**1. AMAÇ**

Fakültemize başvuruda bulunan kişilere ait bilgilerin güvenliğinin sağlanması, verilerin doğru olarak toplanması, depolanması ve kullanılmasına ilişkin uygulamalarımızı ve güvenlik önlemlerimizi dâhili olarak gözden geçirmek ve kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemlerini almak ve bunun devamlılığını sağlamaktır.

**2. KAPSAM**

Tüm fakülte personelini ve hastalarını kapsar.

**3. TANIMLAR**

**3.1. HBYS:** Hastane Bilgi Yönetimi Sistemi

**4. SORUMLULAR**

Başta üst yönetim olmak üzere, bilgi işlem sorumluları, ilgili firmalar ve tüm çalışanlar sorumludur.

**5. FAALİYET AKIŞI**

**5.1. Yazılım Donanım Destek Birimi:** Fakültemiz teşhis tedavi hizmetlerinde; yasal mevzuat şartlarının karşılanmasından, hizmet sunumunda hasta ihtiyaç ve beklentilerine cevap verecek şekilde gerçekleşmesinden sorumludur. Bu amaçla kurulan Bilgi İşlem Birimi yazılım ve donanım açısından 24 saat kesintisiz hizmet vermektedir.

**5.2. Hastane Bilgi Yönetim Sisteminde Yer Alan Modüller Tek Bir Veri Tabanı Üzerinde**

**Yönetilmelidir:** Hastane Bilgi Yönetim Sisteminde (HBYS) yer alan temel modüllerin tümü (Hasta Kayıt, Klinik, Depo, Ayniyat, Laboratuvarlar, Vezne, Faturalandırma, Radyoloji, Personel Modülü) aktif olarak kullanılmaktadır. Ayrıca; Bölümlerin malzeme ve demirbaş istemlerinin yapılması, onaylanması, satın alınması, depoya teslim edilmesi ve bölümler tarafından teslim alınması HBYS üzerinden gerçekleşmektedir. Hastane Bilgi Yönetim Sistemi’nde (HBYS) yer alan modüller tek bir veri tabanı üzerinden yönetilir. HBYS’de yer alan temel modüllerin tümü aktif olarak kullanılır.

**5.3. HBYS’ de Personel Bilgi Modülü Bulunmalıdır:** Personel bilgi modülü personelin; Fotoğrafını, Çalıştığı Bölümünü, Kan grubunu, İletişim bilgilerini, İzin ve Rapor bilgilerini, Eğitim durumunu, Sertifikalarını, Almış olduğu hizmet içi Eğitimleri ve Yabancı Dil Bilgilerini güncel olarak bulundurmaktadır.

**5.4. HBYS’ ye Bağlı Tüm Bilgisayarlara Yönelik Düzenleme Yapılmalıdır:** HBYS üzerinde bağlı bulunan tüm Bilgisayarların bulunduğu Bölüm, Marka, Model, Seri Numarası, Demirbaş Numarası, Donanım ve Yazılım Adı, İşletim Sistemi, Ek aksamlar, Alınma Tarihi ve varsa Garanti süresi bulunmaktadır. Bu çizelgenin bir örneği Bilgi İşlem Sorumlusu, Kalite yönetim Birimi ve Taşınır Kayıt Biriminde mevcuttur.

**5.5**. Fakültemizde Bilgi Güvenliğini Sağlamaya Yönelik Olarak Aşağıdaki Uygulamalar Hasta bilgilerinin girişi HBYS’ de tanımlanan alanlara yapılmaktadır.

♦ Hasta bilgilerinin güvenliği için, tüm kullanıcılara her kademede yetkilendirme yapılır ve kontrol edilir.

♦ Çalışanlar yetki düzeyleri ile ilgili olarak bilgilendirilir.

♦ Her kademedeki Fakülte personeli ancak yetkilendirilmiş olduğu işlemleri, diğer fakülte prosedürlerine uygun olarak uygular. Aynı görevi icra eden çalışanlar aynı yetki gruplarına sahip olarak çalışır.

