1.GİRİŞ
Hastanemizde kullanılmakta olan kritik BT (Bilgi Teknolojileri) hizmetlerinin durmasına veya büyük oranda devre dışı kalmasına neden olabilecek (uygulama ve VTYS sunucularından, kurum sorumluluğunda bulunan ağ cihazlarından, şebeke elektriği/jeneratör/kesintisiz güç kaynağı/iklimlendirme gibi destekleyici altyapı hizmetlerinden kaynaklanan) bir olay/arıza meydana gelmesi halinde, sistemin yeniden normal fonksiyonları ile çalışır hale getirilmesi maksadıyla Kurum tarafından yapılacak işlerin açıklanması beklenmektedir.

2.AMAÇ
Bu Prosedürün amacı; İl Sağlık Müdürlüğüne bağlı ..... Hastanesi tarafından gerçekleştirilen kritik BT hizmetlerinin sunumuna kesintisiz bir şekilde devam etmek, türü ve nedeni ne olursa olsun herhangi bir kesinti ya da olay durumunda, önceden belirlenmiş kritik iş süreçlerini kabul edilebilir seviyede sunma yeteneğini sağlamak için belirlenmiş iş sürekliliği yöntemini ortaya koymaktır.
Bu prosedür ile 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 amaçlanmaktadır.

3.KAPSAM
Hastanelerimizde çalışan tüm personellerimiz iş sürekliliğinin kapsamı içerisinde yer almaktadır. Ayrıca imha edildiğinde, bozulduğunda veya kullanılamaz hale geldiğinde, Müdürlüğümüze bağlı hastanelerin güvenilirliğini veya çalışabilirliğini etkileyebilecek uygulamalar, sistemler ve donanımlar İş sürekliliği kapsamında yer almaktadır ve bunlar bizim için kritik varlık anlamına gelmektedir.
Yürütülen iş, işlem ve sürecin kritik olabilmesi için aşağıda belirlenen durumlardan en az birine uygun olması gerekir;
• Kurum için yasal, finansal, operasyonel ve benzeri büyük riskler oluşturur,
• Stratejik olarak önemli ya da geniş kitleleri etkiler,
• İnsan hayatını ya da toplum sağlığını olumsuz yönde etkiler,
• Kurumsal itibarı maddi ya da manevi olumsuz bir şekilde etkiler nitelikte olması gerekir.
Hastanelerimizdeki en kritik varlıklar Sağlık Bilgi Yönetim Sistemi (SBYS) kapsamında hizmet vermek amacıyla kullanılan yazılımsal (veri tabanı, işletim sistemleri vb.) ve donanımsal (sunucu, bilgisayar vb.) varlıklardır.

4.İŞ SÜREKLİLİĞİ STRATEJİSİ:
İş sürekliliği planları geliştirilirken; kritik hizmetleri sunan ve bu hizmetlerden faydalanan/faydalanacak iç ve dış paydaşların ihtiyaç ve gereksinimleri analiz edilmiştir. Hastanemiz için kritik varlık/süreç analiz formu hazırlanarak doldurulmuştur. İşin yürütülmesi için ihtiyaç duyulan yazılım, donanım ve diğer teknolojik bileşenler ve bilgi işlem araçlar kritik varlık/süreç analiz kısmında belirlenmiştir.
Sağlık Bilgi Yönetim Sistemi (SBYS) firması ile sözleşme kapsamında iş sürekliliğinin sağlanması konusunda gerekli yükümlülükler belirlenmiştir.
İş sürekliliği kapsamında hastanemizin en kritik varlığı Sağlık Bilgi Yönetim Sistemi kapsamında verilen hizmetlerdir. SBYS hizmetinin sağlayıcısı özel yazılım firmalarıdır. Hizmeti kullananlar firma personelleri ve hastane çalışanlarıdır. Hizmetin çıktısından faydalananlar vatandaşlar ve diğer kamu kurumlarıdır. SBYS sürekli veri girişi ve çıkışı olan sistem olması sebebiyle 7/24 kesintisiz çalışması gereken bir iş sürecidir. Bu sebeple veriler sürekli yedeklenir. Herhangi bir veri kaybına karşı gerekli tedbirler alınır.

