1-Amaç

- Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmek,
- Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,
- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
- Bilgi Güvenliği Yönetim Sistemini sürekli gözden geçirmek ve iyileştirmek,
- Bilgi Güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmek,
- Hasta yada çalışanlara ait tıbbi ve kişisel bilgilerin, doğru ve güvenli şekilde kayıt altına alınması ve depolanması ile ihtiyaç duyulan doğru bilginin doğru bilginin, bilgi mahremiyeti ve güvenliği gözetilerek, doğru zamanda, doğru kişiye ulaştırılmasını sağlamak.

2-Kapsam

Bilgi Güvenliği Politikası aşağıdaki varlık ve teknoloji kategorilerini kapsamaktadır:
-Veri dosyaları, sözleşmeler ve benzeri tüm bilgi varlıkları,
-Uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları,
-Yönlendirici cihazları, güvenlik cihazları, sistem yönetim sunucuları, yasal yükümlülükler kapsamında kurulmuş sunucu sistemleri, uydu sistemleri, bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıklar,
-Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,
-Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıkları,
-Kurum tarafından üretilen, kullanılan ve/veya geliştirilen tüm veriler

-Hastane bünyesinde faaliyet gösteren tüm birimlerde çalışan personeller, sunucular, hizmet sağlayıcılar,

3-Sorumlular

Üst yönetim, tüm hastane çalışanları,

4-Tanımlar

Sunucu: Ana bilgisayar

Donanım: Bilgisayarın fiziki parçalarıdır.

Otomasyon: Bir işin insan ile makine arasında paylaşılmasıdır.

Anti-virüs Programı: Hastane otomasyon sistemine dışarıdan ve içeriden gelebilecek tehditlere ve kötü amaçlı yazılımlara karşı koruma amaçlı bir programdır.

Uzaktan Erişim: Başka bir yerdeki bir bilgisayara IP adresi yordamıyla bağlanma çeşididir.

İnternet: Tüm dünyaya yayılmış, birbirleri ile bağlantılı, yani birbirleri ile "konuşabilen" yüz binlerce bilgisayardan oluşan bir ağdır.

Bellek: Bilgi depolama ünitesidir.

Log-on: Oturum açmak

HBYS: Hastane Bilgi Yönetim Sistemi

Spam: İstek dışında gönderilen reklam içerikli mail.

Junk: Gereksiz (çöp)

Firmware: Donanımların veya cihazın işlevlerini nasıl yerine getireceklerini bildiren ve genellikle tekrar yazılabilir olan ufak kodlar.
SSID (Hizmet Seti Kimliği): Bir kablosuz ağı tanımlayan addır.

Reset: İlk duruma getirmek, sıfırlamak.

5- BILGİ YÖNETİM SİSTEMİ (BYS) YÖNETİM SÜRECİ

a. Bilgi Güvenliği Komisyonu

AD SOYAD	UNVAN
Satılmış BİLGİN	Başhekim
Uğur OKUR	İdari Mali İşler Müdürü
Sina Cafer DEMİR	İdari Mali İşler Müdür Yardımcısı
Serpil ALAN	Kalite Yönetim Direktörü
Fatih ERKOÇ	Bilgi İşlem Sorumlusu
Coşkun ÇELEN	Bilgi İşlem Yazılım Destek

b. Bilgi Güvenliği Komisyonunun Görev, Yetki ve Sorumlulukları

- Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde Bilgi Güvenliği Politikaları Yönergesine bağlı olarak çalışma grupları tarafından hazırlanacak olan kılavuzlarla ilgili yenilenme kararlarını verir,
- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlar,

BİLGİ GÜVENLİĞİ

İnsan Kaynakları ve Zafiyetleri Yönetimi

- Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
- Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
- ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kâğıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
- Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
- İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kâğıt kesme makinasında imha edilmelidir.
- Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
- Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
- Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
- Göreve yeni başlayan ve ayrılan personeller **"Bilgi Güvenliği İşe Başlama ve İşten Ayrılma Süreç Prosedürü"**nde belirtildiği şekilde **"İşe Başlama ve İlişiği Kesme Belgesi"** ni doldurarak gerekli tanımlamaları yapılmalıdır. Birimler arası görev değişikliğinde "**Görev Değişikliği formu"** doldurulur.
- Bilgi güvenliği konusunda çalışanlara farkındalık eğitimi verilmelidir.

Kişisel Sağlık Verilerinin Korunması ve Güvenliği

- Kurumumuzda göreve başlayan tüm personele **"Bilgi Güvenliği Farkındalık Bildirgesi"** tebliğ edilir. Kuruma ait gizli bilgilere erişim ihtiyacı olan tüm personel **" Personel Gizlilik Sözleşmesi "** ni okuyarak imzalamalıdır. Veri paylaşımı yapılan firmalar ile (SBYS, Laboratuvar hizmet alımları, Görüntüleme hizmet alımları gibi) **"Kurumsal Gizlilik Sözleşmesi"** yapılmalıdır.
- Gizlilik sözleşmesinde belirtilen yükümlülüklerin bir veya birkaçına uyulmaması durumunda hukuki ve cezai yaptırım uygulanır.
- Bilgi Yönetim Sistemine ait verilen tüm yetkiler, yetki talep eden kişilerin ve birim sorumlusunun imzası ile kayıt altına alınarak verilmelidir.
- Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletmez.
- Hastanın sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programlar vs. buna dâhildir.
- Hasta dosyasının bir kopyası hastaya teslim edilir. Hiçbir hasta kaydı, elektronik veya kâğıt ortamında (Bakanlığın bu konuda çıkardığı genelgeler hariç) hiçbir kuruma veya üçüncü şahıslara sözlü veya yazılı olarak teslim edilemez.
- Hastanın dosyası izlenmeli, gelişigüzel ortada bırakılmamalı, bilgisayar ekranında başkalarınca okunabilecek şekilde bırakılmamaktadır.
- Telefonla konuşurken hasta ile ilgili özel, mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen gösterilmelidir.
- Bütün hasta sağlık kayıtları fiziksel olarak korunmuş mekânlarda saklanmaktadır.
- Yönetimsel analizler yapmak için veri tabanındaki veriler bir yerden başka bir yere aktarılırken, kayıtlarda bulunan kişisel kimlik tanımlayıcıları kayıttan çıkartılmakta ve analizler hasta ile hastalık bilgisi eşleştirmeden yapılmaktadır.

İletişim/İnternet Erişim Güvenli Kullanımı

- Bilgisayar ağı erişim ve içerik denetimi yapan bir güvenlik duvarı üzerinden internete çıkmaktadır.
- Hastanemizde içerik filtreleme sistemi kullanılmaktadır. İstenmeyen siteler (pornografik, oyun, kumar vs.) yasaklanmıştır.
- Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgisi olmayan sitelerde gezinmek yasaktır.
- İş ile ilgisi olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek ve indirmek yasaktır.
- İnternet üzerinden, kurumun yetkili birimlerinden onay alınmaksızın kurum adına elektronik işlem yapılamaz.
- İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez.
- Bütün kurum bilgisayarları anti-virüs yazılımına sahiptir.
- Anti-virüs güncellemeleri sunucular vasıtası ile yapılmaktadır. Sunucuların internete bağlantısı olup otomatik olarak veri tabanlarını güncellemektedir.
- Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmaktadır.
- Zararlı programları (virüs, solucan, Truva atı…) hastanemiz bünyesinde oluşturmak ve dağıtmak yasaktır.
- Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramaz.
- Bilinmeyen kaynaklardan gelen cd-rom ve dvd-rom lar anti-virüs programı tarafından taraması otomatik olarak yapılmaktadır.
- Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
- Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

Kablosuz Erişim:

- Erişim cihazlarında ki güncellemeler sunucu tarafından düzenli olarak taranmakta ve Bilgi işlem Birimi tarafından güncellemeler yapılmalıdır.

