| REV. NO | AÇIKLAMA | YAYIN/REV. TARİHİ | SORUMLU |
|---|---|---|---|
| 00 | Yeni yayınlanmıştır. | 15.09.2008 | N.DÖNDER |
| 01 | Bilgi güvenliği revizyonu yapıldı | 29.03.2010 | Ö.ALTUNDİŞ |
| 02 | HKS kapsamında revizyonlar yapıldı. | 31.08.2012 | A.ÖZKAN |
| 03 | Versiyon-5 Kapsamında Revizyon Yapıldı. | 04.01.2017 | S.DİKİCİ |
| 04 | Gözden geçirildi | 15.05.2018 | S.DİKİCİ |
| 05 | Gözden geçirildi | 22.01.2019 | S.DİKİCİ |
| 06 | Versiyon-6 Kapsamında Revizyon Yapıldı | 13.04.2022 | S.SÜMEN |

# 1. 1. AMAÇ

## 1. AMAÇ

Ali Osman Sönmez Onkoloji Hastanesi'nde bilgi yönetim sisteminin detaylarının belirlenmesi ve bilgi güvenliğinin sağlanması amacıyla uygulanan işlemlerin politikasını ve şeklini belirler.

## 2. KAPSAM

Bu doküman kurumumuz bilgi yönetimi işlemleri, genel HBYS kullanım ve erişim kuralları ve bilgi güvenliği konularını kapsar.

## 3.KISALTMALAR

**HBYS:** Hastane Bilgi Yönetim Sistemi

**BGYS:** Bilgi Yönetim Sistemi

**KVK:** Kişisel Verileri Koruma

**KVKK:** Kişisel Verileri Koruma Kanunu

**SGK:** Sosyal Güvenlik Kurumu

**DÖF**: Düzeltici Önleyici Faaliyet

**UPS:** United Parcel Service (Kesintisiz güç kaynağı)

## 4.TANIMLAR

**Varlık:** Ali Osman Sönmez Onkoloji Hastanesi iş süreçleri için değeri olan, kaybı halinde işlerin aksayacağı, insan, yazılım, donanım, itibar, bilgi gibi unsurların tümüdür.

**Gizlilik:** Bilginin sadece yetkili kişiler tarafından erişilebilir olmasıdır.

**Bütünlük:** Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılmasıdır.

**Erişilebilirlik:** Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an erişilebilir olmasıdır

**Bilgi Güvenliği Ekibi:** bilgi yönetiminden sorumlu ekip

**Bilgi güvenliği ihlal olayı:** İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

**Bilgi Güvenliği Yönetim Sistemi (BGYS):** Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.

## 5. SORUMLULUKLAR

### 5.1 Onay ve yürürlülük

Bu prosedür Hastane Müdürü'nün onayından sonra yürürlüğe girer. Bu prosedürün yürütülmesinden; yönetilmesinden ve güncellenmesinden Bilgi İşlem personeli sorumludur. Bilgi İşlem Sorumlusu, Hastane İşletim Sistemini kullanan tüm çalışanlar sorumludur.

**5.2 Prosedürün kullanıcıları**

Uygulanmasından bilgi yönetim sistemi ile her türlü iletişimi olan tüm personel sorumludur.

**6. PROSEDÜR**

**6.1. Destek Birimi**

**6.1.1.** Kurumumuzda bilgi yönetiminden sorumlu Bilgi Güvenliği Ekibi mevcuttur. Ekip, Başhekim' e bağlı olarak çalışmaktadır. Bilgi Güvenliği Ekibi, Bilgi İşlem Teknik Donanım, Bilgi İşlem Yazılım ve Bilgi İşlem Koordinasyondan oluşmaktadır. Yazılım Destek Ekibi 'ndeki firma yetkilileri 7/24 teknik desteğin sağlanmasıyla görevlidirler. Gerek duyulması durumunda, ekipteki firma yetkilileri aranarak yaşanan soruna müdahale etmeleri sağlanmaktadır. Bilgi Güvenliği Ekibi'ndeki personellerin listesi ve gerekli iletişim bilgileri güncel hali santralde bulunur.

