi kapsamlı bir bölümdür. Teknik bilgilerin aşağıdaki alt bölümleri içermesi tavsiye edilir)

9.15.11.10.1. Giriş,

9.15.11.10.2. Bilgi toplama,

9.15.11.10.3. Açıklık analizi,

9.15.11.10.4. Kullanma /aıklık onayı,

9.15.11.10.5. Kullanma sonrası etki,

9.15.11.10.6. Varsa diđer testler (sosyal mühendislik/fiziksel sızma testi/DoS/DDoS vb.),

9.15.11.10.7. Kullanılan araçlar.

9.15.11.11. Testlere ait grafiksel gösterimler,

9.15.11.12. Tavsiye özeti.

9.15.12. Sızma testi raporları yukarıda bahsi geçen maddeler asgari kalmak suretiyle kurumun ihtiyaçlarına göre deđiştirilebilir.

9.15.13. Sızma testi raporunun stajyer sızma testi uzmanı dıřındaki diđer uzmanlar tarafından hazırlanması ve imzalanması gerekir.

9.15.14. Oluřturulan rapor, Kurumsal SOME Ekip lideri ve Bilgi Güvenliđi Yetkilisi tarafından deđerlendirilerek acil eylem planı oluřturulur ve aıklıkların kapatılması için alıřmalar bařlatılır.

9.15.15. Yapılan alıřmalar sonucunda ortaya ıkan sonuçlar, kurumun bilgi güvenliđi alt komisyonuna sunulur. Kapatılmayan zafiyetler risk tablosuna iřlenir ve riskin azaltılması için mümkün olan önlemler alınır.

9.15.16. Hazırlanan raporlar GİZLİ gizlilik derecesi ile sınıflandırılır. Gerek yazılı kopyaları gerekse elektronik kopyaları mutlaka güvenli bir ortamda saklanır.

10. HABERLEŐME GÜVENLİĐİ

10.1. Ađ Güvenliđi

10.1.1. Bilgisayar ađları; küçük bir alan içerisindeki veya uzak mesafelerdeki bilgisayar ve/veya iletiŐim cihazlarının iletiŐim hatları aracılıđıyla birbirine bađlandığı, dolayısıyla bilgi ve sistem kaynaklarının farklı kullanıcılar tarafından paylaŐıldığı, bir yerden başka bir yere veri aktarımını mümkün kılan iletiŐim sistemleridir.

10.1.2. Ađ güvenliđi, bir kuruluşun bilgisayar ađına bađlı olarak çalışan varlıklarının ve ađ trafiđinin güvenliđini sađlamak üzere, uygulamakta olduđu politikalar ve kontrol önlemleridir. Ađ güvenliđi, bilgi güvenliđinin sađlanması için en önemli bileŐenlerden biridir.

10.1.3. Ađ güvenliđi, kurum bilgi güvenliđi politikaları kapsamında alınacak idari ve teknik tedbirler ile sađlanır. Bu maksatla çeŐitli yazılım ve donanımlar kullanılır.

10.1.4. Daha güvenli bir iletiŐim ortamı sađlamak amacıyla (Aile Sađlıđı Merkezleri, 112 Komuta Kontrol Merkezleri, müstakil bir binada çalışan ve ađa bađlı aktif cihaz sayısı 10'dan az olan birimler hariç) Bakanlıđımıza bađlı tüm kurum ve kuruluşların geniŐ alan ađı bađlantıları, internet erişimleri SBA üzerinden sađlanır.

10.1.5. Aile Sađlıđı Merkezleri, 112 Komuta Kontrol Merkezleri, müstakil bir binada çalışan ve ađa bađlı aktif cihaz sayısı 10'dan az olan birimlerin internet erişimleri doğrudan ADSL aboneliđi vb. yöntemlerle sađlanır.

10.1.6. SBA mimarisi uyarınca illere bađlı uç noktalar, (istisnai bazı büyük iller hariç) her il için birer adet olacak şekilde tesis edilmiŐ “toplama noktası” olarak adlandırılan yapılar üzerinden, SBA Merkez Bulutuna ve internete bađlanır.

10.1.7. Buluta bađlı kullanıcıların internet erişimleri il toplama noktasında bulunan internet bađlantısı üzerinden gerçekleştirilir.

10.1.8. Aktif cihaz sayısının 10'dan az olması nedeniyle SBA İl bulutuna doğrudan bađlı olmayan yerlerde, İnternet bađlantısında kullanılan aktif ađ cihazlarının desteklemesi durumunda, internet trafiđi il toplama noktasında bulunan güvenlik duvarı ile tesis edilen IPSec VPN benzeri bir tünel üzerinden geçirilerek, trafiđin filtrelenmesi ve iz kayıtlarının tutulması imkânı sađlanır.

10.1.9. İnternet üzerinden vatandaşlar tarafından erişilen uygulamalara ait sunucular (kurumların herkese açık web sayfaları, hastanelerin laboratuvar sonuçlarının sorgulandıđı uygulamalar vb.), SBA'ya bađlı kullanıcılar tarafından erişilen sunucular (muhtelif SBYS uygulama sunucuları, etki alanı sunucuları, dosya sunucuları vb.) ve VTYS sunucuları güvenlik duvarları vasıtası ile tesis edilen DMZ bölgesine konulur.

10.1.10. Uzaktan çalışma maksadıyla internet üzerinden SBA'ya bađlı cihazlara erişim yapılması halinde alınması gereken güvenlik tedbirleri, Kılavuz'un 6.14 (Uzaktan Çalışma ve Erişim) maddesinde açıklanmıştır.

10.2. Uç Nokta (Yerel Alan Ađı) Ađ Güvenliđi

10.2.1. SBA'ya bađlı olsun veya olmasın, bir yerel alan ađında ađ güvenliđi ile ilgili uygulanması gereken tedbirler takip eden maddelerde sıralanmıştır.

10.2.2. Yerel alan ađının fiziki güvenliđi için Kılavuz'un 8.3.5 (Kablolama Güvenliđi) maddesinde belirtilen tedbirler alınır.

10.2.3. Kablosuz sistemler kullanılarak tesis edilen yerel alan ađları için burada yazılı olan hususlara ilave olarak Kılavuz'un 10.3 (Kablosuz Ađ Güvenliđi) maddesinde belirtilen tedbirler alınır.

10.2.4. Ađa bađlanacak bilgisayarların ađ yöneticileri tarafından belirlenecek ölçütleri taşıyan, kimliđi tanımlanmış ve dođrulanmış olması gerekir. Bu maksatla mümkünse ađ tabanlı erişim kontrol sistemleri (NAC) kullanılır. NAC tabanlı çözümlerin olmaması durumunda, ađa bađlanacak cihazların MAC adresleri, bađlanacağı kenar anahtarın ilgili portuna elle tanımlanarak yetkisiz, kimliđi bilinmeyen cihazların ađa erişimi engellenir.

10.2.5. Yerel alan ađlarında, port kısıtlaması yapılamayan, yönetim yeteneđi olmayan ađ dağıtım kutuları (hub) veya eski nesil kenar anahtarlar kullanılmaz.

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

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

10.2.8. Ađa bađlanan tıbbi cihazlar, sunucular ve istemci bilgisayarlar farklı VLAN'lara konulur. Çok kritik ve hassas verilerin bulunduđu, izole edilmesi gereken cihaz ve sistemler için gerekiyorsa mikro segmentasyon yapılır.

10.2.9. SBA altyapısında alıřan rn veya cihazların ikincil bađlantı yntemleri zerinden internete dhil edilmesi (rneđin ađa bađlı bir tıbbi cihaza 4G kablosuz modem takılarak dođrudan internet eriřimi sađlanıp gncelleme yapılması, ađa bađlı bilgisayarın cep telefonu ile oluřturulan bir kablosuz eriřim noktası zerinden internete bađlanması vb.) kesinlikle yasaktır.

10.2.10. Herhangi bir nedenle byle bir bađlantı ihtiyaçı olması halinde, sz konusu bađlantı iin SBSGM'nin yazılı onayı alınması ve yazılı onayda belirtilen ilave gvenlik tedbirlerinin uygulanması gerekir.

10.2.11. Bakanlıđın yazılı onayı alınmaksızın yukarıda belirtilen řekilde internet bađlantılarının yapıldıđının tespit edilmesi halinde, ilgililer hakkında idari ve yasal iřlemler yapılır.

10.2.12. Hastanelerin misafir ađları ile SBA'ya bađlanan yerel alan ađları fiziksel olarak veya farklı VLAN'lar oluřturulmak suretiyle ayrıştırılır.

10.3. Kablosuz Ađ Gvenliđi

10.3.1. Kablosuz eriřim noktası olarak kullanılan cihazların ynetimi iin kullanılan parolalar deđiřtirilir. Kurum parola politikasına uygun olarak karmařık parola verilir.

10.3.2. Cihazların varsayılan yayın adı (SSID deđeri) deđiřtirilir.

10.3.3. Bađlantı ayarları iin řifreleme etkinleřtirilir. řifreleme seeneđi etkinleřtirilirken ađa eriřim iin kullanılmak zere nc taraflar tarafından tahmin edilemeyecek karmařık bir parola belirlenir. řifreleme yntemi olarak;

10.3.3.1. ncelikle WPA3 Gvenlik protokol kullanılır. WPA3 desteklemeyen cihazlarda retici firmaların yayımlamıř olduđu gncel yazılım srme ykseltilir.

10.3.3.2. Uyumluluk, gvenilirlik, performans ve gvenlik ile ilgili nedenlerle WEP ve WPA1 kullanımı uygun deđildir.

10.3.4. Kablosuz ađa bađlanacak kullanıcı sayısı kısıtlı ise ilave gvenlik nlemi olarak ađa bađlanacak cihazların MAC adresleri, kablosuz eriřim cihazı zerinde tanımlanır.

10.3.5. Eriřim noktasının sinyal gc kapsama alanı, ihtiyaca cevap verecek řekilde en aza indirilir.

10.4. Veri Aktarımı Güvenliđi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10.4.16. Şifreleme araçları olarak Kılavuz'un 7.2 (Kriptografik Araç ve Yöntemler) maddesinde belirtilen kriptografik yöntemler kullanılır. Bu çerçevede;

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

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.

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

10.4.16.4. Şifrelemede kullanılacak parolanın, Kılavuz'un 6.3 (Parola Güvenliđi) maddesinde detayları verilen parola politikasında belirtilen ölçütler (en az 8 karakter, büyük ve küçük harf karışık, en az bir özel karakter, en az bir rakam, kelime anlamı olmayan vb.) ile uyumlu olması gerekir. Bu şartları sağlamayan bir parola kullanılması durumunda, şifre kırma yazılımları ile şifreli verilere ulaşılması ihtimali olduğu dikkate alınır.

10.4.16.5. 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.)

10.4.17. e-Posta ile Veri Aktarımı:

10.4.17.1. Hedef kişi, Sağlık Bakanlığı çalışanı ise ve “*[@saglik.gov.tr](mailto:*@saglik.gov.tr)” uzantılı kurumsal e-Posta hesabı varsa, dosya aktarımı için en pratik yöntem olarak Sağlık Bakanlığı Kurumsal e-Posta Sistemi tercih edilir.

10.4.17.2. Hedef adres “*[@saglik.gov.tr](mailto:*@saglik.gov.tr)” uzantılı tüzel e-Posta adresi ise bu hesaba birden fazla kişinin ulaşabileceđi dikkate alınır ve gönderme işlemi konusunda daha fazla hassasiyet gösterilir.

10.4.17.3. ÇOK GİZLİ, GİZLİ ve ÖZEL gizlilik derecesindeki bilgiler önce 10.4.16’de belirtilen şekilde şifrenmeyi müteakip e-Posta eki olarak gönderilir. HİZMETE ÖZEL bilgilerin şifrenmesine gerek yoktur.

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 şifrenir.

10.4.18. Dosya Paylaşım Ortamları ile Veri Aktarımı:

10.4.18.1. FTP yapısı itibarıyla güvenli bir paylaşım ortamı olarak kabul edilmez.

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 şifrenir.

10.4.19. Taşınabilir Medya ile Veri Aktarımı:

10.4.19.1. Bakanlık taşınabilir medya kullanım politikası, Kılavuz’un 4.4 (Taşınabilir Ortam Yönetimi) maddesinde açıklandığı gibidir.

10.4.19.2. Taşınabilir medya yapısı itibarıyla çalınma, kaybolma gibi tehditlere maruz kalma ihtimali nedeniyle, başka bir aktarım yöntemi olmadığı durumlarda kullanılır.

10.4.19.3. ÇOK GİZLİ, GİZLİ ve ÖZEL gizlilik derecesindeki bilgiler taşınabilir medya ortamında şifreli olarak muhafaza edilir.

10.4.19.4. Kurum Kontrolünde Olmayan Ortamlar Üzerinden Veri Aktarımı:

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.

10.4.19.6. Gizli kalması gereken bilgiler hiçbir şekilde açık (şifresiz) olarak bu ortamlarda tutulamaz ve aktarılamaz

10.4.19.7. Aktarım yapılacak kişi/kurumun Bakanlığımız kontrolündeki sistemlere erişim izni yok ise HİZMETE ÖZEL olanlar da dâhil daha üst düzey gizlilik derecesi taşıyan tüm bilgiler, yukarıda belirtilen şekilde şifrelenmek suretiyle kurum kontrolünde olmayan sistemler üzerinden paylaşılabilir.

10.4.20. Web Servisleri Üzerinden Veri Aktarımı

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.

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 Kılavuz'un 7.2 (Kriptografik Araç ve Yöntemler) maddesinde belirtilen hususlara dikkat edilir.

10.4.20.3. Yönetimsel olarak uygulanabilir olması halinde, web servislerine iletişim için zaman ve/veya IP adresi bazında filtre kullanılması hususu dikkate alınır.

10.4.20.4. Web servisi kapsamında kullanılan mesajlar bir doğrulama mekanizmasından geçirilir. XML (Extensible Markup Language) servisler için belirlenen XML şemasına uygun olduğu denetlenir. Şema doğrulamasından geçemeyen istekler kabul edilmez.

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.

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.

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 sürekliliđi sağlanır.

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 aşılırsa reddedilir.

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.

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.

10.4.20.11. Web servisleri sürekli olarak kontrol edilir ve deđişen teknoloji ve ihtiyaçlara göre gerekli güvenlik güncellemeleri yapılır.

10.4.20.12. Ayrıca alınan kayıtlar düzenli olarak incelenir. Varsa yetkisiz erişimler tespit edilerek güvenlik önlemleri arttırılır.

10.5. Gizlilik Sözleşmeleri

10.5.1. Bakanlığımıza ait gizli kalması gereken bilgilerin korunması maksadıyla, Bakanlık merkez ve taşra teşkilatı ile bađlı kuruluşlarda görev yapan ve kendilerine herhangi bir nedenle kurumun bilgi ve bilgi işleme tesislerine erişim yetkisi verilen tüm çalışanlar ve tedarikçiler ile gizlilik sözleşmeleri yapılır.

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

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.

10.5.4. Korunacak bilginin niteliđi ve durumun özelliđine göre, imzalanacak

gizlilik sözleşmelerinin içeriđi deđişebilir. Bununla birlikte hazırlanacak olan gizlilik sözleşmelerinde mutlaka ařađıda sıralanan hususların bulunması gerekir.

10.5.4.1. Korunacak bilginin tanımı,

10.5.4.2. Gizliliđin süresiz muhafaza edilmesi gereken durumlar da dâhil olmak üzere anlaşma süresi,

10.5.4.3. Anlaşma sona erdiđinde yapılması gereken eylemler,

10.5.4.4. Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar,

10.5.4.5. Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiđi,

10.5.4.6. Gizli bilgilerin kullanım izni ve bilgileri kullanmak için tarafların hakları,

10.5.4.7. Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,

10.5.4.8. Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesi halinde diđer tarafın bilgilendirme zorunluluđu ve bildirim nasıl yapılacađı,

10.5.4.9. Teslim edilen bilgilerin iade veya imhasına ilişkin hükümler,

10.5.4.10. Sözleşmenin ihlali durumunda yapılması beklenen eylemler.

10.5.5. Kamu personeli ile yapılacak gizlilik ve ifřa etmeme düzenlemelerinde, personelin statüleri geređi bađlı oldukları başta 657 sayılı Devlet Memurları Kanunu olmak üzere diđer yasal mevzuat dikkate alınır.

10.5.6. Kişisel ve kurumsal gizlilik sözleşmesi olarak;

10.5.6.1. Geçici süreli olarak çalışan yüklenici firma çalışanları, stajyerler gibi personele KLVZ-EK-12 Personel Gizlilik Sözleşmesi imzalatılır.

10.5.6.2. Yüklenici firmalar ve diđer kurum ve kuruluşlardan KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesi alınır.

10.5.6.3. Başta 657 sayılı Kanun'a tabi personel olmak üzere diđer kamu çalışanlarına, hizmetin yapılması esnasında kişisel olarak uymaları gereken bilgi güvenliđi ile ilgili hususları açıklamak/hatırlatmak maksadıyla hazırlanmış olan KLVZ-EK-17 Bilgi Güvenliđi Farkındalık Bildirgesi tebliđ edilir.

10.5.7. Söz konusu sözleşmeler, SBSGM için hazırlanmış olup her kurumun kendi ihtiyaçlarına özgü olarak güncelleme gerektirir.

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.

10.6. Veri Aktarım Anlaşmaları

10.6.1. 21.06.2019 tarihli ve 30808 sayılı Resmî Gazete’de yayımlanarak yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmelik’in “Kişisel Sağlık Verilerinin Aktarılması” başlıklı 15’inci maddesi gereğince veri aktarım işlemlerinde dikkat edilmesi gereken hususlar aşağıdaki maddelerde sıralanmıştır.