- Erişim cihazlarına kolayca erişilebilir olmaması için tavana monte edilmelidir.
- Cihaza erişim için güçlü bir şifre kullanılmaktadır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır.

HBYS Kullanımı; Hastane Bilgi Yönetim sistemi HBYS modülü hastaların kimlik, adres, karne, ve kurum bilgileri dahil kayıtlarının yapıldığı, hastaya muayene sırasının verildiği, hastaya verilen hizmetlerin işlenebildiği, laboratuvar ve ileri tetkiklerin sonuçlarına ulaşabildiği, hastaların daha önceki kayıtları ve bir sonraki muayeneye gelmelerinde hastalara hangi tanı ve hizmetlerin yapıldığı, hastanın tahakkuk bilgilerinin görülebildiği bir sistemdir.

PACS Kullanımı; Hekim tetkik istemi yaptıktan sonra görüntüleme birimi bilgilendirme ekranına düşer. Hastanın kimlik doğrulaması yapılarak çekim alanına alınır. İstem yapılan bölgeye göre, sistem otomatik olarak görüntüleri ekrana aktarır. Çekimler tamamlandıktan sonra, ayarlama yapılıp hekim bilgilendirme ekranına sistem tarafından otomatik gönderilir.

LBYS Kullanımı; Hekim tetkik istemi yaptıktan sonra laboratuvar birimi bilgilendirme ekranına düşer. Hastanın kimlik doğrulaması yapılıp sistemden kabulü yapılır, mahremiyeti sağlanarak kan alma birimine alınır. İstenilen tetkiklere göre barkod çıkartılıp uygun tüplere yapıştırılır. Numune kabul yapılarak, çalışılır. Laboratuvar sonuçları zamanında hekim bilgilendirme ekranına sistem tarafından otomatik gönderir.

WEB Kullanımı; Hastane WEB sitesi Sağlık Bakanlığının belirlediği standarda uygun olarak tasarlanır. Web sitesinin hizmeti; Dış paydaşlara hastane tanıtımı, yönetim, personel tanıtımı, hizmet verilen üniteler, sağlık rehberi, özellikli hizmetler, hasta rehberi, hastanede yapılan tetkik sonuçlarına online ulaşılır özellikli hizmet birimleri ve verilen hizmet kalite standartları, iletişim ve ulaşım hizmeti bilgilerine ulaşılır.

Dosya Sunucusu Kullanımı; Bilgi güvenliği sağlayarak, personele sunulan dokümanlar değiştirilemez bir şekilde uzaktan erişim sağlanır.

E-posta Kullanımı

- Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
- Bakanlık ile ilgisi olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamı içerisine iliştirilen öğelerde dâhildir.
- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Kurum işlevleri dışında, kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
- Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalı ve Bilgi İşlem Yazılım Birimine haber verilmelidir.
- Kullanıcıların kullanıcı kodu, şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal Bilgi işlem birimine bilgi verilmelidir.
- Çalışanlar e-posta ile uygun olmayan içerik (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb) paylaşmamalıdır.
- Kurum çalışanları mesajlarını düzenli olarak kontrol etmekte ve kurumsal mesajlar cevaplandırılmalıdır.
- Kurum çalışanları e-postaların kurum dışında ki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludur.
- İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.
- Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
- Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.
- Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.
- Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.
- Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.

Son Kullanıcı Güvenliği

- Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir.
- Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı loglanarak kayıt altına alınmalıdır.
- Güvenlik zafiyetlerine karşı, son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır.
- Son kullanıcılar bilgisayarlarında ki ve sorumlusu oldukları cihazlarda ki bilgilerin düzenli olarak yedeklerini almalıdır.
- Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.
- Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde hastaneye ait olmayan USB flash bellek ve/veya harici hard disk gibi taşınabilir medya kullanmamalıdır.

HBYS' YE İLİŞKİN YAZILIMSAL SÜREÇLER

Şifre Güvenliği

- HBYS kullanıcıları programın zorunlu bırakması nedeniyle şifrelerini 6 ayda bir değiştirmek zorundadır.
- Şifreler en az 8 hane olmalıdır.
- Şifrelerde harf ve rakam kullanılmalıdır.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Şifreler başkası ile paylaşılmamalı, kağıtlara ya da elektronik ortamlara yazılmamalıdır.
- Şifre, kullanıcı adı ile aynı olmamalıdır.
- Şifre ardışık rakamlardan oluşmamalıdır.
- Herhangi bir kişiye telefonda şifre verilmemelidir.
- Şifreler aile bireyleriyle paylaşılmamalıdır.
- Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
- Sistemde şifreler %100 korumalı olacak şekilde ayarlanmıştır.

HBYS İşletimi ve Değişiklik Yönetim Süreçleri

HBYS işletimi; Bakanlıkların yayınlamış olduğu talimatlar ve güncellemeler doğrultusunda, hastane başhekimi başkanlığında toplanan ekip ile yapılacak olan öneriler değerlendirilir. İşletimi sağlanır.

Değişiklik yönetim süreci; Bakanlıkların yayınlamış olduğu talimatlar ve çalışanların önerileri doğrultusunda, hastane başhekimi başkanlığında toplanan ekip ile yapılacak olan öneriler değerlendirilir. Uygun görülen değişiklikler ve yeni işleyişler uygulamaya geçilir.

Varlık Yönetimi;

Varlık, kurum için değeri olan herhangi bir şey olarak tanımlanabilir. Standart envanter yönetimi bakış açısıyla, maddi değeri olan tüm varlıklar yürürlükteki Taşınır Mal Yönetmeliği ya da Kamu İdarelerine Ait Taşınmazların Kaydına İlişkin Yönetmelik uyarınca kayıt altına alınır ve ilgili yönetmeliklerde belirtilen usuller ile takibi yapılır.

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

Bilgi Varlıkları; üretilen bilginin işlenmesi, saklanması, iletilmesi, korunması, sürekliliğinin sağlanması ve yok edilmesi için kullanılır. BGYS kapsamında varlıklar; yazılım ve donanım şeklinde bulunur. BY.PR.08 BİLGİ SAKLAMA ORTAMLARI YOK ETME PROSEDÜRÜ, BY.PR.10 YEDEKLEME PROSEDÜRÜ, BY.PR.11 ERİŞİM KONTROL PROSEDÜRÜ bulunur.

BGYS kapsamında varlık envanterine esas olan varlık kategorileri aşağıdaki gibidir.

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

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.
Yazılımlar: İşletim sistemleri, ofis uygulamaları, HBYS yazılımları, laboratuvar yazılımları, tıbbi görüntüleme yazılımları, kurumsal yazılımlar (EBYS, ÇKYS, KPS, HİTAP vb.) vb.
Fiziksel varlıklar: Sunucular, masaüstü bilgisayarlar, taşınabilir bilgisayarlar, depolama birimleri, yedekleme birimleri (kasetler, hard diskler vb.), aktif cihazlar (anahtarlama cihazı, güvenlik duvarı, yönlendirici, ağ erişim cihazı, anahtar, modem, erişim noktası vb), fakslar, fotokopiler, yazıcılar, santraller, telefonlar, evrak imha cihazları, ağa bağlı olarak çalışan veya ağa bağlanma arayüzleri olan tıbbi cihazlar vb.
İnsan Kaynakları: Çalışanlar
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.
Mekânlar: Yönetim ve hizmet odaları, sunucu odaları, arşiv odaları, tıbbi kayıt saklama odaları vb.

Varlık Envanterinin Tespiti

Çalışmanın bilgi güvenliği alt komisyonundan alınan yetki ve destekle, Kurumun üst yönetimi tarafından görevlendirilecek bir ekip vasıtasıyla yapılması gerekir. Ekibe kurumun bilgi güvenliği yetkilisinin başkanlık etmesi sağlanır.