**5.6. Bilgi Güvenliğini Sağlamaya Yönelik Düzenleme**

**5.6.1. Sunucu Güvenliği:** Fakültemizde bulunan sunucular bilgi işlem ünitesi içerisinde ayrı bir bölümde izinsiz erişimin engellendiği alanda çalışmaktadır. Ancak yetkili kişilerce ilgili birime girilmektedir. Sunucuların bulunduğu alan su basması, yangına karşı her türlü önlemi alınmış ve yedekli klima sistemi ile soğutulmakta olup ayrıca sıcaklık ve nem bilgileri de düzenli olarak kayıt altına alınmaktadır. Sıcaklık değerleri 18-22 derece, nem %30-50 arasında olması sağlanmaktadır. Bunun yanında yedekli güç kaynakları (UPS) mevcut olup, periyodik bakımları yapılmaktadır. Kurumda bulunan bütün sunucuların kayıtları tutulur. Bu kayıtlarda sunucunun yeri, sorumlu kişisi, donanım, işletim sistemi üzerinde çalışan uygulama bilgileri yer alır. Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs gibi koruma amaçlı yazılımların güncel olmalarına dikkat edilir. Sunucuların yazılım ve donanım bakımları üretici firmanın uygun gördüğü süreler dâhilinde yetkili kişiler tarafından veya teknik servis tarafından yapılır.

**5.6.2. Yedekleme:** Bütün hasta kayıtları ve yedeklenmiş hasta bilgileri fiziksel olarak Kestel Merkez Yerleşkesi Bilgi İşlem Daire Başkanlığında saklanmaktadır. Hasta kayıtlarının yedeklenmesi Bilgi İşlem tarafından günlük olarak yapılmaktadır. Yedeklemeler aracılığı ile yılda bir kez veri kurtarma testi uygulanır, Yedeklemeden alınan (örnek veri ile) geri dönüşün sağlanıp sağlanmadığı ve veri kaybının olup olmadığı kontrol edilir, Test kayıt altına alınır, gerektiğinde düzeltici önleyici faaliyet başlatılır.

**5.6.3. Kişisel Sağlık Kayıtlarının Güvenliği:** Veri tabanı güvenliğini sağlamaya yönelik tedbirler alınır. Veri tabanı sistem loğları (Hasta kayıt logları, Hasta Hizmet logları, Hasta Fatura Logları, Hasta Poliklinik logları, Tanımlama Logları, Hasta Dosya logları, Veri tabanı oturum logları, Sağlık kurulu kayıt loğları) kayıt altında tutulur ve gerektiğinde idare tarafından izlenebilir. Veri tabanı ile ilgili sorumlu kişilerin iletişim bilgileri santralde ve birimlerde bulunmaktadır. Kullanıcıların ara yüze bağlanmak için kullandıkları şifreler şifreli bir şekilde saklanmaktadır. Veri tabanı üzerinde tüm işlemler loglanır. Kullanıcılar veri tabanına yapılacak müdahale (yama ve güncelleme vb.) öncesinden bilgilendirilir. Verileri yetkisiz erişime, yetkisiz şekilde değiştirilmelerine, açıklanmalarına veya imha edilmelerine karşı korumak için uygun önlemleri alınmıştır. Hastanın özlük bilgileri ve kurum bilgileri sadece üst yönetimin onayı ile bilgi işlem birimi tarafından değiştirilebilir. Kullanıcıların bilgileri silme yetkileri yoktur. Hastalarla ilgili her türlü kaydın kim tarafından, hangi tarihte girildiği, ulaşma, değiştirme bilgisi fakülte bilgi işlem programı log kayıtları altında tutulmaktadır. Hastaların klinik kayıtlarına yalnızca konu ile ilgili yetkilendirilmiş kişinin giriş yaptığı hastane bilgi işlem programında “Güvenlik Sistemi” adı altında izlenebilmektedir.

**5.6.4.** HBYS’de Oluşan Sorunların Çözümü: Bilgi İşlem Sorumlusu ve Teknik Destek Ekibi gerekli çalışmaları yapar. HBYS ile ilgili sorunlarda çalışanlar kiminle nasıl irtibat kuracağı konusunda bilgilendirilir. Sorun giderilinceye kadar işlerin aksamamasına yönelik yapılması gerekenler bölüm bazında belirlenmiştir. HBYS tekrar aktif olduğunda bu süreçte elde edilen verilerin HBYS’ye kim tarafından ve nasıl kaydedileceği Bilgi İşlem Sorumlusu tarafından belirlenmiştir. HBYS ile ilgili sorunlar ve çözümler kayıt altına alınır. Sorunun oluştuğu tarih ve saat, bildirimin yapıldığı tarih ve saat, sorunun çözüldüğü tarih ve saat kayıt altına alınır. Sorunlar ile ilgili aylık istatistiksel çalışma yapılır, sorunlar ile ilgili gerekli düzeltici önleyici faaliyet başlatılır.