10.6.2. Kişisel sağlık verilerinin yurtiçinde aktarımında 6698 sayılı Kanun’un 8’inci maddesine, yurtdışına aktarımında ise Kanun’un 9’uncu maddesine riayet edilir.

10.6.3. Kişisel sağlık verilerinin, 6698 sayılı Kanun’un 8’inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası ve 28’inci maddesi kapsamında kamu kurum ve kuruluşlarına aktarılması için protokol düzenlenir. Düzenlenen protokolde, kişisel veri koruma mevzuatının genel ilkeleri ile veri güvenliğine ilişkin hükümlere ve protokol kapsamında hangi verilerin aktarılacağına yer verilir. Verilerin aktarımı, teknik altyapının uygun olması hâlinde KamuNET üzerinden gerçekleştirilir.

10.6.4. Kişisel sağlık verilerinin aktarımı talepleri, talep edilen sağlık verilerinin ilgili olduğu Bakanlık birimi tarafından 6698 sayılı Kanun ve ilgili diğer mevzuat açısından değerlendirilir, değerlendirme sonucuna göre SBSGM tarafından işlem tesis edilir.

10.6.5. Doğrudan taşra teşkilat birimlerine yapılacak veri aktarım talepleri için, ihtiyaç duyulması halinde, talep edilen sağlık verilerinin ilgili olduğu Bakanlık biriminden görüş istenir ve verilecek talimata göre hareket edilir.

10.6.6. Veri aktarımı esnasında, 6698 sayılı Kanun’un 12’nci maddesinde yer alan veri güvenliğine ilişkin yükümlülükler riayet edilir. Teknik ve idari tedbirlerin alınmasında, Kurum tarafından hazırlanan Kişisel Veri Güvenliđi Rehberi ve SBSGM tarafından yayımlanmış olan Sağlık Bilgi Güvenliđi Politikaları Kılavuzu esas alınır.

10.6.7. Aktarıma konu olan veriler özel nitelikli kişisel veriler (sağlık verileri bu kategoridedir) ise;

10.6.7.1. Verilerin e-posta yoluyla aktarılması gerekiyorsa Őifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,

10.6.7.2. Tařınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle Őifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,

10.6.7.3. Farklı fiziksel ortamlardaki sunucular arasında aktarma geręekleřtiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının geręekleřtirilmesi,

10.6.7.4. Verilerin kađıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kiřiler tarafından görölmesi gibi risklere karřı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerekir.

11. TEDARİKÇİ İLİŐKİLERİ

11.1. Mal ve Hizmet Alımları Güvenliđi

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 Tebliđleri ve yönetmeliklerinin tanımlamış olduđu usul ve esaslara göre yapılır.

11.1.2. Satın alma faaliyetine konu olan iş kapsamında; yüklenicinin yükümlülüklerini gerçekleştirmesi için yükleniciye özel koruma ihtiyacı olan veri/bilgi teslim edilmesi, ilgili kurumun fiziki alanlarında personel çalıştırılması veya kurum bilgi sistemlerine (uzaktan erişimler dâhil) erişim yapılması ihtiyacı olması halinde; satın alma için hazırlanan teknik ya da idari şartnamelere “Bilgi Güvenliđi Gereksinimleri” başlıđı altında asgari olarak aşağıdaki hususlar eklenir:

11.1.2.1. Yüklenici sözleşmeye konu yükümlülüklerini ifa ederken, Bakanlık Bilgi Güvenliđi politikalarına uymak zorundadır. Bakanlığın Bilgi Güvenliđi Politikaları, “Sađlık Bakanlıđı Bilgi Güvenliđi Politikaları Yönergesi” ve “Sađlık Bakanlıđı Bilgi Güvenliđi Politikaları Kılavuzu”nda açıklanmıştır. Bahse konu dokümanlara, Bakanlığın resmi web sitesinden erişilebilir.

11.1.2.2. Bakanlık/Kurum BGYS Politikaları uyarınca, idareye ait bilgilerin korunması maksadıyla, yükleniciler ile “Kurumsal Gizlilik Sözleşmesi” ve söz konusu iş kapsamında çalışacak olan yüklenici personeli ile “Personel Gizlilik Sözleşmesi” imzalanır. Bahse konu dokümanların boş halleri, hazırlanan teknik veya idari şartnameye eklenir.

11.1.2.3. İhaleyi kazanan firma ile sözleşmenin imzalanmasını takiben kurumdaki yetkili makam (Satın Alma Birimi ve/veya Kurum Bilgi Güvenliđi Yetkilisi) huzurunda “Kurumsal Gizlilik Sözleşmesi” imzalanır.

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

11.1.2.5. Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, “Personel Gizlilik Sözleşmeleri” idareye teslim edildikten sonra tanımlanır.

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

11.1.3. Kamu kurum ve kuruluşlarınca temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediđine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınır.

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

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

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

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

11.1.3.5. Bilgi güvenliđi olay müdahale prosedürleri (özellikle olay bildirim ve olay müdahalesinde işbirliđi kuralları).

11.1.4. “Kurumsal Gizlilik Sözleşmesi” ve “Personel Gizlilik Sözleşmesi” olarak SBSGM tarafından kullanılan ve örneđi Kılavuz’un ekinde yer alan sözleşmeler kullanılabilir. Bahse konu sözleşmelerin içeriđi, satın almaya konu mal veya hizmetin türüne ve kurumun kendine övgü ihtiyaçlarına bađlı olarak revize edilip kullanılabilir.

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

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

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

11.1.8. Tedarikçinin çalıştırılacağı personelin adli sicil kayıtlarını sorgulayıp, bunları idareye bildirmesi istenir. Projelerde çalışacak personelin; TCK’nın 53’ncü maddesinde belirtilen süreler geçmiş olsa bile devletin güvenliđine 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 olmaması gerekir.

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

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

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

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

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

11.2. SBYS Firmaları ile İlişkilerde Dikkat Edilecek Hususlar

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

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

11.2.3. Taşra birimleri tarafından gerçekleştirilecek SBYS alımlarında, SBSGM tarafından yayımlanan Hastane Bilgi Yönetim Sistemi Alım Kılavuz'unda belirtilen esaslar çerçevesinde hareket edilir.

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

11.2.5. SBYS yazılımları, sađlık kuruluşları içerisindeki entegre edilebilir cihazlar, sistemler ve Bakanlıđın tanımladıđı ve yürüttüğü uygulamalarla uyum sađlamak zorundadır.

11.2.6. SBYS yazılım üreticileri, Bakanlık Kayıt Tescil Sistemine (KTS) kayıt olarak akredite olurlar. Üreticilerin KTS'ye kayıt olabilmesi için istenilen sertifikalar ve belgeler ilgili mevzuatta belirtilmiştir.

11.2.7. Bakanlık tarafından istenilen sertifika ve belgeleri teslim eden SBYS yazılım üreticileriyle, KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesi imzalanır ve üretici firma KTS'ye kaydedilir.

11.2.8. KTS'ye kayıt olan SBYS yazılım üreticileri Bakanlık tarafından yayımlanan sađlık bilişimi standartlarına uygunluk açısından denetlenir.

11.2.9. Sađlık bilişimi standartlarına ve ilgili mevzuatlara uyumlu olmayan; bilgi, belge, sertifika ve doküman eksiđi olan SBYS yazılım üreticileri, KTS web sayfasında pasif listeye alınır. Eksiđi olmayan SBYS yazılım üreticileri ise aktif listede yer alır.

11.2.10. İlgili mevzuat kapsamında SBYS yazılım üreticilerine eksikliklerini gidermeleri için süre verilir. Bu süre içerisinde eksikliklerini gideren SBYS yazılım üreticileri aktif listeye alınır.

11.2.11. Kullanılmasına karar verilen sađlık bilişimi standartları ve veri gönderiminde dikkat edilecek hususlar SBSGM web sayfasında yayımlanır ve güncellenir.

11.2.12. Sađlık hizmeti sunucularınca SBYS yazılım üreticilerinden, ürettiđi SBYS yazılımının minimum şartlara uyum sađladığını gösteren “KTS Kayıt Belgesi” istenir. KTS kayıt belgesinin geçerliliđi KTS web sayfası üzerinden sorgulanır.

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

11.2.14. Sađlık kuruluşları ile SBYS yazılım üreticisi arasında yaşanabilecek uyuşmazlıklarda uygulanacak cezai şartların SBYS yazılım üreticisi ile yapılacak sözleşmelerde yer alması sađlanır.

11.2.15. Sađlık kuruluşları ve aile hekimleri, SBYS yazılım üreticisi ve bayileriyle ayrıca gizlilik sözleşmesi imzalamalıdır. Sađlık tesisleri ve aile hekimleri bu maksatla KLVZ-EK-13 Kurumsal Gizlilik Taahhütnamesini kullanabilecekleri gibi kendileri de sözleşme metinlerini oluşturabilirler.

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

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

11.2.18. 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.

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

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

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

11.2.22. Kişisel sağlık verileri özel nitelikli kişisel veriler kapsamında olması sebebiyle; sözleşme süresince veya sonrasında kayıtlı tüm veriler hiçbir surette, hiçbir zaman SBYS üreticisinde kalmak üzere kopyalanamaz, çıktı alınamaz, firma sunucularına aktarılamaz, ifşa edilemez.

11.2.23. SBYS yazılımları tüm sistem genelindeki kullanıcı, işlem ve bilgi düzeylerinde bilgi gizliliđini ve güvenliđini sağlamak zorundadır. Her kullanıcının gerektiğinde deđiştirilebilir kişisel bir parolası olmalıdır. Bu parola ile farklı bir lokasyonda oturum açıldıđında ilk oturum otomatik olarak kapatılmalıdır. Bir kişiye ait parolanın birden çok kişi tarafından kullanılmasına izin verilmemelidir.

11.2.24. Çeşitli yetki düzeyleri ve grupları tanımlanabilmeli, yetki deđişimi SBYS Yöneticisi tarafından yapılabilmelidir. Verilere erişim bu tanımlamalar çerçevesinde yapılmalıdır.

11.2.25. SBYS'de kullanıcılar için saat bazında sisteme giriş sınırlandırması yapılabilmelidir.

11.2.26. SBYS’de kullanıcıların otomasyona giriş-çıkış zamanları ve geçersiz giriş denemeleri istenildiğinde raporlanabilmelidir.

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

11.2.28. SBYS yazılımlarında Kılavuz’un 6.3 (Parola Güvenliđi) maddesinde belirtilen parola özellikleri tanımlanabilmeli ve bu kurala uymayan parolalar kabul edilmemelidir.

11.2.29. Sağlık kuruluşu ile ilişkisi kalıcı olarak kesilen tüm personelin SBYS erişim yetkisi tamamen ve otomatik olarak iptal edilmelidir.

11.2.30. Geçici olarak sağlık kuruluşunda bulunmayan (izin, rapor, geçici görev kurs, eğitim vb.) personelin SBYS’ye girişi otomatik olarak engellenmelidir.

11.2.31. Sunucu işletim sistemi, sunucu yazılımları, veri tabanında yapılacak yapısal değişiklikler gibi tüm sistemi etkileyen güncellemeler mesai saatleri dışında veya hasta yoğunluğunun en az olduđu saatlerde yapılmalıdır. Acil müdahale edilmesi gereken bir arıza durumunda ise mesai saatleri içinde güncelleme yapılabilir.

12. BİLGİ GÜVENLİĐİ İHLAL OLAYI YÖNETİMİ

12.1. İhlal Bildirimi ve Olay Yönetimi

12.1.1. Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, deđişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumları bilgi güveni ihlali olarak tanımlanabilir. Bakanlık çalışanları ve vatandaşlar tarafından tespit edilen Sağlık Bakanlığı ile ilgili her türlü bilgi güvenliği ihlal olayı <https://bilgiguvenligi.saglik.gov.tr/> adresinde yer alan merkezi ihlal bildirim sistemine girilir.

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

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

12.1.4. Merkezi ihlal bildirim sistemine girilen olaylar, SBSGM ekipleri tarafından ön deđerlendirmeye 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-18 Olay Bildirim ve Müdahale Formunun 1'inci Bölümünü (Olay Bildirimi) doldurur ve kurumsal ihlal bildirim hafızası oluşturmak üzere saklar.

12.1.5. Küçük çaplı, yalnızca kendi kurumunu ilgilendiren ve bilgi güvenliği yetkilisi ya da kurumsal SOME tarafından kendi imkânları ile yerel olarak çözülebilecek olaylara kurumun SOME'si veya bilgi işlem personeli tarafından gerekli müdahale yapılır. Müdahale sonrasında KLVZ-EK-18'in 2'nci Bölümü (Olay Müdahale) doldurularak e-Posta ile bilgiguvenligi@saglik.gov.tr adresine gönderir.

12.1.6. Hizmet verdiği kurumla birlikte diđer 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 istediđi durumlarda Sektörel SOME'den görüş/destek alır. Olayın çözümünde KLVZ-EK-18'in 2'nci Bölümünü (Olay Müdahale) doldurarak bilgiguvenligi@saglik.gov.tr adresine gönderir.

12.1.7. Yaşanılan olayın Sağlık Bakanlığı, diđer 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-18'in 2'nci Bölümü (Olay Müdahale) doldurularak kayıt altına alınır.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12.1.9.15. Kişisel Bilgilerin Kötüye Kullanımı: Kişisel verilerin işlenmesine ilişkin süreçlerde 6698 sayılı Kanun'da 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.

12.2. Kanıt Toplama

12.2.1. Delillerin değişmesini, bozulmasını önlemek ve delilleri korumak amacıyla olay yerinin güvenliği sağlanır. Olay yerine girişler kontrol altına alınır. Yetkisiz girişlere izin verilmez. Olay yerinden çıkış yapan kişilerin üzerinde adli delil oluşturabilecek materyal olup olmadığı kontrol edilir.

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

12.2.3. Delil niteliđi taşıyan tüm materyaller açıklayıcı bilgi içerecek şekilde etiketlenir. Bilgisayara bađlı tüm bađlantılar, bađlantı noktasını gösterecek şekilde etiketlenir ve sistem bađlı olduğundan ayrılmaz.

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

12.2.5. Olay yerindeki bilgisayar kapalı ise kesinlikle açılmaz.

12.2.6. Bilgisayar açık ise ekranının fotoğrafı çekilir ve üzerinde çalışan programlar kayıt altına alınır. Bilgisayarın sistem tarih ve zaman bilgileri ve inceleme esnasındaki gerçek tarih ve zaman bilgisi kaydedilir. Yapılan işlemlerde, her aşamada ayrı ayrı kayıt tutulur. İşlemlerin kimin tarafından yapıldığı ve kullanılan yazılım ve donanım bilgileri kayıt altına alınır.

12.2.7. Deđişme olasılıđı yüksek olan dijital deliller, öncelikli olarak ele alınır. Bilgisayarın kapatılması veya yeniden başlatılması uçucu delillerin kaybolmasına sebep olacaktır. Bu nedenle veri kayıt işlemlerine, bellek ve ön bellekte bulunan uçucu verilerin kopyalanması ile başlanır. Bu işlem yapılmadan hiçbir şekilde bilgisayarın kapatılmaması gerekir.

12.2.8. Bilgisayar kapatıldığında, sistem yapılandırma dosyaları ve geçici dosya sistemleri deđişebilir. Bilgisayarın kapatılması delil bütünlüğünü bozar ve delili deđiştirebilir. Olay yerindeki kapalı bir bilgisayarı açmak da yine aynı şekilde delillere zarar verebilir. Delillerin zarar görmemesi için veri toplama ve kayıt işlemlerinin ilgili teknik uzmanlar tarafından “canlı analiz” şeklinde yapılması gerekir.

12.2.9. Bilgisayarın dijital imza (hash) değeri alınır. İmajların gizliliđi, erişilebilirliđi ve bütünlüğü sađlanır. 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 tutanađa yazılır.

12.2.10. Yedeklenecek diskin hafızası şüpheli bilgisayar diskinden büyük olur.

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

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

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

12.2.14. Doğruluđu ve güvenilirliđi kabul edilmiş yazılım ve donanımlar kullanılır.

13. İŐ SÜREKLİLİĐİ YÖNETİMİ

13.1. İŐ Sürekliliđi Genel YaklaŐımı

13.1.1. İŐ sürekliliđi; kurumun vermekte olduđu kritik biliŐim hizmetlerinin sunumuna kesintisiz bir Őekilde devam etmesi veya türü ve nedeni ne olursa olsun, herhangi bir kesinti ya da olay durumunda, önceden belirlenmiŐ kritik İŐ süreçlerini, önceden tanımlanmıŐ kabul edilebilir seviyede sunma yeteneđini sađlayan yöntemdir. Kurum İŐ süreçlerinde hizmet sürekliliđi yeteneđini; etkin bir risk yönetimi, öncelikli hizmetlerini kesintiye uğratabilecek olayların tanımlanması, bu olayların bertaraf edilmesi için gerekli tedbirlerin alınması, olay anında ve sonrasında kritik hizmetlerin en hızlı ve etkin nasıl ayađa kaldırılacađının senaryolarla planlanması ve bu senaryoların tatbikatlarla test edilmesi ile elde eder.

13.1.2. Bu bölümde anlatılan İŐ sürekliliđi, bilgi varlıklarının İŐ sürekliliđinin sađlanmasına yönelik tedbirleri kapsamaktadır. YaŐanacak her türlü afet ve acil durumda sunulan hizmetlerin sürdürülebilir olması, fiziksel ve fonksiyonel olarak afet ve acil durumlara hazırlıklı olunması, zamanında, hızlı ve etkili müdahalede bulunularak en kısa sürede olađan İŐleyiŐe dönülmesi için alınması gereken tedbirler ve yapılması gereken çalıŐmalar “Hastane Afet ve Acil Durum Planı (HAP) Hazırlama Kılavuzu”nda ayrıntılı olarak anlatılmıŐ, örnek planlar verilmiŐtir.