**6.1.2.** Ali Osman Sönmez Onkoloji Hastanesi'nde Bilgi Güvenliği Ekibi, bilgi yönetim sistemi ile ilgili durumların değerlendirilmesi, olası riskler için risk analizi yapılması ve risklerin bertaraf edilmesi ve sonuçların gözlemlenmesinden sorumludur. Risklerin bertarafı için belirtilen periyot içinde gerekli önlemler alınmalıdır. Risklerin analizi ve bertarafı için Düzeltici önleyici Faaliyetler Prosedürü ile belirtilen adımlar izlenerek düzeltici önleyici faaliyet başlatılır.

**6.1.3.** Kurumumuzda Bilgi Güvenliği Ekibi, HBYS sisteminde tanımlı kullanıcıların yetki düzeylerini kayıt altına alır. Kullanıcıların yetki durumları HBYS sisteminde kayıt altında tutulmaktadır. Bilgi Güvenliği Ekibi yetkilerin güncel durumunu izler ve gerektiğinde HBYS' deki yetkilendirme bilgilerinin güncelliğini sağlar. Yetkilendirme düzeylerinde herhangi bir değişiklik olduğunda ilgili kullanıcılara yapılan değişikliklerle ilgili gerekli bilgiyi vermekle de yükümlüdür.

**6.2. HBYS**

**6.2.1.** Kurumumuzda kullanılan HBYS sistemi tüm birimlerimiz için tek bir veritabanından yönetilmektedir. Hasta Kayıt-Kabul, Hasta Yatışı, Poliklinik, Klinik, Eczane, Depo, Satınalma, Ayniyat, Laboratuvar, Vezne, Faturalandırma, Radyoloji, Personel modülü başta olmak üzere HBYS' de mevcut tüm modüllerin aktif olarak kullanılması sağlanmaktadır. Gerektiğinde personele HBYS kullanımı ile ilgili eğitimler düzenlenir.

**6.2.2.** Bilgi Sistemi kapsamında kullanılan tüm bilgisayarlarda güncel bir anti virüs yazılımı yüklenmeli, güncelliği sağlanmalıdır.

**6.2.3.** Kurumumuzda kullanılan sunucu üzerinden erişimi sağlanan HBYS sistemi üzerindeki tüm hareketler izlenmeli ve sistem loglarının sürekli olarak tutulur. Loglar, sisteme yapılan girişler, yapılan işlemler, değiştirilen sistem ayarları, sistem tarafından verilen uyarılar ve hata mesajlarını detaylı olarak kayıt altına alınır ve yönetici yetkisi düzeyinde kullanıcıların erişebileceği şekilde, istenildiği zaman kayıtlar incelenebilmektedir. Ayrıca Log kayıtlarını tutan veritabanı tablosu salt okunur şekildedir, hiçbir kullanıcı bu tablo üzerinden kayıtların düzenlemesini yapamaz. HBYS sisteminin veri tablolarına erişim sadece yönetici yetkisi verilmiş kullanıcılar tarafından yapılmaktadır.

**6.2.4. HBYS sisteminde sorun/hata oluşması durumunda;**

**6.2.4.1.** Problemin giderilmesi için 7/24 destek veren Bilgi İşlem Birimi' ne bildirilmesi gerekmektedir. Bilgi İşlem Çalışanlarının iletişim bilgileri santralde de mevcuttur. Diğer İşletim ve Bilgi Sistemleri ile ilgili istek ve talepler; Bilgi Sistemleri Arıza Bildirim/ Teknik Dektek Talep Formu ile yapılmakta ve aciliyet durumuna göre değerlendirilmektedir.