5. SORUMLULAR: Bu planın işletilmesinden Başhekim ve Üst yönetim, Bilgi Güvenliği Sorumlusu, Bilgi İşlem Birimi Çalışanları, Sivil Savunma Amiri ve Teknik Servis Çalışanları başta olmak üzere tüm SBYS kullanan hastane personeli sorumludur.

6. TANIMLAR
6.1. Risk: Gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eden, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayba ya da zarara uğrama ihtimali. Zarara ve kayba neden olacak bir olayın bilişim sistemleri varlığı üzerinde gerçekleşme olasılığı olarak tarif edilebilir.
6.2. Risk Yönetimi: Bir kurum ya da kuruluşun çalışabilirliği olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilme süreci. Kurum çalışanlarına zarar verebilecek olumsuzlukları belirleme, değerlendirme, yönetme ve kontrol etme sürecidir.
6.3. İş Sürekliliği: Kurum'a ait kritik iş süreçlerinin sürekliliğinin sağlanması ve kesinti durumunda en kısa zamanda ayağa kaldırılmasına ilişkin esasların hususları belirlemek amacıyla, aşağıdaki hususlar göz önüne alınarak iş sürekliliği yönetimi gerçekleştirilir.
6.4. Varlık: Sistemin bir parçası olup ve kurum için değeri olan her şey. Bilgi, donanım, yazılım, haberleşme cihazları, doküman, üretilen hizmet, personel
6.5. Tehdit: Herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyeli.
6.6. Tehditler: Doğal Tehditler: Deprem, sel, yıldırım düşmesi, fırtına, toprak kayması vb.. Çevreye Bağlı Tehditler: Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vb.. İnsan Kaynaklı Tehditler: İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar.

6.7. Gizlilik: Bilginin yetkisiz kişilerin eline geçmemesi ve yetkisiz erişime karşı korunmasıdır. Bilgiye yetkisiz erişimlerin engellenmesi olarak da ifade edilebilir.
6.8. Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmemesi. Yetkili kişilerin erişimi neticesinde kendine özgü bilgi mahremiyetinin korunması şeklinde tarifimümkündür.
6.9. Erişilebilirlik: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır. İhtiyaç halinde kolay ulaşılabilir olması hali olarak da ifade edilir.
6.10. Bilgi Güvenliği: Bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesiniönlemektir.
6.11. Çalışanlar: Hekim, Hemşire, Teknisyen, Tekniker, Sağlık Memuru, VHKİ, Memur, Hizmetli, Sürekli İşçi ve tüm kurum çalışanlarıdır.
6.12. Yazılımlar: Sağlık Bilgi Yönetim Sistemi (SBYS), Kalite Yönetim Sistemi, İşletim Sistemi, Anti Virüs, vb.
6.13. Bilgiler: Hasta teşhis ve tedavi bilgileri, istatistik bilgileri, Verimlilik ve Kalite Yönetim Sistemi verileri, maaş, döner sermaye ve ek ödeme bilgileri, ihale ve satın alma verileri.

7. İŞ SÜREKLİLİĞİ ORGANİZASYONU:

