1. Amaç

İÜ Onkoloji Enstitüsü'ne başvuran kişilerin kişisel sağlık bilgileri gizli ve özeldir. Kurumumuz bu bilgilerin gizlilik ve güvenliğini korumakla yükümlüdür.

Bu prosedürün amacı, Enstitümüz bünyesinde oluşturulan her türlü verilerinin kaydedilmesi, saklanması ve kullanılmasına ilişkin kuralları, uygulamaları ve güvenlik önlemlerini belirleyerek; Kurumumuza ve Kurumumuza başvuran hastalara ait tüm bilgilerin mahremiyetini sağlamaktır.

2. Kapsam

Bu prosedür, Kurumumuzda elektronik ve/ya da basılı ortamda üretilen ve saklanan tüm bilgilere ilişkin düzenlemeleri, ISO15189 standardı bilgi sistem güvenliği işleyişi dahilinde tüm İÜ. Onkoloji Enstitüsü çalışanlarını ve İÜ. Onkoloji Enstitüsüne hizmet sağlayan üçüncü taraf kullanıcılarını kapsar.

3. Sorumlular

İÜ. Bilgi İşlem Daire Başkanlığı, İÜ. İstanbul Tıp Fakültesi Bilgi İşlem Yöneticisi, İÜ. İstanbul Tıp Fakültesi Sistem Yönetim Sorumlusu, İÜ. Onkoloji Enstitüsü Müdürü, İÜ. Onkoloji Enstitüsü Başhekimi, İÜ. Onkoloji Enstitüsü Bilgi İşlem Süreç Yöneticisi, İÜ. Onkoloji Enstitüsü Bilgi İşlem Otomasyon Destek Sorumlusu, İÜ. Onkoloji Enstitüsü Bilgi İşlem Donanım Destek Sorumlusu sorumudur.

4. Tanımlamalar

HBYS: Hastane Bilgi Yönetim Sistemi

İÜ: İstanbul Üniversitesi Rektörlüğü

İTF: İÜ. İstanbul Tıp Fakültesi

OE: İÜ. Onkoloji Ensititüsü

Bigi Güvenliği: Bilginin, bir varlık olarak hasarlardan korunması

Veri: Bilgisayar ortamına taşınmış, işlenebilir her türlü bilgi parçası.

Veri Tabanı: Bilgisayar kullanımında çözüme erişmek için işlenebilir duruma getirilmiş verilerin toplamı

Sunucu: Veri tabanını içeren fiziksel bilgisayar ortamı.

Yedekleme: Sunucu üzerinde bulunan kritik öneme sahip dosyaların birer kopyalarının alınarak saklanması işlemi

Yedekleme Ortamı: Yedekleme işlemi esnasında kullanılan fiziksel kayıt ortamları (Harici depolama, USB flash, CD veya DVD).

Firewall: Birçok farklı filtreleme özelliği ile bilgisayar ve ağın gelen ve giden paketler olmak üzere internet trafiğini kontrol altında tutar.

Web Sitesi Sonuç Bildirim Ortamı: İÜ. Onkoloji Enstitüsü web sitesinden onayları verilmiş ve kesinliğe kavuşmuş olan hasta sonuçlarının görüntülenebilmesi.

Donanım (*Hardware*): Bilgisayarın fiziksel kısımlarına verilen genel ad.

Yazılım (*Software*): Bilgisayar sistemi içinde donanımı kullanmak için gerekli programlar.

Kimlik Tanımlama (*Identification*): Kullanıcının kimliğini bilgi sistemine beyan etmesidir.

Yetkilendirme (A*uthorization*): Kullanıcıların hangi yetkilere sahip olduğunun, hangi bilgi varlıklarına hangi yetkilerle erişeceğinin belirlenmesidir.

Grup Politikaları (*Group Policy*): Network güvenliğini sağlamak amacıyla network ortamındaki kullanıcıların bilgisayarlarına bazı kurallar oluşturmak.

Modül: HBYS programının ana parçaları. (Hasta İşlemleri, Yönetim, Sistem, Muhasebe modülleri)

5. Uygulamalar

5.1. Genel İlkeler

5.1.1. OE'de bilgi güvenliği ile ilgili tüm işlemlerde 24/3/2016 tarih ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu temel alınır.

5.1.2. OE; gerek veri ve bilgilerin iletimi, paylaşımı, işlenmesi, yönetimi ve saklanması için, TC akademik ve yönetsel, gerekse hizmet sunum alanlarında kullanılabilecek yasalarına ve OE misyonuna uygun; vizyonunu destekleyen sistematik bir yaklaşımla bilgi yönetim sistemini planlar, uygular, uygulama sonuçlarını kontrol edip irdeler ve kontrol sonuçlarının gerektirdiği önlemleri alır. Kurumumuz, tüm çalışanlarına ve hizmet sunduğu topluma güvenilir, ulaşılabilir, izlenebilir, sürdürülebilir, sağlıklı bilgi yönetim sistemlerini sunar ve bu sistemleri güncel koşullar ve kurumun gereklilikleri doğrultusunda sürekli geliştirip iyileştirir.