**6.2.4.2.** Bilgi İşlem çalışanları sorunun başladığı tarih ve saat, bildirimin yapıldığı tarih ve saat, ve sorunun çözümünün ne zaman tamamlandığı ile ilgili bilgilileri HBYS Sorun Takip Formu kullanarak kayıt altına alır. Sorunla ilgili gerekli iyileştirme çalışmaları yapılır. DÖF açılarak, takip ve kayıt edilir.

**6.2.5. HBYS arıza/hata giderilene kadar birimlerde yapılacaklar:**

**6.2.5.1.** Mesai saatleri içinde ve dışında bir sorun meydana gelmişse, kritik birimler (laboratuvar, hasta kabul, acil servis, radyoloji) sorun giderilene kadar hasta mağduriyeti yaşanmaması için, SGK onayı almadan, hastanın kimlik fotokopisi ve basılı formlar kullanılacak işlemler yapılır.

**6.2.5.2.** Laboratuvar sistemi sonuç veremez, tetkik sonucu antetli kağıda elle yazılarak, imzalanır. Sorun giderilince; hasta kaydı açılır, numune tekrar çalışılır ve sisteme kaydedilir. Maksimum 12 saat içinde tüm HBYS sorunları çözümlenir.

**6.2.6.** İşe yeni başlayan çalışan HBYS'yi kullanacaksa İlgili birim yöneticisi tarafından Bilgi İşlem Sorumlusuna çalışanın hangi grup yetkiye sahip çalışan olduğu bilgisi verilir. HBYS'de bulan personel modülüne çalışan kaydedilir. Personel modülünde çalışan ile ilgili aşağıdaki bilgiler bulunur:

- Personel kimlik bilgileri
- Çalışana ait fotoğraf
- Mesleği
- Çalıştığı birim
- Kan grubu
- İletişim Bilgileri (Telefon, adres)
- Kan grubu
- İzin ve rapor bilgileri
- Eğitim Durumu
- Serifikaları
- Hizmet içi eğitimleri
- Yabancı dil bilgisi
- Cinsiyeti, Doğum Tarihi
- İşe giriş tarihi

Bilgi işlem çalışanı; personel kartı üzerinden çalışana, aynı yetki grubundaki diğer çalışanlarla aynı yetkileri tanımlar. Çalışana HBYS yetkileri ve kullanıcı eğitimi yapılır.

**6.2.7.** İşten ayrılan çalışanlar olduğunda; ilgili birim sorumlusu, çalışanın yetkilerinin iptali için bilgi işlem birimi ile iletişime geçer ve HBYS'de ayrılan çalışanın yetkileri kaldırılır.

### 6.3. Yetkilendirme

**6.3.1.** Ali Osman Sönmez Onkoloji Hastanesi içerisindeki programları kullanan kullanıcılar, Bilgi İşlem Sorumluları tarafından yetkilendirme ve bilgi sınırlaması yapılmaktadır. Yetkilendirme kullanıcıların sadece kendi işleri ile ilgili işlemleri yapabilmesi, ilgili olmayan bilgilere ulaşamaması ve/veya işlem yapamamasını sağlar.

**6.3.2.** Kullanıcılar ilk işe başladıklarında bilgi işlem biriminin belirttiği rol ile yetkilendirilirler. Rol tanımları HBYS içerisinde kişinin görmesi gereken ekranların gruplanmış şeklidir. Kişiye verilen rol dışında başka bir bilgiye ihtiyaç olması durumunda bölüm yöneticisinin bilgi işlem birimine bildirmesiyle, onaylanan kişiye yetki verilmesi işlemini Bilgi İşlem Personeli gerçekleştirir.

**6.3.3.** HBYS programında Birim Yöneticisinin talep ettiği yetkilendirmeler, Bilgi İşlem Sorumlusu tarafından Hastane Genel Müdürü'ne iletilir. Hastane Müdürü onaylarsa yetkilendirme yapılır.

**6.3.4.** Yetkisiz girişlere sistem izin vermemektedir.

**6.4. Sunucuların Güvenliği:** Ana surver (Sistem)Odası, sadece sunucuların bulunduğu, yetkili dışında ulaşımı engellenmiş, suya karşı yalıtımı yapılmış, UPS e bağlı, sıcaklığı sürekli 18-22℃ ve %30-60 olacak şekilde ortam ısı- nem takibi yapılan, klima bulunan ayrı bir alandır.