13.1.3. İŐ sürekliliđi kurma nedenleri; hizmet sürekliliđini sađlamak ve kesintilere yeterli Őekilde yanıt verme kabiliyetini kazanmak olabileceđi gibi yasa, yönetmelik ve sözleşmelerden kaynaklanan sorumlulukları yerine getirmek de olabilir.

13.1.4. Etkin bir bilgi güvenliđi İŐ sürekliliđi sistemi kurulduđunda kurumun Őu çıktıları elde etmesi beklenir;

- Kritik süreç ve varlıkların hizmet sürekliliđinin sađlanması,
- Dokümanite edilmiŐ ve tatbikatlarla test edilmiŐ bir olay/kriz yönetim kabiliyeti,
- Hizmet verdiđi ve/veya yükümlü olduđu paydaŐlarının gereksinimlerini anlamıŐ ve bu gereksinimlere cevap verecek İŐ süreçlerinin kurulmuŐ olması.

13.1.5. Kritik İŐ sürekliliđi yönetimi sadece İŐ sürekliliđi planı hazırlanması, yedekleme yapılması, felaket merkezi oluŐturulması, prosedürler, detaylı talimatlar oluŐturulması deđil; bunların bütünlüŐik olarak hizmet sürekliliđinin iyileŐtirilmesi amacıyla uygulanmasıdır.

13.1.6. İş sürekliliđi planları, verilen hizmetleri önceliklendirme, olası tehdit ve zafiyetleri deđerlendirenerek gerekli önlemleri almak suretiyle hizmet sürekliliđini sađlama, hizmetlerin kesintiye uğramasına neden olan olaylara önceden tanımlanmış senaryolarla müdahale etme, süreçleri onarma ve planlı olarak yeniden başlatma konularında kılavuzluk yapan dokümanite prosedürlerdir.

13.1.7. İş sürekliliđi planları, felaket kurtarma çözümleri deđil, felaketin olumsuz sonuçlarının oluşmasını önlemeye odaklanan eylem planlarıdır. Felaket kurtarma senaryoları iş sürekliliđi planlarının bir parçasıdır. Felaket kurtarma çözümleri, felaket sonrasında verilerin kurtarılmasına odaklanırken, iş sürekliliđi çözümleri, hem verilerin erişilebilirliğini gözetir hem de kurumun felaket sonrasında en hızlı şekilde yeniden hizmet verebilmesine odaklanır.

13.2. İş Sürekliliđi Adımları

13.2.1. Kurumsal iş sürekliliđi yönetim sisteminin kurulması ve işletilmesi için öncelikle iş sürekliliđi kapsamının belirlenmesi gerekir. Bunun için ilk adım kritik iş süreçlerinin çıkarılması ve önceliklendirilmesidir. İş sürekliliđi kapsamı bu şekilde oluşturulur.

13.2.2. Kapsam belirlendikten sonra bu iş süreçlerine ilişkin mevcut durum analizi yapılır. Mevcut durum analizinde kurumun kritik iş süreçlerinin fotoğrafı çekilir. Yürütölen bu hizmetleri kesintiye uğratabilecek tehditler var mı, bu tehditlerle ilgili süreçte zayıf noktalar var mı gibi hususlar incelenir ve detaylı analiz edilir. Başarılı bir mevcut durum analizi için kurumsal risk yönetimi sürecinin kurum kültürü olarak benimsenmiş, risk haritaları çıkarılmış ve kurumsal kabul edilebilir risk seviyesi belirlenmiş olmalıdır.

13.2.3. İş sürekliliđinin kapsamının belirlenip, mevcut durum analizi yapıldıktan sonra, hangi iş sürecinin kesintisiz hizmet verebilmesi için hangi kaynaklara ihtiyaç olduđunun dokümanite edilmesi ile kaynak planlaması ortaya koyulur.

13.2.4. Her başarılı süreç yönetiminde olması gerektiđi gibi iş sürekliliđi süreci için roller ve sorumluluklar atanır.

13.2.5. Atanmış olan sorumlular tarafından hizmetleri kesintiye uğratabilecek olumsuz senaryolar tatbikatlarla test edilir, sonuçlar deđerlendirilir, varsa aksaklıklar giderilir ve sürekli takip edilir.

13.2.6. Kritik Varlıkların / Süreçlerin Tanımlanması

13.2.6.1. Kurum tarafından gerçekleştirilen tüm iş süreçleri önemli kabul edilirken, bir olay meydana gelmesi durumunda, kurum mevcudiyeti ve itibarı açısından

kritik önem taşıyan süreçlerin ayađa kaldırılmasına öncelik verilir. İş sürekliliđi yönetimi için öncelikle kritik iş süreçlerinin ve bu süreçlerde kullanılan sistemlerin belirlenmesi ve listesinin oluşturulması gerekir.

13.2.6.2. Yürütölen iş, işlem ve sürecin kritik olabilmesi için aşıđıda belirlenen durumlardan en az birine uygun olması gerekir;

13.2.6.2.1. İş sürecinin kesintiye uğraması ya da yavaşlaması durumunda kurum için yasal, finansal, operasyonel ve benzeri büyük riskler oluşur.

13.2.6.2.2. İş sürecinin etkilediđi ya da etkilendiđi sistem ya da paydaşlar, stratejik olarak önemli ya da geniş kitlelerdir.

13.2.6.2.3. İş süreci insan hayatını ya da toplum sađlığını etkilemektedir.

13.2.6.2.4. İş sürecinin kesintiye uğraması kurumsal itibarı maddi ya da manevi olumsuz bir şekilde etkileyecek niteliktedir. (Örneđin SBYS'ler)

13.2.6.3. Kritik varlıklar / süreçler belirlenirken;

13.2.6.3.1. Süreç ile ilgili iç ve dış yükümlölükler,

13.2.6.3.2. Süreçten yararlanan / hizmet alan paydaşların hizmet sürekliliđi ihtiyaçları,

13.2.6.3.3. Yasal ve düzenleme amaçlı atanan sorumluluklar,

13.2.6.3.4. Protokollerle anlaşmaya varılmış hizmet zorunlulukları,

13.2.6.3.5. Hizmetin sürdürölmesinde başarısız olunması durumunda sonuçlarının ne büyüklükte olacağı gibi hususlar dikkate alınarak KLVZ-EK-19 İş Sürekliliđi Formları arasında yer alan "Kritik Süreçler / Varlıklar Listesi" oluşturulur ve iş sürekliliđi kapsamı belirlenir.

13.2.6.4. Kritik iş süreçlerinin tanımlanmasında yararlanılacak ve kritik süreçler / varlıklar listesi ile ilişkilendirilecek dokümanlar;

13.2.6.4.1. Varsa hizmet bekleyen ve yasal yükümlölüklerle bađlı olunan dış paydaşlarla yapılan protokollerin listesi,

13.2.6.4.2. Tedarikçiler ile yapılan sözleşmeler,

13.2.6.4.3. Kurumdan beklenen kritik hizmetlerin sađlanmasını destekleyen tüm iş süreçlerinin / faaliyetlerin envanteridir.

13.2.7. Mevcut Durum Analizi

13.2.7.1. Kritik iş süreçlerinin sürekliliđinin sađlanmasına ilişkin gerekli olan koşulların ortaya koyulduđu ve iş sürekliliđine engel olabilecek olası tehditlerin tespit edildiđi aşamadır.

13.2.7.2. İş etki analizleri ve risk işleme çalışmalarının deđerlendirilmesi ile mevcut durum ortaya koyulur.

13.2.7.3. İş etki analizi, iş kesintisine neden olabilecek durumlar ve bunların etkilerinin deđerlendirilmesidir. Kesintiye neden olabilecek durumlar, darboğazlar, zafiyetler göz önüne alınarak süreçlerin kapsamlı bir fotoğrafı çekilir, sınıflandırılır (az önemliden en önemliye dođru sıralanır) ve buna yönelik olarak risk işleme çalışmaları yapılır.

13.2.7.4. İş sürekliliđinin temelinde risk yönetimi vardır. İş etki analizinden edinilen bilgilere göre kesintiye yol açabilecek olayların riskleri tanımlanır. Risk yönetimi, iş etki analizleri ile ilişkilendirilmiş risk deđerlendirme raporunun hazırlanması vb. süreçler Kılavuz'un 5.3 (Risk Yönetimi) maddesinde açıklanmıştır. İş sürekliliđi için planlama yapılırken kurumsal risk yönetimi dikkate alınır.

13.2.7.5. İş etki analizleri ve risk deđerlendirme çalışmaları neticesinde; kritik iş süreçlerine yönelik tehditler, zafiyetler, olasılıklar ve alınacak önlemler ile mevcut durum analizi ortaya koyulur.

13.2.8. Kaynak Planlaması

13.2.8.1. Kritik iş süreçlerinin en temel fonksiyonlarının, en az veri kaybı ile en kısa sürede tekrar hizmet verebilir duruma getirilmesinin sađlanması için hangi kaynaklara ne kadar ihtiyaç duyulduđunun ve bu kaynakların maliyetinin çıkarılması gerekir.

13.2.8.2. Kaynak planlaması yapılırken o işin sürekliliđinin sađlanması için ihtiyaç duyulan tüm mali kaynaklar, teknoloji, alt yapı, tedarik edilecek malzemeler, bina, ulaşım ve benzeri kaynak tipleri ve tanımlanmış yetkinlikleri ile beraber personel detaylı olarak belirlenir ve KLVZ-EK-19 İş Sürekliliđi Formları içinde örneđi yer alan "Kaynak İhtiyaç Listesi" oluşturulur.

13.2.8.3. İş sürekliliđi kaynak ihtiyaç listesi, 24 saat – 72 saat – 1 hafta gibi iş kurtarma fazları için ayrı ayrı detaylı olarak oluşturulabilir. 24 saat fazında en

temel ihtiyalar planlanırken, devam eden fazlarda daha detaylı ihtiya duyulacak kaynaklar belirtilebilir.

13.2.8.4. Kaynak planlarken kriz yönetim merkezi olarak kullanılabilir 7X24 kullanıma uygun, internet bağlantısı, telefon/mobil telefon, taşınabilir bilgisayar, projeksiyon cihazı, yazı tahtası, muhtelif kırtasiye donanım ve imkanlarının hazır bulunduđu kriz yönetim merkezinin de belirlenerek kararının alınması gerekir.

13.2.9. Roller ve Sorumluluklar

İş sürekliliđi süreçlerinin standartlara uygun ve etkin şekilde işletilebilmesi için oluşturulması gereken organizasyon yapısı ve roller Şekil 3'te açıklanmıştır.

13.2.9.1. Üst Yönetim;

13.2.9.1.1. Üst Yönetim kritik iş süreçlerinin sürekliliđinin sağlanmasından birinci derecede sorumludur.

13.2.9.1.2. Bilgi güvenliđi alt komisyonu tarafından belirlenen iş sürekliliđi hedeflerini onaylar. (Örnek iş sürekliliđi hedefi: X faaliyetlerinin Y zamanda ayađa kaldırılması, X faaliyeti felaket senaryosunun Y kez tatbikatlar ile test edilmesi vb.)

13.2.9.1.3. İş sürekliliđinde yer alacak personelin görev yetki ve sorumluluklarını belirler.

13.2.9.1.4. Kritik iş süreçlerinin, iş sürekliliđi gereksinimlerini ve iş ihtiyalarını belirler veya görevlendirmiş olduđu personel tarafından belirlenmesini sağlar.

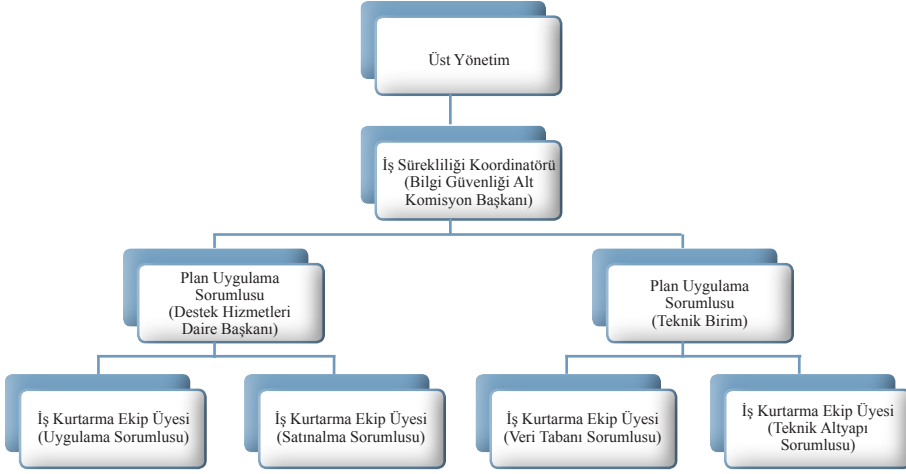
13.2.9.1.5. Belirlenen kaynakların sağlanmasını taahhüt eder.

13.2.9.1.6. İş sürekliliđinin sağlanması için sürekli test ve tatbikatları destekler ve bunun için gerekli faaliyetlerin gerçekleştirilmesini sağlar ve kontrol eder.

13.2.9.1.7. İş sürekliliđi hedeflerini, rol ve sorumlulukları, iş sürekliliđi taahhüdünün bulunduđu iş sürekliliđi politikasını oluşturur ve yayımlar.

13.2.9.2. İş Sürekliliđi Koordinatörü;

13.2.9.2.1. Bilgi güvenliđi alt komisyonu başkanı aynı zamanda kurumun iş sürekliliđi koordinatörü olarak görev yapar.



Şekil 3: İş Sürekliliği Organizasyonu

13.2.9.2.2. Felaket ya da kesintiye neden olan büyük çaplı olayların nasıl yönetileceği ve verilen hizmet ve faaliyetlerin belirlenen sürelerde nasıl geri döndürüleceğini tanımlayan İş Sürekliliği Planlarının oluşturulmasından ve işletilmesinden sorumludur.

13.2.9.2.3. Kurumun bağlı olduğu güncel mevzuat, yasa, yönetmelik ve sözleşmelerden doğan yaptırım ve yükümlülükleri takip ederek İş Sürekliliği Planlarının güncellenmesini sağlar.

13.2.9.2.4. İş sürekliliği planlarının test edilmesi için tatbikatlar düzenler, kayıt altına alınmasını sağlar.

13.2.9.2.5. İş sürekliliğini etkileyecek ya da iş sürekliliğinden etkilenebilecek taraflarla iletişimi sağlar.

13.2.9.2.6. İş sürekliliğinin sağlanabilmesi için plan uygulama sorumluları ve iş kurtarma ekiplerinin görev dağılımını belirler ve ekiplerin yetkinliğini arttırmak amacıyla iş sürekliliği eğitimlerini planlar.

13.2.9.2.7. Planın devreye alınması ve hasar onarımı sonrası normal çalışma durumuna geri dönülmesi kararlarını verir.

13.2.9.3. Plan Uygulama Sorumluları:

13.2.9.3.1. Kurum organizasyon şemasındaki ilgili yöneticiler ve onların atadıkları sorumlulardan oluşur.

13.2.9.3.2. Planın uygulanmasında, İş Sürekliliđi Koordinatörü tarafından verilen görevlerin gerçekleştirilmesinden sorumludur.

13.2.9.3.3. Acil ve beklenmedik bir durumla karşılaşıldığında kendisine bađlı personeli koordine eder. İş sürekliliđi koordinatörüne bilgi akışını sağlar.

13.2.9.3.4. İş sürekliliđi planının uygulanması için ilgili iş sürecinden sorumlu olan personel ve yedeklerinin yer aldığı iş kurtarma ekiplerini oluşturur.

13.2.9.3.5. Yedekten geri dönme işlemleri, ađ konfigürasyonunun restorasyonu, iş uygulamalarının sunucular üzerine kurulum ve konfigürasyonu gibi süreçlerin gerçekleştirilmesinden sorumludur.

13.2.9.4. İş Kurtarma Ekipleri

13.2.9.4.1. Plan uygulama sorumlularının vermiş olduđu işlerden sorumludur.

13.2.9.5. Genel Sorumluluklar;

13.2.9.5.1. Hizmetlerin erişilebilirliđinin sağlanması için planlamalar dođru bir şekilde yapılır.

13.2.9.5.2. Hizmetlerin erişilebilirlik ve sınıflandırma ile ilgili gereksinimleri hizmet sahipleri tarafından belirlenir.

13.2.9.5.3. Kritik iş süreçlerinde yer alan personel, iş sürekliliđi planlarında belirtilen görevleri yerine getirmekle ve iş süreklilik tatbikatlarına katılmakla sorumludur.

13.3. İş Sürekliliđi Stratejisi Belirleme

13.3.1. İş sürekliliđi planları geliştirilirken; kritik hizmetleri sunan ve bu hizmetlerden faydalanan/faydalanan iç ve dış paydaşların ihtiyaç ve gereksinimleri, toplantı veya anket gibi çalışmalar ile analiz edilir. Analizler için KLVZ-EK-19 İş Sürekliliđi Formları içinde örneđi yer alan “Kritik Varlık/Süreç Analiz Formu” kullanılır. Anket veya toplantılardan elde edilecek sonuçlarda asgari olarak aşağıdaki soruların yanıtları elde edilmelidir;

13.3.1.1. İşin yürütülmesi için ihtiyaç duyulan yazılım, donanım ve diđer teknolojik bileşenler ve bilgi işlem araçları nelerdir? Ekipman ve sistem gereklilikleri nelerdir? (Bu aşamada “İş Sürekliliđi Kaynak İhtiyaç Listesi” kesinleştirilir)

13.3.1.2. Özel sözleşme ya da yasa ve mevzuatlara bađlı olarak yerine getirilmesi gereken minimum yükümlülükler nelerdir?

13.3.1.3. Sürecin çıktısı olan hizmetin kullanıcıları kimlerdir?

13.3.1.4. Hizmet sürekliliđinin sađlanması için bađımlı olunan hizmetler, iş sürekliliđini etkileyebilecek dâhili ve harici taraflar kimler/nelerdir? Sürecin iş sürekliliđinin sađlanması için hangi sistemlere sürekli erişim gereklidir?