5.1.3. OE bilgiyi yönetirken; tüm kullanıcılarına (rolleri ve yetkileri doğrultusunda) adil davranır; kullanıcıların ihtiyaç duydukları bilgiye (yine rolleri ve yetkileri doğrultusunda) erişebilmelerini sağlar, bilginin kontrolsüz paylaşımını önler; etik değerleri, kullanıcı mahremiyetini ve haklarını korur, kullanıcı kolaylığını gözetir, bilginin bütünlüğünü sağlar ve bilgi güvenliğini tehdit edebilecek olası her türlü riske ve tehlikeye karşı gerekli önlemleri alır.

5.1.4. Bilgi yönetiminde kullanılan altyapı; gerektiğinde yedeklemeyi ve yedeklenen verilere yeniden ulaşabilmeyi, özellikle kritik verilerde verilerin kim tarafından ne zaman girildiğini (ya da değiştirildiğini) belgelemeyi mümkün kılar.

5.1.5. Bilgi güvenliği uygulamaları ile; OE'nin idari, mali, akademik, yönetsel ve fonksiyonel verileri ile hasta bilgilerinin güvenliği sağlanır. Kesintisiz veri/bilgi akışı mümkün kılınarak OE'nin temel ve destekleyici fonksiyonlarında süreklilik sağlanır. OE'nin akademik ve bilimsel kimliği, prestiji korunur. Bilginin etkin ve verimli yönetilmesini sağlanır.

5.1.6. Bilgi güvenliği aşağıdaki ilkeler doğrultusunda ele alınır:

Gizlilik (Confidentiality): Bilginin yetkisiz kişilerin erişimine kapalı olması.

Bütünlük (Data Integrity): Bilginin kazara ya da kasıtlı olarak bozulmasının önlenmesi, içeriğinin korunması; bilginin her şeyden önce doğru ve kesin oluşu, şüphe uyandırmayan bir durumda oluşu.

Süreklilik-Kullanılabilirlik (Availability): Bilginin her ihtiyaç duyulduğunda kullanımına hazır durumda olması.

İzlenebilirlik ya da Kayıt Tutma (Accountability): Bilgi Yönetim Sisteminde gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almak.

Kimlik Sınaması (Authentication): Kullanıcının iddia ettiği kişi olduğundan emin olunmasıdır.

5.2. Bilgi ve İletişim Güvenliği, Gizliliği

5.2.1. Bilginin Mülkiyeti:

5.2.1.1. OE'ye ait özel sırlar, mali bilgiler, sistem bilgileri gibi kurumsal bilgilerin gizliliği esastır ve kurumun mülkiyeti altındadır.

5.2.1.2. "6698 Sayılı Kişisel Verilerin Korunması Kanunu" ve "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik" uyarınca tıbbi kayıtlar dahil hasta bilgilerinin, öğrenci bilgilerinin, çalışan bilgilerinin gizliliği esastır ve kurumun güvencesi altındadır.

5.2.1.3. OE'de çalışılan süre içinde veya daha sonrasında bu bilgilerin kurumdaki görevin gerektirdiği durumlar haricinde kullanılması kesinlikle yasaktır.

5.2.1.4. Kurumumuzda herhangi bir kullanıcının burada tanımlanan yöntemlere, uygulamalara uymadığı/ihlal ettiği durumlarda o kullanıcıya, mevcut kanun ve yönetmelikler çerçevesinde İÜ disiplin politikaları doğrultusunda; oluşan zararın/gerçekleşen ihlalin büyüklüğüne/kritikliğine göre uygun yaptırım uygulanır. OE, gerekli yaptırımın icrası konusunda tavizsiz davranır.

5.2.1.5. Tüm kullanıcılar bilgi güvenliği ve HBYS kullanım ilkeleri, bu ilkelerin ihlali durumunda doğacak yasal yükümlülükler ve sistemin yapısı içinde kendilerinden beklenen işlevler ile ilgili eğitilirler.

5.2.1.6. Tüm çalışanlarımızın hasta bilgilerini gizli tutma yükümlülükleri vardır. Güvenlik ihlali
durumunda gerekli yasal işlemler başlatılır.

5.2.1.7. OE Personeli kurum ve hasta bilgilerini hastane içindeki ortak alanlarda (asansör, koridor, yemekhane, ve benzeri mekanlarda) konuşmaz, paylaşmazlar.

5.2.2. Erişim Kontrolü

5.2.2.1. Kimlik Tanımlama ve Şifreleme Politikası

5.2.2.1.1. Kullanıcılar sadece kendilerine ait özel kullanıcı adı ile Bilgi İşlem Birimi tarafından sisteme tanımlanırlar. Her kullanıcının kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabının olduğu sadece bir adet kullanıcı adı bulunmaktadır. Özel görevlendirmeler haricinde kullanıcılara bir den fazla kullanıcı adı tanımlanmaz.

5.2.2.1.2. HBYS kullanıcılarının kullanıcı hesapları açılır ve geçici şifre verilir. Kullanıcılar kendi şifrelerini oluşturur.

5.2.2.1.3. Şifre verilen her çalışandan "Bilişim Sistemleri Kullanım Taahhütnamesi Formu" ıslak imzalı olarak alınır ve insan kaynaklarına teslim edilir.

