**1. AMAÇ:** Hasta ya da çalışanlara ait tıbbi ve kişisel bilgilerin, doğru ve güvenli şekilde kayıt altına alınması vedepolanması 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 Bilgi Yönetim 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 işlemlerinbilgisayar tarafından otomatik olarak yürütülmesi.

**5. SORUMLULAR:** Başhekim, 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.BİLGİ GÜVENLİĞİ:**

**6.1.1. Sunucuların Güvenliği:**

Merkezde 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 girişlerinde SERVER ODASI GİRİŞ ÇIKIŞ KONTROL FORMU’na kayıt yapılır.

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 formuna kayıt edilmektedir. (Sıcaklık 18-22 °C Nem %45-%70 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.

**6.1.2. Kişisel Verilerin Korunması:** Kullanıcılar, hasta ile ilgili bilgiler girilir, muayene ve reçete girildikten sonrahasta kaydı kapanır. Tekrar kullanıcılar bilgileri değiştirmek istediklerinde kaydı tekrar açarlar ve bu değiştirme işlemleri log kayıtlarında ayrı bir veri tabanında saklanır. Kişisel bilgiler kişinin kendisi veya mahkeme tarafından istenildiği takdirde verilir.

**6.1.3. İnternet erişim ve kullanım:**

1. Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar (lar) ı üzerinden internete çıkmalıdır. Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
2. Kurum içinde free vpn, Proxy server, Tor, torrent, hotspot vb. uygulamaların kullanılması yasaktır.
3. Kurumun politikaları doğrultusunda içerik filtreleme sistemleri kullanılmaktadır.
4. Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmaktadır.
5. Kurumun ihtiyacı ve olanakları doğrultusunda güncel antivirüs sunucuları kullanılmaktadır
6. Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri kontrol edilmektedir.
7. İnternete giden ve gelen bütün trafik virüslere karşı taranmaktadır. Gerekli durumlarda engellemeler yapılmaktadır.
8. Mesai saatleri içerisinde iş ile ilgili olmayan video, müzik vb. aşırı veri çeken streming media kullanılmamaktadır.
9. Mesai saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemektedir.
10. Kurumsal alanlarda verilen internet hizmetinin şahsi iş ve işlemlerde kullanılamaz.
11. Kurum network güvenliği açısından yönetilemeyen switch (Hub çoklayıcı) kullanılmamaktadır.
12. Kurum network güvenliği açısından Hub, acces point vb. cihazların bilgi işlem birimi izni dışında kurum networküne kesinlikle bağlanmamaktadır.
13. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.
14. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumum bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.
15. Kurum network güvenliği acısından mümkün olduğunca VLAN yapısı kullanılmalıdır.
16. Merkezi olarak kullanılan HBYS hizmetleri ve bakanlığımız uygulamalarına erişimin aksamaması, bant genişliği trafiğini sağlıklı yönetilmesi, siber saldırı tehditlerine karşın gerekli önlemleri almak için internet erişim düzenlemeleri gerekli hallerde İl Sağlık Müdürlüğü tarafından değiştirilir.
17. Kamusal hizmetlerin yürütülmesinde erişim engeli yaşayan personeller için **Ayrıcalıklı Erişim Talep Forumu**’yla ıslak imzalı olarak İl Sağlık Müdürlüğüne resmi yazı ile bildirilerek gerekli değerlendirme yapılacaktır.
18. Yasaklanması gereken siteler bilgi güvenliği yönetim komisyonu tarafından belirlenip onaylandıktan sonra uygulamaya konulacaktır. Ancak kurum bilgi güvenliğini tehlikeye düşürecek bir durumda (siber saldırı, veri kaybı vb.) onay alınması beklenmeden uygulamaya geçilebilecektir.