Hastanemizde kullanılan (SBYS) Sağlık Bilgi Yönetim Sistemine dair kurumun en kritik bilgilerinin işlendiği veri tabanlarında ve bu veri tabanlarının saklandığı fiziksel ve sanal sunucularında olağan çalışmalarını kesintiye uğratacak ve/veya hizmet sunmasını engelleyecek acil durumlar karşısında iş sürekliliği organizasyonunu gerçekleştirilecek faaliyetler Başhekim, Bilgi Güvenliği Komitesi, Bilgi İşlem Sorumlusu ve yüklenici firma tarafından yürütülür.
İş sürekliliği organizasyonunu yürütmekte sorumlu olan Başhekim, Bilgi Güvenliği Komitesi, Bilgi İşlem Sorumlusu ve yüklenici firmanın görevleri aşağıda belirtilmiştir.
7.1. Başhekim: İş sürekliliğinin sağlanması için liderlik eder, müdahale için verilen kararları onaylar, gerekli kaynakların kullanımını sağlar. Olay sonrası operasyonlar, mali durum, yönetim yapısı gibi ana konularda, kurum dışındaki yetkililere ve diğer tüm hak sahiplerine yapılacak açıklamalara onay verir.
7.2. Bilgi Güvenliği Komitesi: Başhekim ile koordineli olarak çalışır, Kurumun kriz öncesindeki durumuna geri dönebilmesi için stratejik seviyede kararları alır, uygulanmasını sağlar ve ilgili grupların işleyişine yön verir. Sağlık Bilgi Yönetim Sistemi'nde acil ve beklenmedik bir durumla karşılaşıldığında kendisine bağlı personeli koordine eder. Acil durumun yaşandığı birimin yetkisini aşan işlemlerde (harcamalar, personelin iş düzeninin değiştirilmesi, personelin uzun süreli çalıştırılması, bazı servislerin kapanması vb.) lüzum gördüğü hizmet ve faaliyetlerde gerekli yetkilendirmeleri yapar. Gerekli durumlarda hizmet ve ürün tedarikçilerinin sürece dâhil edilmesini sağlar.
7.3. Bilgi İşlem Sorumlusu: Acil ve beklenmedik durumdan etkilenen (SBYS) Sağlık Bilgi Yönetim Sistemine dair kurumun en kritik bilgilerinin işlendiği veri tabanları ve bu veri tabanlarının saklandığı fiziksel ve sanal sunucuları olağan çalışmalarının yürütülmesinden sorumlu ilgili birim sorumlusudur. Mevcut durumla ilgili Başhekim ve Bilgi Güvenliği Komitesine bilgi vermek ve gerekli durumlarda hizmet ve ürün tedarikçisi olan Sağlık Bilgi Yönetim Sistemi kurulum ve işletilmesini sağlayan yüklenici firma ile birlikte iş kurtarma planının uygulanmasını sağlamakla sorumludur.
7.4. Yüklenici Firma: Acil durumun ortaya çıkması halinde koordinasyonda kendisine verilen görevleri yerine getirir, talimatları / alınan kararları uygulamak, proaktif önlemler alarak kriz etkilerinin yayılmasını önlemek ve kurumsal imajımızı olumsuz etkileyecek faktörleri önlemeye/ortadan kaldırmaya yönelik çalışmalara katılmak/yapmakla sorumludur. Sağlık Bilgi Yönetim Sistemine (SBYS) dair kurumun en kritik bilgilerinin işlendiği Kurum veri tabalarının replikasyonu ve olağanüstü durumda devreye alınması işlemleri ve tüm bunlar için gerekli yazılım ve lisansların sağlanmasından yüklenici firma sorumludur. Olağan çalışmalarını kesintiye uğratacak ve/veya hizmet sunmasını engelleyecek olağanüstü durumda sistemin yedek veri tabanından kayıpsız olarak yürütülmesi ve olağanüstü durum sonrası tekrar esas veri tabanının aktive edilerek kullanıma sunulması için SBYS hizmeti satın alınan Yüklenici firma tarafından iş kurtarma planı için müdahale ekibi oluşturur.
Müdahale ekibi;
• Acil durumun ortaya çıkması halinde koordinasyonda kendisine verilen görevleri yerine getirir, talimatları / alınan kararları uygulamak,
• Sunucu, işletim sistemleri ve uygulamaların ihtiyaç duyduğu diğer bileşenlerin ayağa kaldırılmasını sağlamak,
• Uygulamaların ve verilerin yedeklerden geri döndürülmesi, LAN ve WAN bağlantıların, ağ elemanlarının ve ilgili konfigürasyonların restorasyonunun gerçekleştirilmesini sağlamak,
• İş uygulamalarının sunucular üzerinde kurulum ve konfigürasyonunun gerçekleştirilmesini sağlamaklasorumludur.
• Sistemin ayağa kaldırılması sonrası sistem bütünlüğü kontrol etmek ve devamlılığı sağlamak.
Teknik Personeline Ulaşım
• HBYS biriminde görevli teknik personel ve İş sürekliliği faaliyetleri kapsamında görevlendirilmiş kişilerin