5.2.2.1.4. Belli bir kullanıcıya ayrılmış şifre hangi şartla olursa olsun başkalarına verilemez.

5.2.2.1.5. Kullanıcılar kendilerine ait olan kullanıcı kimliklerinin ve şifrelerinin korumaları konusunda sorumludur. Kullanıcıların kullanıcı hesaplarını ve parolalarını başkalarıyla paylaşmaması, aksi takdirde kullanıcı hesabıyla yapılan tüm işlemlerden kullanıcı hesap sahibinin sorumlu tutulur. Başkasına ait kimlikle veya şifreyle işlem yapmak kesinlikle yasaktır.

5.2.2.1.6. Çalışanların işten ayrılması durumunda tüm şifreleri ve kullanıcı yetkileri, İnsan Kaynakları Birimi tarafından Bilgi İşlem Birimi'ne haber verilerek kullanıma kapatılır.

5.2.2.1.7. Kurumda görev değiştiren kullanıcının iş gereksinimi varsa söz konusu gereksinime göre erişim haklarının yeniden düzenlenir.

5.2.2.1.8. Şifre güvenliği açısından şifrelerin belirli aralıklarla değiştirilmesi (en geç 60 gün) önerilir.

5.2.2.1.9. Kullanıcı şifreleri rakam, büyük harf, küçük harf ve özel karekter uyumunu birlikte sağlayan en az sekiz haneli parametre içermektedir.

5.2.2.2. Yetkilendirme

5.2.2.2.1. Erişim kontrol politikası kullanıcılara erişim izinlerinin uygun şekilde verilmesini sağlamaktadır. Kurum için kritik derecede hassas bilgi varlıklarına erişim uygun bir şekilde kısıtlanmaktadır.

5.2.2.2.2. HBYS programlarına kullanıcı adı ve şifre ile giriş yapılır.

5.2.2.2.3. Özel olarak yetkilendirme yapılmadığı sürece tüm bilgi varlıklarına erişimin yasaktır.

5.2.2.2.4. Kullanıcılara sadece iş sorumluluklarını veya iş gereksinimlerini yerine getirmelerine yetecek kadar izin verilir.

5.2.2.2.5. Her kullanıcı için yapacağı işlere göre profil ayarlaması yapılır; verilen yetkilere göre kullanıcıların gördüğü ekranlar değişmektedir. Her kademedeki personel; ancak yetkilendirilmiş olduğu işlemleri, kurum prosedürlerine uygun olarak uygular.

5.2.2.2.6. Aynı görevi icra eden çalışanlar aynı yetki gurubuna sahiptirler.

5.2.2.2.7. Yetkilendirilmemiş kişiler tarafından yapılan herhangi bir işlemi saptayan birim sorumluları, bu durumu yeterli delillerle birlikte en kısa zamanda üst yönetime bildirir.

5.2.2.2.8. Herhangi bir şekilde fazla yetkiye sahip kullanıcıların bu yetkiyi kullanarak iş sorumluluklarının veya iş gereksinimlerinin dışında bilgiye ulaşmanı engellenir.

5.2.2.2.9. Fazla/gereksiz yetkinin anlaşılması durumunda yetkilendirmeden sorumlu kişilere ve Enstitü Müdürü'ne haber verilir.

5.2.2.2.10. Dosya, dizin ve diğer objelere erişim izinlerinin gruplara verilmesi, gerekmediği sürüce kişilere özel izin verilmesinden kaçınılır.

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

5.2.2.2.12. Yetkilerin kötüye kullanılması halinde ağır sorumluluklar doğuracağı oryantasyon eğitimi kapsamında çalışanlara anlatılır.

5.2.2.2.13. Tıbbi kayıtlarda yetkilendirme:

- **Doktor:** Görevli ait olduğu anabilim dalından sağlık hizmeti alan hastalara tıbbi öykü ve tedavi bilgilerinin tümüne erişebilir. Tetkik sonuçlarını görebilir. Elektronik ortama kaydedilmesi gereken, hastaya ait tüm bilgileri girebilir. Yatan hastaların taburculuğundan önce epikrize ekleme yapabilir. Kendi hastalarının epikriz ve ameliyat raporunda değişiklik yapabilir. Onay işlemlerini kendi şifresi ile yapmakla yükümlüdür. Onaylamadan önce kendisine ait raporlar üzerinde silme ve değişiklik yapabilir. Tetkik birimlerinde görevli hekimler, tetkik için kendilerine başvuran hastaların önceden yapılmış işlemlerini görür, işlem detaylarını göremez. Kendileri ile ilgili tetkik raporlarını sisteme girer ve onaylar.

- **Hemşire:** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Kendi yetkileri altında tanımlanmış olan hasta işlemlerini, hastaya ait sarf ve işlem girişlerini yapabilir ve değiştirebilir. İlaç-malzeme çıkışı yapabilir. Hekim orderlarının uygunluğunu kontrol edebilir, hemşirelik uygulamalarını, hastanın vital bulgularını sisteme girebilir.

- **Veri Giriş Personeli:** Hastayla ilgili yapılmış işlemleri sisteme ekler. Hasta yatış - çıkış işlemleri için gerekli evrakları düzenler. Hastanın tanılarını, yapılan tıbbi işlemleri ve tetkikleri dokümante eder. Hatalı yapılan işlemleri Bilgi İşlem Birimine bildirir.

- **Faturalama Birimi:** Hastaların faturalamasını ve anlaşmalı kurumlara gönderimini yapar.

- **Başeczacı ve Eczacı:** Eczane ile ilgili tüm yetkilere sahiptir. Kalfadan farklı olarak, kurumdaki tüm ara depoların stoklarını görür, fatura girdilerini kontrol edebilir.