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

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

Varlık envanteri, sadece fiziksel varlıklar veya bilgi sistem teçhizatından oluşmaz. Varlıklar belirlenirken, başta hassas bilgilerin işlendiği kritik iş süreçleri olmak üzere, bu süreçlere konu olan tüm kurumsal bilgi varlıklarının ortaya çıkarılması gerekir. Envanterde yer alan her bir varlık için "varlık sahibi" belirlenir. Varlık sahibi gerçek bir kişi olabileceği gibi, bir birim ya da kurum da olabilir. 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 değeri nedeniyle daha sıkı güvenlik tedbirleri uygulanır.
Envanterde yer alan her bir varlık için "varlık sahibi" belirlenir. Varlık sahibi 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 değeri nedeniyle daha sıkı güvenlik tedbirleri uygulanır. Kurum bilgi varlıklarının tespitinde örneği KLVZ-EK-05 Kurum Bilgi Varlıkları Envanter Çizelgesi kullanılabilir veya kurumun kendi özelliklerine uygun bir başka çizelge geliştirilebilir.
Varlık sahipleri;
Varlıklarını envantere doğru olarak kaydettirmekten, Varlıklarına uygun gizlilik derecesi ve varlık değeri atamaktan, varlıklarının uygun şekilde korunmasından, Varlıklara erişecek kişi veya süreçleri için erişim izinlerini planlamaktan, bunlarla ilgili kararları vermekten, Varlıkların silinmesi ya da imha edilmesinde uygun işlemlerin uygulanmasından sorumludur. Çalışanlar ve dış tarafların kullanıcıları; iş akitleri, sözleşmeleri veya anlaşmaları sona erdiğinde, ellerinde olan tüm kurumsal varlıkları iade etmekle mükelleftir.

Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi

Kurum bilgi varlıkları, içerdikleri verilerin hassasiyeti, kurum için taşıdıkları önem ve yasal zorunluluklar dikkate alınarak uygun bir şekilde sınıflandırılır/ gizlilik derecesi verilir. Bilgi varlıklarına (resmi yazılar dâhil) verilecek gizlilik dereceleri için 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe giren "**Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar**" dikkate alınır. Buna

göre; İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda kişi güvenliği veya milli güvenlik açısından saygınlık ve çıkarlarımıza **hayati derecede** zararlar verebilecek, yabancı bir devlet için faydalar temin edebilecek ve güvenlik bakımından **olağanüstü** sonuçlar doğurabilecek bilgiler "**çok gizli**", İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından, saygınlık ve çıkarlarımıza **büyük zarar** verebilecek, yabancı bir devlet için faydalar temin edebilecek özellikler taşıyan bilgiler "**gizli**", İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından saygınlık ve menfaatlere zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek bilgiler "**özel**", İçerdiği bilgi itibarıyla ÇOK GİZLİ, GİZLİ veya ÖZEL gizlilik dereceleriyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi durumunda gerçek ve tüzel kişilerin itibarını sarsacak bilgiler "**hizmete özel"** olarak sınıflandırılır. Çok gizli gizlilik dereceli evrak ve dokümanlar, Kurumun en üst düzey yöneticisi tarafından belirlenen ve yazılı olarak görevlendirilen kişi veya kişiler tarafından hazırlanır ve özel usullere göre dağıtımı yapılır. Bu tip evrak ve dokümanlar korumalı odalarda, kasa, çelik masa veya diğer tipte çelik dolaplar içinde muhafaza edilir. Gizli, özel ve hizmete özel evrakların gizlilik derecesi, yazıyı hazırlayan makam tarafından tayin edilir. Gizli ve özel evraklar kilitli çelik dolaplarda, hizmete özel evraklar ise masa gözlerinde kilitli olmak şartıyla muhafaza edilir.

Yukarıda sıralanan gizlilik derecelerinden hiçbirisi ile sınıflandırılmayan ve özel bir koruma gerektirmeyen evrak ve dokümanlar, "**tasnif dışı**" olarak kabul edilir. 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. 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. 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. Resmi yazı şeklinde olmayan ancak içerdikleri bilgilerin hassasiyeti açısından sınıflandırılmaya ihtiyaç duyulan diğer bilgi varlıklarının sınıflandırılması için de yukarıda belirtilen gizlilik dereceleri kullanılır. Bu varlıkların korunması ve erişim haklarının düzenlenmesi için alınacak tedbirler, yapılacak olan risk analiz neticesine göre belirlenir ve bu Kılavuz'un 6.1 (Erişim Kontrol Politikası) maddesi gereği hazırlanacak kurum erişim kontrol politika/prosedürü içerisinde ayrıntılı olarak açıklanır.

İş Sürekliliği Yönetim;

İş sürekliliği; kurumun vermekte olduğu kritik bilişim hizmetlerinin sunumuna kesintisiz bir şekilde devam etmesi veya türü ve nedeni ne olursa olsun, herhangi bir kesinti ya da olay durumunda, önceden belirlenmiş kritik iş süreçlerini, önceden tanımlanmış kabul edilebilir seviyede sunma yeteneğini sağlayan yöntemdir. Kurum iş süreçlerinde hizmet sürekliliği yeteneğini; etkin bir risk yönetimi, öncelikli hizmetlerini kesintiye uğratabilecek olayların tanımlanması, bu olayların bertaraf edilmesi için gerekli tedbirlerin alınması, olay anında ve sonrasında kritik hizmetlerin en hızlı ve etkin nasıl ayağa kaldırılacağının senaryolarla planlanması ve bu senaryoların tatbikatlarla test edilmesi ile elde eder.

Bu bölümde anlatılan iş sürekliliği, bilgi varlıklarının iş sürekliliğinin sağlanmasına yönelik tedbirleri kapsamaktadır. Yaşanacak her türlü afet ve acil durumda sunulan hizmetlerin sürdürülebilir olması, fiziksel ve fonksiyonel olarak afet ve acil durumlara hazırlıklı olunması, zamanında, hızlı ve etkili müdahalede bulunularak en kısa sürede olağan işleyişe dönülmesi için alınması gereken tedbirler ve yapılması gereken çalışmalar "Hastane Afet ve Acil Durum Planı (HAP) Hazırlama Kılavuzu"nda ayrıntılı olarak anlatılmış, örnek planlar verilmiştir.

İş sürekliliği kurma nedenleri; hizmet sürekliliğini sağlamak ve kesintilere yeterli şekilde yanıt verme kabiliyetini kazanmak olabileceği gibi yasa, yönetmelik ve sözleşmelerden kaynaklanan sorumlulukları yerine getirmek de olabilir.

Etkin bir bilgi güvenliği iş sürekliliği sistemi kurulduğunda kurumun şu çıktıları elde etmesi beklenir;

- Kritik süreç ve varlıkların hizmet sürekliliğinin sağlanması,
- Dokümante edilmiş ve tatbikatlarla test edilmiş bir olay/kriz yönetim kabiliyeti,
- Hizmet verdiği ve/veya yükümlü olduğu paydaşlarının gereksinimlerini anlamış ve bu gereksinimlere cevap verecek iş süreçlerinin kurulmuş olması.

Kritik iş sürekliliği yönetimi sadece iş sürekliliği planı hazırlanması, yedekleme yapılması, felaket merkezi oluşturulması, prosedürler, detaylı talimatlar oluşturulması değil; bunların bütünleşik olarak hizmet sürekliliğinin iyileştirilmesi amacıyla uygulanmasıdır.

İş sürekliliği planları, verilen hizmetleri önceliklendirme, olası tehdit ve zafiyetleri değerlendirerek gerekli önlemleri almak suretiyle hizmet sürekliliğini sağlama, hizmetlerin kesintiye uğramasına neden olan olaylara önceden tanımlanmış senaryolarla müdahale etme, süreçleri onarma ve planlı olarak yeniden başlatma konularında kılavuzluk yapan dokümante prosedürlerdir.