telefonları, 24 saat ulaşılacak şekilde açık olmalıdır. Güncel iletişim bilgileri santral biriminde bulunur. Sorun oluştuğunda, ilgili birimler santral aracılığı ile teknik personele ulaşır. Veri tabanı ile ilgili sorumlu kişilerin iletişim bilgilerinin sorumlu Başhekim Yardımcısında güncel olarak bulundurulmasından, üstlenici firma sorumludur.

8. ACİL VE BEKLENMEDİK DURUMLAR

İş sürekliliği ve iş kurtarma planlarında geçen acil durumlar; kritik sunucunun hizmet dışı kalması, kritik sunuculara geniş çaplı virüs saldırısı gerçekleşmesi, hacker saldırısı, tedarikçinin süreçten ayrılması (iflas vb.), bilgi sızıntısı gibi bilgi sistemlerinin hizmet veremez hale gelmesi gibi bilgi işleme tesislerinin sürekliliğini ve bilgi varlıklarının güvenliğini tehdit eden durumlardır. İş kurtarma planlarında tanımlanan tehditler ve benzeri etkiyi yaratacak güncel siber tehditler acil ve beklenmedik durumlara yol açabilir. Acil durumlar kapsamında yer alan toplumsal olaylar, terör, soygun, bombalı saldırı, biyolojik ve kimyasal saldırılar, deprem, sel, yangın, elektrik kesintisi ve benzeri durumlar Hastane Afet Planı (HAP) uyarınca alınan tedbirler ile yönetilmektedir.

8.1. HEDEF VE VARSAYIMLAR:

İş Sürekliliği Planları'nın temel hedefi bir kesinti ya da olağanüstü durum sonrasında Kurum'un kritik süreçlerini/aktivitelerini belirlenmiş kabul edilebilir süreler içerisinde aktif hale getirmektir. Diğer hedefler aşağıdaki gibi detaylandırılabilir:

• Kurum çalışanlarını ve hastaları korumak, bilgi güvenliğinden emin olmak,
• Kurum varlıklarının korunmasını sağlamak, zararı en aza indirmek,
• Olağanüstü durumun yarattığı tehditleri kontrol etmek, gerekli önlemleri almak,
• Olayın büyüklüğünü değerlendirmek, karşılaşılan zararı en aza indirmek,
• Yasal yükümlülüklerin her an ve her zaman yerine getirilmesini sağlamak,
• Kurum'un marka imajını ve saygınlığını korumak,
• Acil ve olağanüstü durum sırasında hataların oluşmasını önleyici prosedürleri devreye almak, uygulamak ve iş yapış şekillerindeki hataları önlemek,
• Kritik faaliyetleri belirlenen süreler içerisinde başlatmak ve iletişimi yönetmek,
• Acil ve olağanüstü durum sonrasında ortaya çıkan sorunları ve sonuçları değerlendirmektir.

