1. **AMAÇ:** Hasta ya da çalışanlara ait tıbbi ve kişisel bilgilerin, doğru ve güvenli şekilde kayıt altına alınması ve depolanması ile ihtiyaç duyulan doğru bilginin, bilgi mahremiyeti ve güvenliği gözetilerek, doğru zamanda, doğru kişiye ulaştırılmasını sağlamaktır.
2. **KAPSAM:** Tüm hastane çalışanlarını kapsar.
3. **KISALTMALAR:**

   HBYS: Hastane Otomasyon Sistemi

   BİMOB: Bilgi İşlem Merkezi Otomasyon Birimi

   UPS: Uninterruptible Power Supply (Kesintisiz Güç Kaynağı)
4. **TANIMLAR:**

   Otomasyon Sistemi: Entegre Hastane Bilgi Yönetim Sistemi

   Otomasyon: Girdilerin bilgisayara girilmesi ile işlemlerin bilgisayar tarafından otomatik olarak yürütülmesi.
5. **SORUMLULAR:**
   - Başhekim
   - Bilgi İşlemden Sorumlu Başhekim Yardımcısı
   - Bilgi İşlem Sorumlusu
   - Hizmet Satın Alınan Firma Yöneticisi,
   - Firma Sorumluları
   - Tüm Bilgi İşlem Firma Elemanları
   - Hastane Bilgi Yönetimi Sistemini Kullanan Tüm Çalışanlar.

6.FAALİYET AKIŞI:

6.1.YÖNETİM SÜREÇLERİ:

6.1.1.Bilgi Yönetimine İlişkin Faaliyetlerin Yürütülmesi Ve Koordinasyonuna Yönelik Sorumlular Ve Sorumluluklar

1)Hastane Bilgi Yönetimi Sistemini kullanan tüm çalışanlar: HBYS sistemini kullanan tüm çalışanlar hastanedeki mevcut tüm bilgisayarlardan kendilerine verilmiş ve görevleri ile yetkilendirilmiş kullanıcı kodu ve şifresi ile yaptığı tüm işlemlerden sorumludur.(Veri girişi,değiştirmesi,silmesi vb.)

2)Tüm Bilgi İşlem Firma Elemanları:

❖ Bilgi işlem merkezinde görevli personelle hastanede çalışan tüm personellere otomasyon ile ilgili destek vermek.

❖ Hastane birimlerinde çalışan tüm personellerin yazılım üzerinde oluşabilecek yenileme,düzeltme gibi işlemleri tespit edip firma yöneticisine teslim etmek.

❖ Gün içerisinde hastalara ait sevklerin, bilgi eksikliği(tanı,işlem)gibi tespit edip mesai bitiminde kontrol oluşturup aksaklıkları düzeltmek.

❖ 24 saat boyunca icap yöntemi ile hastane çalışanlarına uzaktan veya bizzat hastaneye gelerek soruna müdahale etmek.

❖ Sistem odasının fiziksel durumlarını her gün kontrol edip kayıt altına almak.(ısı,nem)

❖ Yazılım üzerinde her türlü gelişmeye destek vermek.

3)Firma Sorumlusu:

❖ Bilgi işlem merkezi personeli tarafından , hastane çalışanları tarafından bildirilen istekleri yazılım şirketine iletmek,takip etmek ve sonucunu bilgi işlem merkezi sorumlusuna rapor etmek.

❖ Gün içerisinde işlemlerin gün sonunda alınan yedeği sağlam ve çalışır durumda olduğunu kontrol edip imza karşılığı bilgi işlem sorumlusuna teslim etmek.

❖ Hastane ile yazılım şirketi arasında koordineyi sağlamak.

4)Bilgi İşlem Sorumlusu:

❖ Hastaneye ait bilgisayar sisteminin verimli ve amaca uygun çalışmasını sağlamak.

❖ Bilgisayar sistemleri ile ilgili her türlü donanım ve yazılım problemlerinin çözümü, yedeklerinin alınmasını ve bilgilerin arşivlenmesi işlemlerini yürütmek.

❖ Sistemlerin arızalanması durumunda ön inceleme ve bakımını yaparak, gerekli servis hizmetlerinin verilmesini sağlamak.

❖ Bilgisayar sistemlerinin periyodik bakımlarında ve onarımlarında sözleşmeli firma elemanlarını ve çalışmalarını denetlemek, gerekli gördüğü hallerde yazılı-sözlü bilgi vermek.

❖ Her gün mesai başlangıcında bilgisayar sistemleri ve donanımlarının açılmasını, iş bitiminde ise kapatılmasını sağlamak.

❖ Teknik malzemelerin alımında malzemelerin şartnamelere uygunluğunun kontrolünü yapmak.

❖ Faaliyetler çerçevesinde, ihtiyaç duyulan yazılım sistemleri konusunda personele destek vermek; meydana gelen küçük teknik arızaları geciktirmeden gidermek veya giderilmesini sağlamak.

❖ Hastaneye ait elektronik postasına gelen bilgi ve talepleri ilgili birimlere iletmek.

❖ Bilgisayar donanımlarında meydana gelen aksaklıkların giderilmesi için amirine bilgi vermek.

❖ Konusuyla ilgili olarak amiri tarafından verilen diğer işleri yerine getirmek.

6.1.2.Bilgi Yönetim Sistemine ilişkin rol grupları ve yetkileri:

Otomasyon üzerinde yazılımı kullanan tüm personellerin yetkilendirilmesi yapılmıştır. Bu gruplardaki personeller yalnızca kendilerine verilen yetki kadar işlem yapabilir.