İş sürekliliği planları, felaket kurtarma çözümleri değil, felaketin olumsuz sonuçlarının oluşmasını önlemeye odaklanan eylem planlarıdır. Felaket kurtarma senaryoları iş sürekliliği planlarının bir parçasıdır. Felaket kurtarma çözümleri, felaket sonrasında verilerin kurtarılmasına odaklanırken, iş sürekliliği çözümleri, hem verilerin erişilebilirliğini gözetir hem de kurumun felaket sonrasında en hızlı şekilde yeniden hizmet verebilmesine odaklanır.

✓ İş Sürekliliği Adımları

Kurumsal iş sürekliliği yönetim sisteminin kurulması ve işletilmesi için öncelikle iş sürekliliği kapsamının belirlenmesi gerekir. Bunun için ilk adım kritik iş süreçlerinin çıkarılması ve önceliklendirilmesidir. İş sürekliliği kapsamı bu şekilde oluşturulur.

Kapsam belirlendikten sonra bu iş süreçlerine ilişkin mevcut durum analizi yapılır. Mevcut durum analizinde kurumun kritik iş süreçlerinin fotoğrafı çekilir. Yürütülen bu hizmetleri kesintiye uğratabilecek tehditler var mı, bu tehditlerle ilgili süreçte zayıf noktalar var mı gibi hususlar incelenir ve detaylı analiz edilir. Başarılı bir mevcut durum analizi için kurumsal risk yönetimi sürecinin kurum kültürü olarak benimsenmiş, risk haritaları çıkarılmış ve kurumsal kabul edilebilir risk seviyesi belirlenmiş olmalıdır.

İş sürekliliğinin kapsamının belirlenip, mevcut durum analizi yapıldıktan sonra, hangi iş sürecinin kesintisiz hizmet verebilmesi için hangi kaynaklara ihtiyaç olduğunun dokümante edilmesi ile kaynak planlaması ortaya koyulur.

Her başarılı süreç yönetiminde olması gerektiği gibi iş sürekliliği süreci için roller ve sorumluluklar atanır.

Atanmış olan sorumlular tarafından hizmetleri kesintiye uğratabilecek olumsuz senaryolar tatbikatlarla test edilir, sonuçlar değerlendirilir, varsa aksaklıklar giderilir ve sürekli takip edilir.

✓ Kritik Varlıkların / Süreçlerin Tanımlanması

Kurum tarafından gerçekleştirilen tüm iş süreçleri önemli kabul edilirken, bir olay meydana gelmesi durumunda, kurum mevcudiyeti ve itibarı açısından kritik önem taşıyan süreçlerin ayağa kaldırılmasına öncelik verilir. İş sürekliliği yönetimi için öncelikle kritik iş süreçlerinin ve bu süreçlerde kullanılan sistemlerin belirlenmesi ve listesinin oluşturulması gerekir.

Yürütülen iş, işlem ve sürecin kritik olabilmesi için aşağıda belirlenen durumlardan en az birine uygun olması gerekir;

- İş sürecinin kesintiye uğraması ya da yavaşlaması durumunda kurum için yasal, finansal, operasyonel ve benzeri büyük riskler oluşur.
- İş sürecinin etkilediği ya da etkilendiği sistem ya da paydaşlar, stratejik olarak önemli ya da geniş kitlelerdir.
- İş süreci insan hayatını ya da toplum sağlığını etkilemektedir.
- İş sürecinin kesintiye uğraması kurumsal itibarı maddi ya da manevi olumsuz bir şekilde etkileyecek niteliktedir. (Örneğin SBYS'ler)

Kritik varlıklar / süreçler belirlenirken;

- Süreç ile ilgili iç ve dış yükümlülükler,
- Süreçten yararlanan / hizmet alan paydaşların hizmet sürekliliği ihtiyaçları,

Yasal ve düzenleme amaçlı atanan sorumluluklar,

- Protokollerle anlaşmaya varılmış hizmet zorunlulukları,
- Hizmetin sürdürülmesinde başarısız olunması durumunda sonuçlarının ne büyüklükte olacağı gibi hususlar dikkate alınarak BY.FR.11 İş Sürekliliği Formları arasında yer alan "Kritik Süreçler / Varlıklar Listesi" oluşturulur ve iş sürekliliği kapsamı belirlenir.

Kritik iş süreçlerinin tanımlanmasında yararlanılacak ve kritik süreçler / varlıklar listesi ile ilişkilendirilecek dokümanlar;

- Varsa hizmet bekleyen ve yasal yükümlülüklerle bağlı olunan dış paydaşlarla yapılan protokollerin listesi,
- Tedarikçiler ile yapılan sözleşmeler,

Kurumdan beklenen kritik hizmetlerin sağlanmasını destekleyen tüm iş süreçlerinin / faaliyetlerin envanteridir.

✓ **Mevcut Durum Analizi**

Kritik iş süreçlerinin sürekliliğinin sağlanmasına ilişkin gerekli olan koşulların ortaya koyulduğu ve iş sürekliliğine engel olabilecek olası tehditlerin tespit edildiği aşamadır.
İş etki analizleri ve risk işleme çalışmalarının değerlendirilmesi ile mevcut durum ortaya koyulur.
İş etki analizi, iş kesintisine neden olabilecek durumlar ve bunların etkilerinin değerlendirilmesidir. Kesintiye neden olabilecek durumlar, darboğazlar, zafiyetler göz önüne alınarak süreçlerin kapsamlı bir fotoğrafı çekilir, sınıflandırılır (az önemliden en önemliye doğru sıralanır) ve buna yönelik olarak risk işleme çalışmaları yapılır.
İş sürekliliğinin temelinde risk yönetimi vardır. İş etki analizinden edinilen bilgilere göre kesintiye yol açabilecek olayların riskleri tanımlanır. Risk yönetimi, iş etki analizleri ile ilişkilendirilmiş risk değerlendirme raporunun hazırlanması vb. süreçler Kılavuz'un 5.3 (Risk Yönetimi) maddesinde açıklanmıştır. İş sürekliliği için planlama yapılırken kurumsal risk yönetimi dikkate alınır.
İş etki analizleri ve risk değerlendirme çalışmaları neticesinde; kritik iş süreçlerine yönelik tehditler, zafiyetler, olasılıklar ve alınacak önlemler ile mevcut durum analizi ortaya koyulur.

✓ **Kaynak Planlaması**

Kritik iş süreçlerinin en temel fonksiyonlarının, en az veri kaybı ile en kısa sürede tekrar hizmet verebilir duruma getirilmesinin sağlanması için hangi kaynaklara ne kadar ihtiyaç duyulduğunun ve bu kaynakların maliyetinin çıkarılması gerekir.

Kaynak planlaması yapılırken o işin sürekliliğinin sağlanması için ihtiyaç duyulan tüm mali kaynaklar, teknoloji, alt yapı, tedarik edilecek malzemeler, bina, ulaşım ve benzeri kaynak tipleri ve tanımlanmış yetkinlikleri ile beraber personel detaylı olarak belirlenir ve KLVZ-EK-19 İş Sürekliliği Formları içinde örneği yer alan "Kaynak İhtiyaç Listesi" oluşturulur.

İş sürekliliği kaynak ihtiyaç listesi, 24 saat – 72 saat – 1 hafta gibi iş kurtarma fazları için ayrı ayrı detaylı olarak oluşturulabilir. 24 saat fazında en temel ihtiyaçlar planlanırken, devam eden fazlarda daha detaylı ihtiyaç duyulacak kaynaklar belirtilebilir.

Kaynak planlarken kriz yönetim merkezi olarak kullanılabilecek 7X24 kullanıma uygun, internet bağlantısı, telefon/mobil telefon, taşınabilir bilgisayar, projeksiyon cihazı, yazı tahtası, muhtelif kırtasiye donanım ve imkanlarının hazır bulundurulduğu kriz yönetim merkezinin de belirlenerek kararının alınması gerekir.