13.3.1.5. Elektronik verilerin korunması nasıl sađlanmaktadır? Bu veriler korunamazsa nasıl sonuçlar ortaya çıkar? İlgili veriler sürekli erişim için gerekli midir?

13.3.1.6. Personelin temel yeterlilik seviyesi nedir? Herhangi bir felaket durumunda başka birimlerden/dış kaynaklardan personel alınması mümkün müdür? Mümkünse hangi birim ya da kaynaklarla iş birliđi yapılabilir?

13.3.2. Bu aşamada ayrıca iş sürekliliđine engel olabilecek felaket senaryoları oluşturulur ve bu senaryolara nasıl müdahale edileceđi yani kurtarma operasyonlarının (nerede yönetilecek, kim yönetecek ve kime raporlayacak) nasıl yönetileceđi belirlenir. Kurtarma öncelikleri ve kurtarma zaman hedefleri, müdahale eylem planları ve sorumluları KLVZ-EK-19 İş Sürekliliđi Formları içinde yer alan “İş Kurtarma Planı” örneğinde olduđu gibi detaylı olarak dokümanite edilir.

13.3.3. İş sürekliliđi planları; varlık envanteri, bilgi sınıflandırma, bilgi aktarımı, yedekleme, kapasite yönetimi, varlıkların kabul edilebilir kullanımı, risk yönetimi, yasal gereksinimler ve standartlara uyum, konfigürasyon ve deđişim yönetimi, fiziksel ve çevresel güvenlik gibi operasyonel faaliyetlerde kullanılan bilgi güvenliđi dokümanları göz önüne alınarak hazırlanmalıdır.

13.4. İş Sürekliliđi Planı Oluşturma

13.4.1. Bu bölümde řu ana kadar anlatılan tüm bilgiler; iş sürekliliđi planı oluşturulması için idarenin “hangi süreçler kritik, bu süreçlerin sürekliliđini sađlamak için yasa, mevzuat ve sözleşmelerden doğan zorunluluklar neler, iş sürekliliđini tehdit edebilecek unsurlar neler olabilir ve bu tehditleri bertaraf etmek için nasıl hazırlık yapılmalı” gibi durumları analiz ettiđi ve iş sürekliliđi planını desteklemek için dokümantasyon oluşturduđu süreçleri içerir.

13.4.2. İş sürekliliđi planları; kesinti anında bütün ihtiyaç duyulabilecek gereksinimlerin tanımlı olduđu ve ilgili tüm taraflar tarafından bilinen ve uygulanması sırasında karmařaya neden olmayacak řeklinde hazırlanır. İş sürekliliđi planları ařađıdaki içeriđe sahip olmalıdır;

- Amaç ve kapsam,
- İş sürekliliđi hedefleri,
- Planın hangi kořullarda hayata geçirileceđi,
- Olađanüstü durumda kurtarma çalıřmalarında kimlerin görev alacađı ve hangi kurtarma adımlarını gerçekleřtireceđi,
- Olađanüstü durumlarda, gerek organizasyon için gerekse organizasyon dıřında iletiřime geçilecek kiři ve kurumlar, aynı zamanda iletiřimin nasıl sađlanacađı bilgisi,
- İç ve dıř bađımlılıklar,
- Planın hayata geçirilmesi için gerekli olan kaynaklar,
- Tanımlanmıř iletiřim adımları.

13.4.3. İş sürekliliđi planının, dokümanede edilmiř tüm liste ve formların (kritik varlıklar/süreçler listesi, kaynak ihtiyaç listesi, acil durum iletiřim listesi, süreç analiz formu vb.) genel çerçevesini sunan tek bir ana doküman olarak hazırlanması, planın amacının, kapsamının ve hedeflerinin uygulayıcılar tarafından daha anlaşılır olmasını sađlar.

13.4.4. İş sürekliliđi planlarında;

13.4.4.1. İş sürekliliđi planında acil veya olađanüstü durumların neler olduđunun ve “çok acil, acil ve normal” seviyelerin neler olduđunun tanımlanmıř olması gerekir.

13.4.4.2. Herhangi bir olađanüstü durum anında iş sürekliliđi planında yazılı olan faaliyetleri gerçekleřtirecek olan kiřilerin rolleri, sorumlukları ve yetkileri önceden belirlenmiř ve tanımlı olmalıdır.

13.4.4.3. Yapılan olađanüstü durum tanımları uyarınca, iş sürekliliđi planının hangi kořullarda aktive edilmesi gerektiđi ve rol bazında yapılması gerekenlerin belirlenmiř olması gerekir.

13.4.4.4. Olađanüstü durumun sona ermesi sonrasında iş süreçlerinin olađanüstü durum öncesine dönmesi için yapılması gerekenlerin tanımlanması gerekir.

13.4.4.5. Olađanüstü durumun olađan alıřma ortamını kullanılamaz hale getirmesi durumunda alternatif alıřma lokasyonları ve kriz merkezi planlamasının yapılması gerekir.

13.4.4.6. İř sürekliliđi ekibinde bulunan alıřanların iletiřim bilgileri (telefon, e-Posta, adres), kendilerine ulařılmadıđı durumlarda alternatif olarak kullanılacak iletiřim bilgilerine nasıl ulařılacađının plana dâhil edilmesi gerekir.

13.4.4.7. Olađanüstü durum ile ilgili medya ve kamu bilgilendirmesinin nasıl yapılacađına iliřkin kurumsal iletiřim stratejisinin de planda yer alması gerekir.

13.4.5. Kritik iř sürekliliđi yönetimi, bütünleřik olarak hizmet sürekliliđinin iyileřtirilmesi amacıyla uygulanır. Bir yönetim sistemi mantıđı ile iřletilmesi gerekir. Bu nedenle bu süreç önceden hazırlanması ve sürekli gözden geirilmesi gereken bir takım dokümanlarla desteklenmelidir. İř sürekliliđi dokümanları;

13.4.5.1. Bilgi güvenliđi tehdit listesi ve ihlal olayları olay müdahale süreç dokümanları,

13.4.5.2. Kritik varlıklar / süreçler listesi,

13.4.5.3. Kaynak ihtiyaç listesi,

13.4.5.4. Kritik tedarikiler, acil durum ilk müdahale ekip üyeleri ve yedeklerinin yer aldıđı acil durum iletiřim listesi,

13.4.5.5. Uzmanlık, yetkinlikler ve tanımlanmıř sorumlulukları ile iř sürekliliđinin sađlanmasıyla ilgili sorumlu personel ve yedeđinin yer aldıđı iř telefonu, ev telefonu, cep telefonu, iř ve kiřisel e-Postası ve normal iletiřimin kullanılmayacađı durumlarda irtibat kurmanın yollarını ieren acil durum iletiřim listesi,

13.4.5.6. Felaket sonrası kritik faaliyetler iin kurtarma sırası (acil veya olađanüstü durum yönetimi (kurtarma), devam etme ve normale dnüş) ieren olay müdahale planları, tatbikat ve testlerin kayıtları,

13.4.5.7. Sistem kapasitesi ve eřik deđerlerin izlenme raporları,

13.4.5.8. Kritik hizmetin sürdürülmesine destek olan altyapı envanteri (donanım, yazılım, teknik ekipmanlar, sunucular, veri tabanları, internet vb.) ve yedekleme planları

13.4.5.9. Tatbikat test uygulama formu,

13.4.5.10. İş süreklilik planı sonrası yapılan deđerlendirme formu.

13.5. İş Sürekliliđi Planlarını Tatbikatlar ile Test Etme

13.5.1. Tatbikatlar öngörülen risklere karşı hazırlık seviyesinin ölçüldüğü aktivitelerdir. Kapsamlı bir hazırlık süreci gerektirir aksi halde ciddi kesintilerin yaşandıđı olumsuz durumlar ile karşılaşılabılır.

13.5.2. Tatbikat türleri maliyet, zaman, karmaşıklık, efor ve normal operasyonda oluşacak kesintiler açısından farklı özelliklere sahiptir.

13.5.3. Tatbikat türleri ve açıklamaları Tablo-1’de verilmiştir.

Tatbikat Türü	Tanım
Kavramsal tatbikat	İş sürekliliđi planı ve ilgili dokümantasyonun gözden geçirilmesidir.
Detaylı kavramsal tatbikat	Kavramsal tatbikatın daha detaylı olarak yerine getirilmesidir. Bu tatbikat türünde planda yer alan her adımın üzerinden geçilerek eksiklikler tespit edilmeye çalışılır.
Simülasyon	Bu tatbikat türünde örnek bir olay üzerinden iş sürekliliđi planı çalıştırılır. Tatbikat sırasında süreç veya sistemlerde herhangi bir kesinti gerçekleştirilmez. İş sürekliliđi planı kesinti gerçekleşmiş gibi düşünülerek çalıştırılır ve tatbikatı yapılır.
Bileşen veya servis tatbikatı	İş süreçlerinin bir kısmı için gerçekleştirilir. İş süreçlerinde kesintiye neden olabilecek bir olay gerçekleştirilir ve süreç tekrar çalışır hale getirilir. Bu tatbikat çalışan bir sistem üzerinde gerçekleştirildiđinden, kurumun acil durum tatbikatı kapsamında olmayan operasyonunu aksatmayacak biçimde planlanması gereklidir.
Tam tatbikat	İş sürekliliđi planının tamamının test edilmesidir. Tam tatbikat kurum süreçlerinin felaketten kurtarma merkezinde tekrar çalıştırılmasını da kapsayan detaylı bir tatbikattır.

Tablo 1. Tatbikat Türleri

13.5.4. İş sürekliliđi tatbikatları; tatbikata hazırlık, tatbikatın gerçekleştirilmesi ve tatbikatın deđerlendirmesi olmak üzere üç adımda gerçekleştirilir.

13.5.5. Tatbikata hazırlık: Varsa daha önce gerçekleştirilen tatbikat planları ve sonuçları incelenir. Tatbikat zamanı, senaryosu, deđerlendirme ölçütleri ortaya koyulur. Tatbikat riskleri deđerlendirilir ve tatbikat programı yapılır. KLVZ-EK-19 İş Sürekliliđi Formları içinde yer alan Tatbikat Test Uygulama Formu, yapılacak tatbikata özđu ihtiyaçlara göre özelleştirilmek suretiyle kullanılabilir.

13.5.6. Tatbikatın gerçekleştirilmesi: Tatbikatlar bir önceki adımda hazırlanan plana uygun olarak icra edilir. Tatbikat kanıtları kayıt altına alınır. Tatbikatın bitmesi sonrasında ilgili taraflar ve katılımcılar bilgilendirilir.

13.5.7. Tatbikatın deđerlendirilmesi: Tatbikat bulguları incelenerek tatbikat deđerlendirme raporu hazırlanır. Varsa yaşanan sıkıntılar, iş sürekliliđinde görev alan personelin performansı, kullanılan kaynak ve ortamın yeterliliđi gibi hususlar raporda belirtilir.

13.5.8. Sürekli iyileştirmenin sağlanması için planlar belirli sıklıkla tatbikatlar ile test edilir. Planların test edilme sıklığı planlarda belirtilmelidir.

13.5.9. Tatbikatlardan elde edilen bulgular, kurumların bilgi güvenliđi dokümantasyonuna ve bir sonraki eğitime dâhil edilir.

1.13.5.10. Tatbikat sonuçlarına göre planlar tekrar gözden geçirilir, gerekiyorsa düzeltici faaliyet planlanır, ihlal olayları müdahale süreçleri ve risk çalışmalarına yansımaları deđerlendirilir.

14. UYUM

14.1. Yasal Gereksinimlere Uyum

14.1.1. İdarenin kanuniliđi ilkesi, hukuk devletinin temel ilkelerindedir. Bu ilke geređince idarenin iř ve iřlemleri bir kanuna dayanmalı, aynı zamanda bu iř ve iřlemler kanunlara aykırı olmamalıdır. Yani kanunlar, idarenin faaliyette bulunabilmesinin hem řartı, hem de sınırı durumundadır. Burada “kanunlar” ifadesinden salt TBMM tarafından ıkarılan kanunları deđil normlar hiyerarřisi geređi “anayasa, uluslararası szleřmeler, kanun, kanun hkmnde kararname, tzk, ynetmelik, ynerge/genelge ve idare tarafından ıkarılan diđer yazılı talimatları anlamak gerekir.

14.1.2. İdarenin kanuniliđi ilkesi geređi, Bakanlıđımız merkez teřkilatı ve bađlı kuruluşlar tarafından yapılacak her trl iř ve iřlemin kanuni bir dayanađının bulunması, bu iř ve iřlemlerin mevzuata aykırı olmaması ve kanunlarca zorunlu tutulan konuların yerine getirilmesi iin gerekli tedbirlerin alınması; zetle yasal gereksinimlere uyum sađlanması gerekmektedir.

14.1.3. İdare iin makul gvenlik tedbirlerinin alınması, yalnızca siber olaylara iliřkin tedbirlerin alınması olarak algılanmamalıdır. Yasal ykmllkleri ihmal ya da ihlal davaları, cezalar veya olumsuz medya haberlerinin de kurumsal imajı ya da deđerleri siber olaylarla aynı oranda tehdit edebileceđi gz nnde bulundurulmalıdır.

14.1.4. İdare, ilgili tm kanuni yasal, dzenleyici, szleřmeye dayalı řartlar ve bu gereksinimleri karřılama yaklařımını aık tanımlamak, yasal dzenlemelerin gerekliliklerine uyum iin talimat ya da prosedrleri yayımlamak ve gncel tutmakla sorumludur.

14.1.5. Yasal gereksinimler; bilgi teknolojileri ile ilgili gvenlik gereksinimleri, fikri mlkiyet hakları / telif hakları yasaları, gizlilik, veri řifreleme ve verileri koruma yasaları řeklinde olabilir. Yasa ve ynetmeliklerin takip edildiđinden emin olmak iin ncelikle tm uyum gerektiren dzenlenmelerin yer aldıđı bir liste oluřturulmalıdır. rnek liste KLVZ-EK-20 Yasal Mevzuat Uyumunu İin Takip Listesinde yer almaktadır.

14.1.6. Kanunlar ve ynetmelikler, gvenlikle ilgili olayların sıklıđı ve etkisinin byklđ, geliřen teknoloji ve ihtiyalara bađlı olarak deđiřebilen yařayan varlıklardır. Siber suların Trk Ceza Kanunu'nda ilk yer alıřı 6 Haziran 1991 tarihli 3756 Sayılı Trk Ceza Kanunu'nun bazı maddelerinin deđiřtirilmesine dair Kanun ile olmuřtur. Bu deđiřikliđin 20. maddesi ile “Biliřim Alanında Sular” bařlıđı altında bir blm eklenmiř ve bir bilgisayar programların, verilerin

veya diđer unsurların hukuka aykırı olarak ele geerilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çođaltılması 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 ettiđi 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 güvenliđi birimlerinin işi olarak deđerlendirilmemeli, hukuk, insan kaynakları, idari mali işler gibi birimlerden de destek alınması gerekmektedir.

14.1.7. Hangi şartların kurumu etkileyebileceđinin belirlenmesinin ardından geçerli güvenlik önlemlerinin uyumluluk için yeterli olup olmadıđının veya gereksinimleri karşılamak için ek önlemlerin alınması gerekir. Örneđin, 5651 sayılı Kanun uyarınca, Bilgi Teknolojileri Kurumu (BTK) her kurum için bazı yükümlülükler getirmiştir. Bu yükümlülüklerden biri de zaman ve tarih mührü ile erişim iz kayıtlarının tutulmasıdır. İdare ilgili yasa geređi; öncelikle yükümlülüklerini anlamalı, uygulamakta olduđu bir iz kayıt yöntemi varsa yasanın gerekliliklerini karşılayıp karşılamadıđını kontrol etmeli ve eđer gerekiyorsa ek önlemler almalıdır.

14.2. Lisanslama ve Fikri Mülkiyet Hakları

14.2.1. Fikri mülkiyet insan zekâsının, entellektüel birikiminin, zihinsel yaratıcılıđının ortaya çıkarmış olduđu müzikten, edebiyata, endüstriyel tasarımlardan bilimsel buluşlara kadar uzanan geniş bir yelpaze içinde yer alan ürünleri kapsar. Bu ürünler düşünce safhasında kaldıđı ve üreticisi dışındakilerle paylaşılmadıđı sürece korumaya konu olmazlar. Ancak bu düşüncelerin ve ürünlerin, uygun şekilde kayıt altına alınmalarını takiben diđer kişilerle paylaşımaları ve özellikle bu ürünlerin kazanç amacıyla ticarete konu olmaları söz konusu olduđu zaman korunmaları gerekir.

14.2.2. Fikri mülkiyet, sınai mülkiyet hakları ve telif hakları olmak üzere iki ana başlık altında incelenir.

14.2.3. Sınai mülkiyet hakları; teknolojik buluşlar, patentler, mal ve hizmetlerin ticari markaları, modeller, endüstriyel tasarımları ve cođrafi işaretleri kapsar. Bu haklar 6769 Sayılı Sınai Mülkiyet Kanunu ile korunur. Tescil işlemleri, Türk Patent ve Marka Kurumu tarafından koordine edilir.

14.2.4. Telif hakları; edebiyat, müzik, sanat ürünleri ve görsel-işitsel ürünler, filmler, bilgisayar program ve yazılımlarını ortaya çıkaran kişilerin bu ürünler üzerindeki haklarını içerir. Bu haklar 5846 sayılı Fikir ve Sanat Eserleri Kanunu ile korunur. Konu ile ilgili faaliyetler, T.C. Kültür ve Turizm Bakanlığı Telif Hakları Genel Müdürlüđu tarafından yürütülür.