- **Eczacı Kalfası:** İlaç çıkış, stok sayımı yapar, iade alır, eczane içi stok hareketlerini görür. Birimlerden gelen eczaneyle ilgili talepleri karşılar, iadeleri alır. İlaç ve tıbbi malzeme ile ilgili işlemleri yapar. Stok takibi yapar.

- **Laboratuvarlar/tetkik birimleri teknisyenleri:** Numune kabulünü yapar, çalışılmak üzere ilgili cihazlara gönderir, çalışılan testlerin teknisyen onayını yapar.

- **Vezne:** Hasta protokolünü sisteme girer, borç tahsil eder. Hasta dışında gelişen nakit giriş ve çıkışlarını HBYS sistemine kayıt eder.

- **Gelir İdaresi:** Dekont eşleme ve alacak takibi yapar. Vezne tahsilatlarını sorgular.

- **İstatistik Bürosu:** Girilmiş işlem, tetkik sayılarını çekebilir.

- **Ameliyathane Ekran Yetki Grubu:** Ameliyat rapor ve hasta dosya, ilaç ve

malzeme kontrolü yapar.

5.2.2.3. Fiziksel Erişim

5.2.2.3.1. Kritik varlıkların bulunduğu fiziksel ortamlara giriş kapıları kilitli tutulmaktadır.

5.2.2.3.2. Bilgi sistem aygıtları ve bilgi içeren her türlü ekipmanlara fiziksel erişimin kullanıcısı başında bulunmadığı zaman zarfında kontrol altındadır.

5.2.2.3.3. Sistem odasına girmeye yetkili olmayan ama bakım/onarım, danışmanlık vb. gibi amaçlarla sistem odasında çalışma ihtiyacı olan kişilerin, İTF Sistem Yönetim Birimi veya yetki verdiği ilgili personel nezaretinde çalışılır.

5.2.2.3.4. Manuel tutulan hasta kayıt ve bilgilerinin saklandığı arşivin fiziksel erişim koşulları "Arşiv İşleyiş Prosedürü" ne göre izlenir.

5.2.2.4. Ağ ve Network Cihazlarına Erişim

5.2.2.4.1. Kurumumuzda bilgiye erişimlerin büyük kısmı bilgisayar ağları üzerinden gerçekleşmektedir. Kullanıcılar istemciler vasıtasıyla ağ üzerinden, sunucular üzerindeki bilgilere erişerek işlerini yerine getirmektedirler. Bu erişimler yerel ağlar üzerinden olabildiği gibi internet benzeri geniş ağlar üzerinden de olabilmektedir. Ağ erişim kontrolünde temel amaç ağ üzerinden ulaşılabilecek bilgilere yetkisiz erişimleri engellemektir. Yetkisiz erişimleri engellemek için uygun kimlik doğrulama mekanizmaları uygulanır. Bu yöntemde; İTF Sistem Yönetim Birimi tarafından active directory **(Domain)** alanındaki ağa bağlı bilgisayarların yerel güvenlik duvarları aktif hale getirilerek sadece kendi aralarında veri alışverişi yapmaları sağlanır.

5.2.2.4.2. Kullanıcıların internet üzerindeki erişebileceği servislerin tanımlanır (http, https ve smtp gibi) ve söz konusu servisler dışındaki başka servislere erişim talepleri İTF Sistem Yönetim Birimi tarafından değerlendirilir ve onaylanır.

5.2.2.4.3. Kurum dışından kurumun bilgi ağı servislerine yapılacak bağlantıların yetkisiz erişimlere izin vermeyecek şekilde denetlenir ve kontrol altına alınır.

5.2.2.4.4. Kurum içinde gizlilik seviyelerine uygun bilgi ağlarının kurulması ve kritik bilgi içeren ağların uygun kontrollerle (kimlik doğrulama, yetkilendirme, sınır koruma vb.) korunur.

5.2.2.5. Üçüncü Taraf Erişimleri

5.2.2.5.1. OE HBYS sistemine yalnızca anlaşmalı kurumlar erişebilmektedir.

5.2.2.5.2. HBYS yazılımına erişim VPN programları (Teamwiever vb.) üzerinden veya kurumdaki HBYS sistemiyle entegrasyon yapılmış "Web Service" üzerinden gerçekleşmektedir.

5.2.2.5.3. Bilgi sistemlerine dış erişim yetkisi verilecek kurum ve kuruluşlara, erişim ve gizlilik şartlarının belirtildiği İTF Sistem Yönetim Birimi tarafından Bilgi Sistemleri Uzaktan Erişim Gizlilik Sözleşmesi Formu imzalatılır.

5.2.2.5.4. Dış erişim yapacak kurum ve kuruluşa İTF Sistem Yönetim Birimi tarafından güvenlik duvarı üzerinde gerekli izinler verilir.

5.2.2.5.5. Erişim yapacak 3. taraf firma; sözleşmede tanımlanan ilkelere göre erişim yapacağı zaman doğrudan ya da ilgili Birim Sorumluları tarafından İTF Sistem Yönetim Birimi'ne bilgi verilir.

5.2.2.5.6. Erişim süreciyle ilgili detaylı loglar İTF Sistem Yönetim Birimi tarafından sistemde ayrıca tutulmaktadır. Gerektiğinde bu kayıtlara erişilebilir.