Server bulunduğu alanda her ihtimale karşılık uygun yangın tüpü bulundurulmaktadır. Server bulunduğu alan belirli periyodlarla haşerelere karşı ilaçlama ve takibi yapılmaktadır. Sistemin yerden yüksekliği sağlanmaktadır. Elektrik güvenliği açısından server UPS sistemine bağlı olarak çalıştırılmaktadır.

#### 6.4.1. Sorumluluklar

Kurum bünyesindeki bütün dahili sunucuların yönetiminden yetkilendirilmiş Bilgi İşlem çalışanları sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılacaktır.

- Bütün sunucular (kurumun sahip olduğu) kayıtlıdır.
- Bütün bilgiler tek bir merkezde güncel olarak tutulur.

**6.4.2.** Ana surver (Sistem odası) ve HBYS (yazılım, donanımla ilgili sorunlar, bilgi güvenliği, bilgi mahremiyeti, kullanıcı hataları vb) ile ilgili riskler analiz edilir ve oluşabilecek risklere yönelik iyileştirme çalışmaları yapılır.

#### 6.4.3. Genel Konfigürasyon Kuralları

- İşletim sistemi konfigürasyonları Bilgi İşlem biriminin talimatlarına göre yapılacaktır.
- Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- Servislere erişimler loglanacak ve erişim kontrol metotlarıyla koruma sağlanır.
- Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
- Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec VPN gibi şifrelenmiş ağ)

üzerinden yapılmalıdır.

- Sunucular fiziksel olarak korunmuş sistem odalarında bulunur.
- Sunucu odasının sıcaklık değeri 18-22 °C; nem değeri % 30 - % 50 arasında olmalıdır. Sunucu odasının sıcaklık nem kaydı Isı Nem Takip Formu kullanılarak, sabah ve aksam olmak üzere günde 2 defa kaydedilir.
- Server odasında çıkabilecek yangın için, kapının yanında yangın söndürme tüpü bulunmaktadır.

### 6.5. Yedekleme

a) Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve ısı bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, HBYS düzenli olarak günde 3 kez,

a) Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkacaktır. Ağ güvenlik duvarı (firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve Internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır. Ağın dışından ağın içine erişimin denetimi burada yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmelidir.

b) Verinin operasyonel ortamda online olarak ayni disk sisteminde farklı disk ölümlerinde ve offline olarak Manyetik kartuş, DVD veya CD ortamında yedekleri alınır.

c) Taşınabilir ortamlar (Manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından farklı odada ve farklı binada güvenli bir şekilde saklanır.

d) Veri yedekleri mesai saatleri dışında yönetim ve bilgi işlem tarafından belirlenen gizli bir yerde muhafaza edilir. Sadece bilgi işlem sorumlusu ve yönetim sorumlusu dışına kimsenin erişim yetkisi bulunmamaktadır.

e) Veri yedeklerinin teslim alınması ve burada yazılı kurallar gözetilerek saklanmasına ilişkin yetkili / sorumlu personel Bilgi İşlem Sorumlusu (Rackment sunucu olduğundan telefon üzerinden yönlendirme yapılır) olarak belirlenmiştir.

f) Dolabın üzerine “yangında önce kurtarılacaktır” ibaresi yazılır.

g) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.

h) Yapılan yedeklemeler ile en yılda iki kez veri kurtarma testi uygulanır. Geri yükleme ile geri dönüşüm sağlanıp, sağlanmadığı, veri kaybının olup olmadığı kontrol edilir ve etkinlikleri doğrulanır. Veri kurtarma testinin yapıldığı tarih ve zaman Bilgi İşlem Sorumlusu tarafından kayıt altına alınır.