**6.1.4. E-Posta Kullanım:**

1. Kurumsal iş ve işlemlerini yapabilmek için her kullanıcının Sağlık Bakanlığı eposta hesabı olmalıdır.
2. Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.
3. Kurum ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.
4. Kullanıcı, Kurumun e-posta sistemini taciz, su istimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Kullanıcılar bu tür özelliklere sahip bir mesaj alındığında kurum bilgi güvenliği sorumlusuna haber verilmelidir. Ayrıca kurumun web sitelerinde yer alan Olay Bildirim Formunu kullanarak veya “https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir” adresinden ihlal bildirimi yapılmalıdır.
5. Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçlar ile e-posta gönderilmemelidir.
6. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, bilgi güvenliği birim sorumlusuna haber verilmelidir.
7. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
8. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
9. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.
10. Kurumsal E-posta kişisel amaçlar için kullanılmamalıdır.
11. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e- postalara herhangi bir işlem yapmaksızın bilgi güvenliği sorumlusuna haber vermelidir.
12. Kullanıcı, kurumsal mesajlarını, kurum iş akışının aksamaması için zamanında cevaplandırmalıdır.
13. Kullanıcı, kurumsal e-postalarının, kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.
14. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar bilgi güvenliği sorumlusuna haber verilmelidir.
15. Kullanıcı parolaları, en az 8 karakterden oluşmalı ve parolalarda; en az 1 tane harf, en az 1tane rakam ve en az 1 tane özel karakter (@,+,$,#,&./,(,\*,- ,}.=... ) bulunmalı; parola içeriğinde kullanıcı adını soyadını açık bir şekilde yazmamalıdır.
16. Kullanıcı, kendilerine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren Bilgi İşlem Birimine haber vermelidir.
17. Bakanlığımız tarafından talep edilen birimlere özel olarak verilen tüzel e-posta hesapları “***Tüzel Kişiler E-posta Talep Formu”*** kullanılarak yapılmalıdır.
18. Bakanlığımız tarafından talep edilen birimlere özel olarak verilen tüzel eposta hesapları direkt kullanıcı hesaplarına yetkilendirilmiştir. Yetkilendirilen kişilerin birim değişikliği veya kurumda ayrılması durumunda ilgili birim tarafından Bilgi İşlem Birimine haber verilmelidir. Haber verilmemesi durumunda doğacak her türlü zarardan ilgili birim sorumlu olacaktır.

**6.1.5. Uzaktan Erişim**:

1. Kurum sunucularına erişim için SSL VPN kullanılmalıdır.
2. SSL VPN ile bağlantı verilen kullanıcılar sadece yetkisi olduğu sunuculara erişecek şekilde erişim kısıtlaması yapılmalıdır.
3. SSL VPN gerçekleştirecek kullanıcılara(firma ve kurum personeli) mutlaka kurumsal gizlilik sözleşmesi imzalatılmalıdır. Eğer firmanın Kurumsal gizlilik sözleşmesi yok ise ilgili firma ile kurumsal gizlilik sözleşmesi de imzalanır.
4. SSL VPN gerçekleştirecek kullanıcılar(firma personeli) mutlaka Kurumsal SSL VPN Erişim Talep Formunu imzalamalıdır.
5. SSL VPN gerçekleştirecek kullanıcılar(kurum personeli) mutlaka Personel SSL VPN Erişim Talep Formunu imzalamalıdır.
6. Kullanıcılara Sunucu yönetimi için sadece ihtiyaç duyulan portlara erişim yetkisi verilmelidir. Yetkili kullanıcıların erişimi için TELNET yerine SSH ve RDP gibi şifreli protokoller kullanılmalıdır.
7. Kullanıcılara sadece yetkisi olduğu sunucularda erişim yetkisi verilmelidir.
8. Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.
9. Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir.
10. Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, sshkey) ile yapılmalıdır.
11. Kullanıcıların sunucu yönetim için sağlanan erişimde kısıtlı erişim yetkileri tanımlanmalıdır.
12. Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir.
13. Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, Bilgi İşlem Birimine teslim edilmelidir. Bilgi İşlem Birimi nezaretinde ve tarafından yürütülmelidir.
14. Kurumun yedekleme sistemlerine sadece kurum personeli erişim yapmalıdır. Firmaların yapacakları tüm işlemler Bilgi İşlem Birimi nezaretinde yürütülmelidir.
15. Ağ cihazlarının şifreleri default şifrelerde bırakılmamalı ve kompleks şifreler (parola güvenliği ilkelerine uygun olarak) kullanılmalıdır.
16. Kullanıcı bilgisayarlarına uzak bağlantıda kullanılan uygulamalarda (Netsupport, anydesk, radmin vb. programlarda) Bağlantı sağlanacak kullanıcının onayı ile bağlantı sağlanmalıdır. Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.
17. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeler yapılmış olmalıdır.
18. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