14.2.5. Bakanlıđımıza bađlı tm birimlerce yapılan her trl iř ve iřlemlerde, fikri mlkiyet haklarına saygılı davranılır. Bu hakların korunması iin gerekli tedbirler alınır.

14.2.6. Lisanslı yazılım kullanımı ile ilgili hususlarda Bařbakanlık'ın 2008/17 sayılı Genelge'sinde belirtilen esaslara dikkat edilir. Genelge ile lisanslı yazılım kullanımı ile ilgili iřlerde "birinci derecede" sorumluluđun "ilgili kamu kurum ve kuruluřunda bilgi iřlem nitesi veya bu iřten sorumlu birimde alıřanlara" verilmiř olduđu dikkate alınır.

14.2.7. eřitli maksatlar iin tedarik edilen yazılımlar, kurumların tařınır kayıt birimleri tarafından envantere alınmak suretiyle kayıt altına alınır. Ayrıca Kılavuz'un Varlık Ynetimi bařlıklı blmnde belirtilen KLVZ-EK-05 Kurum Bilgi Varlıkları Envanter izelgesine iřlenir.

14.2.8. Yazılımlara ait lisans belgeleri, yazılımın reticisi firma tarafından sađlanan lisans takip/indirme sayfasına eriřim řifresi, varsa CD/DVD ve benzeri materyal, USB dongle vb. anahtarlar, ilgili projenin yrtldđu birimde muhafaza edilir.

14.2.9. Herhangi bir proje veya faaliyet kapsamında yeni bir yazılım tedarik edilmesi ihtiyaı olduđunda, tedarik faaliyetine bařlanmadan Kurumun bilgi iřlem sorumlusu ve tařınır kayıt birimi ile koordinasyon kurulur.

14.2.10. Bakanlıđımıza ait hibir cihazda, reticisi tarafından aıklanmıř lisanslama politikasına aykırı bir řekilde (lisanslama/kullanım anahtarının kırılması, yazılımın izinsiz olarak kopyalanması vb.) yazılım kullanılamaz.

14.2.11. Lisans erevesinde izin verilen kullanıcı sayısının ařılmaması iin gerekli tedbirler alınır. Lisans szleřmesi erevesinde izin verilen lisans birim sayısının ařılması (iřlemci, disk, sunucu, kullanıcı, adet vb.) durumunda Kılavuz'un 9.3 (Kapasite Ynetimi) ve 13.2.8. (Kaynak Planlaması) maddelerinde belirtilen sreler devreye alınır.

14.2.12. eřitli isimler altında (open source, freeware, shareware) cretsiz olarak dađıtılan yazılımlar, zararlı geler barındırma ihtimaline karřı test edilmeden kuruma ait bilgisayarlara kurulmaz.

14.2.13. Bakanlık alıřanlarınca, grev tanımlarının bir parası olarak resmi bir hizmetin ifası iin kurum kaynakları kullanılmak suretiyle retilen (her trl bilgi, belge, rapor, dokman, grafik, kitapık, sunum, tasarımı, proje, yazılım vb.) fikri mlkiyete konu olabilecek varlıkların mlkiyeti, Bakanlıđımıza aittir. Bakanlık sz konusu varlıkları, ilgili mevzuat uyarınca kendi adına tescil ettirebilir. Kiřiler, sz konusu varlıklar zerine kiřisel bir hak iddia edemezler.

14.2.14. Aksi kararlařtırılmadıkça, tedarik sözleşmeleri kapsamında yüklenici firmalar tarafından yapılan/yaptırılan tasarım, geliştirme ve/veya eklemelere ilişkin ortaya çıkan fikri mülkiyet hakları Bakanlığımıza aittir. Bu kapsamda, yükleniciler tarafından geliştirilen (tasarım, yazılım, yazılım kodu, algoritma vb.) fikri mülkiyete konu olabilecek varlıklar, sözleşme süresi sonunda idare tarafından teslim alınır. Yükleniciler ve/veya çalışanları, söz konusu varlıklar üzerinde kişisel/kurumsal bir hak iddia edemezler. Bakanlık, söz konusu fikri mülkiyet haklarından Yükleniciyi bir lisans sözleşmesi çerçevesinde (bedeli mukabili veya bedelsiz olarak) faydalandırabilir.

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

14.2.16. Telif hakları kapsamında korunan kitaplar, makaleler, raporlar ve diđer belgeler hiçbir şekilde kopyalanamaz, çoğaltılmaz ve dağıtılamaz.

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

14.3. Kişisel Verilerin Korunması Mevzuatı

14.3.1. Anayasa'nın 20'ci maddesinin, 6698 sayılı Kanun'un ve Kişisel Sağlık Verileri Hakkında Yönetmelik'in, kişisel verilerin korunmasına ilişkin hükümlerine azami düzeyde hassasiyet gösterilir.

14.3.2. Kişisel verilerin ve kişisel sağlık verilerinin işlenmesinde, 6698 sayılı Kanun'un 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.

14.3.3. Kişisel verilerin ve kişisel sağlık verilerinin aktarılmasında, 6698 sayılı Kanun'un 8'inci ve 9'uncu maddesinde ve ayrıca bu Kılavuz'un 10.6 (Veri Aktarım Anlaşmaları) maddesinde yer alan hükümlere riayet edilir.

14.3.4. 6698 sayılı Kanun'un 12'nci maddesinin birinci fıkrası uyarınca veri sorumlusu; verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek, verilerin muhafazasını sağlamak amaçlarıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

14.3.5. 6698 sayılı Kanun'un 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.

14.3.6. 6698 sayılı Kanun'un 12'nci maddesinin üçüncü fıkrası uyarınca veri sorumlusu, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Dolayısı ile kanun hükümlerine uyumluluđun sağlanıp sağlanmadığı hususunda veri sorumlusu, veri işleyeni (HBYS işletimi hizmeti veren yüklenici) denetleyebilir.

14.3.7. 6698 sayılı Kanun'un 12'nci maddesinin dördüncü fıkrası uyarınca veri sorumlusu ile veri işleyen (HBYS işletimi hizmeti veren yüklenici), öğrendiđi kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

14.3.8. Kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ile 140'ıncı madde hükümleri uygulanır.

14.3.9. 6698 sayılı Kanun hükümlerine uygunsuzluk nedeniyle KVKK tarafından verilecek idari para cezaları ile ilgili kişiler tarafından açılacak davalarda hükmedilecek maddi ve manevi tazminat davaları, kusurlu olması hâlinde veri işleyen (SBYS işletimi hizmeti veren yüklenici) tarafından ödenir.

14.4. 5651 Sayılı Kanun ile Uyum

14.4.1. Türkiye'de internet ile ilgili en kapsamlı düzenleme 2007 yılında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile sağlanmıştır.

14.4.2. 5651 sayılı Kanun ile temel olarak aşağıdaki hususlarda düzenlemeler yapılmıştır:

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

14.4.2.2. Erişimin engellenmesi usul ve esasları düzenlenmiştir.

14.4.2.3. İnternet ortamında yayımlanan içerik nedeniyle haklarının ihlal edildiđini iddia eden kişilere ilişkin; içeriğın yayından çıkarılmasını sağlama ve cevap hakkı uygulamalarına ilişkin usul ve esaslara yer verilmiştir.

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

14.4.2.5. Türkiye’de internet ortamındaki yayınlardan Kanun’da belirtilen katalog suçlara ilişkin şikâyetlerin yapılabileceđi internet bilgi ihbar merkezi (ihbarweb.org.tr) kurulmuştur.

14.4.3. Bakanlığımız bađlısı kurum ve kuruluşlarda tesis edilmiş olan ağların hemen hemen tamamına yakını bir şekilde internet ortamına bađlı olarak çalışmakta ve Kanun’da belirtilen internet aktörlerinden “**İçerik Sağlayıcı, yer sağlayıcı veya toplu kullanım sağlayıcı**” rollerinden bir veya birkaçına girebilmektedir.

14.4.4. “Erişim sağlayıcı” kuruluşlar, abonelerine ticari olarak internet erişimi sağlayan telekomünikasyon firmaları olup Bakanlığımıza bađlı hiçbir kurum bu kategoriye girmemektedir.

14.4.5. İçerik sağlayıcı, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, deđiştiren ve sağlayan gerçek veya tüzel kişilerdir. Bakanlık merkez teşkilatı, bađlı kuruluşlar ve taşra teşkilatı birimleri web sayfaları vasıtası ile kullanıcılara içerik sundukları için “**İçerik Sağlayıcı**” konumundadır.

14.4.6. İçerik Sağlayıcı;

14.4.6.1. İnternet ortamında kullanıma sunduđu her türlü içerikten sorumludur.

14.4.6.2. İçerik sağlayıcı, bađlantı sağladığı başkasına ait içerikten sorumlu deđildir. Ancak, sunuş biçiminden, bađlantı sağladığı içeriđi benimsediđi ve kullanıcının söz konusu içeriđe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur.

14.4.7. Yukarıda belirtilen nedenlerle; Bakanlığımıza bađlı kurum ve kuruluşların web sayfalarında yer alan her türlü içeriđin mutlaka bir sahibi olmalı ve kayıt altına alınmalı, kurumun web sayfasında içerik yayımlama ile ilgili usul ve esaslar belirlenmeli, yazılı hale getirilmeli ve titizlikle uygulanmalıdır.

14.4.8. Kılavuz’un 6.12 (Merkezi Web İçerik Yönetim Sistemine Erişim) maddesinde belirtilen sistem vasıtasıyla sunulan içerikten, sistemi işleten SBSGM deđil ilgili web sitesine içeriđi koyan kişi veya kurumlar sorumludur.

14.4.9. Yer sağlayıcı, internet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.

14.4.10. Yer Sağlayıcı;

14.4.10.1. Yer sađladıđı hukuka aykırı içerikten, ceza sorumluluđu ile ilgili hükümler saklı kalmak kaydıyla, Kanun ve ilgili mevzuat hükümlerine göre BTK, adli makamlar veya hakları ihlal edilen kişiler tarafından haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduđu ölçüde, hukuka aykırı içeriđi yayından kaldırmakla,

14.4.10.2. Yer sađlayıcı trafik bilgisini ve bu bilgilerin dođruluđunu, bütünlüđünü ve gizliliđini teyit eden deđer kendi sistemlerine günlük olarak kaydetmek ve bu verileri iki yıl süre ile saklamakla sorumludur.

14.4.10.3. Yer sađlayıcı trafik bilgisi, internet ortamındaki her türlü yer sađlamaya iliřkin olarak; kaynak IP adresi, hedef IP adresi, bađlantı tarih ve saat bilgisi, istenen sayfa adresi, iřlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgilerdir.

14.4.11. Bakanlık merkez, bađlı kuruluşlar ve tařra teřkilatı birimlerine ait web sayfalarının ve uygulamaların sunumunda kullanılan yazılım ve donanımları iřleten birimler “Yer Sađlayıcısı” konumundadır. Bu kapsamda;

14.4.11.1. Web siteleri, Merkezi Web İçerik Yönetim Sistemi vasıtasıyla sunuluyorsa yer sađlayıcısı SBSGM,

14.4.11.2. Web siteleri ve uygulamaları, kuruma ait sunucu/sistemler vasıtası ile sunuluyorsa yer sađlayıcısı ilgili kurumun kendisi,

14.4.11.3. Web siteleri barındırma hizmeti, hizmet alımı ile SBYS firmaları veya diđer üçüncü kişilerden alınıyorsa yer sađlayıcısı ilgili SBYS firması veya üçüncü kişiler olmaktadır.

14.4.12. Web siteleri barındırma hizmeti, hizmet alımı ile SBYS firmaları veya diđer üçüncü kişilerden alınıyorsa, 14.4.10 maddesinde yer alan hususun ilgili firmalar tarafından yapılmasını temin etmek için hizmet sözleşmelerine konu ile ilgili maddelerin koyulması ve yapılacak firma denetimleri ile bu verilerin alındıđının kontrol edilmesi gerekir.

14.4.13. İnternet toplu kullanım sađlayıcılar, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanađı sađlayan gerçek ve tüzel kişilerdir. Bakanlıđımıza ait kurum ve kuruluşlarda tesis edilen biliřim altyapısı kullanılmak suretiyle, son kullanıcılara internet ortamına eriřim sađlanıyorsa, ilgili kurum ve kuruluşlar “İnternet Toplu Kullanım Sađlayıcı” konumundadır.

14.4.14. İnternet Toplu Kullanım Sađlayıcıları;

14.4.14.1. Eriřim kayıtlarını ve bu kayıtların dođruluđunu, bütünlüđünü ve gizliliđini teyit eden deđeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri 2 (iki) yıl süre ile saklamakla,

14.4.14.2. Konusu suç oluřturan içeriklere eriřimi önleyici tedbirleri almak amacıyla içerik filtreleme (İnternet ortamında web adresi, alan adı, IP adresi, kelime ve benzeri ölçütlere göre eriřimi engelleyen yazılımları ve donanımları) sistemini kullanmakla,

14.4.14.3. Kamuya açık alanlarda internet eriřimi sađlayan toplu kullanım sađlayıcılar, SMS ve benzeri yöntemlerle kullanıcıları tanımlayacak sistemleri kurmakla sorumludur.

14.4.14.4. Eriřim kaydı olarak kullanıcılara iç ađda dađıtılan IP adres bilgilerinin, IP adreslerinin kullanıma başlama ve bitiş zamanlarının ve bu IP adreslerini kullanan bilgisayarların MAC adreslerinin, hedef IP adreslerinin, bir veya birden fazla IP adresinin portlar aracılıđı ile kullanıcılara paylařtırılması yöntemi ile sunulan internet eriřim hizmetinde kullanıcılara tahsis edilen gerçek IP ve port bilgilerinin kayıt altına alınması gerekir.

14.4.15. İnternet toplu kullanım sađlayıcılar, konusu suç oluřturan içeriklere eriřimi önleyici tedbirleri almak amacıyla içerik filtreleme sisteminin yanı sıra, ilave tedbir olarak güvenli internet hizmeti de alabilirler.

14.5. Bilgi Güvenliđi Denetimleri

14.5.1. Kılavuzda yer alan kontrol önlemlerinin Bakanlıđımıza bađlı birimler tarafından uygulanma düzeyini tespit etmek, varsa aksaklıkları belirlemek ve düzeltici faaliyetlerde bulunmak amacıyla bilgi güvenliđi denetimleri yapılır.

14.5.2. Bilgi güvenliđi denetimleri “yerinde denetim” ve “sistem güvenlik testleri” şeklinde gerçekleştirilir.

14.5.3. Sistem güvenlik testleri ile ilgili hususlar, Kılavuz’un 9.15 (Sistem Güvenlik Testleri) maddesinde açıklanmıřtır.

14.5.4. Yerinde denetimler, Kılavuzda yer alan konuların (tamamının veya seçilecek bazı maddelerin) uygulanma/gerçekleřtirilme durumunun, Bakanlık tarafından görevlendirilecek denetçiler vasıtasıyla kontrol edilmesi suretiyle yapılır.

14.5.5. Yerinde denetimler, ilgili kurumların en üst düzey yöneticileri imzasıyla yapılacak talep veya yetkili makamlar (Bakan, Bakan Yardımcısı, SBSGM Genel

Müdürtü) tarafından verilecek talimatlara istinaden planlı olarak yapılır. Denetim için önceden hazırlanan yazılı kontrol formları/soru listeleri kullanılır.

14.5.6. Talep üzerine yapılacak denetimler için SBSGM'deki ilgili birimlerde görev yapan denetçi personelin iş yükü dikkate alınarak planlama yapılır.

14.5.7. Denetim; sorumlu personel ve son kullanıcılar ile yüz yüze görüşme yapılması, varsa kayıtların incelenmesi, gerekiyorsa ölçümlerin yapılması suretiyle gerçekleştirilir. İhtiyaç var ise Kılavuz'un 9.15 (Sistem Güvenlik Testleri) maddesinde belirtilen teknik testler de yapılabilir.

14.5.8. Bilgi güvenliđi denetimi yapacak personelin (denetçiler) denetim yapma tekniđi ve denetlenecek konular hakkında eğitim almış personel olması gerekir.

14.5.9. Denetimler, Bakanlık personeli tarafından (SBSGM personeli, bađlı kuruluşlar ve il sađlık müdürlükleri bünyesinde görev yapan personelden Bakanlık tarafından bilgi güvenliđi denetimi yapmak üzere seçilen ve denetçi eğitimi almış kişiler) yapılır.

14.5.10. Denetimlerin çeşitli nedenlerle, Bakanlık personeli tarafından yapılamaması durumunda, Bakanlık tarafından yetkin görülen ve onaylanan yetkili denetim kurumları tarafından da denetim yapılabilir.

14.5.11. Talep edilmesi halinde, Sađlık Bakanlıđı Denetim Hizmetleri Başkanlıđı tarafından Denetim Hizmetleri Yönergesi'nin ilgili maddesi uyarınca yapılacak "bilgi teknolojileri" denetimleri için uzman personel görevlendirilir.

14.5.12. Sađlıkta Kalite ve Akreditasyon Daire Başkanlıđı tarafından yapılan kalite denetimleri içinde yer alan bilgi yönetimi/bilgi güvenliđi ile ilgili ölçümler, bilgi güvenliđi denetimlerinin bir parçası olarak değerlendirilir.

EKLER

Eklerin içeriklerinin güncel ihtiyaçlara göre sık sık deęiřmesi nedeniyle, son hallerine <https://bilgiguvenligi.saglik.gov.tr/Home/Mevzuat> adresinden erişim sağlanacaktır.