ı) Yedekleme ve veri kurtarma testinde herhangi bir problem ile karşılaşılırsa iyileştirme çalışmaları başlatılır.

i) Yedeklenen veriler offline ortamda süresiz olarak hastane yönetimi tarafından saklanır.

### 6.6. Kişisel Sağlık Kayıtlarının Güvenliği

#### 6.6.1. Bilgi Güvenliği Hedefleri ve Prensipleri

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri

yürütülmektedir. Her bir varlık için risk seviyesinin kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir.

Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir ve kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

**6.6.2. Bilgi Güvenliği Sözleşmeleri**

Kullanıcılar kurumumuzca tanımlanmış Bilgi Yönetim Sistemi Kullanıcı Gizlilik Sözleşmesi imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Personel ‘’Bilgi Güvenliği Kullanıcı Sözleşmesi’’ (Taahhütnamesi) işe alınan her çalışanın imzaladığı bir belgedir. Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mali vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

- Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; veri gizliliğinin, değiştirilmediğinin (bütünlüğünün) ve erişilebilirliğinin sağlanmasıdır.
- Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.
- Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar (hastanın tedavisinden sorumlu sağlık personeli) ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidirler. Ancak hastanın yazılı onayı ve diğer sağlık çalışanları bu veriye erişebilirler.
- Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.
- Hasta dosyasının bir kopyası hastaya teslim edilmelidir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir." Hastanın rızası olmadan hiçbir çalışan yazılı veya sözlü olarak hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.
- Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara ve kurumlara iletilemez. Hastanın kullandığı ilaçlar, diyet programlan vs. buna dâhildir.
- Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi.
- Telefonda konuşurken hastanın mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.
- Bütün hasta sağlık kayıtları (online bilgi veya yedek medya) fiziksel olarak korunmuş mekanlarda saklanmalıdır.
- Elektronik sağlık kayıtlarına internet ortamından erişim, ancak yetkilendirilmiş kullanıcılara güvenli erişim sağlandığında mümkün olabilir.
- Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya kurumumuzun Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir,
- Sağlık kayıt dosyalarının saklandığı kağıt veya elektronik medyalar (kartuş, CD, DVD, Flash disk, HDD, vb.) güvenli bir ortamda saklanmalıdır,

- Üçüncü şahısların ve/veya kuruluşların hasta sağlık kayıtlarına erişimiyle ilgili olarak, 01.08.1998 tarih ve 23420 sayılı Resmi Gazetede yayınlanan "Hasta Hakları Yönetmeliği" nin ilgili maddeleri uygulanır.

### 6.7. Internet Erişim ve Kullanımı

Bütün kullanıcılar ve Bilgi İşlem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır,

- Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkacaktır. Ağ güvenlik duvarı (firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve Internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır. Ağın dışından ağın içine erişimin denetimi burada yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmelidir.
- Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografik, oyun, kumar, şiddet içeren vs) yasaklanabilmelidir.
- Anti-virüs gateaway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik (smtp, pop3, ayrıca mümkünse http ve ftp vs) virüslere karşı taranmalıdır.
- Kurumlar internet erişimlerinde firewall, anti-virüs, içerik kontrol vs. güvenlik kriterlerini hayata geçirmelidirler.
- Ancak Yetkilendirilmiş Bilgi İşlem çalışanları ve yöneticiler internete çıkarken bütün servisleri kullanma hakkına sahiptir. Bunlar; www,ftp,telnet, ping, traceroute vs.
- Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ,MIRC,Messenger v.b. mesajlaşma ve sohbet programları gibi chat programlarının kullanılmamalı, bu chat programları üzerinden dosya alışverişinde bulunulmamalıdır.
- Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemesi ve dosya indirimi yapılmamalıdır.
- 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. Kurumsal işlevlere yönelik yazılım ihtiyaçları için ilgili prosedürler dâhilinde ilgili Bilgi işlem sorumlusuna müracaat edilmesi gerekmektedir.
- Üçüncü şahısların kurum internetini kullanmaları Bilgi işlem sorumlularının izni ve bu konudaki kurallar dâhilinde gerçekleştirilebilecektir.