**6.1.6. Kablosuz erişim:**

Hastanenin bazı bölüm ve birimlerinde mevcuttur. Hastane bölümlerinde çalışan tüm personelin otomasyon sistemine girdiği, kullanıcı adı ve parolası şifreli bir 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, kimseye gösterilemez. 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 hastane internet ağına bağlı olan tüm bilgisayarların hangi zamanda, hangi internet sitesine bağlandığını, ne kadar süreyle o sayfada kaldığı gibi tüm bilgiler Çorum İl Sağlık Müdürlüğü bünyesinde bulunan güvenlik duvarında yedeklenip log cihazında log’ları kayıt altına alınmalıdır. Oluşabilecek virüs saldırıları için Çorum İl Sağlık Müdürlüğü bünyesinde bulunan merkezi anti virüs lisansı ile bilginin güvenliği sağlanmalıdır. Fiziksel güvenlik duvarı ve anti virüsün güncellemelerini ve üst versiyon yüklenmelerini Çorum İl Sağlık Müdürlüğü bünyesinde bulunan yönetim konsolu üzerinden takip edilip yapılmaktadır.

**6.2. BYS' ni Oluşturan Alt Sistemler (SBYS, LBYS, PACS, Web, E-Posta, Dosya Sunucu, Varsa Diğer Bilgi Yönetim Alt Sistemler)**

**SBYS:** HBYS içerisinde laboratuvar, radyoloji gibi tetkik birimlerinde gerçekleştirilen tüm operasyonlardan, ameliyathane, hastane eczanesi, sicil veya insan kaynakları birimlerine varıncaya kadar farklı uzmanlıklar üzerine çalışan birçok yazılımın bir araya gelerek oluşturduğu yazılım grubu demektir. Hastanemizde web tabanlı BYS sistemi kullanılmaktadır. Web tabanı sunucuları Erol Olçok Eğitim Araştırma Hastanesinde bulunmaktadır.

**LBYS:** LBYS hastanenin BYS sistemi içerisinde bulunmaktadır. Ayrı bir LBYS sistemi hizmeti alınmamış olup BYS sistemine entegre olarak kullanılmaktadır.

**PACS:** Hastane bilgi yönetim sistemlerinde gerçekleştirilen tetkik operasyonlarında cerrahi operasyonlarda izleme dinleme operasyonlarında kullanılan tıbbi cihazlar ile bütünleşik olarak yani tıbbi standart dil formatında da haberleşerek bilgi alışverişinde bulunabilir. Örneğin PACS yapılarında mamografi, DI, MR, tomografi gibi cihazlardan görüntü alıp bunları birlikte çalıştığı diğer programlara verebilmelidir. Hastanemizde BYS’ye entegre olarak çalışan PACS sistemi kullanılmaktadır. Veri tabanları hastanemizde saklanmaktadır.

**Web:** Hastanemizde web tabanlı olarak BYS sistemi kullanılmaktadır. Web tabanı sunucuları Erol Olçok Eğitim Araştırma Hastanesinde bulunmaktadır.

**E-Posta:** Hastanemizde saglik.gov.tr uzantılı e posta adresleri kullanılmaktadır. E postalar kişiye özgü ve hastanenin kurumsal e postası olarak iki gruptadır. Hastane e posta kullanım yetkisi hastane yönetimi tarafından belirlenerek kullanıcıya açılmaktadır.

**Dosya Sunucu:** Hastanemizde BYS sistemine entegre olan dosya sunucu sistemi kullanılmakta. Dosya sunucu sisteminden hastanemizde kullanılmakta olan dokümanlar kalite birimi tarafından paylaşılmakta ve kullanıma sunulmaktadır.

**Diğer Bilgi Yönetim Alt Sistemler:**

**EBYS:** Hastanemizde EBYS sistem yetkiler hastane yönetiminin belirlediği kişilere kişiye özgü kullanım olarak verilmektedir.