5.2.2.6. Sorumluluklar

5.2.2.6.1. Erişim kontrol politikası ile ilgili sorumluluklar belirlenmiştir.

5.2.2.6.2. Erişim kontrol politikasının geliştirilmesinde, gözden geçirilmesinde, uygulanmasında ve güncellenmesinde kurum içinde İTF Sistem Yönetim Birimi yardımcı olacaktır.

5.2.2.6.3. Erişim kontrol politikasının kullanıcılar tarafından bilinmesini ve anlaşılmasını sağlamaktan, diğer tüm politika ve prosedürlerin bu politika ile tutarlı olmasından Kalite Koordinatörlüğü sorumludur.

5.2.2.6.4. Kullanıcıların OE yapısına ve güvenlik ihtiyacına uygun olarak, varlıklara erişim için gerekli yetkilendirme veya yetkilendirme isteğini onaylamak Enstitü Müdürlüğü'nün ve Başhekimliğin sorumluluğundadır.

5.2.2.6.5. Kullanıcılar erişim kontrol politikası ile beraber ilgili politika ve prosedürdeki kuralları bilmekten ve bu kurallara uymaktan sorumludur.

5.2.2.6.6. Kullanıcılar Bilgi varlıklarına erişim hakkı istemek için kurum tarafından onaylanmış süreç ve prosedürleri kullanmaktan sorumludur.

5.2.2.6.7. Kullanıcılar şifre bilgilerini korumaktan sorumludur.

5.2.2.6.8. Kullanıcılar bilgi kendi kullanımlarındayken bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini mevzuat tarafından belirlenen önemlere uygun olarak korumaktan sorumludur.

5.2.2.7. Uygulama ve Ceza

5.2.2.7.1. OE Bilişim Sistemleri Kullanım Taahütnamesi Formu' nda gizlilik şartları net bir şekilde ifade edilmiştir.

5.2.2.7.2. Bu sözleşmedeki kuralları ihlal edenler hakkında disiplin süreci başlatılması veya gerekli yasal işlem başlatılması gibi uygulamalar tatbik edilir.

5.2.3. Veritabanı Yönetimi

5.2.3.1. Veritabanı üzerinde en yüksek yetkiler İÜ. Bilgi İşlem Daire Başkanlığı tarafından belirlenen veritabanı yöneticisinde bulunur.

5.2.3.2. Veritabanına direk bağlantı kuracak ve veritabanı üzerinde işlem yapacak yazılımcıların kullanıcı profilleri veritabanı yöneticisi tarafından belirlenir ve denetlenir.

5.2.3.3. Veritabanı yöneticisi, veritabanı erişim ve işlem loglarını tutmakla yükümlüdür.

5.2.3.4. Veritabanı yöneticisi, verilerin bütünlüğünden ve alınan veritabanı yedeklerinin bütünlüğünden sorumludur.

5.2.3.5. Veritabanı yada veri tablolarına ancak yönetici olarak yetkilendirilmiş kişiler ulaşabilir.

5.2.3.6. Tüm kullanıcıların yaptığı işlemler kayıt altına alınır ve bilgi işlem tarafından izlenir.

5.2.4. İletişim Güvenliği

5.2.4.1. Tüm çalışanlarımızın hasta bilgilerini ve Kurum bilgilerini gizli tutma yükümlülükleri vardır. Güvenlik ihlali durumunda gerekli yasal işlemler başlatılır.

5.2.4.2. OE Personeli, kurum ve hasta bilgilerini hastane içindeki ortak alanlarda (asansör, koridor, yemekhane, ve benzeri mekanlarda) konuşmaz, paylaşmazlar. Aksi durumda gerekli yasal işlemle başlatılır.

5.2.4.3. OE Personeli, kurum ve hasta bilgilerini mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapamazlar. Aksi durumda gerekli yasal işlemle başlatılır.

5.2.4.4. OE Personeli, kurum ve hasta bilgilerini sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapamazlar. Aksi durumda gerekli yasal işlemle başlatılır.

5.2.4.5. OE Personeli, kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapamazlar, kurumsal e-postalarını şahsi amaçlarla kullanmazlar. Aksi durumda gerekli yasal işlemle başlatılır.

5.3. Güvenlik

5.3.1. Donanım Güvenliği

5.3.1.1. Bilgisayar donanımı için gerekli tesisat ve araçların, bilgi sistemlerinin ve üretici firmaların öngördüğü donanımların uygun ve verimli şekilde çalışacağı çevre şartlarına uygun olarak kurulumu sağlanır.

5.3.1.2. Network kablolarının geçmesi için özel hatlar döşenerek bilgisayarların bulunduğu odalara kadar getirilir.

5.3.1.3. Tesis Güvenliği Prosedürüne göre cihazların yangına karşı güvenliği sağlanır.

5.3.1.4. Tüm bilgisayarlar ve elektrik kesintisinden etkilenebilecek cihazlar, kesintisiz güç kaynağına bağlı çalıştırılır. Bu güç kaynağı ani güç dalgalanmalarında cihazların etkilenmemesi amaçlı olup aynı zamanda elektrik kesintisini müteakip 7-10 saniye içerisinde devreye girecek olan jeneratör sistemine bağlıdırlar. Ayrıca cihazların 7 gün 24 saat tam kapasite çalışabilmesi, ani güç değişimlerinden kaynaklanabilecek arızalardan etkilenmemesi ve jeneratörün devreye girme süreci boyunca anında devreye giren UPS mevcuttur. Jeneratörün genel kontrolü her gün Teknik İşler Sorumlusu tarafından kontrol edilip Jeneratör Kontrol Formu'na kaydedilir.