✓ **Roller ve Sorumluluklar**

İş sürekliliği süreçlerinin standartlara uygun ve etkin şekilde işletilebilmesi için oluşturulması gereken organizasyon yapısı ve roller Şekil 3'te açıklanmıştır.

Üst Yönetim;

Üst Yönetim kritik iş süreçlerinin sürekliliğinin sağlanmasından birinci derecede sorumludur.

Bilgi güvenliği alt komisyonu tarafından belirlenen iş sürekliliği hedeflerini onaylar. (Örnek iş sürekliliği hedefi: X faaliyetlerinin Y zamanda ayağa kaldırılması, X faaliyeti felaket senaryosunun Y kez tatbikatlar ile test edilmesi vb.)

İş sürekliliğinde yer alacak personelin görev yetki ve sorumluluklarını belirler.

Kritik iş süreçlerinin, iş sürekliliği gereksinimlerini ve iş ihtiyaçlarını belirler veya görevlendirmiş olduğu personel tarafından belirlenmesini sağlar.

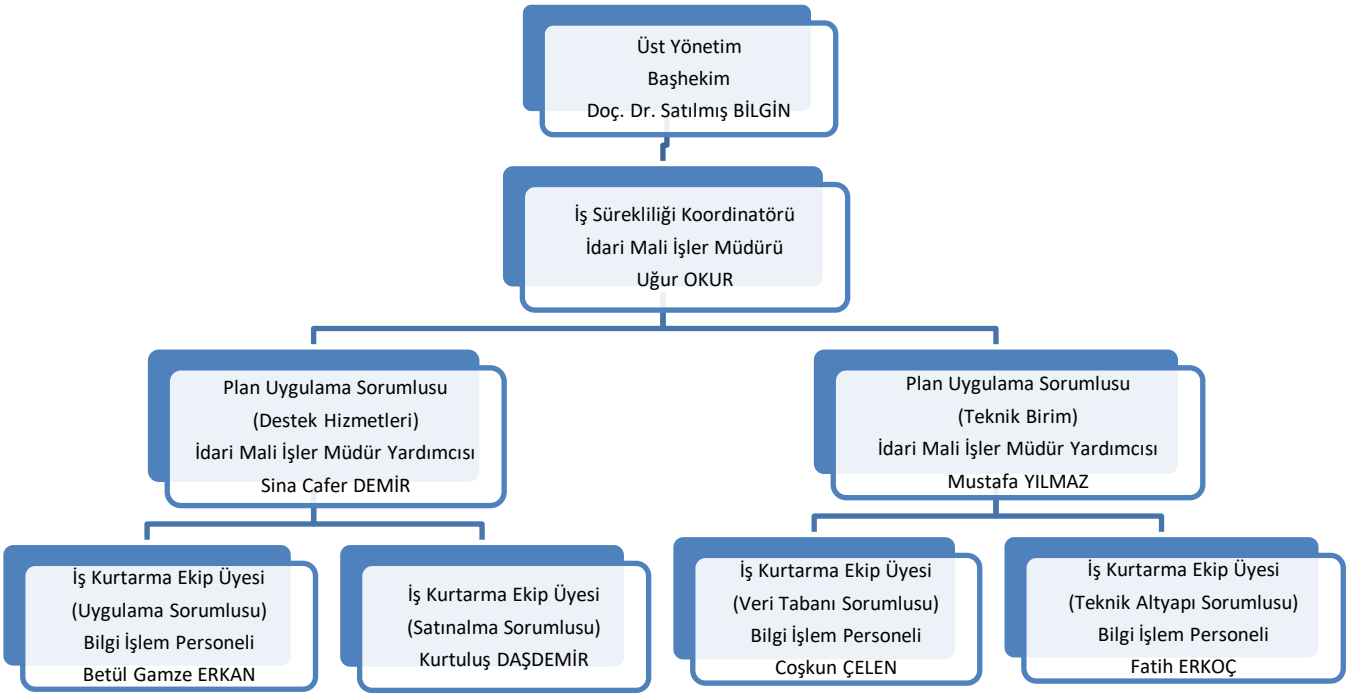
Belirlenen kaynakların sağlanmasını taahhüt eder.

İş sürekliliğinin sağlanması için sürekli test ve tatbikatları destekler ve bunun için gerekli faaliyetlerin gerçekleştirilmesini sağlar ve kontrol eder.

İş sürekliliği hedeflerini, rol ve sorumlulukları, iş sürekliliği taahhüdünün bulunduğu iş sürekliliği politikasını oluşturur ve yayımlar.

İş Sürekliliği Koordinatörü;

Bilgi güvenliği alt komisyonu başkanı aynı zamanda kurumun iş sürekliliği koordinatörü olarak görev yapar.



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.

Kurumun bağlı olduğu güncel mevzuat, yasa, yönetmelik ve sözleşmelerden doğan yaptırım ve yükümlülükleri takip ederek İş Sürekliliği Planlarının güncellenmesini sağlar.

İş sürekliliği planlarının test edilmesi için tatbikatlar düzenler, kayıt altına alınmasını sağlar.

İş sürekliliğini etkileyecek ya da iş sürekliliğinden etkilenebilecek taraflarla iletişimi sağlar.

İş sürekliliğini etkileyecek ya da iş sürekliliğinden etkilenebilecek taraflarla iletişimi sağlar.

İş sürekliliğinin sağlanabilmesi için plan uygulama sorumluları ve iş kurtarma ekiplerinin görev dağılımını belirler ve ekiplerin yetkinliğini arttırmak amacıyla iş sürekliliği eğitimlerini planlar.

Planın devreye alınması ve hasar onarımı sonrası normal çalışma durumuna geri dönülmesi kararlarını verir.

Plan Uygulama Sorumluları;

Kurum organizasyon şemasındaki ilgili yöneticiler ve onların atadıkları sorumlulardan oluşur.

Planın uygulanmasında, İş Sürekliliği Koordinatörü tarafından verilen görevlerin gerçekleştirilmesinden sorumludur.

Acil ve beklenmedik bir durumla karşılaşıldığında kendisine bağlı personeli koordine eder. İş sürekliliği koordinatörüne bilgi akışını sağlar.

İş sürekliliği planının uygulanması için ilgili iş sürecinden sorumlu olan personel ve yedeklerinin yer aldığı iş kurtarma ekiplerini oluşturur.

Yedekten geri dönme işlemleri, ağ konfigürasyonunun restorasyonu, iş uygulamalarının sunucular üzerine kurulum ve konfigürasyonu gibi süreçlerin gerçekleştirilmesinden sorumludur.

İş Kurtarma Ekipleri

Plan uygulama sorumlularının vermiş olduğu işlerden sorumludur.

Genel Sorumluluklar;

Hizmetlerin erişilebilirliğinin sağlanması için planlamalar doğru bir şekilde yapılır.

Hizmetlerin erişilebilirlik ve sınıflandırma ile ilgili gereksinimleri hizmet sahipleri tarafından belirlenir.

Kritik iş süreçlerinde yer alan personel, iş sürekliliği planlarında belirtilen görevleri yerine getirmekle ve iş süreklilik tatbikatlarına katılmakla sorumludur.

Hizmetlerin erişilebilirlik ve sınıflandırma ile ilgili gereksinimleri hizmet sahipleri tarafından belirlenir.

Kritik iş süreçlerinde yer alan personel, iş sürekliliği planlarında belirtilen görevleri yerine getirmekle ve iş süreklilik tatbikatlarına katılmakla sorumludur.