**6.3. SBYS İŞLETİMİ VE DEĞİŞİKLİK YÖNETİM SÜRECİ:**

**6.3.1.Yazımsal Süreçler:**

Bilgi işlem personeli yaptıkları işle ilgili düzeltme, güncelleme, değişiklik gibi işlemleri hastane çalışanlarına 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.

|  |
| --- |
| **Arıza Tipi, Arıza Müdahale ve Arıza Giderme Süreleri** |
| **Arıza Tipi** | **Müdahale Süresi****(Saat)** | **Arıza Giderme Süresi** **(Saat)** |
| Seviye I | 2 | 4 |
| Seviye II | 4 | 8 |
| Seviye III | 8 | 16 |

**6.3.2.Sorunların Çözümü**

Hastane çalışanları HBYS üzerinden Arıza Bildirim Talep Modülü ile bilgi işlem servisi çalışanlarıyla irtibat kurulur.

Bilgi işlem personeli arasında iş bölümü oluşturuldu. Donanım, yazılım ve teknik arıza 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 ve işlem kapatılır.

**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.

**Yönetime Açık Hastane Bilgi Sistemi İşlemleri:**

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

**6.4.BİLGİ SİSTEM DONANIM VE ALT YAPISINA, YÖNETİM VE TALEP SÜREÇLER:**

**6.4.1. Network Donanım Cihazlarının;**

Ana omurgayı (Merkez Switch) taşıyan cihazın, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar. Ağ cihaz ve yazılımlarını kurar, internet ve intranet (iç ağ) 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 (metro internet – Çorum İl Sağlık Müdürlüğü) ve kablosuz iletişim cihazlarının (wireless cihazlar – hastane kendi bünyesinde) 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 anti virus 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.

**6.4.2. 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.

**6.4.3.İşletim Sistemlerinin;**

Yazılım güncelleştirmelerini, yamalarını, 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) çalışırlılığını izler ve kontrol ederler.

**6.4.4.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.

**6.4.5.Yazılım Geliştirme**

Kurumsal kullanıcılardan gelen hastane hizmetlerine yönelik yazılım taleplerini değerlendirmek Bilgi işlem birimince hazırlanan ve onaylanan yazılım talepleri ile analiz çalışmalarını yapmak. Programın çalışması için gerekli kaynakları belirlemek ve sistem yönetimine Hastane Müdürünün onayı sonrasında bildirmek Yazılım geliştirme platformu ve temel yazılım geliştirme mimarisi belirlenir.

**6.4.6.Web Uygulamaları ve Web Tasarım Çalışmaları**

Web uygulamaları bakanlığımız tarafından geliştirilen web sayfa ara yüzleri kullanılarak yapılmaktadır. 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 içerikleri geliştirmek ve yönetmek (istek, şikâyet, bilgi edinme, hizmetlerimiz vb.)

**6.4.7.Sistem Operatörleri**

Hastane uygulamalarının çalışırlılığını izler, performanslarını varsa loglarını izler. 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.

**6.5 VARLIK YÖNETİMİ**

Varlık, “kuruluş için değeri olan herhangi bir şey” , olarak tanımlanıyor. Türlerine göre varlıları incelediğimizde altı temel tür varlık karşımıza çıkıyor. En yaygın tür “bilgi varlığı”dır. Bilgi varlığı, bulunduğu biçim ve cinsinden bağımsız olarak, kurumsal bilgilerdir. Hasta bilgileri ister bir veri tabanında dursun ister taşınabilir bilgisayarın içindeki bir dosyada ya da basılı bir kâğıtta basılı halde olsun, kurum için aynı öneme sahip varlıklardır. Kullanım kılavuzları, iş sürekliliği planları, denetim kayıtları, arşivlenmiş kayıtlar yine bilgi varlığı örneği olarak değerlendirilebilir.

Yazılım varlıkları ikinci sırada yer alır. Uygulama yazılımları, işletim sistemleri ve uygulama geliştirme araçları bu

grupta karşımıza çıkacak örnekler arasındadır.
Fiziksel varlıklar aslında hem anlaması, hem de sıralaması en kolay gruptur.
Bilgisayarlar, iletişim cihazları, taşınabilir veri saklama ortamları başta olmak üzere kurumsal bir envanterde yer alabilecek, elle tutulabilen tüm varlıklar fiziksel varlık sayılabilir. Servisler başlığı ile özetlenebilecek varlık türüne, teknik detayı ile ilgilenmeden sadece bir hizmet olarak aldığımız ve kullandığımız varlıklar girebilir. En temel servisler arasında ısıtma, havalandırma, aydınlatma, güç (elektrik) hizmetleri dışında veri ve ses iletişimini sayabiliriz.