Kurum, İş Etki ve Risk Analizi çalışmasını da değerlendirerek aşağıdaki senaryolar için planın oluşturulmasına karar verilmiştir:

• Binaların kullanımına engel teşkil eden bir durumun yaşanması
• Bilgi sistemleri kesintisi
• Kritik personele ulaşılamaması

İş Sürekliliği Planı kapsamında dikkate alınan varsayımlar aşağıdaki gibidir:

• Alternatif lokasyonlar ve lokasyonların altyapı sistemleri kullanılabilir durumdadır.
• Çalıştırılacak uygulama ve işletilecek süreçler/aktiviteler için kabul edilebilir kesinti süreleri ve veri kurtarma noktası hedefleri, analiz sırasında belirlenen değerler ile uyumlu haldedir.
• BT bileşenleri için gerekli veri kurtarma noktası hedeflerine uygun yedekleme mekanizmaları kurulmuş ve test edilmiş durumdadır.
• Uzaktan çalışma talimatları, gerekli donanımlar, donanım üzerindeki uygulamalar (laptop, VPN, telefon), hesaplar hazır durumdadır.
• Acil ve olağanüstü durumda görev alacak ekiplerin hem kendi hem ekip üyelerinin hem de diğer ekiplerdeki üyelerin erişim bilgileri mevcuttur. Kullanılabilen tüm iletişim araçları ile haberleşme sağlanır.
• Süreçlerin/aktivitelerin gerçekleştirilmesi için bağımlı olunan kurum ve kuruluşlar ile iletişim kurulabilir durumdadır, kontak kişilerin erişim bilgileri mevcuttur.
• Acil ve olağanüstü durumda çalışacak minimum personel sayısı ve hangi personelin çalışacağı belirlenmiş durumdadır. Bu personel, acil ve olağanüstü durumda nasıl davranacakları, kimlerle bağlantıya geçecekleri ve işlerini nasıl devam ettirecekleri konusunda bilgi sahibidir.
• Olağanüstü durum süresince ortaya çıkacak ek masrafları onaylamak üzere bir ya da birden fazla Üst Yönetici (Yönetim Ekibi) hazır bulunur.

8.2. ACİL DURUM SENARYOLARI

Yangın: Yangını çağrıştıracak bir durum ile karşılaşıldığında (duman, yanık kokusu, vb.) ya da doğrudan yangın tespit edildiğinde (otomatik/manuel) tüm personelin yapması gerekenler aşağıda belirtilmiştir:

• Duman detektörlerinin yangını algılamadığı durumlarda personel tarafından yangın ihbar butonları kullanılır veya 4444 koduyla kırmızı kod uygulaması başlatılır.
• Çalışanlar, Acil Durum Ekibinin talimatları doğrultusunda çalışma ortamındaki gerekli güvenlik önlemlerini alarak bulunduğu alanı hızlı ve dikkatli bir şekilde terk eder ve Kurum'un belirlenen yerindeki toplanma alanına gider. Yangın söndürme ekibi sivil savunma amiri yönetiminde Hastane Afet Planına göre olaya müdahil olur.
• Tehlike çıkış merdivenleri kargaşaya sebebiyet vermeden kullanılır. Kesinlikle asansör kullanılmaz.
• Görgü tanıkları veya bina güvenliği tarafından ilgili yerlere (itfaiye, cankurtaran, polis, vb.) bilgi verilir.

Deprem: Sarsıntı başladığında personel tarafından yapılması gerekenler aşağıda belirtilmiştir:

• Personel; dolap gibi devrildiğinde yaralayıcı olabilecek eşyalardan uzak durarak, başını çanta, minder, kitap, klasör gibi eşyalarla koruyarak kendine güvenli bir yer bulur. Burası kolon, perde duvarlarının yanı ya da masa altları olabilir. Masanın altına girilip baş iki el ile örtülerek cenin pozisyonunda üzerine düşen eşyalardan korunur.
• Çalışanlar, Acil Durum Ekibi'nin talimatları doğrultusunda çalışma ortamındaki gerekli güvenlik önlemlerini alarak bulunduğu alanı hızlı ve dikkatli bir şekilde terk eder ve Kurum belirlenen merkezdeki yerindeki toplanma alanına gider. (Merkez Hastane Afet Planı doğrultusunda belirli alanlardır.)
• Tehlike çıkış merdivenleri kargaşaya sebebiyet vermeden kullanılır. Kesinlikle asansör kullanılmaz.
• Görgü tanıkları veya bina güvenliği tarafından ilgili yerlere (itfaiye, cankurtaran, polis, vb.) bilgi verilir.
Terörizm: Terörist saldırısının (savaş vb.) söz konusu olduğu durumlarda yapılması gerekenler aşağıda belirtilmiştir:
• Görgü tanıkları veya bina güvenliği tarafından ilgili yerlere (itfaiye, cankurtaran, polis, vb.) bilgi verilir.
• Binanın tahliyesine polis ile beraber karar verilir, Hasta tahliyeleri HAP planında belirtilen esaslar ve sivil savunma amiri koordinesinde yapılır. Binadan tahliye olan personel toplanma yerine gider.