### 6.8. E-Posta Kullanımı

#### 6.8.1. Yasaklanmış Kullanım

- Kurumun e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi

gerekmektedir.

- Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilg ilere azami biçimde özen gösterilmesi gerekmektedir.
- Kurum ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dâhildir.
- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
- 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.

### 6.8.2. Kişisel Kullanım

Kurumda kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır.
Ayrıca iş dışındaki e-postalar farklı bir klasör içerisinde saklanmalıdır.

- Kurum personeli tarafından internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında Kurum tarafından belirlenen "gizlilik notu" ve "sorumluluk notu" bilgileri yer almalıdır.
- Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
- Gizli ve hassas bilgi içeren elektronik postalar kriptolanarak iletilmelidir.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
- Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
- Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir
- Elektronik postaların sık sık gözden geçirilmesi, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmaması ve bilgisayardaki kişisel klasöre çekilmelidir.

### 6.8.3. E-Posta Yönetimi

Kurum e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.

### 6.8.4. E-Posta Virüs Koruma

Virüs, solucan, Truva At' veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslerle bulaşmış e-postalar Anti-virüs sistemleri tarafından analiz edilip temizlenmelidir. Ağ güvenlik yöneticileri bu sistemden sorumludur.

## 6.9. Şifre Kullanımı

### 6.9.1.Genel

- Bütün sistem seviyeli şifreler (örnek, root, administrator, enable, vs) en az üç ayda bir değiştirilmelidir.
- Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir.
- Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
- Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.
- Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.
- Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır. Bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki ana noktalara uymalıdır.

### 6.9.2. Ana Noktalar

#### 6.9.2.1. Genel Şifre Oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları;( kullanıcı şifreleri, web erişim şifreleri, e- posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri v.s( Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir**.**

**Zayıf şifreler aşağıda belirtilen karakteristiklere sahiptir.**

- Şifreler sekizden daha az karaktere sahiptirler.
- Şifreler sözlükte bulunan bir kelimeye sahiptir.
- Aaabbb,quwerty,zyxwuts,123321 vs. gibi sıralı harf veya rakamlar.
- Yukarıdaki herhangi bir kelimenin geri yazılış şekli.
- Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek gizli1, gizli2)

**Güçlü şifreler aşağıdaki karakteristiklere sahiptir.**

- Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)
- Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir. (0-9,!@#$%A&*O_+I---=VO[]:<>?,/)
- En az sekiz adet alfa numerik karaktere sahiptir.
- Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
- Aile isimleri gibi kişisel bilgilere ait olmamalıdır.
- Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Kolayca hatırlanabilen şifreler oluşturulmalıdır.

#### 6.9.2.2. Şifre Koruma Standartları

Kurum bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanmayınız. (örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde) değişik işlemler için farklı şifreleme kullanın. Örnek unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanınız. Kurum bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler kuruma ait gizli bilgiler olarak düşünülmelidir.

- Aşağıdakilerin yapılmayacakların listesidir.
  - Herhangi bir kişiye telefonda şifre vermek
  - E-posta mesajlarında şifre belirtmek
  - Üst yöneticinize şifreleri söylemek
  - Başkaları önünde şifreler hakkında konuşmak
  - Aile isimlerini şifre olarak kullanmak
  - Herhangi form üzerinde şifre belirtmek
  - Şifreleri aile bireyleri ile paylaşmak
  - Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmek
- Herhangi bir kimse şifre istediğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem Birimi yetkilisini aramasını söyleyiniz.
- Uygulamalardaki "şifre hatırlama" özelliklerini seçmeyiniz.(örnek: Outlook, İnternet Explorer vs)
- Tekrar etmek gerekirse, şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.
- Şifreler an az altı ayda bir değiştirilmelidir( sistemlerin şifreleri ise en az üç ayda bir değiştirilmelidir).
- Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

#### 6.9.2.3. Uygulama Geliştirme Standartları

Uygulama geliştiricileri programlarında aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

- Bireylerin (grupların değil) kimlik doğrulaması (authentication) işlemini destekleyebilmelidir.
- Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.
- Kural yönetim sistemini desteklemelidir,(örnek; bir kullanıcı diğer bir kimsesin şifresini bilmeden fonksiyonlarına devam edebilmesi.)
- Mümkün olduğu kadar TACACS+ , RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

#### 6.9.2.4. Uzaktan Erişen Kullanıcılar için Şifre Kullanımı

Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılacaktır.