Bu rol grupları;

- Öğretim Üyesi
- Araştırma Görevlisi
- Klinik Hemşiresi
- Anabilim dalı Sekreteri
- Klinik sekreteri
- Poliklinik sekreteri
- Satın alam
- Kalite
- Faturalama vb.

Çalışanların yetkileri düzenlenmiştir ve kayıt altına alınmaktadır. Aynı görevde çalışan personellerin yetkileri de aynıdır.İşe yeni başlayan personel bilgi işlemden **Kullanıcı Yetkilendirme Formu** doldurarak birim yöneticisinin onayı ile kullanıcı adı ve şifresi verilir.İşten ayrılırken ise ilişik kesmek için bilgi işleme başvurarak ilişik kesilir.

6.1.3.Disiplinler arası yetkilendirme aşağıdaki gibidir:

Başhekim: Hastanedeki tüm bilgilere ulaşır.

Doktor: Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Elektronik ortamda kayıtlı olması gereken tüm hastaya ait tüm bilgileri girebilir. Onay işlemlerini kendi şifreleri ile yapmakla yükümlüdürler. Onaylanmadan önce kendilerine ait raporlar üzerinde silme ve değişiklik yapabilir. Hasta 'Adli Olgu' ise hasta raporu ancak Uzman tarafından girilebilir ve aynı Uzman tarafından onaylandıktan sonra değiştirilemez.

Müdür: İdari ve mali işlemlerle ilgili tüm bilgilere erişebilir.

Hemşire: Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir.

Silme ve değiştirme yetkileri yoktur. Kendi işlerine ait laboratuar ve preop. –postop. hasta bilgilerini, hastaya ait sarf ve işlem girişlerini yetkileri dahilinde yapabilirler.

Klinik Sekretarya: Doktorun istemlerini ve sarfları hastanın hesabına ekler. Hatalı yaptığı işlemleri sorumlularına bildirirler. Sorumluların düzeltemediği işlemleri BİMOB e bildirir. Hasta yatış -çıkış işlemleri için gerekli evrakları düzenler. Hasta taburcu işlemlerini yapar.

Personel Sicil Birimi: Personel özlük bilgilerine ulaşabilir, mesai, izin, sevk, rotasyon gibi personelin tüm işleyişini otomasyon üzerinden gerçekleştirir.

Döner Sermaye Birimi: Ay içerisinde başvuran tüm hastaların faturalamasını ve anlaşmalı kurumlara teslimatı yapar. Döner sermayeden sorumlu başhekim yardımcısı kurumlara

yapılan faturaların tutarlarını ve yapılan işlemleri görebilir inceleyebilir.

Eczane: Katlardan gelen eczaneyle ilgili taleplerin girişlerini yapar, otomasyon üzerinden girişlerin ve ilaçların karşılamasını yapar. Hastaların reçeteleri doğrultusunda ilaçların takibini sağlar.

Radyoloji: Hastaların radyolojik işlemlerini yapar. Tetkik işlemlerinin sonuçlarını otomasyon üzerinden raporunu yazar.

Laboratuar: Doktorların hastaları için, yaptığı istemleri alır, çalışmasını yapar ve otomasyon üzerinde hastanın sonuçlarını girer. Otomatik cihazlar için bu işlemler barkotlu sistem ile çalışır. Hasta test sonuçları Laboratuar Uzman Doktoru tarafından onaylandıktan sonra istem yapan kişiler tarafından hasta dosyasında sonuçlar görülebilir. Hastalar muayene oldukları poliklinikten ve web üzerinden (hastane web sayfası) sonuçları alabilirler.

Poliklinik Sekretarya: Hastaların gelişte otomasyon programına kayıtlarını yapar. Yatış öncesi işlemleri gerçekleştirir.

❖ Her kademedeki çalışan sadece yetkilendirilmiş olduğu işlemleri yürütebilmektedir.

❖ Yetkilendirilmemiş kimseler tarafından yapılan herhangi bir işlemi saptayan bölüm yetkilileri bu durumu en kısa zamanda yeterli delilleri ile birlikte bağlı bulunduğu birime iletilmek üzere bir üst yetkiliye bildirmektedir.

❖ Tüm çalışanlar otomasyon üzerinde yetkili oldukları bilgileri herhangi bir şekilde farklı ortamlarda paylaşamaz bilgi taşıyamaz.

❖ Kullanılan yazılımlarla ilgili şifreler kullanıcılara BİMOB tarafından verilir ve belli periyotlarda değiştirilmesi istenir. Yetkilendirilen çalışan, şifrelerin kullanılması ve korunması konusunda sorumlu tutulmaktadır.

6.1.4.Kullanıcılara verilen şifrelerle ilgili işlemler aşağıdaki şekilde yürütülmektedir:

❖ Belirli bir şifre ile yapılan tüm işlemlerin idari ve yasal sorumluluğu söz konusu şifrenin tanımlanmış kullanıcısına ait olduğundan, verilen şifre kullanıcı tarafından değiştirilerek kullanılır.

❖ Çalışanların yer değiştirmesi veya işten ayrılması durumunda şifrenin kapatılma işlemleri: Bilgi güvenliği açısından ilişiği kesilen personelin şifresinin bir an önce iptali esastır. İlişiği kesilen personelin tüm şifreleri ve kullanıcı yetkileri kullanıma kapatılır.