İş Sürekliliği Stratejisi Belirleme

İş sürekliliği planları geliştirilirken; kritik hizmetleri sunan ve bu hizmetlerden faydalanan/faydalanacak iç ve dış paydaşların ihtiyaç ve gereksinimleri, toplantı veya anket gibi çalışmalar ile analiz edilir. Analizler için BY.FR.11 İş Sürekliliği Formları içinde örneği yer alan "Kritik Varlık/Süreç Analiz Formu" kullanılır. Anket veya toplantılardan elde edilecek sonuçlarda asgari olarak aşağıdaki soruların yanıtları elde edilmelidir;

İşin yürütülmesi için ihtiyaç duyulan yazılım, donanım ve diğer teknolojik bileşenler ve bilgi işlem araçları nelerdir? Ekipman ve sistem gereklilikleri nelerdir? (Bu aşamada "İş Sürekliliği Kaynak İhtiyaç Listesi" kesinleştirilir)

Özel sözleşme ya da yasa ve mevzuatlara bağlı olarak yerine getirilmesi gereken minimum yükümlülükler nelerdir?

Sürecin çıktısı olan hizmetin kullanıcıları kimlerdir?

Hizmet sürekliliğinin sağlanması için bağımlı olunan hizmetler, iş sürekliliğini etkileyebilecek dâhili ve harici taraflar kimler/nelerdir? Sürecin iş sürekliliğinin sağlanması için hangi sistemlere sürekli erişim gereklidir?

Elektronik verilerin korunması nasıl sağlanmaktadır? Bu veriler korunamazsa nasıl sonuçlar ortaya çıkar? İlgili veriler sürekli erişim için gerekli midir?

Personelin temel yeterlilik seviyesi nedir? Herhangi bir felaket durumunda başka birimlerden/dış kaynaklardan personel alınması mümkün müdür? Mümkünse hangi birim ya da kaynaklarla iş birliği yapılabilir?

Bu aşamada ayrıca iş sürekliliğine engel olabilecek felaket senaryoları oluşturulur ve bu senaryolara nasıl müdahale edileceği yani kurtarma operasyonlarının (nerede yönetilecek, kim yönetecek ve kime raporlayacak) nasıl yönetileceği belirlenir. Kurtarma öncelikleri ve kurtarma zaman hedefleri, müdahale eylem planları ve sorumluları BY.FR.11 İş Sürekliliği Formları içinde yer alan "İş Kurtarma Planı" örneğinde olduğu gibi detaylı olarak dokümante edilir.

İş sürekliliği planları; varlık envanteri, bilgi sınıflandırma, bilgi aktarımı, yedekleme, kapasite yönetimi, varlıkların kabul edilebilir kullanımı, risk yönetimi, yasal gereksinimler ve standartlara uyum,

konfigürasyon ve değişim yönetimi, fiziksel ve çevresel güvenlik gibi operasyonel faaliyetlerde kullanılan bilgi güvenliği dokümanları göz önüne alınarak hazırlanmalıdır.

İş Sürekliliği Planı Oluşturma

Bu bölümde şu ana kadar anlatılan tüm bilgiler; iş sürekliliği planı oluşturulması için idarenin "hangi süreçler kritik, bu süreçlerin sürekliliğini sağlamak için yasa, mevzuat ve sözleşmelerden doğan zorunluluklar neler, iş sürekliliğini tehdit edebilecek unsurlar neler olabilir ve bu tehditleri bertaraf etmek için nasıl hazırlık yapılmalı" gibi durumları analiz ettiği ve iş sürekliliği planını desteklemek için dokümantasyon oluşturduğu süreçleri içerir.

İş sürekliliği planları; kesinti anında bütün ihtiyaç duyulabilecek gereksinimlerin tanımlı olduğu ve ilgili tüm taraflar tarafından bilinen ve uygulanması sırasında karmaşaya neden olmayacak şeklinde hazırlanır. İş sürekliliği planları aşağıdaki içeriğe sahip olmalıdır;

Amaç ve kapsam,

İş sürekliliği hedefleri,

- Planın hangi koşullarda hayata geçirileceği,
- Olağanüstü durumda kurtarma çalışmalarında kimlerin görev alacağı ve hangi kurtarma adımlarını gerçekleştireceği,
- Olağanüstü durumlarda, gerek organizasyon için gerekse organizasyon dışında iletişime geçilecek kişi ve kurumlar, aynı zamanda iletişimin nasıl sağlanacağı bilgisi,
- İç ve dış bağımlılıklar,
- Planın hayata geçirilmesi için gerekli olan kaynaklar,
- Tanımlanmış iletişim adımları.

İş sürekliliği planının, dokümante edilmiş tüm liste ve formların (kritik varlıklar/süreçler listesi, kaynak ihtiyaç listesi, acil durum iletişim listesi, süreç analiz formu vb.) genel çerçevesini sunan tek bir ana doküman olarak hazırlanması, planın amacının, kapsamının ve hedeflerinin uygulayıcılar tarafından daha anlaşılır olmasını sağlar.

İş sürekliliği planlarında;

İş sürekliliği planında acil veya olağanüstü durumların neler olduğunun ve "çok acil, acil ve normal" seviyelerin neler olduğunun tanımlanmış olması gerekir.

Herhangi bir olağanüstü durum anında iş sürekliliği planında yazılı olan faaliyetleri gerçekleştirecek olan kişilerin rolleri, sorumlukları ve yetkileri önceden belirlenmiş ve tanımlı olmalıdır.

Yapılan olağanüstü durum tanımları uyarınca, iş sürekliliği planının hangi koşullarda aktive edilmesi gerektiği ve rol bazında yapılması gerekenlerin belirlenmiş olması gerekir.

Olağanüstü durumun sona ermesi sonrasında iş süreçlerinin olağanüstü durum öncesine dönmesi için yapılması gerekenlerin tanımlanması gerekir.

Olağanüstü durumun olağan çalışma ortamını kullanılamaz hale getirmesi durumunda alternatif çalışma lokasyonları ve kriz merkezi planlamasının yapılması gerekir.

İş sürekliliği ekibinde bulunan çalışanların iletişim bilgileri (telefon, e-Posta, adres), kendilerine ulaşılamadığı durumlarda alternatif olarak kullanılacak iletişim bilgilerine nasıl ulaşılacağının plana dâhil edilmesi gerekir.

Kritik iş sürekliliği yönetimi, bütünleşik olarak hizmet sürekliliğinin iyileştirilmesi amacıyla uygulanır. Bir yönetim sistemi mantığı ile işletilmesi gerekir. Bu nedenle bu süreç önceden hazırlanması ve sürekli gözden geçirilmesi gereken bir takım dokümanlarla desteklenmelidir. İş sürekliliği dokümanları;

Bilgi güvenliği tehdit listesi ve ihlal olayları olay müdahale süreç dokümanları,

Kritik varlıklar / süreçler listesi,

Kaynak ihtiyaç listesi,

Kritik tedarikçiler, acil durum ilk müdahale ekip üyeleri ve yedeklerinin yer aldığı acil durum iletişim listesi,

Uzmanlık, yetkinlikler ve tanımlanmış sorumlulukları ile iş sürekliliğinin sağlanmasından sorumlu personel ve yedeğinin yer aldığı iş telefonu, ev telefonu, cep telefonu, iş ve kişisel e-Postası ve normal iletişimin kullanılamayacağı durumlarda irtibat kurmanın yollarını içeren acil durum iletişim listesi,
Felaket sonrası kritik faaliyetler için kurtarma sırası (acil veya olağanüstü durum yönetimi (kurtarma), devam etme ve normale dönüş) içeren olay müdahale planları, tatbikat ve testlerin kayıtları,
Sistem kapasitesi ve eşik değerlerin izlenme raporları,

Kritik hizmetin sürdürülmesine destek olan altyapı envanteri (donanım, yazılım, teknik ekipmanlar, sunucular, veri tabanları, internet vb.) ve yedekleme planları

Tatbikat test uygulama formu,

İş süreklilik planı sonrası yapılan değerlendirme formu.

İş Sürekliliği Planlarını Tatbikatlar ile Test Etme

Tatbikatlar öngörülen risklere karşı hazırlık seviyesinin ölçüldüğü aktivitelerdir. Kapsamlı bir hazırlık süreci gerektirir aksi halde ciddi kesintilerin yaşandığı olumsuz durumlar ile karşılaşılabilir.