8.3. BT SÜREKLİLİK PLANI

İş kurtarma stratejileri:
• Öncelikli süreçlerin ve sistemlerin tespiti için tüm iş birimleri ile başhekim eşliğinde yapılan iş etki analizlerinin sonucunda belirlenen Kurtarma Zamanı Hedefi ve Kurtarma Noktası Hedefi kullanılır. Sistem Odası, Olağanüstü Durum Merkezi ve içerisindeki sistemler bu doğrultuda olağanüstü duruma hazırlanır. Ayrıca kıymetli evraklar ve sürecin devamlılığı/yedeği için saklanması gerekli olan yazılı/basılı dokümanlar da bu doğrultuda gözden geçirilir.
• Kurtarma Zamanı Hedefi ve Kurtarma Noktası Hedefi 5 ayrı zaman dilimine yayılır:
• 0-6 saat,
• 6 saat-12 saat,
• 12 saat-24 saat,
• 24 saat-48 saat,
• 48 saat üstü.
• Bir gün içerisinde kurtarılması hedeflenen aktiviteler yüksek öncelikli olarak değerlendirilmektedir. Yüksek öncelikli aktivitelerin kurtarılmasına önem verilir.
• Veri kurtarma hedefi 12 saate kadar olan sistemler Yüksek Öncelikli olarak değerlendirilmektedir. Yüksek öncelikli olarak belirlenen sistemlerin kurtarılmasına önem verilir.
• İş kurtarma faaliyetleri temel olarak aşağıdaki 2 yöntemden birisi ile yapılır:
o İşlemlerin manuel olarak devam ettirilmesi (çalışma alanından bağımsız olarak)
o Sistem Odası'nda (Server odası-Bilgi işlem odası) bulunan yedek sistemler aracılığıyla faaliyetlerin devam ettirilmesi
• Uygulamalara uzaktan bağlantı hakkı verilebilecek personel (çalışmalarını bireysel olarak devam ettirebilecek) belirlenir, gerekli bilgilendirmeler yapılır, ilgili altyapı ve kaynaklar hazırlanır.
• Olağanüstü durum 'da çalışmak üzere minimum personel sayısı, personel bilgileri ve yedekleri önceden belirlenir. Bu personele olağanüstü durumda nasıl davranacakları, kimlerle bağlantıya geçecekleri ve işlerini nasıl devam ettirecekleri konusunda bilgi verilir.
• Çalışan kişiler ve yönetim kadrosuna mevcut duruma ve alınan kararlara ilişkin bilgilendirme (iletişimin tahsisi) HAP ta belirlenmiş İletişim Ekibi tarafından gerçekleştirilir. Alternatif çalışma sahasına ulaşımı İdari Mali Hizmetler Müdürü koordine eder.
• Medya ile iletişimi, mevcut durum ile ilgili kamu ve özel kurum bilgilendirmelerini İletişim Ekibi gerçekleştirir.
• İş kurtarma faaliyetleri, planlarda yazıldığı gibi belirlenen personel tarafından yerine getirilir. BT Birimi son kullanıcı desteği, saha gözetimi ve koordinasyonun sağlanması konularında görevlidir.
• BT altyapı hizmetleri ilk önce ayağa kaldırılır.
• Başka bir lokasyonda çalışılmasını gerektirecek bir olağanüstü durumda Kurum'a gelen çağrılar diğer ilgili lokasyonlara yönlendirilir. Ayrıca, posta yolu ile gelen evrakların da ilgili adrese iletilmesi sağlanır.
• Olağanüstü durum süresince ortaya çıkacak ek masrafları onaylamak üzere bir ya da birden fazla üst yönetici hazır bulunur.
Her durumda kurumun bilgi işlem birimi HBYS hizmeti alınan firma ile sürekli iletişimde kalmalı, Jeneratör, kesintisiz güç kaynağı gibi server odasını besleyen elektrik arızaları olması durumunda teknik personel kuruma çağrılmalı veya kurum dışı teknik destek alınacak ise İdari Mali İşler Müdürlüğü tarafından koordine edilmelidir.