6.1.5. Otomasyon Bilgi İşlem Çalışanlarının Yetkilendirme İşlemleri:

Aşağıda belirtilen işlemler doğrultusunda BİMOB çalışanları yetkilendirmektedir.

- Yazılım kurma ve silme işlemleri
- Bilgi Sistemleri Yöneticisine açık otomasyon sistemi işlemleri

- Üst yönetime açık otomasyon sistemi işlemleri

6.1.6.Yazılım Kurma ve Silme İşlemleri:

N.E.Ü. Tıp Fakültesi Hastanesi bünyesinde kullanılma kararı alınmış otomasyon sistemi dahilindeki her türlü yazılımın kurma, silme ve düzenleme işlemleri ile işletim sistemi ayarlarının yapılması ve değiştirilmesi BİMOB yetkisindedir. BİMOB bilgisi dışında herhangi bir yazılım kurma ve silme işlemi ve işletim sistemi ayarları yetkilendirilmemiş bir işlem olarak değerlendirilecektir ve tamamen ilgili cihazın kullanıcısının sorumluluğundadır.

6.1.7. Otomasyon sistemi işlemleri:

Hastane bilgi yönetim sistemi işlemleri, BİMOB' in onayladığı şartlar kapsamında saptanan çalışanın yetkisinde olacaktır. Verilen standart yetkiler dışında istenilen bir yetki, bağlı bulunduğu yöneticinin onayından sonra, uygun görüldüğü seviyede BİMOB tarafından verilir.

6.2.BİLGİ GÜVENLİĞİ:

6.2.1. Sunucuların Güvenliği:

❖ Sunuculara tahsis edilmiş bir bağımsız oda bulunmaktadır

❖ Oda Şifreli kilit sistemi ile kilit altında ve şifreler sadece bilgi işlem personelinin bilgisindedir. Görevlendirme olmayan personel bu odaya girememektedir.

❖ Oda hastanenin 2. katında bulunmaktadır. Oda içinde su tesisatı bulunmamaktadır.

❖ Sunucu Odalarında elektrik kesilmesi durumunda odada bulunan bağımsız **UPS** devreye girmektedir. Hastane genelinde bulunan **UPS** bu odadaki bağımsız **UPS** yi desteklemektedir.

❖ Isı ve nem takibi yapılarak **Sıcaklık Ve Nem Takip Formu** kayıt edilmektedir.(Sıcaklık 18-22 °C,Nem %30-%50 arasında bulunmaktadır)

❖ 2. Klima yedek olarak bulunmaktadır

❖ Bütün sunucuların yeri,sorumlu kişisi,donanımı ve işletim sistemi üzerinde çalışılan uygulama bilgileri liste halinde bilgi işlem biriminde ve kalite biriminde bulunmaktadır.

❖ Sunucuları içinde bulunduğu oda 24 saat kamera görüntüsü ile izlenmektedir.

6.2.2. Yedekleme:

➢ Yedekleme harici bellek, ağ üzerinde çalışan bilgi işlem merkezinde 1 adet PC, sunucunun kendi üzerinde ve morfoloji binasında sunucu odası tarafında 1 adet PC'de yedeklenmektedir.

➢ Yedekleme sunucuda günlük olarak yapılmaktadır. Arşivlemesi harici bellekte 25 günlük, diğer PC'lerde aylık olarak yapılmaktadır.

➢ Veriler yedekleme yapıldıktan sonra offline ortamda saklanmaktadır.

➢ Veri yedeklemesi kurumun kritik BT işlemlerinden birisidir. Kurum politikasında yedekleme konusu mutlaka yer almalı ve veri yedeklemesi için yönetim prensiplerini ortaya koyan bir

politika bulunmalıdır. Kurum verisinin yedekleme işlemleri yedekleme politikasına göre yerine getirilmelidir.

- Kurumun bütün verisinin, kurum çapında kullanılan işletim sistemlerinin ve uygulamaların tamamının yedeği uygun ve düzenli olarak alınmalıdır.
- Yedekleme sistemi iş sürekliliği planında yer alan veri yedekleme ihtiyacını karşılamalıdır.
- Yedeği alınacak veri ve uygulamalar için sınıflandırma yapılmalı ve her bir sınıf için kabul edilmeli veri kaybı süresi belirlenmelidir.
- Kabul edilir veri kaybı süresi yönetim tarafından onaylanmalıdır.
- Yedekleme işlemlerinin sağlanması için yedekleme politikasına uygun olarak bir yedekleme planı oluşturulmalıdır.
- Yedekleme işlerine ait kayıtlar tutulmalıdır.
- Başarısız olan yedekleme işleri takip edilmeli ve yedeği alınamamış verinin yedeği alınmalıdır.
- Yedekleme medyaları etiketlenmeli ve hangi medyada hangi yedeğin bulunduğuna dair kayıtlar tutulmalıdır.
- Yedekleme medyalarının kopyaları alınarak ana sistem odasına zarar verebilecek felaketlerden etkilenmeyecek kadar uzakta ve güvenli olarak depolanmalıdır.
- Yedeklenmiş verinin düzenli aralıklarla geri döndürme testi yapılmalıdır.
- Yedekleme altyapısı, yedekleme ve geri döndürme işlemleri için talimatlar hazırlanmalıdır.
- Yedeklemesi alınacak bilginin seviyesi belirlenmelidir.
- Yedekleme kopyalarının doğru ve tam kayıtları ve dokümante edilmiş geri yükleme süreçleri sağlanmalıdır.
- Yedeklemenin türü (tam yedekleme/değişen kayıtların yedeklenmesi), yedeklemenin sıklığı iş gereklerine, güvenlik gereksinimlerine ve bilginin kritiklik derecesine göre belirlenmelidir.
- Yedeklerin bir kopyası doğal afetlerden ve olası tehlikelerden korumak maksadıyla ana merkezden uzak bir merkezde saklanmalıdır.
- Yedekleme bilgisine uygun seviyede fiziksel ve çevresel koruma sağlanmalıdır.
- Herhangi bir tehlike durumunda kullanımını sağlamak maksadıyla yedekleme bilgisi düzenli olarak test edilmelidir.
- Geri yükleme süreci düzenli olarak kontrol ve test edilmelidir.
- Gizliliğin önemli olduğu durumlarda yedeklemelerin kriptolu olarak alınması göz önünde bulundurulmalıdır. Bu kapsamda özellikle kişisel sağlık bilgilerinin kriptolu olarak yedeklenmesine dikkat edilmelidir.