KLVZ-EK-01 İŐE BAŐLAMA FORMU

Adı Soyadı			
Unvan/ Y¼klenici Firma			
Birimi			
BaŐlama Tarihi/...../20.....		
Tamamlanması Gereken BaŐlıklar	İlgili Birim / KiŐi	Kurum alıŐanı Adı Soyadı / İmza	İŐe BaŐlayan KiŐi Adı Soyadı / İmza
Kimlik - GiriŐ Kartının ıkarılması	Personel Birimi		
Oryantasyon Eđitimi	Eđitim Koordinasyon Birimi		
e-Posta Hesabının Aılması	e-Posta Birimi		
BGYS Farkındalık Eđitimi	BGYS Birimi		
EBYS Aılması	EBYS ve e-İmza Birimi		
EBYS Eđitimi	EBYS ve e-İmza Birimi		
Zimmet OluŐturulması	TaŐınır Kayıt Birimi		
Personel Gizlilik S¼zleŐmesi İmzalatılması	Birim Sorumlusu		

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

KLVZ-EK-02 İŐTEN AYRILMA FORMU

Adı Soyadı			
Unvanı/ Yüklenci Firma			
Birimi			
İŐten Ayrılma Tarihi/...../20.....		
Tamamlanması Gereken Başlıklar	İlgili Birim / KiŐi	Kurum alıŐanı İsim/Soy İsim İmza	İŐten Ayrılan KiŐi İsim/Soy İsim İmza
Yaptıđı İŐ ve İŐlemlerle İlgili Dokümantasyon ve Bilgilendirme Devri Yapılması	Birim Sorumlusu		
VPN Hesaplarının Kapatılması	Ađ Yönetimi Birimi		
Veri Tabanı Kullanıcı Hesabının Kapatılması	Veri Tabanları ve Orta Katman Yönetimi Birimi		
e-Posta Hesabının Kapatılması ve İlgili e-Posta Gruplarından ıkartılması (DanıŐman, Firma Personeli ve Emekli Olanlar İin Hesap kapatılmalıdır.)	e-Posta Birimi		
EBYS Kapatılması	EBYS ve e-İmza Birimi		
Zimmet Devri	TaŐınır Kayıt Birimi		
Kimlik - GiriŐ Kartının İade Edilmesi	Personel Birimi		

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

Not: İlgili birim tarafından yapılan kontrollerde kiŐinin kapatılacak bir kaydı bulunmuyor ise kontrol edildiđine dair imza atılması gerekmektedir.

KAYITTAN DÜŐME TEKLİF VE ONAY TUTANAĐINA İLİŐKİN 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 tutanađın 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 dolduđunda 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				
S. No	Marka	Model	Seri No	HDD Seri No
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

İmha edilmesini talep ettiđim/ettiđimiz diskin/disklerin erisindeki veriler nedeniyle ileride gündeme gelebilecek adli ve idari soruřturmalarda sorumluluđun řahsıma/řahsımıza ait olduđunu kabul ve beyan ederim/ederiz./...../20.....

Disk İinde Bulunan Verilerin
Sahibi Kiři(ler)

Dayanıklı taşınır kayıtlarında bulunan ve tarihli ve sayılı onay ile oluřturulan komisyon üyelerinin deđerlendirmesi sonucunda, ekonomik ömrünü tamamladıđı, teknik ve fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dıřı bırakılması gerektiđi “**Kayıttan Düşme Teklif ve Onay Tutanađı**” ile tespit edilen taşınırların veri depolama üniteleri HEK komisyonunda bulunan üyelerin gözetiminde imha edilmiřtir./...../20.....

Teknik Uzman Üye

Taşınır Kayıt Kontrol Yetkilisi

Komisyon Bařkanı

KLVZ-EK-05 KURUM BİLGİ VARLIKLARI ENVANTER ÇİZELGESİ

No	Varlık	Türü	Tanım	Adet	Sahibi	Fiziksel Konum	Cinsi	İşletim Sistemi	Bilgiyi işleyen yazılımlar	Bilgiyi işleyen donanımlar	Gizlilik Derecesi	Açıklama
1	SBYS Sunucusu	Donanım	SBYS Uygulama Sunucusu	1	Teknik Destek Birimi	Hastane Sunucu Odası	Blade Sunucu	windows sever 2012			Gizli	Üzerinde SBYS Veritabanı çalışan sunucudur.
2	SBYS Uygulama Bilgisayarı	Donanım	SBYS İstemci Bilgisayar	5	SBYS Uygulama Veri Giriş Sorumlusu	Hasta Kabul Deski	Masaüstü Bilgisayar	Windows 10 pro			Gizli	Üzerinde SBYS Uygulaması çalışan istemci bilgisayardır.
3	İhale Dosyaları	Fiziksel Bilgi Varlıkları	Hastane satın alma ihale dosyaları		Satın Alma Birimi	Satın Alma Birim Arşivi	Klasör		İhale kayıt sistemi	x sunucusu	Gizli	Alim işi ihale dosyaları
4	VPN Yazılımı	Yazılım	Özel sanal ağ yazılımı	1	Teknik Destek Birimi						Gizli	Forticlient özel sanal ağ yazılımı
5	SBYS Uygulama Yazılımı	Yazılım	Sağlık bilgi yönetim sistemi yazılımı	1	Teknik Destek Birimi						Gizli	X Firması tarafından destek alınan SBYS Yazılımı
6	Hasta Kabul Süred	İş Süreçleri	Rutin Hasta Kabulü		Hasta kabul elemanı				SBYS		Gizli	Bireyin yaşamında acil, ciddi bir tehlike ve hayatı fonksiyonlarını etkileyen acil bir durum olmadıkça zaman yapılan kabul işlemidir.
7	Sistem Erişim Logları	Kurumsal Bilgi Varlıkları	Sistem Yöneticisi erişim logları		İdari Yönetim						Gizli	Sistem kaynaklarına yapılan erişim bilgileri
8	Hasta Kabul Elemanları	İnsan Kaynakları	X Firması üzerinden istihdam edilen hasta kabul personeli	15	İdari Yönetim							Hasta kabul işlemlerini gerçekleştiren firma üzerinden istihdam edilen personel
9	Ameliyathane İklimlendirme Cihazı	Altyapı	Ameliyathane bulunan iklimlendirme cihazı	2	İdari Yönetim							X markalı klima cihazı
10	Sunucu odası	Mekânlar	SBYS sunucularının bulunduğu sunucu odası	1	İdari Yönetim	X lokasyonu 2.kat						Sunucu odası

KLZV-EK-06 RİSK HESAPLAMA FAKTÖRLERİ

VARLIK DEĞERİ TABLOSU

GÜVENLİK HEDEFİ	DÜŞÜK (1)	ORTA (2)	YÜKSEK (3)	ÇOK YÜKSEK (4)
GİZLİLİK	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik bilgi önemli değildir. Kontrol dışı değişen hassas olmayan bilgiler kurumu etkilemez / çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi önemlidir. Kontrol dışı değişen hassas olmayan bilgiler kurumu etkiler. (Elektronik imza / kayıt onay mekanizmasının kullanıldığı bilgi varlıkları)	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi önemlidir. Kontrol dışı değişen hassas olmayan bilgiler kurumu etkiler. (Her kayıt için onay sürecinin olduğu, değişiklik kayıtlarının tutulduğu bilgi varlıkları)	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, veri tabanları erişimleri sağlayan şifre ve /veya parolalar, kurum stratejileri vb - yetkisiz kişilerin eline geçmesi durumunda Sağlık Bakanlığımıza büyük ölçüde zarar verecek her türlü bilgi.)
BÜTÜNLÜK	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik 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 orta vadede telafi edilebilir. (Kurumda verilen hizmetlerde her hangi bir kesinti/aksama her hangi bir kesinti/aksama durumuna tolere edilebilecek süre 1 saat olup, bu süre içinde erişilebilir hale getirilmesi gereken bilgi varlıkları - IIS- Uygulama sunucuları – veri tabanı - FW)	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. Kurumda verilen hizmetlerde her hangi bir kesinti/aksamaya tahammül bulunmamaktadır.
ERİŞİLEBİLİRLİK / KULLANILABİLİRLİK	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen hassas olmayan bilgiler 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 bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. (Kurumda verilen hizmetlerde her hangi bir kesinti/aksama her hangi bir kesinti/aksama durumuna tolere edilebilecek 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 kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir. (Kurumda verilen hizmetlerde her hangi bir kesinti/aksama her hangi bir kesinti/aksama durumuna tolere edilebilecek süre 1 saat olup, bu süre içinde erişilebilir hale getirilmesi gereken bilgi varlıkları - IIS- Uygulama sunucuları – veri tabanı - FW)	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. Kurumda verilen hizmetlerde her hangi bir kesinti/aksamaya tahammül bulunmamaktadır.

1. Tanımlanan her bir varlık için, varlık sahibi tarafından değer atanmalıdır.
 2. Bir varlığın değerini belirlemek için Genel Müdürlüğümüz tarafından oluşturulan temel referans; varlığın gizlilik, bütünlük ve/veya erişilebilirliğini yitirdiğinde oluşabilecek zarardır. Yenne koyma maliyeti, gizli bilginin ifşası neticesinde oluşabilecek kurumsal itibar gibi soyut kavramlar da göz önüne alınmalıdır.
 3. Varlık sorumusu, varlığa değer belirleme aşamasında gizlilik, bütünlük ve erişilebilirlik için ayrı değerler atayabilir. Örneğin bir web sitesi için değer atanırken;
 - *web sitesinin gizlilik değeri için düşük - 1 puan (açığa çıkan bilgi kuruma zarar vermez),
 - *web sitesinin bütünlük değeri için orta - 2 puan (3 saate kadar ulaşılamaması durumunda hizmet süreci aksamaz)
 - *web sitesinin erişilebilirlik değeri için yüksek - 3 puan (kontrol dışı değişen bilgi kuruma zarar verir) atayabilir.
- Bu durumda varlığa verilecek nihai değer, belirlenen tüm değerlerin toplamı olacaktır.
- Varlık sahibi tarafından varlığa atanan değer, varlığın korunması için harcanacak kaynakların belirlenmesi için referans değer oluşturacağı için dikkatlice değerlendirilerek atanması gerekir.



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

GİZLİLİK ETKİ DEĞERİ	
Düşük (1/2)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliđi olayının sonucunda riskin gizliliđe etkisi düşük olur. Kurum imajı etkilenmez, zarar çok kısa vadede telafi edilebilir ve iş süreci aksamaz.
Orta (3)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliđi olayının sonucunda riskin gizliliđe 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 güvenliđi olayının sonucunda riskin gizliliđe 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 güvenliđi olayının sonucunda riskin gizliliđe etkisi çok yüksek şiddette olur. Yıkıcı / felaket düzeyinde etki gerçekleşir. Kurum çok ciddi itibar kaybına uğrar. Yasal yükümlülükler doğurur ve çok yüksek ek maliyetler doğar.

BÜTÜNLÜK ETKİ DEĞERİ	
Düşük (1/2)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliđi 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 güvenliđi 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 güvenliđi 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 güvenliđi olayının sonucunda riskin bütünlüğe etkisi çok yüksek şiddette olur. Bütünlüğün sağlanamaması felaket düzeyde etkiye neden olur. Yasal yükümlülükler doğurur, çok yüksek ek maliyetler doğar.



ERİŞİLEBİLİRLİK ETKİ DEĞERİ	
Düşük (1/2)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliđi 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 güvenliđi olayının sonucunda riskin erişilebilirliğe etkisi orta derecede olur. Belirli bir hizmette yavaşlama ya da küçük çapta iş kesintileri oluşur. Erişilemeyen bilgi orta vadede yerine koyulabilir.
Yüksek (4)	Tehdidin gerçekleşmesi durumunda oluşan bilgi güvenliđi 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 güvenliđi 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-08 E-POSTA TALEP FORMU / GERÇEK KİŞİLER

		HİZMETE ÖZEL												
		E-POSTA TALEP FORMU - GERÇEK KİŞİLER İÇİN												
Kodu	Yayımlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa										
BG.FR.18	10.1.2013	12.12.2016	1	1										
SIRA	T.C. Kimlik Numarası	Yazışmalarda Görünmesi/Tercih Edilen İsim	Sistem Adının Noktadan Önceki Kısmı	Sistem Adının Noktadan Sonraki Kısmı	SİSTEM ADI	Mevcut Yapıldığı Görevi	Bağlı Yöneticisi epostası (@sağlik.gov.tr maili olmak)	DAİRE BAŞKANLIĞI veya DENGE BİRİMİ (diğer 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														

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

KLVZ-EK-09 E-POSTA TALEP FORMU / TÜZEL KİŞİLER

Kodu BG.FR.19		Yayınlama tarihi 10.1.2013	Revizyon Tarihi 12.12.2016	Revizyon No 1	Sayfa 1							
 HİZMETE ÖZEL E-POSTA TALEP FORMU - TÜZEL (BİRİM) KİŞİLER İÇİN 												
Bu Sütünlarda Türkçe Harf Kullanmayınız. Tanımlanacak "SİSTEM ADI" sütunları 20 karakteri geçemez												
Sıra	Yazışmalarda Görünmesi Tercih Edilen İsim	Sistem Adının Nektadan Önceki Kısmı	Sistem Adının Nektadan Sonrakı Kısmı	Sistem Adı	Kullanım Yeri	Bağlı Yöneticisi epostası (@sağlik.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												
15												

KLVZ-EK-10 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 Adısaglik.gov.tr		
Veri Tabanı İhtiyacı Var mı?	Evet	Hayır	
Sistem Gereksinimleri	Talep Edilen	Sađlanan	
İşlemci			
Bellek			
Disk Alanı			
İşletim Sistemi			
Sunucu Rolü			
Load Balancer İhtiyacı			
Uygulama Bilgileri	IIS, SQL, PHP vb		
Ađ Gereksinimleri			
Talep Edilen Portlar			
Kullanım Amacı			
Sunucu Talebi Yapan Kişinin Görev ve Sorumlulukları			
<ul style="list-style-type: none"> • Sunucudaki bilgilerin ve içeriklerin sorumluluđu sunucu sahibine aittir. • Sunucuya ait erişim bilgileri sadece yetkili kullanıcıya verilir. Tanımlanan bu yetkili hesaplar devredilemez veya deđiştirilemez. • Sunucuya ait erişim bilgileri yetkili dışında kimse ile paylaşılabilir. Sorumluluk yetki tanımlanmış olan kullanıcıya aittir. • Sunucu sahibi, sunucu üzerindeki aykırı işlemler sonucu doğabilecek tüm hukuki ve cezai sorumluluđu kabul etmektedir. 			

KLVZ-EK-11 VERİ TABANI / KULLANICI OLUŐTURMA FORMU

1. ORTAK BÖLÜM:

TALEPTE BULUNAN ORGANİZASYON						
KURUM / KURULUŐ / GENEL MÜDÜRLÜK						
BAŐKANLIK / DAİRE BAŐKANLIđI						
BİRİM VEYA ŐUBE						
TALEP İLE İLGİLİ TEMAS PERSONELİ						
ADI VE SOYADI						
TC KİMLİK NO						
TELEFON NUMARASI						
E-POSTA ADRESİ						
UYGULAMA BİLGİLERİ						
UYGULAMA ADI						
UYGULAMA İLE İLGİLİ ÖZET BİLGİ						
KULLANILACAK VERİ TABANI YÖNETİM SİSTEMİ	ORACLE	MS SQL	POSTGRE	MONGO DB	MYSQL	ELASTIC
VERİ TABANI ADI						

2. VERİ TABANI OLUŐTURMA TALEPLERİ İÇİN DOLDURULACAK BÖLÜM:

DİL VE KARAKTER KÜMESİ SEÇENEđİ	
TAHMİNİ VERİ TABANI BOYUTU (BİR YIL SONRASI İÇİN) (GB)	

3. KULLANICI OLUŐTURMA TALEPLERİ İÇİN DOLDURULACAK BÖLÜM:

KULLANICI ADI	
ŐEMA ADI	

TALEP EDEN
AD/SOYAD
İMZA

TALEP EDEN
BİRİM SORUMLUSU
İMZA

TALEP EDEN
DAİRE BAŐKANI
İMZA

FORMUN KULLANIMI İLE İLGİLİ HUSUSLAR:

1. Mevcut bir veri tabanı için yeni kullanıcı ekleme işlemleri için 1 ve 3'üncü bölümler doldurulur.
2. Sistem Yönetimi ve Bilgi Güvenliđi Dairesi Başkanlığınca (gerekiyorsa) 1'inci bölümde ismi yazan temas personeli (telefon veya e-Posta) ile iletişime geçilerek taleple ilgili detay bilgiler alınır.
3. 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.
4. Kullanıcı oluşturma işlemlerinde, işlemin gerçekleştirildiđi bilgisi, temas personeline e-Posta ile bildirilir.
5. Veri tabanı yöneticileri ile iletişim için dbagrubu@saglik.gov.tr e-Posta adresi kullanılır.

KLVZ-EK-12 PERSONEL GİZLİLİK SÖZLEŞMESİ

Bu sözleşme / / 20..... tarihinde, aşağıda yer alan hükümler çerçevesinde, (T.C. Sağlık Bakanlığı Genel Müdürlüğü /Kurumu/..... İl Sağlık Müdürlüğü)³ (Kurum) ile aşağıda kimlik bilgileri yazılı kişi (Personel) arasında akdedilmiştir.

1. TANIMLAR:

Kuruma Ait Gizli Kalması Gereken Bilgiler:

1.1 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan “Gizlilik Dereceli Evrak ve Gerecin Güvenliđi Hakkındaki Esaslar” ile tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belge.

1.2 Kurum tarafından işlenen (24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan) kişisel veriler ile (21/06/2019 tarihli ve 30888 sayılı Kişisel Sağlık Verileri Hakkında Yönetmelik ile tanımlanan) kişisel sağlık verileri.

1.3 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 sistemleri içerisinde saklanan veriler, donanım/yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduđu işler.

1.4 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:

2.1 Personel, kuruma ait gizli bilgilerin korunması için aşağıdaki kurallara uyacağıının beyanı olarak bu sözleşmeyi imzalar.