9. İŞ KURTARMA PLANLARI İÇERİĞİ

İş kurtarma planları içerisinde her bir varlık için; sistem bileşenleri, iş sürecinin bağlı ve bağımlı olduğu süreç ve uygulamalar, roller ve sorumluluklar, tehdit ve yanıtlar gibi olağanüstü bir durumdan olağan duruma geçilmesi için gerekli olan tüm bilgiler tanımlanmıştır. Ayrıca, iş kurtarma planlarında;

• Kesinti esnasında manuel operasyonlara başvurulması,
• Önemli verilerin öncelikli yedeklenmesi,
• Kritik ve acil olarak yerine getirilmesi gereken faaliyetler için yedek sistemlerin devreye girmesi,
• Kritik ancak tolere edilebilir kesinti süresine sahip faaliyetler için mevcut sistemlerin onarımının beklenmesi gibi kurtarma stratejisi yöntemleri yer almaktadır.

10. PROSEDÜRÜN DEVREYE ALINMASI
İş sürekliliğini kesintiye uğratacak herhangi bir olay / kesinti durumunun ilk anında Bilgi İşlem Sorumlusu ilgili yüklenici firma temsilcileri ile görüşerek durum bilgi özeti alır. Tespit edilen durumun detaylarını Başhekim ile paylaşır. Başhekim verilen bilgi dâhilinde Bilgi Güvenliği Komitesini toplayarak acil durum ilan eder. Çalışmaların düzenli yürütülebilmesi için Olay Yönetim merkezinde toplanılır.
İlk toplantıda Başhekim;
• Planın neden devreye alındığını açıklar,
• Olayın etkilerini açıklar,
• Ekipler tarafından neler yapılacağını anlatır,
• İşleri planlandığı şekilde ekipte yer alan kişilere tevdi eder.
İş Sürekliliği Planının doğru işlemesi, bilgi taleplerine zamanında cevap verilmesi ve bilginin eksiksiz olarak aktarılması için bu kapsamda, acil ve beklenmedik bir durumda çalışanlar, birimler, müdahale ekipleri ve diğer paydaşlar etkin bir haberleşme çerçevesinde bilgilendirilir.