6.2.3.İş Sürekliliği Yönetimi

- Kuruluşun karşılaşabileceği risklerin olasılığı, zaman içerisindeki etkisi, kritik iş süreçleri belirlenmelidir.
- Kritik iş süreçleri kapsamındaki varlıklar belirlenmelidir.
- Hangi bilgi güvenliği olaylarının iş sürekliliğinde kesintilere neden olduğu ve etkisi araştırılmalıdır.
- Operasyonel risk yönetiminin olabileceği gibi tüm iş sürekliliği sürecinin bir parçasının sigorta ettirilmesi değerlendirilmelidir.
- Önleyici ve zararı azaltıcı ilave kontroller uygulanmalıdır.
- Belirlenmiş bilgi güvenliği gereksinimleri için yeterli finansal, kurumsal, teknik ve çevresel kaynakların tahsis edilmesi sağlanmalıdır.
- Personel güvenliği, bilgi işleme tesisleri ve kurumsal varlıkların korunması garanti altına alınmalıdır.
- Kabul görmüş iş sürekliliği stratejisi paralelinde bilgi güvenliği gereksinimlerine işaret eden iş sürekliliği planları formüle ve dokümante edilmelidir.
- Uygulamaya konulan plan ve süreçlerin düzenli olarak test edilmesi ve güncellenmesi sağlanmalıdır.
- İş sürekliliği yönetiminin kurumun süreçleri ve yapısı ile birleştirilmesi, iş sürekliliği yönetim sorumluluklarının kurum içerisinde uygun seviyelere atanması konuları göz önüne alınmalıdır.

6.2.4. Kişisel Sağlık Kayıtların Güvenliği:

Kullanıcılar, hasta ile ilgili bilgileri girilir, muayene ve reçete girildikten sonra hasta kaydı kapanır. Tekrar kullanıcılar bilgileri değiştiremez. Kişisel bilgiler kişinin kendisi veya mahkeme tarafından istenildiği takdirde verilir.

6.3.ERİŞİM VE YETKİ KONTROLÜ:

6.3.1. İnternet Erişim Ve Kullanım:

İnternet erişimi idari birimler, bilgi işlem ve poliklinikler olarak 3 ayrıldı. İdari birimler resmi site ve haber kaynaklı siteler dışı kapalıdır.(Tüm filtrelemeler alizer cihazında logları kayıt altında tutulmaktadır.)Tüm loglar izlenebilir durumdadır. Bilgi işlem Tüm sitelere açıktır. Poliklinikler resmi siteler ve haber siteler dışı tüm sitelere erişim kapalıdır.

6.3.2. E-Posta Kullanım:

İdari birimler e posta gelen ve giden olarak kullanabilir, diğer birimlere kapalıdır.

6.3.3. Uzaktan Erişim:

Dış ortamdan iç ortama hangi durumlarda bağlanacağını belirten ilgili firma ile hastane idaresi arasında gizlilik sözleşmesi bulunmaktadır. Dış ortamdan bağlanıldığı durumlar kayıt altına alınmaktadır.

6.2.4. Kablosuz Erişim:

Hastanenin bazı bölüm ve birimlerinde mevcut olup artırma ve kapsamı genişletme çalışmaları devam etmektedir.

❖ Hastane bölümlerinde çalışan tüm personelin otomasyon sistemine girdiği, kullanıcı kodu ve parolası md5 metodu kullanılarak şifreli şekilde veri tabanında tutulmaktadır.

❖ Her kullanıcının yetkileri otomasyon üzerinden birim yöneticisi tarafından onaylanarak belirlenir.

❖ Hastane içinde içeriği hasta mahremiyetini etkileyecek olan bilgiler otomasyon sisteminde yetkilendirilip, bilgi işlem personeli dahil kimseye gösterilmez. Yalnızca başhekimliğin onay verdiği kullanıcılara görme yetkisi verilir.

❖ Kullanıcıların sisteme kaydettiği nitelikli hizmetlerin hiçbiri yönetim onayı olmadan, bilgi işlem personeli haricinde hiçbir personel tarafından silinemez.

❖ Gün içerisinde otomasyon sistemine girilen tüm işlemler (Sekreter, hemşire, doktor) tümü gün sonunda saat 23:30'da yedekleme işlemi otomatik olarak başlamaktadır.