Olağanüstü durum ile ilgili medya ve kamu bilgilendirmesinin nasıl yapılacağına ilişkin kurumsal iletişim stratejisinin de planda yer alması gerekir.

Tatbikat türleri maliyet, zaman, karmaşıklık, efor ve normal operasyonda oluşacak kesintiler açısından farklı özelliklere sahiptir.

Tatbikat türleri ve açıklamaları Tablo-1'de verilmiştir.

Tatbikat Türü	Tanım
Kavramsal tatbikat	İş sürekliliği planı ve ilgili dokümantasyonun gözden geçirilmesidir.
Detaylı kavramsal tatbikat	Kavramsal tatbikatın daha detaylı olarak yerine getirilmesidir. Bu tatbikat türünde planda yer alan her adımın üzerinden geçilerek eksiklikler tespit edilmeye çalışılır.
Simülasyon	Bu tatbikat türünde örnek bir olay üzerinden iş sürekliliği planı çalıştırılır. Tatbikat sırasında süreç veya sistemlerde herhangi bir kesinti gerçekleştirilmez. İş sürekliliği planı kesinti gerçekleşmiş gibi düşünülerek çalıştırılır ve tatbikatı yapılır.
Bileşen veya servis tatbikatı	İş süreçlerinin bir kısmı için gerçekleştirilir. İş süreçlerinde kesintiye neden olabilecek bir olay gerçekleştirilir ve süreç tekrar çalışır hale getirilir. Bu tatbikat çalışan bir sistem üzerinde gerçekleştirildiğinden, kurumun acil durum tatbikatı kapsamında olmayan operasyonunu aksatmayacak biçimde planlanması gereklidir.
Tam tatbikat	İş sürekliliği planının tamamının test edilmesidir. Tam tatbikat kurum süreçlerinin felaketten kurtarma merkezinde tekrar çalıştırılmasını da kapsayan detaylı bir tatbikattır.

Tablo 1 Tatbikat Türleri

İş sürekliliği tatbikatları; tatbikata hazırlık, tatbikatın gerçekleştirilmesi ve tatbikatın değerlendirmesi olmak üzere üç adımda gerçekleştirilir.

Tatbikata hazırlık: Varsa daha önce gerçekleştirilen tatbikat planları ve sonuçları incelenir. Tatbikat

zamanı, senaryosu, değerlendirme ölçütleri ortaya koyulur. Tatbikat riskleri değerlendirilir ve tatbikat programı yapılır. BY.FR.11 İş Sürekliliği Formları içinde yer alan Tatbikat Test Uygulama Formu, yapılacak tatbikata özgü ihtiyaçlara göre özelleştirilmek suretiyle kullanılabilir.

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.

Tatbikatın değerlendirilmesi: Tatbikat bulguları incelenerek tatbikat değerlendirme raporu hazırlanır. Varsa yaşanan sıkıntılar, iş sürekliliğinde görev alan personelin performansı, kullanılan kaynak ve ortamın yeterliliği gibi hususlar raporda belirtilir.

Sürekli iyileştirmenin sağlanması için planlar belirli sıklıkla tatbikatlar ile test edilir. Planların test edilme sıklığı planlarda belirtilmelidir.

Tatbikatlardan elde edilen bulgular, kurumların bilgi güvenliği dokümantasyonuna ve bir sonraki eğitime dâhil edilir.

Tatbikat sonuçlarına göre planlar tekrar gözden geçirilir, gerekiyorsa düzeltici faaliyet planlanır, ihlal olayları müdahale süreçleri ve risk çalışmalarına yansımaları değerlendirilir.

	İŞ SÜREKLİLİĞİ FORMLARI			
KOD:BY.FR.11	YAY TAR.: 05.11.2020	REV.TAR: 00	REV. NO: 00	SYF. NO/SAYI: 1/1

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	HBYS sunucu işletim sistemi ve yazılımları
Hizmetin sunulmasını destekleyen uygulamalar	HBYS yazılımı
Kullanıcı tarafındaki uygulamalar	HBYS doktor, hemşire ve tıbbi sekreter ekranları
İnsan Kaynağı	HBYS Firması destek personeli
Veri Tabanı	ORACLE veri tabanı
Tesisler	Sistem odası
Tedarikçiler	KARDELEN YAZILIM firması
Veri tabanı Yedek alma stratejisi	Tam Yedekleme / değişen kısımların yedeğinin alınması / İşlem log kayıtları
Veri tabanı Yedek alma sıklığı	Günde 3 kez
Sunucu Yedeklilik Durumu	Yok

İŞ KURTARMA PLANI						
Kritik İş Hizmeti Adı: Hastane Bilgi Yönetim Sistemi			**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	Acil durum Hap aktive edilir BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu	Bilgi işlem sorumlusu ve tüm birim sorumluları	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu Kliniklerde Hasta Dosyası	Bilgi işlem sorumlusu ve tüm birim sorumluları		
Kritik sanal sunucunun hizmet dışı	Acil Durum Hap aktive edilir. BY.FR.01 Bilgi	Bilgi işlem sorumlusu ve tüm birim	BY.FR.01 Bilgi İşlem Acil Eylem B	Bilgi işlem sorumlusu ve tüm birim		

kalması	İşlem Acil Eylem B Plan Formu devreye alınır.	sorumluları	Plan Formu Kliniklerde Hasta Dosyası	sorumluları		
Kritik sunuculara geniş çaplı virüs saldırısı gerçekleşmesi	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu devreye alınır.	Bilgi işlem sorumlusu ve tüm birim sorumluları	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu Kliniklerde Hasta Dosyası	Bilgi işlem sorumlusu ve tüm birim sorumluları		
Hacker saldırısı	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu devreye alınır.	Bilgi işlem sorumlusu ve tüm birim sorumluları	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu Kliniklerde Hasta Dosyası	Bilgi işlem sorumlusu ve tüm birim sorumluları		
Tedarikçinin süreçten ayrılması (iflas vb.)	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu devreye alınır.	Bilgi işlem sorumlusu ve tüm birim sorumluları	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu Kliniklerde Hasta Dosyası	Bilgi işlem sorumlusu ve tüm birim sorumluları		
Bilgi sızıntısı	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu devreye alınır.	Bilgi işlem sorumlusu ve tüm birim sorumluları	BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu Kliniklerde Hasta Dosyası	Bilgi işlem sorumlusu ve tüm birim sorumluları		

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.)					

Hastanede iş sürekliliğini sağlamak adına 24 saat kesintisiz donanım ve yazılım destek birimleri hizmet verir. HBYS devre dışı kaldığı süre boyunca poliklinik ve GETAT birimlerinde "BY.FR.01 Bilgi İşlem Acil Eylem B Plan Formu" çıktı olarak bulunur. Kliniklerde de hasta dosyası içeriği basılı olarak bulunmaktadır. Server odasında yedekli klima ve güç kaynağı, ayrıca farklı binada bulunan yedekleme ünitesi ve yedek server da bulunmaktadır. Olağan üstü durumlarda HAP aktive edilir. Acil Afet depolarında ilgili formlar çıktı olarak dosyalanmış olup, görevli personeller tarafından iş akışı başlatılır.

Hastane iş sürekliliğinde HBYS devreye girdiğinde kullanılan matbu evrakların sisteme girişleri, birim sorumluları ve ilgili personeller tarafından ivedilikle sağlanır.