11. MANUEL OPERASYONLAR
Sağlık Bilgi Yönetim Sistemi'nin (SBYS) olağan çalışmasını ve hizmet sunumunu engelleyecek duruma gelirse izlenecek yollar belirlenmiştir.
SBYS'nin devre dışı kalması ile hastanemiz faaliyetleri ve hizmet sunumunun aksatılmadan, manuel olarak yürütülmesine uygundur. İş sürekliliğin sağlanması için hazırlanan form, rapor, defter vs. belirlenen dokümanlar ile
manuel olarak çalışmaya devam edilmesi sağlanacaktır. Birimlerin SBYS'nin devre dışı kalması ile hizmeti aksatmadan devam edeceği faaliyetler şu şekildedir:
11.1. Hasta Kayıt/ Kabul İşlemleri: Hasta kayıt ve kabul işlemlerinde SBYS'nin devre dışı kaldığı durumlarda, Bilgi Güvenliği Komitesinin alınan kararlar doğrultusunda hasta kayıt işlemleri yapılır.
a. Hastaların Sosyal Güvenlik Kurumu müstahaklık sorgulaması yapılamayacağından, hastalara bilgilendirme yapılır.
b. "Hasta Tanıtım Kartı" nın hasta ilgili alanlarını hasta, randevu ve hekim bilgileri kısmını Hasta kayıt birimi çalışanları tarafından tam ve eksiksiz doldurulur.
c. Hastaların kimlik belgesinin fotokopisi alınarak "Hasta Tanıtım Kartı" nın ilgili alanları kontrol edilir.
d. MHRS randevulu hastalar, MHRS web sitesi üzerinden kontrol edilerek hekimine, randevusuz hasta acil ve engelli hasta kliniğine hasta kayıt birimi çalışanlarına tarafından doldurulan "Hasta Yönlendirme Formu" ile yönlendirilir.
e. Acil durumun sona ermesiyle doldurulan formlar ve alınan kimlik fotokopilerinden yararlanarak hastalara ait veriler SBYS sistemine giriş yapılır.

11.2. Radyoloji Birimi: Radyoloji işlemlerinde SBYS'nin devre dışı kaldığı durumlarda, Bilgi Güvenliği Komitesinin alınan kararlar doğrultusunda yapılır.
a. Klinik tarafından "Röntgen İstek Fişi" doldurularak yönlendiren hastanın aciller öncelikli olmak üzere sıraya alınır.
b. Röntgen cihazlarının kurulu olduğu bilgisayarda cihaz için yapılan ara yazılıma manuel kayıtları girilir ve çekim işlemleri yapılır.
c. Çekilen görüntüler ya CD olarak hasta ile kliniğe gönderilir yada hastane lokal ağındaki; Hastane Ortak/Radyoloji klasörüne hastanın adı soyadı veya T.C. Kimlik numarası ile adlandırılarak resim olarak kaydedilir.

d. "Röntgen İstek Fişi" daha sonra SBYS'ye girilmek/kontrolü yapılmak üzere saklanır.
11.3. Klinik İşlemleri: Klinik işlemlerinde SBYS'nin devre dışı kaldığı durumlarda, Bilgi Güvenliği Komitesinin alınan kararlar doğrultusunda yapılır.

12. ACİL DURUMUN SONA ERMESİ
Plan uygulandıktan ve alternatif sunucular ayağa kaldırılarak sistem bütünlüğü sağlandıktan sonra normal hizmetin yeniden tesis edilmesi kararı verilir. Bu karar, Başhekim tarafından tüm ilgili tarafların görüşü alındıktan sonra verilir. Acil durumun sona ermesiyle öncelikli olarak hizmetin devre dışı kaldığı zaman boyunca yapılan manuel operasyonlarla yapılan iş/işlemler SBYS sistemine kaydedilir, radyoloji görüntüleri PACS sistemine entegre edilir.

12. PROSEDÜRÜN YÜRÜTÜLMESİ

12.1. DAĞITIM PROSEDÜRÜ

İş Kurtarma Planları ve destekleyici dokümanlar; acil olayın yönetebilmesini, kritik faaliyetlerin devam ettirebilmesini ve geri kazanmasını sağlamak için bütünlük içinde Kalite birimi uhdesinde muhafaza edilmektedir. İş Sürekliliği çerçevesindeki tüm prosedür ve ekleri ile eğitime dönük diğer döküman ve bilgiler ilgili birim ve ekiplerle yerel lokal ağ üzerinden paylaşılır.

12.2. İŞ SÜREKLİLİĞİ VE ACİL DURUM EĞİTİMLERİ

İş Sürekliliği Prosedürü kurum kültürünün bir parçası haline getirilmesi, prosedür kapsamında yapılması gerekenlerin kavranması, ilgili Müdahale Ekibi ve diğer kritik süreçlerde yer alan personelinin görev ve sorumlulukları hakkında bilgilendirilmesi amacıyla yılda bir kez eğitim programı düzenlenir.