❖ Personele ait özlük bilgileri ise yalnızca İnsan Kaynakları personeli tarafından görülüp, yetkileri yönetim tarafından belirlenir. Yetkili personel dışında kimse personel özlük bilgilerine erişemez.

❖ Gün içerisinde hastane internet ağına bağlı olan tüm bilgisayarların hangi zamanda, hangi internet sitesine bağlandığını, ne kadar süreyle o sayfada kaldığı gibi tüm bilgiler hastane fiziksel güvenlik duvarında yedeklenip log'ları kayıt altına alınmalıdır.

❖ Oluşabilecek virüs saldırıları için hastanenin 2 yıllık imzalanan anti virüs lisansı ile bilginin güvenliği sağlanmalıdır. Fiziksel güvenlik duvarı ve anti virüsün güncellemelerini ve üst versiyon yüklenmelerini bilgi işlem sorumlusu takip eder.

6.4.FİZİKSEL VE ÇEVRESEL GÜVENLİK KONTROLÜ YÖNETİMİ

6.4.1. Fiziksel Güvenlik Sınırı;

- Bilgi işleme servisini korumak amacıyla herhangi bir fiziksel sınır güvenliği tesisi kurulmuş olmalıdır. (Kart kontrollü giriş, duvarlar, insanlı nizamiye)
- Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmalıdır.

6.4.2. Fiziksel Giriş Kontrolleri;

- Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmalıdır.
- Kapsam ve prosedürü idarelerce belirlenmek suretiyle ziyaretçilerin giriş ve çıkış zamanları belirlenmelidir.
- Hassas bilgilerin bulunduğu alanlar (kimlik doğrulama kartı ve PIN koruması gibi yöntemlerle) yetkisiz erişime kapatılmalıdır.
- Kapsam ve prosedürü idarelerce belirlenmek suretiyle tüm personel ve ziyaretçiler güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartlarını devamlı takmalıdır.
- Güvenli alanlara erişim hakları düzenli olarak gözden geçiriliyor olmalıdır.

6.4.3. Ofislerin ve Odaların Güvenliğinin Sağlanması;

- Ofisler ve odalarla ilgili fiziksel güvenlik önlemleri alınmalıdır.
- Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmalıdır.
- Kritik tesisler kolayca ulaşılamayacak yerlere kurulmuş olmalıdır.
- Binada bilgi işlem faaliyetlerinin yürütüldüğüne dair işaret, tabela vb. bulunmamasına dikkat edilmelidir.
- Bilgi işlem merkezlerinin konumunu içeren dâhili/harici telefon rehberleri halka kapalı olmalıdır.

6.4.4. Harici ve Çevresel Tehditlerden Korunma;

- Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karsı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.
- Komşu tesislerden kaynaklanan potansiyel tehditler göz önünde bulundurulmalıdır.
- Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir yerde konuşlandırılmış olmalıdır.

6.4.5. Güvenli Alanlarda Çalışma;

- Güvenli çalışma alanlarındaki personel veya bu alanda yürütülmekte olan çeşitli faaliyetlerde bulunan personel ve üçüncü parti çalışanları için "ihtiyacı kadar bilme" prensibi uygulanmalıdır.
- Kayıt cihazlarının güvenli alanlara sokulmasına engel olunmalıdır.
- Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor olmalıdır.
- Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir.
- Güvenli bölgelere örneğin sistem odasına yapılan girişler kayıt altına alınmalıdır.
- Bilgi işlem servisleri ile dağıtım ve yükleme alanları ve yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmiş olmalıdır.

6.5.İLETİŞİM VE İŞLETİM GÜVENLİĞİ

Bilgi sistemlerinin iletişim ve işletim görev ve sorumlulukları kuruluşun varlıklarının yetkisiz veya kasıtsız olarak değiştirilmesi ve yanlış kullanılmasını engellemek maksadıyla ayrılmalıdır. Hiçbir personel denetimsiz veya yetkisiz olarak sistemlere erişemez ve sistemleri değiştiremez.
Bilgi İşleme ve İşletim yönetimi aşağıda belirtilen konuları kapsar;
• Bilgi işleme ve bulundurma gereksinimlerinin belirlenmesi,
• Bilginin yedeklenmesi,
• En erken işe başlama ve en geç işi tamamlama zamanlarının belirlenmesi,
• Sistem kullanım kısıtları hata mesajlarını yöneten talimatların oluşturulması,
• Beklenmeyen işletim ve teknik sorunlar karşısında destek irtibatları belirlenmesi,
• Güvenli çıktı alma talimatlarının hazırlanması,
• Sistem hatası durumunda yeniden başlatma ve kurtarma süreçlerinin belirlenmesi,
• Sistem izleme kayıtlarının yönetiminin planlanması ve uygulanması.

6.5.1.Uygulama geliştirme, test ve operasyonel sistemlerinin ayrılması;

- Yazılımın geliştirme sistemlerinden uygulama sistemlerine aktarımı kuralları belirlenmeli ve dokümante edilmelidir.
- Geliştirme ve uygulama yazılımları ayrı işlemcilerde, ayrı sistemlerde, ayrı etki alanlarında veya kütüphanelerde çalıştırılmalıdır.
- İhtiyaç olmadığı durumlarda operasyonel sistemlerde derleyici, editör, ve diğer geliştirme araçları bulundurulmaz.
- Test sistemi operasyonel sistemle mümkün olduğunca aynı sistem olmamalıdır.
- Kullanıcılar test ve uygulama sistemlerinde farklı kullanıcı tanımları kullanmalıdır.