2.2 Personel, Sağlık Bakanlığı Bilgi Güvenliđi Politikaları Yönergesi ve Bilgi Güvenliđi Politikaları Kılavuz’unda yer alan koşullara uygun hareket eder.

³ Uygun olanı yazılır. Diğerleri silinir.

2.3 Personel, bu sözleşme hükümlerine uygun davranmaktan, ihlali halinde ise Bakanlığa, Kuruma ve üçüncü kişilere vereceđi her türlü zarardan sorumludur. Sözleşmenin ihlal edilmesi sonucu doğacak tüm hukuki ve cezai sorumlukları peşinen kabul eder.

2.4 Personel, Kurumda uygulanmakta olan BGYS kapsamında yayımlanmış politika, prosedür, süreç ve sözleşmelere uygun davranır. Bahse konu dokümanlarda belirtilen hususları eksiksiz olarak yerine getirir.

2.5 Personel, Kurum tarafından kendisine teslim edilmiş veya erişim yetkisi verilmiş olan gizli kalması gereken bilgileri, sadece görevi ile ilgili işler için kullanır. Bu bilgileri kendi gizli bilgisi gibi korur ve bilmesi gereken yetkili kişiler haricinde hiç kimse ile paylaşmaz. Personel, bilgi paylaşabileceđi kişiler konusunda tereddütte kalırsa, bilginin sahibi olan veya süreci yöneten birim ile irtibata geçerek bu bilgileri kimlerle paylaşabileceđini teyit eder.

2.6 Personel, özel olarak yetkilendirildiđi durumlar dışında, hizmet verilen tarafların yetkilileri de dâhil olmak üzere yetkisi olmayan hiç kimse ile gizli kalması gereken bilgileri paylaşmaz. Yetkisi olmadığı halde, bulunduğu görev ve makamı kullanarak kendisinden bu bilgileri talep eden kişileri yöneticisine bildirir.

2.7 Personel, görevi kapsamında kendisine teslim edilmiş olan gizli kalması gereken bilgileri, ilgili mevzuata uygun olarak korur, işler ve aktarır. Bu bilgileri, yetkisi olmayan üçüncü kişilerin yanında konuşmaz.

2.8 Personel, gizli kalması gereken bilgileri hiçbir kişi, grup, kurum veya kuruluşun menfaati için kullanmaz.

2.9 Personel, görevi ile ilgili olsun veya olmasın, edindiđi 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 süresiz olarak devam eder.

2.10 Personel, görevi nedeniyle edindiđi gizli bilgiler hakkında, yasal zorunluluklar ve kurum tarafından resmi olarak izin verilmesi halleri dışında, yazılı veya sözlü açıklama yapamaz.

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

2.12 Personel, bilgi sistemlerinde kullanılan/yer alan programları, verileri veya diđer unsurları hukuka aykırı olarak ele geçirme, deđiřtirme, silme giriřiminde bulunamaz ve bunları nakledemez veya çođaltamaz.

2.13 Personel, Kurumun bilgisi veya onayı dıřında, proje ve faaliyetlerde kullanılan veriler ve sistemler üzerinde, görevin gerektirdiđi iř ve iřlemler dıřında deđiřiklik yapamaz.

2.14 Personel, hangi amaçla olursa olsun görevi kapsamında Kurumda edindiđi bilgileri, proje ve faaliyetlerde kullanılan çeřitli řekillerde (basılı, dijital, manyetik vb.) bulunabilecek olan verileri yetkisiz ve izinsiz olarak kullanamaz, kopyalayamaz, taşıyamaz ve aktaramaz.

2.15 Personel, Kurum tarafından kendisine emanet edilen bilgisayar, tablet, telefon, taşınabilir medya gibi cihazları sadece göreve yönelik, kurumsal faaliyetler için kullanır. Bu cihazlarda kurumun bilgisi dıřında hiřbir mekanik ya da yazılımsal yapılandırma deđiřikliđi yapamaz.

2.16 Personel, Kurum tarafından kendisine verilen ya da tanımlanan kullanıcı adı/parolayı hiř kimseyle paylaşmaz. Parolasının gizli kalması için gereken tüm tedbirleri alır. Kurumdan ayrılması halinde kullanıcı adı/parolayı iptal ettirir. Kullandıđı bilgisayar ve/veya diđer veri depolama ortamlarına oluřturduđu veri, bilgi ve belgeler dâhil tüm belgeleri, cihazları ve ofis malzemelerini eksiksiz olarak ilgisine teslim eder ve bunların hiřbir kopyasını alamaz.

2.17 Personel, Bakanlık ve/veya Kurum sunucuları üzerinden kendisine tahsis edilen e-İmza/mobil imza, kullanıcı adı/parola ve/veya IP/MAC adresini kullanarak gerçekteřtirdiđi her türlü etkinlikten, kurum biliřim kaynakları kullanılarak oluřturduđu ve/veya kendisine tahsis edilen kurum biliřim kaynađı üzerinde bulundurduđu her türlü içerikten (belge, doküman, yazılım vb.) sorumludur.

2.18 Personel, 5651 sayılı Kanun geređi tutulması gereken kayıtlara ilave olarak; Kurum tarafından uygun görülen diđer sistemlerin, uygulamaların, kullanıcı iřlemlerinin, bilgi sistem ađındaki verilerin ve veri akıřının iz kayıtlarının hukuki ve idari süreçlere kaynak teřkil etmesi ve sistemlerin güvenli bir řekilde iřletilmesi amacıyla tutulabileceđini peřinen kabul eder.

2.19 Bakanlık/Kurum tarafından kiřilere tahsis edilen e-Posta hesabı sadece iřle ilgili kurumsal faaliyetler için kullanılır. Personel, kendi hesabı kullanılarak gönderilen tüm e-Postalardan kiřisel olarak sorumludur.

2.20 Personel, sosyal medya hesaplarını kullanırken görevinin gerektirdiđi dikkat ve özeni gösterir. Kuruma ait gizli kalması gereken bilgiler, sosyal medya ortamlarında paylaşılmaz.

2.21 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.

2.22 İşbu sözleşme iki nüsha olarak imzalanır, bir nüshası Kurumun Personel biriminde saklanır. Diğer nüshası ise personelin kendisine verilir.

2.23 Kurumda görev yapan Personel, çalışma süresi sona erdiğinde ya da kurumdan ilişđi herhangi bir gerekçeyle kesildiğinde, KLVZ-EK-02 İşten Ayrılma Formunu doldurur ve ilgili birim sorumlusuna teslim eder.

3. YAPTIRIMLAR:

3.1 Yukarıda sayılan kurallardan biri ya da birkaçının ihlâlinin tespit edilmesi halinde, güvenlik ihlâline yol açan personel hakkında işlem başlatılır.

3.2 Yapılan ihlalin ilgili kanunlar geređi suç ve ceza öngören bir fiil olması halinde, ilgili personel hakkında suç duyurusunda bulunulur.

3.3 Ayrıca idari bir tedbir olarak, yapılan ihlalin 3.2 maddesinde belirtildiđi şekilde suç olup olmadığına bakılmaksızın, Kurum tarafından ihtiyaç duyulması halinde; 657 Sayılı Devlet Memurları Kanunu'na tabi olanlar için aynı Kanun'un 125'inci maddesinde sayılan hükümlere göre, 657 Sayılı Devlet Memurları Kanunu'nun dışında kalan çalışanlar ile ilgili olarak (danışmanlar, firma personeli vb.) sözleşmelerinde belirtilen özel hükümlere göre, yoksa genel hükümlere göre idari işlem tesis edilir.

3.4 Kişisel veriler ile gizli bilgilerin hukuka aykırı olarak üçüncü kişilere aktarılması ve/veya onların erişimine açılması ya da kullanımına sunulması hâlinde;

3.4.1 Cezaî bakımdan 5237 sayılı Türk Ceza Kanunu'nun madde 135. vd. hükümlerine,

3.4.2 İdarî bakımdan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 18'inci madde hükmüne,

3.4.3 Hukukî bakımdan 4721 sayılı Türk Medeni Kanunu'nun madde 23. vd. hükümlerine,

3.4.4 Sözleşme hukuku kapsamında muhtelif konulara ilişkin süreçler bakımından 6098 sayılı Türk Borçlar Kanunu'nun madde 112. vd. hükümlerine göre, söz konusu hükümlerin ilgili durum bakımından yasal uygulama alanlarının bulunduğu ölçüde, yetkili merci ve kişilerce işlem tesis 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.

İLGİLİ PERSONELİN		
T.C. Kimlik No		Birim Sorumlusu
Adı, Soyadı		
Cep Telefonu		
İkametgâh Adresi		
e-Posta Adresi		
Çalıştığı Firma & Kurum		Firma Sorumlusu
Çalıştığı Proje & Birim		(Firma Personeli için)
Proje & Sözleşme Bitiş Tarihi		Başkan/ Daire Başkanı
İmza		

KLVZ-EK-13 KURUMSAL GİZLİLİK TAAHÜTNAMESİ

1. TARAFLAR, AMAÇ VE İŞİN TANIMI

1.1 (.....Genel Müdürlüğü/.....Kurumu/.....İl Sağlık Müdürlüğü)
.....adresinde faaliyet göstermekte olup bundan sonra “**Kurum**” olarak anılacaktır.

1.2. Kurum ile aramızda 1.3. maddede yazılı iş/faaliyet kapsamında, Sözleşme, Protokol veya benzeri adlar altında imzalanmış ve/veya imzalanması planlanan akdi ilişkinin amaçlarını gerçekleştirmek üzere Kuruma ait ve “gizli bilgi” niteliği taşıyan yazılı ve/veya sözlü bilgilere ulaşacak olmamız sebebiyle, aşağıdaki hususlara riayet etmeyi peşinen kabul ve taahhüt ederiz.

1.3. İş/Faaliyet Tanımı⁴
.....
.....
.....
.....

2. GİZLİ BİLGİNİN TANIMI

2.1. Aşağıdaki bilgileri kesinlikle “**GİZLİ BİLGİ**” olarak kabul ederiz:

2.1.1 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan “Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar” ile tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belge.

2.1.2 Kurum tarafından işlenen 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan kişisel veriler ile 21/06/2019 tarihli ve 30888 sayılı Kişisel Sağlık Verileri Hakkında Yönetmelik ile tanımlanan kişisel sağlık verileri.

⁴ Yapılacak işe ait KİK ihale kayıt numarası, sözleşme imza tarihi ve konusu veya ilgili protokolün adı (veya konusu) ve tarihi yazılır.

2.1.3 Bakanlıđa veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, alıřan bilgileri, sistem bilgileri ve alıřılan sre iinde derlenen tm bilgiler, materyaller, programlar ve dokmanlar, bilgisayar sistemleri ierisinde saklanan veriler, donanım/yazılım ve tm diđer dzenleme ve uygulamalar ile yklenici ve alıřanlarının alıřma sresi ierisinde yapmıř olduđu iřler.

2.1.4 Aıklanması halinde kiři ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kiři veya kuruma haksız yarar sađlama ihtimali bulunan her trl bilgi ve belge.

3. GİZLİ BİLGİNİN KORUNMASI

3.1. Bu gizli bilgiyi;

3.1.1 T.C. Sađlık Bakanlıđı tarafından yayımlanmıř yrrlkteki Bilgi Güvenliđi Politikası Ynergesi ve Bilgi Güvenliđi Politikaları Kılavuz’unda belirtilen tedbirleri almak suretiyle korumayı,

3.1.2 Herhangi bir nc kiřiye hangi suretle olursa olsun vermemeyi, aıklamamayı, deđiřtirmemeyi, ođaltmamayı ve/veya kamuya duyurmamayı,

3.1.3 İřin yrtlmesi haricinde dođrudan ya da dolaylı olarak hibir Őekilde ve sebeple kullanmamayı,

3.1.4 nc kiřiler tarafından dođrudan ya da dolaylı olarak ulařılmaması iin gerekli tm tedbirleri almak suretiyle saklamayı,

3.1.5 Gizli bilgilerin tutulduđu ortamlar ile ilgili iřlemlerin kayıtlarının olması aısından eriřimleri ve yapılan iřlemleri loglamayı, bu logların eriřimine, deđiřtirilmesine ve silinmesine izin vermemeyi ve yukarıda sayılan surette sonulanacak sair davranıřlardan kaınmayı taahht ederiz.

3.2. Kendi gizli bilgilerimizi korumakta gsterdiđimiz zenin aynısını, Kurumun gizli bilgisini korumakta da gstereceđimizi, sadece zorunlu hallerde ve iřin geređi bu bilgiyi đrenmesi gereken alıřanlarımıza iřin yrtlmesi iin gereken nispette ve bilginin korunması iin her trl azami nlemi olarak verebileceđimizi; Kurumun gizli bilgilerine eriřecek personelimize Kurum tarafından kullanılan ‘‘Personel Gizlilik Szleřmesini imzalatacađımızı; alıřanlarımızın bilginin gizliliđi hususunda bu Taahhtname ve Personel Gizlilik Szleřmesi ykmllklerine aykırı davranmayacaklarını ve byle davranmaları halinde dođrudan tarafımızın sorumlu olacađını peřinen kabul ve taahht ederiz.

3.3. Kurumdan temin etmiř olduđumuz gizli bilgilerin bu Taahhünameye aykırı biçimde açıklandığından haberdar olduđumuzda, derhal ve yazılı olarak Kuruma durumu bildirmekle yükümlü olduđumuzu da kabul, beyan ve taahhüt ederiz.

4. GİZLİ BİLGİ TANIMINA GİRMEYEN DURUMLAR

4.1. Ařağıdaki bilgilerin gizli bilgi olarak nitelendirilmeyeceđini kabul ve beyan ederiz.

4.1.1 Bakanlıđın veya Kurumun bizzat kendisi tarafından alenileřtirilmiř bilgiler,

4.1.2 Açıklanmasına Bakanlık veya kurum tarafından yazılı olarak onay verilmiř bilgiler,

4.1.3 Yürürlükte olan bir kanuna ya da verilmiř olan bir mahkeme kararına istinaden açıklanması gereken bilgiler.

4.2. Bu Taahhünamenin 4.1.3 maddesi geređince gizli bilgiyi açıklamaya mecbur kalmamız halinde, gizli bilgiyi açıklamadan önce Kuruma derhal yazılı bir bildirimde bulunacađımızı, gizli bilgiyi sadece hukuken gerektiđi kadar açıklayacađımızı ve bu açıklamanın kapsamına iliřkin olarak Kuruma yazılı olarak bildirimde bulunacađımızı, 4.1.3 maddesi kapsamında bilgi paylaşımında bulunmuř olmamızın bu Taahhünamedeki yükümlülüklerimizin sona erdiđi anlamına gelmediđini beyan, kabul ve taahhüt ederiz.

5. DENETİM VE REFERANS

5.1. Kurumun gerekli gördüđü hallerde, önceden haber vermek kaydıyla tesis ve sistemlerimizde, bu taahhünamenin konusu ve kapsamı ile sınırlı kalmak şartıyla, bilgi güvenliđi denetimleri yapma hakkına sahip olduđunu kabul ve beyan ederiz.

5.2. Kurumun resmi kurumlarca denetlenmesi halinde bu denetim kapsamında tarafımızdan bilgi ve belge talep edilmesi halinde, tarafımızdan talep edilen bilgi ve belgeleri derhal sađlamakla yükümlü olduđumuzu beyan, kabul ve taahhüt ederiz.

5.3. Kurumun bu konuda açık yazılı izni olmadıkça görsel ya da yazılı medya aracılıđıyla T.C. Sađlık Bakanlıđı ve kurumu referans olarak gösteremeyeceđimizi ya da reklam aracı olarak ve/veya reklam amacıyla kullanmayacađımızı beyan, kabul ve taahhüt ederiz.

6. GİZLİ BİLGİLERİN İADESİ

6.1 Bu Taahhütnamenin sona ermesi veya feshedilmesi veya Kurum tarafından daha önce talep edilmesi durumunda, masrafları tarafımıza ait olmak üzere zilyetliğimizde bulunan gizli bilgi içeren her türlü dokümanı ve bunların kopyalarını derhal Kuruma iade edeceğimizi beyan, kabul ve taahhüt ederiz.

6.2 Bilgisayar dâhil herhangi elektronik cihaz veya mecraya yaptığımız kayıtları geri alınamaz şekilde yok edeceğimizi, Kurum tarafından talep edilmesi durumunda söz konusu gizli bilgileri barındıran diskleri bedelsiz olarak Kuruma teslim edeceğimizi; kayıtların yok edilmesi ve/veya gizli bilgi barındıran disklerin tespiti faaliyetine Kurum tarafından görevlendirilecek bir uzman personelin refakat etmesine izin vereceğimizi kabul ve taahhüt ederiz.

6.3. 6.2 maddesinde belirtilen kayıtların geri alınamaz bir şekilde yok edildiğini, bir şirket yetkilisinin imza edeceği tutanakla belgeleyeceğimizi beyan, kabul ve taahhüt ederiz.

7. TAZMİNAT VE CEZAI ŞART

7.1. Bu Taahhütnameden doğan yükümlülüklerimizi tamamen veya kısmen ihlal etmemiz halinde, doğrudan ve dolaylı tüm zarar ve ziyanı karşılayacağımızı şimdiden kabul, beyan ve taahhüt ederiz.

7.2. Bu maddede yer alan tazminat ödeme yükümlülüğüne ek olarak, bu Taahhütnameden doğan yükümlülüklerimizi tamamen veya kısmen ihlal etmemiz nedeniyle idari veya adli makamlarca Kuruma kesilecek her türlü cezayı ilk talep halinde tazmin edeceğimizi, ayrıca bu cezaların doğmasına neden olan aykırılıklar nedeniyle ortaya çıkan her türlü zararı karşılayacağımızı kabul, beyan ve taahhüt ederiz.