	BİLGİ İŞLEM ACİL EYLEM B PLAN FORMU			
KODU: BY.FR.01	**YAYIN TARİHİ: 24.02.2017**	**REVİZYON TARİHİ: 30.07.2019**	**REVİZYON NO: 01**	**SAYFA NO: 1/1**

HASTA BİLGİLERİ

ADI SOYADI :
TC KİMLİK NO :
SİCİL NO :
YAKINLIĞI :

KURUMU: BAĞKUR ☐ KENDİSİ ☐
SSK ☐ BAKMAKLA YÜKÜMLÜ ☐
EMEKLİ SANDIĞI ☐ EMEKLİ ☐
YEŞİLKART ☐ DİĞER ☐

KAYIT ALAN :
İMZA :
ADI SOYADI :

Hastanın Adı Soyadı – İmzası :

POLİKLİNİK
İMZA :
KAŞE :

PROTOKOL NO :
Öntanı – Tanı :

POLİKLİNİK İŞLEMLERİ

	520010	Konsültasyon Ücretleri (her bir hekim için)
	520020	Acil Poliklinik Muayene Ücreti
	520030	Normal Poliklinik Muayene Ücreti
	520050	Sağlık Kurulu Rapor Ücretleri
	520060	Tek Hekim Rapor Ücretleri

MÜDAHALELER

	Yara pansumanı ☐Küçük ☐Orta ☐Büyük
	Yanık pansumanı ☐Küçük ☐Orta ☐Büyük
	Yara debridmanı ☐Küçük ☐Orta ☐Büyük
	Kesi süturasyonu ☐Küçük ☐Orta ☐Büyük
	Yabancı cisim çıkarma……
530410	Sütur alınması

	530140	IM Enjeksiyon
	530150	IV Enjeksiyon
	530080	Damar yolu açılması
GETAT UYGULAMALARI		
	101890	Akupunktur Ücreti
		Sülük Tedavi Ücreti
	101950	Hacamat (Kupa Terapi) Ücreti
		Ozon Terapi Ücreti
		Proloterapi Ücreti
		Mezoterapi Ücreti
		Larva (Maggot) Uygulama Ücreti

530260	Lavman
530340	Nazogastrık Sonda Takılması
550360	Eklem içi enjeksiyon ağrı tedavisi
550400	Tetik Nokta / tendon kılıfı / ligament enjeksiyonu
702180	Eklem lavajı
KLİNİK İŞLEMLERİ	
701690	Nörofizyolojik değerlendirme
701700	Postur analizi
701710	Skolyoz değerlendirmesi
701720	Yürüme analizi

İstenilen Tetkikler **Hastaya Reçete Edilen İlaçlar**

AÇIKLAMA

*Bu form otomasyon sistemi arızası durumunda kullanılacaktır.

Güvenli Oturum Açma

- Oturum açma işlemleri yetkisiz erişim olasılığını asgari düzeye indirecek şekilde düzenlenmiş olmalıdır.
- Oturuma giriş sadece tüm girdi verilerinin doğrulanmasından sonra sağlanmalıdır.
- Sistem tarafından izin verilen başarısız giriş denemelerine sınırlama getirilmiş olmalıdır.
- Ağ üstünden şifrenin açık olarak gönderilmemesi sağlanmalıdır.

Uzaktan Erişim

a. HBYS firması yazılım destek elemanlarının, hangi durumlarda uzaktan erişimle, iç ortama erişim yapacağına dair hastane tarafından onaylanmış gizlilik sözleşmesi bulunmalıdır.
b. Yazılım destek elemanlarının yetersiz kaldığı durumlarda, yazılım bakım, güncelleme ve destek hizmetleri için bilgi yönetim sistemi firması yazılım destek elemanları, uzaktan erişim ile destek verebilir.
c. Sistemi kısmen veya bütünüyle çalışamaz hale getiren bir arıza durumunda bilgi yönetim sistemi firması uzaktan erişim ile destek verebilir.
d. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahiptir.
e. Kurum ağına uzaktan erişim ile erişen Bilgi Yönetim Sistemi firması çalışanları Bilgi İşlem Yazılım Biriminden izin almak zorundadır.
f. Ağ yönlendirme kontrolleri, bilgisayar bağlantılarının ve bilgi akışının erişim politikasına uygun gerçekleşmesini sağlayacak şekilde tanımlanmış olmalıdır.

g. Ağ iletişimi kaynak adres ve hedef adreslere bağlı olarak güvenlik duvarı vb. cihazlar aracılığı ile kontrol ediliyor olmalıdır.
h. Uzaktan erişimler bağlanan kullanıcılar "Dış Ortamdan İç Ortama Bağlantı" formuna kaydedilerek hastane yönetimine onaylatılmalıdır.
i. Uzaktan erişim için tek kullanımlık şifre ve geçici süreli erişim hakkı verilir.
j. Periyodik yapılan kontrollerle gereksiz kullanıcı kimlikleri ve hesapları kaldırılmalıdır.
k. Uzaktan erişim için kullanılacak olan servisler ve protokoller güvenlik duvarında tanımlı olmalıdır.

BİLGİ SİSTEM DONANIM VE ALT YAPI YÖNETİM VE TALEP SÜREÇLERİ

Donanım ve alt yapı; Kullanılan sunucu, ağ cihazları, güvenlik cihazları, veri depolama ünitesi, son kullanıcı donanımları, yazıcılar, yedekleme cihazları, kesintisiz güç kaynağı ve sistemlerinin donanımsal periyodik bakımlarının yapılmasını, mevcut problemleri çözmek veya ihtiyaçları karşılamak için gerçekleştirilen faaliyetleri kapsamaktadır.

Yönetim ve talep süreçleri; Bilgi işlem personeli ve yetkili son kullanıcıların gerekli eğitimler doğrultusunda yetkili oldukları cihazların kullanımı sağlanır. Domain sistemi ile yönetim ve kontrol sağlanır. Birimlerin ihtiyacı olan bilgi sistem donanımı; cins ve miktarı yazılı malzeme/onarım ihtiyaçları belirlenir. MC.FR.03 ile talep ve şartname hazırlanır. Gerekli incelemeler ilgili depo tarafından yapılıp, komisyonca değerlendirilir. İhtiyaç tespit komisyonunca stok analizi, maliyet analizi ve verimlilik kriterleri göz önünde bulundurularak sağlık tesisinin ihtiyaçlarının alımı sağlanır.

Sunucu, Çevresel ve Fiziksel Güvenlik Yönetimi

- Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.
- Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- Sunucuların elektrik kesintilerinden etkilenmemesi için hastane güç kaynağından bağımsız kesintisiz güç kaynağı bulunmalıdır.
- Sunucuların oluşabilecek tehditlere karşı yer ile teması kesilerek, bir kabin içerisinde ve yükseltilmiş taban üzerinde muhafaza edilmelidir.
- İklimlendirme şartlarının sağlanması için klima bulunmalıdır. Herhangi bir arıza anında ikinci bir yedek klima bulunmalıdır.
- Sunucu odasına yetkisiz personel girişleri engellenmiştir. Sistem odası kapısında şifreli giriş sistemi bulunmalıdır.
- Sunucu odasına girişler güvenlik kamerası ile izlenerek kayıt altına alınmalıdır.
- Isı ve nem takibi çevrimiçi çalışan ısı nem cihazı ile her gün yarım saatte bir otomatik olarak yapılmaktadır. Isı ve nemlerde ki sapmalarda cihaz üzerinde ki alarm çalmakta ve sunucu odası sorumlularına e-posta ile bilgi mesajı gitmelidir.
- Isı-nem cihazlarında ki anormal değerlerin her ay çıktısı alınarak analiz edilmelidir.
- Sunucu üzerinde çalışan anti virüs ve diğer sunucu yazılımları güncel olarak çalışmalıdır.
- Sunucuların yazılım bakımları hastanede faaliyet gösteren otomasyon firması tarafından sürekli olarak yapılmalı ve 6 ayda bir tutanak altına alınmalıdır.
- Sunucu donanım bakımları yetkili firma tarafından 6 ayda bir yapılmalı ve tutanak altına alınmalıdır.
- Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı ve kullanım politikasına aykırı bir kullanıma olanak verilmemelidir.
- Sunucular üzerinde kesinlikle ticari amaç güden yazılımlar kurulmamalıdır.
- Sunucular güvenlik duvarının arkasında bulunmalıdır.