6.5.2.*Üçüncü taraflardan hizmet alımı esnasında gereken aktarımlar (bilgi, bilgi işleme imkânları ve taşınan diğer unsurlar) planlanmalı ve güvenlik daima göz önünde bulundurulmalıdır. Üçüncü taraf hizmetlerinin izlenmesi ve gözden geçirilmesi kapsamında;*

- Hizmet performans seviyesinin anlaşmaya uyumlu olduğu izlenmelidir.
- Üçüncü tarafça hazırlanan hizmet raporları gözden geçirilmeli, anlaşmada belirtildiği şekilde geliştirme toplantıları yapılmalıdır.
- Alınan hizmete ilişkin üçüncü taraf tarafından tutulan güvenlik olayları kayıtları, operasyonel sorunlar, hatalar, hizmet kesintileri gözden geçirilmelidir.
- Varsa tespit edilen sorunlar yönetilmeli ve çözülmelidir.

6.5.3.Üçüncü taraf hizmetlerinde yapılan değişikliklerde;

• Ağdaki değişimler,
• Yeni teknolojilerin kullanımı,
• Yeni ürünlerin daha yeni sürüm ve baskılara uyumu,
• Yeni geliştirme araç ve ortamları,
• Hizmetlerin verildiği fiziksel yerin değişimi göz önüne alınmalıdır.

6.5.4. Üçüncü taraflardan hizmet alımlarında değişiklik olması durumunda; kuruluş tarafından yapılan değişikliklerde;

• Sunulan hizmetteki gelişmeler,
• Yeni uygulama ve sistemlerin geliştirilmesi,
• Kurumun politikalarındaki değişiklik ve güncellemeler,
• Güvenliği geliştirmek ve bilgi güvenliği olaylarını çözmek için geliştirilen yeni kontroller göz önüne alınmalıdır.

6.5.5.Bilgi işlem teçhizatının kapasite yönetimine ilişkin olarak anahtar konumundaki sistem kaynaklarının kullanım durumu sistem yöneticileri tarafından sürekli izlenir, her yeni veya devam eden faaliyetin kapasite gereksinimi belirlenir. Sistemden en uygun şartlarda verim almak için sistem ayarları sürekli kontrol edilir. Gelecekteki sistem ihtiyaçları, ileriye yönelik planlanan yeni iş uygulamaları ve mevcut kapasite göz önüne alınarak değerlendirilir.

6.6.BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

- Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.
- Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
- Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.
- Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.
- İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
- Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.
- Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.
- Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.
- Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.
- İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.
- Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.
- Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.

Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

- Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
- Kanıtın niteliği ve tamlığını gösteren ağırlığı.

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

- Uyarma,
- Kınama,
- Para cezası,
- Sözleşme feshi.

6.7.HBYS'YE İLİŞKİN YAZIMSAL SÜREÇLER:

6.7.1.Yazımsal Süreçler:

❖ Hastane çalışanları yaptıkları işle ilgili düzeltme, güncelleme, değişiklik gibi işlemleri bilgi işlem personeline iletir.

❖ Bilgi işlem personeli kullanıcı ile birlikte sorunu tespit eder ve yazılımsal değişikliğe gerek olan durum varsa firma sorumlusu ile birlikte yazılım şirketine ait olan internet ortamındaki istek bilgilerini sisteme yazılımsal isteği kaydeder ve raporunu bilgi işlem sorumlusuna teslim eder.

❖ Yazılım şirketi isteği değerlendirip 48 saat içerisinde planlamaya alır. Planlamaya alınan istekler hastane bilgi işlem sorumlusu tarafından kritik derecesi belirlenir. İsteklerin kritik derecesi;

ÇOK KRİTİK: 3 iş günü içerisinde (Yeni çıkan tebliğ, yönetmelik güncellemeleri)

KRİTİK: 5 iş gün içerisinde (Bir bölümün işletmesini aksatacak istekler)

NORMAL: 30 iş günü içerisinde herhangi bir işleve etki etmeyecek, yazılımda düzeltme yapılacak istekler.

❖İstekler yukarıda belirtilen süreler dışına çıkmış ise sözleşmesinde belirtilen cezai işlemler devreye girer.

❖Normal sürelerde yapılan istekler ise bilgi işlem sorumlusu ve isteği yapan kullanıcı tarafından onaylanarak, sistem üzerinden kapatılır.

6.7.2.Sorunların Çözümü

❖ Hastane iç hat telefon numarası ve HBYS üzerinden hasta istek ve değişiklik formu ile bilgi işlem servisi çalışanlarıyla irtibat kurulur.

❖ Bilgi işlem personeli arasında iş bölümü oluşturuldu. Poliklinik ve servisler, donanım ve teknik arıza, görüntüme ve laboratuar, idari birimler olarak bölümlere ayrıldı ve görev paylaşımı yapıldı.

❖ İlgili bölümlerden oluşan sorunlar hemen çözülmeye çalışılır çözülemediği takdirde diğer bilgi işlem personelinden yardım alınır. İşlerin aksamamasına meydan verilmemeye çalışılır.