5.3.2.Bilgisayar Güvenliği

5.3.2.1. Bilgisayarlar Bilgisayar Kullanma Talimatı'na göre kullanılır.

5.3.2.2. OE tarafından görevlendirilecek ekip aracılığı ile Bilgi Sistemleri Bakım Formu'na uygun olarak bilgisayarların bakımı yapılır. Kullanıcıların bilgisayarlarındaki uygunsuz programlar ve dokümanlar belirli aralıklarla kontrol edilir ve gerekli görülmesi halinde temizlenir.

5.3.2.3. OE'de bulunan bilgi sistemlerinde zararlı yazılımlardan korunmak için İTF Sistem Yönetim Birimi tarafından domain'e dahil edilmiş bilgisayarlara NOD32 antivirüs yazılımı yüklenir.

5.3.2.4. OE'de bulunan bilgisayarlarda kullanıcı yapılandırması mevcuttur. Domain'e alınmış bilgisayarların kullanıcıları Grup Politikaları doğrultusunda sadece kendilerine

izin verilen işlemleri yapabilirler.

5.3.2.5. Görüntü analiz sistemlerine ve cihazlara bağlı, domain'e alınmış bilgisayarların açılışı mutlaka şifre ile yapılır, yetkisiz kişilerin cihaz bilgisayarlarına erişmesi engellenir.

5.3.2.6. Bilgisayar sistemleri içinde bulunan bilgilerin ve verilerin güvenliği ile ilgili tüm çalışanlara Bilişim Sistemleri Kullanım Taahhütnamesi imzalattırılır.

5.3.3.Ağ Güvenliği

5.3.3.1. İnternet trafiği ağa entegre edilen, İTF Sistem Yönetim Birimi tarafından yönetilen güvenlik duvarı (Firewall) cihazı ve web filtreleme cihazı ile kontrol edilir. Bu cihazlar sayesinde kullanıcıların, istenmeyen ve kuruma zarar getirebilecek web siteleri, internet uygulamaları, sosyal paylaşım siteleri, çevrimiçi görüşme vb. gibi yasaklı içeriğe sahip sitelere girişleri içerik filtreleme uygulanarak engellenecektir. Sadece Enstitü Müdürü onayı ile izin verilen sitelere yetkilendirilmiş bilgisayarlarla giriş yapılabilecektir.

5.3.3.2. Tüm internet trafiği 5651 no'lu **"İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"** gereği Log kayıtları tutulacaktır.

5.3.3.3. İTF Sistem Yönetim Birimi güvenlik duvarı yazılımının lisans güncelliğini takip eder ve lisans yenilemesi gereken durumlarda İTF Başhekimliği'nin onayıyla lisansın geçerliliği için gerekli işlemleri başlatır.

5.3.4. Ziyaretçilerin İnternet Bağlantıları

5.3.4.1. OE gelen ve internete bağlanmak isteyen ziyaretçiler, ziyaretçiler için tanımlanan kablosuz ağ üzerinden internete bağlanabilirler. Ziyaretçinin internete girdiği bilgisayarın, lokal (laboratuvar) ağdaki domain'e dahil edilmiş olan bilgisayarlara erişimleri engellenir.

5.3.5. Virüs ve Saldırılardan Korunma

5.3.5.1. HBYS virüs saldırılarına karşı virüs koruma programları ile korunur.

5.3.5.2. Domainde yer alan bilgisayarlar için otomatik olarak her gün saat 12:00-13:00 arasında işletim sistemi boyutunda güncelleme denetimi ve güncelleme yapılır.

5.3.5.3. Domainde yer alan her bilgisayara otomatik olarak antivirüs yazılımı yüklenir.

5.3.5.4. İlgili yazlım merkezi yönetim arayüzü ile yönetilir ve güncellemeleri otomatik yapılır.

5.3.5.5. İnternete çıkışlarda Firewall cihazı üzerinde internet paketlerinde virüs taraması yapılmaktadır.

5.4. Veri Bütünlüğü:

5.4.1. HBYS üzerindeki verilere erişim, kullanıcı profillerine tanınan yetkiler aracılığıyla gerçekleştirilir.

5.4.2. Bu yetkiler sayesinde bazı kullanıcılar verileri görebilir, bazı kullanıcılar veriler üzerinde değişiklik yapabilir.

5.4.3. Yapılan işlemlerin belirli kısımları program üzerinden loglanır. Kasıtlı olarak silinen ya da bozulan veriler loglar üzerinden görülerek verinin doğruluğu analiz edilebilmektedir.

5.4.4. Veritabanına direk bağlantı veritabanı yöneticisi ve yazılımcılar tarafından gerçekleştirilmektedir. Veriler üzerinde yapılan tüm işlemler veritabanı yöneticisi tarafından görülüp analiz edilmektedir.

5.5. Süreklilik-Kullanabilirlik:

5.5.1. Sistem odasında yer alan sunucular ve veri depolama cihazları, yedekli bir konfigurasyonda hizmet verecek şekilde, standartlara uygun olarak yapılandırılmıştır.