**5.7. HBYS Üzerinde Yapılan İşlemler İzlenebilirliği:** Salt okunur özellikte ayrı bir veri tabanı ya da tablo mevcuttur. Veri tabanı ya da tablolarda sisteme giriş yapan kullanıcılar, gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalar ile ilgili veriler kayıt altına alınır. Veri tabanı ya da tablolara sadece bilgi sisteminde yönetici olarak yetkilendirilmiş kişiler ulaşabilir.

**5.8. İnternet Erişim ve Kullanımı:** Hiçbir kullanıcı peer-to peer bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örneğin; KaZaA, iMesh, eDonkey, Gnutella, Napster, Aimster, Madster, FastTrak, Audiogalaxy, MFTP, eMule, Overnet, NeoModus, Direct Connect, Asquisition, BearShare, Gnucleus, GTKGnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, XoLoX, OpenNap, WinMX. vb)

♦ Bigisayarlar arası ağ üzerinden resmi görüşmeler haricinde Whatsapp, Telegram vb. mesajlaşma ve sohbet programları gibi chat programlarının kullanılmaması. Bu chat programları üzerinden dosya alışverişinde bulunulmamalıdır.

♦ Hiçbir kullanıcı internet üzerinden Multimedia Streaming (Video, mp3 yayını ve iletişimi) yapamayacaktır.

♦ Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.

♦ İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır.

♦ İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.

**5.9. E-Posta Kullanımı**

♦ Kurumun e-posta sistemi, taciz, suistimal veya herhangi birşekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.

♦ Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

♦ Kişisel kullanım için İnternet’teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

♦ Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

♦ Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

♦ Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

♦ Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

♦ Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.

♦ Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

♦ Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodlar içerebilirler.

♦ Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.

♦ Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre (personel folder) çekilmelidir.

♦ Fakültemiz çalışanları gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Yasadışı ve hakaret edici e-posta haberleşmesi yapılması durumunda yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilir ve kullanıcı hakkında yasal ve idari işlemler başlatabilir.

♦ Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e- postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren yetkililerle temasa geçip durumu haber vermekle yükümlüdürler.

♦ Altı ay süre ile kullanılmayan e-posta kutuları Bilgi İşlem birimi tarafından kaldırılabilir.

Kurumdan ayrılan personel kurumsal e-posta sistemini kullanamaz. E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma, işten ayrılma sebepleriyle kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem birimine en kısa zamanda bildirilmesi gerekmektedir.

**5.10. Şifre Kullanımı**

♦ Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her üç ayda birdir.

♦ Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

♦ Şifreler başkası ile paylaşılmamalı, kağıtlara ya da elektronik ortamlara yazılmamalıdır.

♦ Şifrelemede, küçük ve büyük karakterlere (örnek, a-z, A-Z), hem digit hemde noktalama karakterleri ve ayrıca harflere (örnek, 0-9,!’^+%&/()=?\_;\*) sahip olmalıdır.

♦ En az sekiz adet alfa nümerik karaktere sahiptir.

♦ Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.

♦ Aile isimleri kullanılmamalıdır.

♦ Herhangi bir kişiye telefonda şifre verilmemelidir.

♦ E-posta mesajlarında şifre yazılmamalıdır.

♦ Şifreler aile bireyleriyle paylaşılmamalıdır.

♦ Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.,

♦ Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.

♦ Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

♦ **Uzaktan Erişim:** Uzaktan Erişim, Bilgi işlemden sorumlu personel tarafından üniversite Bilgi İşlem Dairesi Başkanlığının izni dahilinde gerekli görülen durumlarda güvenlik duvarı tarafından korumalı olarak erişim sağlanmaktadır.

**♦ Kablosuz Erişim:** Kablosuz erişim, Fakülte içerisinde kablosuz erişim mevcut olup, otomasyon ile bağlantıyı sağlayacak olan cihazların MAC (fiziksel) adresleri modem üzerinde kayıtlıdır. İzinsiz olarak dışarıdan girişlere kapalıdır.

♦ **Virüs ve Saldırganlardan Korunma;** Virüs ve saldırganlardan korunma sorumluluğu ilgili Daire Başkanlığı ve bilgi işlem sorumlusuna aittir. İlgililer virüs ve saldırganlardan korunma için gerekli donanım ve yazılımı üst yönetime bildirip gerekli tedbirleri alır. Bu tedbirler içinde anti virüs yazılımları ve firewall gibi donanımsal ve yazılımsal aparatları içeren sağlık bakanlığınca istenen asgari şartlardan oluşur. Bu yazılımların güncellenmesini de yapmak yukarda belirtilen ilgililerin sorumluluğundadır, zamanı geldiğinde üst yönetimin haberdar ederek güncellemeleri yaparlar.