❖ İlgili sorun çözüldüğünde çözen bilgi işlem personeli tarafından HBYS kayıt edilir

Bilgi Sistemleri Yöneticisine Açık Hastane Bilgi Sistemi İşlemleri:

❖ Aşağıda belirtilen ve otomasyon sistemi üzerinde normal kullanıcı şifreleri ile yapılamayan işlemler BİMOB' in yetkisinde olacaktır. Bu işlemlerin yapılabilmesi için gereken şifreler BİMOB Sorumlusu tarafından verilecek ve gerektiğinde değiştirilecektir.

❖ Otomasyon sistemi üzerinde rutin kullanım yolları ile ancak yanlış olarak girilmiş ve aynı yollarla değiştirilmesi mümkün olmayan bilgilerin düzeltilmesi.

❖ .Doğru olarak girilmekle beraber kullanıcıların kontrolü dışında yanlış sonuçlar doğuran ve aynı yollarla değiştirilmesi mümkün olmayan bilgilerin düzeltilmesi.

❖ .Yetkilendirmeye uygun olmayan hastane bilgi sistemi işlemlerinin hangi operatörler tarafından ve ne zaman yapıldığının sistem kayıtlarından açığa çıkarılması.

Üst Yönetime Açık Hastane Bilgi Sistemi İşlemleri:

❖ Üst Yönetiminin kurum planlaması, tıbbi, işletme, mali değerlendirmeler ve benzeri amaçlar ile otomasyon sistemi üzerinden alacakları raporlar BİMOB tarafından yapılır.

6.8.SİSTEM ALT YAPISINA İLİŞKİN SÜREÇLER:

6.8.1. Network Donanım Cihazlarının;

❖ Ana omurgayı (Merkez Switch) taşıyan cihazın, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.

❖ Ağ cihaz ve yazılımlarını kurar, internet ve intranet bağlantılarını yönetir

❖ Kenar switch cihazlarının, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.

❖ Routerların, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.

❖ Güvenlik cihazlarının, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.

❖ Kablolu (ADSL, GSHDSL, Metro Ethernet) ve kablosuz iletişim cihazlarının (wireless cihazlar, Optik Laser Hat, Wimax..) iletişim cihazlarının yapılandırılmalarını, yönetimini gerçekleştirir.

❖ Bilgisayar sistemlerinin fiziksel güvenliğinin ötesinde yazılımsal güvenlini de sağlamak.

❖ Elektronik ortamda sisteme olabilecek saldırıları (virus, worm, rootkit, backdoor, trojan, hacker keyloger, spyware v.b.) engellemek,

❖ Sistem odasındaki cihazların bakım ve onarımlarını yapar/yaptırır.

❖ Tüm bilgisayar sisteminin sağlıklı çalışmasını sağlayan antivirus sunucularını, kurar,

günceller, bakımını yapar, sistemin virüs saldırıları nedeni ile kesintiye uğramaması için tedbirler alır. Yeni çıkan virüslere yönelik güncelleştirmeleri sisteme yükler.

- ❖ Tüm bilgisayarların donanımsal ve yazılımsal arızalarını giderir. Son çıkan güncellemeleri takip eder ve hastane sistemindeki tüm bilgisayarlara yükler.

6.8.2. İnternet Bağlantılarının;

- ❖ Hastanenin internet Bağlantısını yönetir, izler yetkili kullanıcıların internete erişimine izin verir.
- ❖ Firewall cihazının yönetimini yapar, IP, port, yetkilendirmesi, erişim kontrol listelerinin tanımlanmasını yapar VPN (sanal Özel Ağ) yapısını yönetir.
- ❖ Filtreleme cihazı aracılığı ile uygun olmayan içeriğe ulaşımı engeller, zararlı sitelerin kullanıcı bilgisayarlarını bozmasına engel olur. Yeni çıkan zararlı siteleri cihaz güncellemeleriyle engeller.
- ❖ Internet kullanıcılarının hastane web sitesine ulaşmasını, Web Sunucusunun güvenli biçimde internet üzerinden internet yayını yapmasını sağlar.
- ❖ Elektronik posta sunucusunu kurar, işletir, kurum kullanıcılarının e-posta alıp göndermesini sağlar.
- ❖ Kurumsal kullanıcıların kendilerine verilen yetkilendirmeler dâhilinde sistem kaynaklarını kullanmasına izin verir.

6.8.3.İşletim Sistemlerinin;

- ❖ Yazılım güncelleştirmelerini, yamalarını, loglarını, performanslarını izlerler.
- ❖ İşletim sistemlerinin yapılandırma/konfigürasyonlarını yaparlar.
- ❖ İşletim sistemlerinin güvenlik ayarlarını yaparlar.
- ❖ İşletim sistemlerinin üzerinde çalıştığı fiziksel sunucuların çalışma düzenini kontrol ederler.
- ❖ Donanım kaynaklarının (Diski, Ram, Kontrol Kartları, Güç Kaynakları, İşlemciler) çalışırlığını izler ve kontrol ederler.

6.8.4.Veritabanlarının;

- ❖ Veri tabanın performansını izlerler.
- ❖ Veri tabanının bakımını gerçekleştirir.
- ❖ Yedeklerinin alınmasını sağlar ve/veya gerçekleştirirler.
- ❖ Yedek alma ve arşivleme işlemi depolama cihazlarını ve kotaları yönetir,
- ❖ İlgili sistemlerde bulunan verilerin yedeğini uygun periyotlar da alır.
- ❖ Programlar her veri güncellemesinde yedeklenir ve DVD medyada arşivlenir.
- ❖ Kullanıcı bilgisayarlarındaki verilerin merkezi olarak yedeklenmesi ve arşivlenmesi teknoloji olarak mümkün olmakla birlikte hali hazırdaki birim imkânları ile gerçekleştirilemediğinden kullanıcılara ait veri yedekleme işlemi kullanıcıların kendileri tarafından müdürlük yedekleme

talimatına uygun olarak yapılmaktadır.