5.5.2. Sunucular, İTF Sistem Yönetim Birimi tarafından Sunucu Envanter Listesinde belirtilmiştir.

5.5.3. Sistemlerin takibi ve kontrolü günlük olarak İTF Sistem Yöneticisi tarafından yapılmaktadır.

5.5.4. Sunucular herhangi bir elektrik kesintisi durumunda devamlılığın sağlanabilmesi amacıyla (diğer UPS'lerden bağımsız) UPS ile desteklenir.

5.5.5. Sunucu odalarına yetkisiz kişilerin girişi kısıtlanır.

5.5.6. Sunucu odalarının sıcaklık ve nem düzeyleri kontrol altına alınır. Sıcaklık Düzeyi 18° - 22° arasında, Nem Oranı: %30 - %60 arasında olacak şekilde uygun klimatizasyon sağlanır. Yedekli çalışılan klimalar bulunmaktadır.

5.5.7. Sunucu odalarında yangına karşı uygun yangın söndürücüler bulundurulur.

5.5.8. Sunucu odalarında suya karşı yalıtım sağlanır.

5.5.9. Bakım anlaşmaları ile sunucuların sürekliliği sağlanır.

5.5.10. Yedekleme İşlemleri

5.5.10.1. Veritabanlarının günlük yedekleri (mesai bitiminden itibaren belirli bir sırayla) İTF Sistem odasındaki HP Data Protector cihazında bulunan 24 adet Kartuş üzerine otomatik olarak alınmaktadır. Yedek alımından sistem yönetim birimi, alınan yedeklerdeki veri bütünlüğünün testinden ise veritabanı yöneticisi sorumludur.

5.5.10.2. Veritabanı yöneticisi tarafından, kurum içerisinde alınan yedekler Çapa Yerleşkesi içerisinden bulunan Bilgi İşlem Biriminde biriminde muhafaza edilmesi sağlanır.

5.5.10.3. Yedekler günlük olarak alınır ve son 1 aydaki tüm günleri içerir.

5.5.10.4. Son 1 ay ile 6 ay arasındaki sürede, her hafta için 1 yedek bırakılır.

5.5.10.5. Son 6 ay ile 12 ay arasındaki sürede, her ay için 1 yedek bırakılır.

5.5.10.6. Yılda bir kez yedeklenen veriler için veri kurtarma testi uygulanır. Veri kurtarma testi ile ilgili detaylar, "Veritabanı Geri Yükleme Talep Formu" ile kayıt altına alınır.

5.6. İzlenebilirlik - Kayıt Tutma – Raporlama

5.6.1.HBYS programında pek çok farklı sınıfta kullanıcı grupları oluşturulmuştur. Kullanıcılar için tanımlanan yetkilere erişim hakları verilerek hasta kayıtları, testler, analizler vb. modüllere erişimleri etkin bir şekilde denetim altında tutulur. Bu roller kurum içinde üstlenilen görev ve sorumluluklara göre oluşturulur.

5.6.2. Yetkilendirmeler (Roller), HBYS üzerinde tanımlanır.

5.6.3. Bilgi sistemleri yetki verilmemiş kişilerin sisteme ulaşımını yetkilendirme yoluyla korumaktadır. Kurum içerisinde bulunan bilgisayarların internet erişimi kısıtlanmıştır. Sadece yetkilendirilmiş kullanıcılar internete erişebilmektedirler. Yerel domain'e bağlı olan bilgisayarlar sadece Bilgi İşlem tarafından izin verilen internet sitelerine erişim yapabilir. Ayrıca, yerel domain'e bağlı olmayan bilgisayarlardan genel erişime izin verilir.

5.6.4. Kurum üst yönetimi tarafından belirlenen HBYS işlemlerinin logu tutulur. Log tutumundan ve analizinden kurum yazılımcıları sorumludur.

5.6.5. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gereği Kurumumuzun internete çıkış logları; son 2 yıllık zaman dilimi için şifrelenerek (hash) tutulur. Bu süreç İTF Sistem Yönetim Biriminin sorumluluğundadır.

5.6.6. Domain'e dahil olan bilgisayarlarda, bilgisayara giriş ve çıkış logları tutulur, günün hangi saatinde domain'deki hangi bilgisayarın hangi domain kullanıcısı tarafından kullanıldığı izlenebilir.

5.6.7. Domain kullanıcılarına yükümlülükleri İTF Sistem Yönetim Birimi tarafından "Aktif Dizin ve Sistem Kullanım Taahhütnamesi" ile iletilir.

5.6.8. Yetki verilen çalışanların hasta verileri ile ilgili yapılan tüm düzenleme ve değişiklikler sistem üzerinde geriye dönülebilmesi için saklanarak kayıt altına alınır ve bu şekilde izlenir. Her kullanıcı kendisine özel tanımlanmış olan kullanıcı adı ve şifre ile sisteme giriş yapmaktadır. HBYS üzerinde yapılan her değişiklik, bu değişikliği yapan kullanıcı adı ile saklanmaktadır. Hatalı girişlerin takibi bu işlemi yapan personelden itibaren bu şekilde takip edilebilmektedir.