8. KISMİ GEÇERSİZLİK

Bu Taahhütname maddelerinden herhangi biri geçersiz sayılır ya da iptal edilirse, bu halin Taahhütnamenin diğer maddelerinin geçerliliğine etki etmeyeceğini kabul ederiz.

9. TAAHHÜTNAME GEÇERLİLİĞİ VE DEĞİŞİKLİĞİ

Kurumun yeni bir Gizlilik Taahhütnamesi yayımlaması ve yayımlanan yeni Gizlilik Taahhütnamesinin tarafımızca imza altına alınması durumunda, bu taahhütname hükümlerinin ortadan kalkacağını ve yeni Gizlilik Taahhütnamesi hükümlerinin geçerli olacağını beyan, kabul ve taahhüt ederiz.

10. DEVİR VE SÜRE

10.1. Bu Taahhütnamenin, imza tarihinden itibaren yürürlüğe gireceđini ve yazılı olarak Kurum tarafından sona erdirilmedikçe yürürlükte kalacağını, Kurum ile aramızdaki akdi ilişki sona erse veya bu taahhütname herhangi bir şekilde sona erdirilse dahi bu Taahhütnamedeki gizlilik yükümlülüklerinin geçerli olmaya devam edeceğini beyan, kabul ve taahhüt ederiz.

10.2. Bu Taahhütnamede yer alan hak ve/veya yükümlülüklerin tarafımızca tamamen ya da kısmen bir başkasına devredilemeyeceđini beyan, kabul ve taahhüt ederiz.

11. YETKİLİ VE GÖREVLİ MAHKEME

Bu Taahhütnamenin yorumunda ve bu Taahhütnamede yer alan hükümlere ilişkin ortaya çıkacak olan tüm uyuşmazlıklarda, Mahkemeleri ve İcra Dairelerinin yetkili ve görevli olduğunu beyan, kabul ve taahhüt ederiz.

12. EKLER

Firma, Kurum veya Kuruluş temsilcisinin bu ve/veya benzeri sözleşme/taahhütnameleri imzalamaya yetkili olduğunu gösterir imza sirküleri.

SAĞLIK BAKANLIđI TEMSİLCİLERİ	FİRMA/KURUM/KURULUŞ YETKİLİ TEMSİLCİSİ
Bu Taahhütnamenin, madde 1.3'te belirtilen iş/faaliyet kapsamında, Ek'te yer alan imza sirküleri ile "Firma/Kurum/Kuruluş" ⁴ adına imza atmaya yetkili kılınmış kişi tarafından imzalandığına şahitlik ederiz.	Bu Taahhütnameyi, madde 1.3'te belirtilen iş/faaliyet kapsamında, yetkili temsilcisi olduğum "Firma/Kurum/Kuruluş" ⁵ adına imzaladığımı beyan ederim.
T.C. Sağlık Bakanlığında Madde 1.3 kapsamında yapılacak iş/faaliyeti takip eden Birim Sorumlusunun Adı, Soyadı, Unvanı, Birimi, İmzası ve Tarih	Yetkili Temsilcinin Adı, Soyadı, Unvanı, İmzası, Kaşesi ve Tarih
T.C. Sağlık Bakanlığında Madde 1.3 kapsamında yapılacak iş/faaliyeti takip eden Birimin bađlı olduğu Daire Başkanının (veya Eşitinin) Adı, Soyadı, Unvanı, Dairesi, İmzası ve Tarih	

⁴ İlgili Firma/Kurum veya Kuruluşun açık adı yazılacaktır.

⁵ İlgili Firma/Kurum veya Kuruluşun açık adı yazılacaktır.

KLVZ-EK-14 VT KULLANICI İŐLEMLERİ VE YETKİLENDİRME TALEP FORMU

YETKİLENDİRME YAPILACAK VERİ TABANI BİLGİLERİ						
ADI SOYADI						
T.C. KİMLİK NO						
TELEFON						
E-POSTA						
UYGULAMA ADI						
VERİ TABANI ADI						
KULLANILACAK VERİ TABANI YÖNETİM SİSTEMİ	ORACLE	MS SQL	POSTGRE SQL	MONGO DB	MYSQL	ELASTIC
YETKİLENDİRME TALEPLERİ						
Veritabanı Kullanıcı Adı	EriŐilmek İstenen Őema Adı	EriŐilmek İstenen Obje Adı	Yetki/Açıklama			

TALEP EDEN
AD/SOYAD
İMZA

TALEP EDEN
BİRİM SORUMLUSU
İMZA

TALEP EDEN
DAİRE BAŐKANI
İMZA

FORMUN KULLANIMI İLE İLGİLİ HUSUSLAR:

Formun Kullanımı ile İlgili Hususlar:

1. İlk defa kullanıcı oluřturma iřlemi için KLVZ-EK-11 VERİ TABANI, KULLANICI OLUŐTURMA TALEP FORMU doldurulur.
2. Yetki talebinin tüm Őema/Objeleri kapsaması halinde ilgili alanlar “Tümü” olarak doldurulur.
3. Yetkilendirme iřlemlerinde, iřlemin gerekleřtirildiđi bilgisi, temas personeline e-Posta ile bildirilir.
4. Veri tabanı yöneticileri ile iletiřim için, VTYS yazılımına bađlı olarak dbagrubu@saglik.gov.tr e-Posta adresi kullanılır.

KLZ-EK-15 GÜVENLİ YAZILIM GELİŐTİRME KONTROL LİSTESİ

SBSGM tarafından hazırlanmış olan Güvenli Yazılım Geliőtirme Kontrol Listesine Bakanlıđımız Bilgi Güvenliđi Web Sayfası BGYS Belgeleri menüsü altında yer alan Ortak Dokümanlar bölümünden erişim sağlanabilmektedir.

KLVZ-EK-16 YEDEKLEME KONTROL LİSTESİ

Kontrol Tarihi	Sunucu Adı	Yedek Periyodu	Durum	Son Başarılı Yedek Tarihi

KLZV-EK-17 BİLGİ GÜVENLİĐİ FARKINDALIK BİLDİRGESİ

1. AMAÇ:

Bilgi Güvenliđi Farkındalık Bildirgesi, T.C. Sağlık Bakanlığı bünyesinde görev yapan kamu çalışanlarının, hizmetin yapılması esnasında veya herhangi bir şekilde öğrendikleri kuruma ait gizli kalması gereken bilgilerin, usulüne uygun olarak korunması için kişisel olarak uymakla sorumlu oldukları bilgi güvenliđi kurallarını tanımlar.

2. KAPSAM:

Bu bildirme, Bakanlık bünyesinde görev yapan kamu çalışanlarını bilgilendirmek amacıyla hazırlanmıştır. Kuruma ait gizli kalması gereken bilgileri işleyen diđer personel (danışmanlar, yükleniciler vb.) için Sağlık Bakanlığı Bilgi Güvenliđi Politikaları Kılavuzu ekinde yer alan “Personel Gizlilik Sözleşmesi” hükümleri uygulanır.

3. YASAL DAYANAK:

Bu bildirme, 657 Sayılı Devlet Memurları Kanunu’nun Gizli Bilgileri açıklama yasađı başlıklı 31’nci maddesine, Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018 sayılı Kararı’nın 2’nci maddesinin b fıkrasına, 02/05/2018 tarihli Sağlık Bakanlığı Bilgi Güvenliđi Yönergesi’ne ve Sağlık Bakanlığı Bilgi Güvenliđi Politikaları Kılavuzu’nun 10.5’nci maddesine istinaden hazırlanmıştır.

4. TANIMLAR:

Bu bildirmede geçen;

4.1 Kurum: T.C. Sağlık Bakanlıđını (merkez teşkilatı, bađlı kurum ve kuruluşlar ve genel müdürlükler ile bunlara bađlı tüm taşra teşkilatı ve birimleri),

4.2 Kuruma Ait Gizli Kalması Gereken Bilgiler:

4.1.1 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan “Gizlilik Dereceli Evrak ve Gerecin Güvenliđi Hakkındaki Esaslar” ile tanımlanmış ve usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belgeyi,

4.1.2 Kurum tarafından işlenen (24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan) kişisel veriler ile (21/06/2019 tarihli ve 30888 sayılı Kişisel Sağlık Verileri Hakkında Yönetmelik ile tanımlanan) kişisel sağlık verilerini,

4.1.3 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,

4.1.4 Bakanlığa veya hizmet sunulan ilgili birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar sistemleri içerisinde saklanan veriler, donanım/yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu işleri ifade eder.

5. PERSONELİN YÜKÜMLÜLÜKLERİ:

5.1 Kuruma ait gizli kalması gereken bilgiler, yasal zorunluluklar ve kurum tarafından resmi olarak izin verilmesi halleri dışında, ilgili mevzuatta belirtilen önlemler alınmak suretiyle koruma altında tutulur. Kurum tarafından aksi belirtilmedikçe, söz konusu bilgiler yasal işleme amaçları haricinde doğrudan veya dolaylı olarak kullanılamaz, başka kişi veya kurumlara aktarılamaz, yayımlanamaz, açıklanamaz veya kişisel kopyaları alnamaz.

5.2 Kuruma ait gizli kalması gereken her türlü bilgi, sır olarak saklanır. Çalışanlar bunları sır olarak saklamak, üçüncü kişilere inceletmemek, söylememek, iletmemek ve açıklamamakla yükümlüdür. Bu yükümlülük, çalışanların Kurum ile ilişkisi sona erse de devam eder.

5.3 Kurumsal ve kişisel sosyal medya hesapları kullanılırken, görevin gerektirdiđi dikkat ve özen gösterilir. Kuruma ait gizli kalması gereken bilgiler, hastalara ilişkin kişisel bilgiler (hasta görüntüleri dâhil) hiçbir şekilde sosyal medya ortamlarında paylaşılmaz.

5.4 Kurum tarafından uygun görülen sistemler, uygulamalar, kullanıcı işlemleri ve bilgi sistem ağındaki verilerin ve veri akışının iz kayıtları; hukuki ve idari süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla toplanabilir.

5.5 Çalışanlara tahsis edilen bilgisayar, tablet, telefon, taşınabilir medya gibi cihazlar, sadece göreve yönelik ve kurumsal faaliyetler için kullanılır.

5.6 Çalışanlara tahsis edilen “kullanıcı adı” ve “parola”lar hiçbir şekilde üçüncü kişiler ile paylaşılmaz. Çalışanlar, kurumdan ayrılmalari halinde kendilerine

tahsis edilen kullanıcı adı ve parolaları iptal ettirmekle; kullandıkları bilgisayar ve/veya diđer elektronik veri depolama cihazlarında oluşturduđu veri, bilgi ve belgeler dâhil tüm dosyaları, cihazları ve ofis malzemelerini eksiksiz olarak kurum yetkilisine teslim etmekle ve bunların kopyalarını almamakla yükümlüdür.

5.7 Çalışanlar, bilgisayarlarını kendilerine tahsis edilen “kullanıcı adı” ve “parola” ile oturum açmak suretiyle kullanır. Çalışma sona erince ilgili oturum veya bilgisayar kapatılarak, üçüncü kişilerin bilgisayardaki bilgilere erişimi engellenir. Bilhassa güvensiz ortamlarda, kurum bilgisayarlarının fiziki güvenliđi için azami çaba sarf edilir.

5.8 Kurum tarafından sağlanan İnternet üzerinden girilen ve girilemeyen tüm siteler ve adresler, bu maksatla oluşturulan kayıt sistemi tarafından (gerekli olduğunda kullanılmak üzere) otomatik olarak kayıt altına alınır. Çalışanlara tahsis edilen kullanıcı adı ve parola kullanılmak suretiyle usulüne uygun olarak kayıt altına alınan işlemlerden, kullanıcı adı tahsis edilen kişi yasal olarak sorumlu tutulur.

5.9 Çalışanlar, kendilerine tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP/MAC adresini kullanarak gerçekleştirilen her türlü etkinlikten kişisel olarak sorumludur. Aynı şekilde kurum bilişim kaynakları kullanılarak oluşturulan ve/veya tahsis edilen bilişim kaynađı üzerinde bulundurulanan her türlü bilgi, belge, doküman, yazılım vb. içeriğinden ilgili kişi şahsen sorumludur.

5.10 Çalışanlar, kendilerine teslim edilen kullanıcı adı ve parolanın gizli kalmasını sağlamakla yükümlüdür. Çalışanların şahsi kusurları nedeniyle kullanıcı adı ve parolalarının üçüncü kişiler tarafından öğrenilmesi halinde, bu bilgiler kullanılarak yapılan iş ve işlemlerden, kusuru bulunan kişi şahsen sorumlu tutulabilir.

5.11 Çalışanlara tahsis edilen *@sađlık.gov.tr uzantılı tüzel ve kurumsal e-posta hesapları, sadece görevle ilgili faaliyetler için kullanılır. Kurum içinde veya dışındaki kişilere iş ile ilgili olmayan toplu ve/veya kişisel e-posta gönderilmez. Çalışanlar, kurum içine veya kurum dışına göndermiş oldukları tüm e-postalardan kişisel olarak sorumludur.

5.12 Çalışanlar, kendilerine teslim edilmiş yazılım, donanım, araç ve gereç üzerinde; kurum bilgisi dışında mekanik (donanım ekleme, kaldırma vb.) ya da yazılımsal deđişiklik (yeni yazılım yükleme, kurum tarafından koyulan bir kısıtlamayı aşmak üzere bilgisayar ayarlarını deđiştirme vb.) yapamaz.

5.13 Çalışanlar, kurum tarafından yüklenen işletim sistemi ve uygulama yazılımları haricinde, ilgili birimlerin bilgisi dışında başka yazılımları yükleyemez. Kurum tarafından yüklenmemiş yazılımlardan doğacak sorumluluk, ilgili bilgisayarın sahibi olan kişiye aittir.

KLVZ-EK-18 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: <input type="checkbox"/> Servis Dışı Bırakma Saldırısı (DoS/DDoS) <input type="checkbox"/> Web Uygulamaları Güvenlik İhlalleri <input type="checkbox"/> Bilgi Sızdırma (Data Leakage) <input type="checkbox"/> Zararlı Yazılım (Malware) <input type="checkbox"/> Dolandırıcılık (Fraud) <input type="checkbox"/> Port Tarama <input type="checkbox"/> Veritabanı Saldırısı <input type="checkbox"/> Diğer (Lütfen açıklayınız):	<input type="checkbox"/> Sosyal Mühendislik <input type="checkbox"/> Veri Kaybı/ Veri İfşası <input type="checkbox"/> Zararlı Elektronik Posta(Spam) <input type="checkbox"/> Parola Ele Geçirme <input type="checkbox"/> Taşınır Cihaz Kaybı <input type="checkbox"/> Kimlik Taklidi <input type="checkbox"/> Oltalama (Phishing) <input type="checkbox"/> Kişisel Bilgilerin Kötüye Kullanımı
4. Olay sistem kesintisine sebep oldu mu? <input type="checkbox"/> Evet <input type="checkbox"/> Hayır	
5. Olayın: <u>Tahmini başlangıç zamanı</u> Tarih : Saat : <u>Tespit edildiđi zaman</u> Tarih : Saat :	
6. Eklemek istedikleriniz:	

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

KLZV-EK-19 İŐ SÜREKLİLİĐİ 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 Kaynađı	HBYS Firması destek personeli
Veri Tabanı	XXX veri tabanı
Tesisler	Sistem odası
Tedarikçiler	XXX firması
Veri tabanı Yedek alma stratejisi	Tam Yedekleme / deđişen kısımların yedeđinin 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-20 YASAL MEVZUAT UYUMU İÇİN TAKİP LİSTESİ

No	İlgili Yasal Mevzuat	Sayı	Yayın Tarihi	Değişim Tarihi	Kaynak
1	663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname	663	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 ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ	28544	30.01.2013		Kamu Sertifikasyon Merkezi

10	Kamu Kurum ve Kuruluşları İçin IPV6'ya Geçiş Planı Genelge	27779	08.12.2010	http://www.mevzuat.gov.tr
11	İnternet Alan Adları Yönetmeliđi	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 BGYS 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 Deđiştirilerek 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

Not: Listede yer alan mevzuat örnek olarak yazılmıştır. Tam bir liste deđildir. İlgili kurumlarca, bilgi güvenliđi açısından dikkate alınması ve uyum sağlanması gereken tüm mevzuatın belirlenmesi, bu listeye kaydedilmesi ve takip edilmesi gerekmektedir.

KATKIDA BULUNANLAR

Adı Soyadı	Unvanı	Birimi
Ahmet ALTUNTAŞ	Birim sorumlusu	SBSGM
Ahmet Esad BERKTAŞ	Birim sorumlusu	SBSGM
Alper ÖZCAN	Birim sorumlusu	SBSGM
Buket ERDOĐAN	Birim sorumlusu	SBSGM
Ayşe GÜL ÇETİN	Birim sorumlusu	SBSGM
Ceyhan VARDAR	Birim sorumlusu	SBSGM
Deniz Tugay YANGI	Birim sorumlusu	SBSGM
Dilek GENÇER ÖZTEKİN	Birim sorumlusu	SBSGM
Dilek KAVAK	Birim sorumlusu	SBSGM
Fatih KARAKÖSE	Birim sorumlusu	SBSGM
Gamze CİMİLLİ	Birim sorumlusu	SBSGM
Gamze KARAKÖSE	Birim sorumlusu	SBSGM
Gizem YILDIZ	Birim personeli	SBSGM
Halil İbrahim ÖZDER	Birim sorumlusu	SBSGM
Mehmet CAVLAMAZ	Birim sorumlusu	SBSGM
Nuran ERDEM	Uzman	Kırklareli İl Sağlık Müdürlüğü
Nurullah ÇAKIR	Birim sorumlusu	SBSGM
Ruhi YİYİT	Birim sorumlusu	SBSGM
Tamer ERDOĐAN	Birim sorumlusu	SBSGM
Ümit MADEN	Birim personeli	SBSGM

(Alfabetik sıraya göre listelenmiştir)