- ❖ Yedekleme cihazlarını izler,
- ❖ Yedekleri güvenli yerlerde saklar.
- ❖ Belirli aralıklarla veri arşivleme çalışması yapar. Güvenli yerlerde muhafaza eder.

6.8.5.Yazılım Geliştirme

- ❖ Kurumsal kullanıcılardan gelen hastane hizmetlerine yönelik yazılım taleplerini değerlendirmek
- ❖ Bilgi işlem müdürlüğünce onaylanan yazılım talepleri ile analiz çalışmalarını yapmak.
- ❖ Programın çalışması için gerekli kaynakları belirlemek ve sistem yönetimine müdürün onayı sonrasında bildirmek
- ❖ Yazılım geliştirme platformu ve temel yazılım geliştirme mimarisi belirlenir.(clien-server/web tabanlı,lokal,Windows vb.)
- ❖ Veri tabanı belirlenir. Yazılım geliştirme dili seçilir.
- ❖ Analiz çalışmalarına dayalı olarak temel fonksiyonların yazımı gerçekleştirilir, menülerin yazılımına başlanır.
- ❖ Programın yazılımı sonrasında çalışma testleri yapılır. Testler sonrasında çıkan bugler düzeltilir.
- ❖ Son kontroller sonrasında veri tabanındaki test verileri silinir,programı yönetecek kişi için kullanıcı tanımlamaları yapılır.Program devreye alınır.
- ❖ Programın devreye alınması sonrasında program kullanıcılarından gelen programla ilgili sorunlar giderilir, kullanıcılara teknik destek verilir.
- ❖ Programın görsel tasarımı kurumsal kimlik standartlarına uygun olarak tasarlanır.

6.8.6.Web Uygulamaları Ve Web Tasarım Çalışmaları

- ❖ Web uygulamaları geliştirme çalışmaları yapılır.
- ❖ Yazılım geliştirme sürecinde tanımlanan temel onay analiz ve ön çalışmalar yapılır.
- ❖ Uygulamaların intranet ya da internet uygulaması olması durumuna göre web sunumu, sistem yönetimi tarafından tahsis edilir, gerekli ağ ve güvenlik ayarları yapılır.
- ❖ Birimlerden gelen, duyuru, birim faaliyetleri, spor etkinlikleri, kültürel etkinlikler, yönetim kararları vb. hastane web sitesinden yayınlanması amacıyla gerekli görüşme, kodlama ve tasarım çalışmaları yapmak.
- ❖ Hastane sitesinde kullanılacak görsel materyalleri temin etmek, üretmek ve kurumsal kimliğe uyumlu olarak sitede kullanmak.
- ❖ Temin edilen materyalleri fish animasyon, ikon, buton üretmek

❖ Kurumsal e-hastanecilik uygulamalarının web sitesi içinde uyumlu biçimde çalışması için kodlama ve görsel tasarım çalışmaları yapmak(e-sonuç, e-randevu, e-kütüphane, yerleşim haritası, hastane bilgi sistemi)

❖ Hastane web sitesi alt uygulamalarını geliştirmek ve yönetmek(istek, şikâyet, bilgi edinme, performans programı, stratejik plan, hizmetlerimiz)

6.8.7.Proje Geliştirme Ve Ar-Ge

❖ Hastanenin iş süreçlerini de göz önünde tutarak, bilgisayar sistemlerinin işleyişine yönelik risk analizleri yapar, rapor hazırlar, üst yöneticilerin dikkatine sunar. Raporda tespit edilen ya da öngörülen risklerin giderilmesine yönelik çözüm önerileri sunar.

❖ Teknolojik gelişmeleri takip eder. Kurum menfaatine olan teknolojik gelişmelerden uygulanabilir olanları tespit eder, rapor hazırlar, üst yöneticilerinin dikkatine sunar. Raporda tespit edilen ve kurum menfaatine olan teknolojilerin gerçekleştirilmesine yönelik uygulama önerileri sunar.

❖ Yukarıda açıklanan raporlar ve müdürlük ihtiyaçları da göz önünde tutularak müdürlük hedeflerinin oluşturulmasına katkıda bulunur.

6.8.8.Sistem Operatörleri

❖ Hastane uygulamalarının çalışırlığını izler, performanslarını varsa loglarını izler.

❖ Varsa yazılımı üreten firma aracılığı ile güncelleştirmeleri yapılır, uygulamada görülen aksaklıklar ilgili firmaya en hızlı yöntemlerle sözlü ve yazılı olarak iletilir.

❖ Hastane uygulamaları aracılığı ile üretilen verilerin yedeklerini alır.

6.9.BİLGİ TEKNOLOJİLERİ VE İMHA YÖNETİMİ

➢ Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.

➢ Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.

➢ Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.

➢ İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.

- Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
- Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
- Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
- Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.
- Hacimsel küçültme işlemi için parçalanmalıdır.
- Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.
- Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

7.İLGİLİ DÖKÜMANLAR:

- **HB.FR.09 Ortam Sıcaklık Ve Nem Takip Formu**
- **BL.FR.01 Kullanıcı Yetkilendirme Ve Gizlilik Sözleşmesi**