5.6.9. Laboratuvar, Patoloji ve Radyoloji sonuç raporlarının formatı ihtiyaçlar doğrultusunda İlgili Birim Sorumluları tarafından belirlenir ve Enstitü Müdürü tarafından onaylandıktan sonra gerekli düzenlemeler yapılıp, gözden geçirildikten sonra HBYS üzerinde güncellenir.

5.6.10. Girilen Laboratuar, Patoloji ve Radyoloji sonuçların doğruluğu İlgili Birim Yöneticisi tarafından gözden geçirilerek onaylanır. Onay yapan kişi yazılım veri tabanında kayıt altına alınır.

5.6.11. Sistem üzerinde test sonuçlarının örnek kalitesi ve sonuçların değerlendirilmesi ile ilgili yorumlar, yetkilendirilmiş kişiler tarafından hasta geliş kaydı detayları ekranında "Açıklama" alanına yazılabilir.

5.6.12. HBYS sisteminde tüm testler için sonuçlanma zamanı önceden belirlenmiştir. Bu sonuç süreleri sistem tarafından otomatik olarak verilmekte ve değiştirilememektedir.

5.7. Donanım ve Yazılım

5.7.1. Bilgisayar donanım bakımları OE Bilgi İşlem Donanım Destek, İTF Bilgi İşlem Birimi Teknik Servisi ve İTF Biomedikal birimi tarafından yapılır.

5.7.2.HBYS üzerinde yapılan değişikliklerin bilgisayar yoluyla duyurulması yeterli olmadığı durumlarda yeni sistemde yapılan değişikliklerin nasıl kullanılacağı eğitim planlanarak çalışanlara öğretilir.

5.7.3. OE içerisinde kullanılan yazılım ve bilgisayar bozuklukları HBYS üzerinden "HBYS Destek Sorun Bildir" modülünden OE Bilgi İşlem Donanım Destek Sorumlusuna bildirilir ve OE Bilgi İşlem Donanım Destek Sorumlusu gerekli müdahaleyi yapar. Problemin çözümünde yetersiz kalınan durumlarda İTF Biomedikal Biriminden ve/ve ya ilgili firmadan teknik destek alınır.

5.8. Sistem Bakımı

5.8.1. Donanımsal veya yazılımsal sistem bakımları, hastane sürecini kesintiye uğratmadan ya da minimuma indirerek yapılır.

5.8.2. Bakımlar aktif çalışan yazılım üzerinden yapılmaz. Aynı yazılımın kopyasının bulunduğu Test Sistemi üzerinden yapılır.

5.8.3. Tüm bakımlar bittikten sonra yeni sürüm olarak aktif duruma OE için en uygun zaman seçilerek geçirilir. Aktif çalışan yazılımlar kapatılıp tekrar açıldığında yeni sistem devreye girer; böylece süreç etkilenmemiş olur.

5.8.4. OE içinde kullanılan yazılımlar 24 saat süreyle aktif çalışır. Sorun saptandığında yazılım firmasının destek ekibine bilgi verilir. Çözüm için gerekli müdahaleler yapılır ve sistem devreye alınır.

5.8.5. OE bilgi sistemlerinde kullanılan bütün yazılımlarda yapılan bakımlar, bakımları yapan kişiler tarafından Servis Raporu ile kayıt altına alınır. Bu raporlar OE tarafından dosyalanarak takip edilir.

5.8.6. Sistem odası ısı ve nem kontrolü klima ile yapılmaktadır. Ayrıca Sistem Yönetim Birimi tarafından günlük olarak kontrol edilir. Nem Oranı: %30 - %60 arasında olacak şekilde uygun klimatizasyon sağlanır. Yedekli çalışılan klimalar bulunmaktadır.

5.8.7. Bilgi sistemlerinde, analiz yapılması veya raporlanmasını etkileyecek hata veya olağan dışı bir arıza durumunda bilgi sistemleri Acil durum planlarına göre işlemler yapılması sağlanır.

5.9. Teknik Destek

5.9.1. OE'de, Çapa yerleşkesi içerisinde yer alan İTF'ye bağlı 7/24 yazılım ve donanım teknik desteği sağlanır.

5.9.2. HBYS ile ilgili aksaklıklar; sistem testleri ya da kullanım sırasında tespit edilen hatalar ve eksiklikler, HBYS üzerinden "HBYS Destek Sorun Bildir" modülünden Bilgi İşlem Birimine bildirilir.

5.9.3. Bilgi İşlem Birimi bildirilen aksaklıkları değerlendirir, kurum içinde müdahale edilip dilemeyeceğine karar verir. Sorun OE Bilgi İşlem Birimi tarafından giderilemeyecek ise İTF Bilgi İşlem Sorumlusundan ve ya İTF Sistem Yönetim Sorumlusundan destek talep edilir.

5.9.4. Mesai dışı zaman dilimlerinde teknik destek ekibine İdare Amirleri ulaşır. Teknik destek ekibinin iletişim bilgileri santralde bulunur.

5.9.5. HBYS'nin devre dışı kaldığı durumlar, mesai saatleri içinde İTF Bilgi İşlem birimi tarafından, mesai saatleri dışında İTF idare amirleri tarafından kayıt altına alınır.

6. İlgili Dokümanlar

1- Bilişim Sistemleri Kullanım Taahhütnamesi Formu

2- Tesis Güvenliği Prosedürü

3- Jeneratör Kontrol Formu

4- Bilgisayar Kullanma Talimatı