Kapsam içindeki tüm önemli varlıkların listelenmesi hem standardın bir gereksinimi, hem de bilgi güvenliğinin sağlıklı yönetimi için önemli bir şarttır. Varlıkların eksiksiz listelenmesi ancak kapsam içindeki süreçlerin detaylı analizi ile mümkün olur. Hastanemizde tüm BYS sistem ve malzemeleri BİLGİSAYAR DONANIM VE YAZILIM ENVANTERİ ile kayıt altına alınmaktadır.

Burada “sahip”lik ilgili varlığın parasını ödeyen anlamında değil, güvenlik ihtiyaçlarını belirleyen kişi olarak tanımlanır. Varlığın sahibi gizlilik, bütünlük ve kullanılabilirlik açısından varlığı doğru şekilde sınıflamalı, varlığa kimlerin hangi haklarla erişmesi gerektiğini tanımlamalı ve tüm bunları düzenli olarak gözden geçirmelidir. Özel durumlar ve istisnalar olmakla birlikte bir varlığın sahibi genellikle ilgili iş sürecinin de sahibidir.

Her kurum kendi kullanımı için kendi sınıflarını belirleyebilir. Sık kullanılan yöntemlerden biri dört seviyeli sınıflamadır. Bu sınıflamada sırasıyla genel kullanıma açık, dâhili kullanım, gizli ve sır sınıfları yer alır. Halka açık varlıklar Hastane web sitesidir. Bu varlık tüm kişilerin kullanımına açık olup kişiler istediği yerden ulaşabilmektedirler.

Dâhili kullanım varlıklar, eksiksiz tüm hastane çalışanları tarafından kullanılan ancak dışarıya açık olmayan varlıklardır. Bu da hastane yönetimi tarafından verilmiş yetki dahilinde kullanılan BYS sistemi intranet olarak tanımlanmaktadır.

Gizli varlıklar kurum içindeki bir ya da iki bölüm tarafından bilinen, tüm çalışanlarla bile paylaşılmayan gizlilik derecesi yüksek varlıklardır. Bunlar BYS de bulunan hasta kayıt sistemi poliklinik defteri e nabız ulaşımı gibi birkaç kişinin kullanımına açılmış varlıklardır.

En üst seviyedeki gizlilik ihtiyacı Sır niteliğindeki varlıklardadır. Bunlar BYS veri tabanı gibi varlıklardır.

**6.6. İŞ SÜREKLİLİĞİ YÖNETİMİ:**

**6.6.1.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.

**6.6.2. Otomasyon Bilgi İşlem Çalışanlarının Yetkilendirme İşlemleri:** Aşağıda belirtilen işlemler doğrultusundaBİMOB çalışanları yetkilendirmektedir.

• Yazılım kurma ve silme işlemleri

• Bilgi Sistemleri Yöneticisine açık otomasyon sistemi işlemleri

• Yönetime açık otomasyon sistemi işlemleri

**6.6.3.Yazılım Kurma ve Silme İşlemleri:** Hastanemizbünyesinde kullanılma kararı alınmış otomasyonsistemi dâhilindeki 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.

**6.6.4. Otomasyon sistemi işlemleri:** Hastane bilgi yönetim sistemi işlemleri, BİMOB’ in onayladığı şartlar kapsamındasaptanan çalışanın yetkisinde olacaktır. Verilen standart yetkiler dışında istenilen bir yetki, bağlı bulunduğu yöneticinin onayından sonra, uygun görüldüğü seviyede BİMOB tarafından verilir.

**6.7. YEDEKLEME**

HBYS yedekleme işlemleri ***“VERİ YEDEKLEME PROSEDÜRÜ”*** ne göre yapılır.

**6.8 BİLGİ TEKNOLOJİLERİ İMHA YÖNETİMİ:**

1. Evraklar idari ve hukuki hükümlere göre belirlenmiş Sağlık Bakanlığı Arşiv Mevzuatına göre uygun olarak muhafaza edilmesi gerekmektedir.
2. 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.
3. Özel ve Çok Gizli evraklar bulunan birimlere evrak imha makinası (kâğıt, cd, dvd, proximity card imha edebilecek nitelikte) temin edilmelidir.
4. Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmî Gazete ’de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış Çevre ve Şehircilik Bakanlığından “ATIK YÖNETİMİ YÖNETMELİĞİ” ve “Basel Sözleşmesine” göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.
5. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek alan belirlenmelidir.
6. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
7. Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
8. 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.
9. Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.