### 6.10. Uzaktan Erişim

- Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir:
- Uzaktan erişim metotları ile kuruma bağlantılarda bilgi sistemlerinin güvenliliğinin sağlanması için aşağıdaki politikalara göz atmak gerekmektedir.
  - Kabul edilebilir Şifreleme Politikası
  - Sanal Özel Ağ (VPN) Politikası
  - Kablosuz haberleşme Politikası
  - Kabul Edilebilir kullanım Politikası

#### 6.10.1. Gereklilikler

- Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. (Sağlık ocakları, hastaneler, grup başkanlıkları da bu kapsam içerisindedir). Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.
- Kurum çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dâhil olmak üzere hiç kimseye veremezler.
- Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.
- Çalışanlar Kurum ile ilgili yazışmalarında Kurumun dışındaki e-posta hesaplarını,(örnek, Hotmail, yahoo,mynet v.s) kullanamazlar.
- ISDN veya telefon hatları ile uzaktan erişen yönlendiriciler minimum olarak CHAP kimlik doğrulama protokolünü kullanmalıdırlar.

### 6.11. Kablosuz Erişim

3.0 Erişim Cihazları (Access Point) ve Kartların Kayıt Olunması Kurumun bilgisayar altına bağlanan bütün erişim cihazları ve alt arabirim kartları (örnek, PC Card) Bilgi İşlem birimi tarafından kayıt altına alınması gerekmektedir. Erişim cihazları periyodik olarak güvenlik testlerinden geçirilmelidir. Ancak Mac adresleri kayıtlı olan cihazlar Kurumun bilgisayar altına erişebilmelidir.

#### 6.11.1. Onaylanmış Teknoloji

Bütün kablosuz erişim cihazları Bilgi işlem güvenlik birimi tarafından onaylanmış olmalıdır ve Bilgi işlemin belirlediği güvenlik ayarlarını kullanmalıdır.

#### 6.11.2. Güvenlik Ayarları

- Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için VVi-Fi Protected Access(WPA) şifreleme kullanılmalıdır. IEEE 802.lx erişim kontrol protokolü ve TACACS ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılabilmelidir.
- Erişim cihazlarında ki firmware'leri düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.
- Erişim cihazlarını kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.
- Cihaza erişim için güçlü bir şifre kullanılmalıdır. Erişim Şifreleri varsayılan ayarda bırakılmamalıdır.
- SSID numaraları yayınlanmamalıdır. Böylece sniffer tarzı cihazların otomatik olarak bu numaraları çözmesi engellenecektir.( hotmail, yahoo, mynet vs ) kullanamazlar.

### 6.12. Uygunsuzlukların Tespiti ve Düzeltici Önleyici Faaliyetlerin Planlanması

Hastalarla ve işleyiş düzeni ile ilgili karşılaşılan her türlü aksaklıkla bir daha karşılaşılmaması için duruma uygun

olarak Uygunsuzluk Yönetimi Prosedürü ve Düzeltici ve Önleyici Faaliyetler Prosedürü'ne göre hareket edilir. Uygunsuzluk Tespit Formu ve Düzeltici ve Önleyici Faaliyet İstek Formu doldurulur.

## 7. İLGİLİ DOKÜMANLAR

### 7.1. Referanslar

7.2.Sağlıkta Kalite Standartları

## 8. YAYIN/DAĞITIM

HBYS ''kullanıcı giriş'' sayfasından yayınlanır