**6.9.BİLGİ YÖNETİMİNE İLİŞKİN FAALİYETLERİN YÜRÜTÜLMESİ VE KOORDİNASYONUNA YÖNELİK SORUMLULAR VE SORUMLULUKLAR**

**1)Hastane Bilgi Yönetimi Sistemini kullanan tüm çalışanlar**: HBYS sistemini kullanan tüm çalışanlar hastanedekimevcut tüm bilgisayarlardan kendilerine verilmiş ve görevleri ile yetkilendirilmiş kullanıcı adı 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.

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 kontrolleri)

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.

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 şartnameleri hazırlamak ve 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 verip sorunun giderilmesi için gerekli tedbirleri almak. Konusuyla ilgili olarak amiri tarafından verilen diğer işleri yerine getirmek.

**6.10.BİLGİ YÖNETİM SİSTEMİNE İLİŞKİN ROL GRUPLARI VE YETKİLERİ:**

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

**Bu rol** **grupları;**

* Doktor
* Servis-Birim Sorumlusu
* Laboratuvar Çalışanları
* Radyoloji Çalışanları
* Acil Hemşiresi
* Acil Tıp Teknisyeni
* Acil Sekreteri
* Bilgi İşlem Çalışanları
* Klinik Hemşiresi
* Klinik sekreteri
* Poliklinik sekreteri
* Satın alma
* Kalite
* Teknik Servis
* Eğitim
* Enfeksiyon
* Personel
* Faturalama vb.

 Çalışanların yetkileri düzenlenmiştir ve kayıt altına alınmaktadır. Aynı görevde çalışan personellerin yetkileri de aynıdır. İşe yeni başlayan personel bilgi işlemden “***PERSONEL BİLGİSAYAR KULLANICI TALEP/DEĞİŞİM FORMU”*** doldurarak kullanıcı adı ve şifresi verilir. İşten ayrılırken ise ilişik kesmek için bilgi işleme başvurarak ilişik kesilir.

**6.10.1.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.

**İdari ve Mali İşler Müdürü:** İdari ve mali işlemlerle ilgili tüm bilgilere erişebilir.

**Sağlık Bakım Hizmetleri Müdürü:** Hasta bakım işlemleriyle ilgili bilgilere erişebilir.

**Hemşire**: Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Silme ve değiştirme yetkileri yoktur. Kendi işlerine aitlaboratuvar 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 sorumlularınabildirirler. 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 işleyişiniotomasyon 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 ilaçlarınkarşılamasını yapar. Hastaların reçeteleri doğrultusunda ilaçların takibini sağlar.

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

**Laboratuvar:** Doktorların hastaları için, yaptığı istemleri alır, çalışmasını yapar ve otomasyon üzerinde hastanın sonuçlarınıgirer. Otomatik cihazlar için bu işlemler barkotlu sistem ile çalışır. Hasta test sonuçları Laboratuvar 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.

**6.11. HATA BİLDİRİMİ**

**6.11.1 Bilgisayar Arızaları**

Kurumumuzda bilgi işleme yönelik arıza bildirimleri Bilgisayar Arıza Bildirimi otomasyon üzerindeki modül bölümünden yapılmakta ve kayıt altına alınmaktadır. Arızlar bilgi işleme bu yoldan iletilir. Bilgi işlem personeli arızayı değerlendirir. Sistem üzerinden sonuçlar kayıt edilir. Kurum içinde halledilebilecek bir sorunsa sorun giderilir. Halledilemeyecek bir sorun ise ve parça değişimi gerekliyse satın alma süreci başlatılır.

**6.11.2 HBYS Arızası**

HBYS arızalarında günün her saatinde bilgi işlem görevlisine bildirim yapılabilir. Bildirim yapılacak kişinin iletişim adresi hastanenin tüm birimlerinde bulunmaktadır. Sorun ilgili şartname hükümlerinde belirtilen süreler içinde giderilir. Sorunun belirtilen sürelerde giderilemediği durumlarda ilgili firmaya cezai hükümler uygulanır.