1-Amaç

- Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmek,
- Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,
- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
- Bilgi Güvenliği Yönetim Sistemini sürekli gözden geçirmek ve iyileştirmek,
- Bilgi Güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmek,

2-Kapsam

Hastane bünyesinde faaliyet gösteren tüm birimlerde çalışan personeller, sunucular, hizmet sağlayıcılar,

3-Sorumlular

Üst yönetim, tüm hastane çalışanları,

4-Tanımlar

Sunucu: Ana bilgisayar

Donanım: Bilgisayarın fiziki parçalarıdır.

Otomasyon: Bir işin insan ile makine arasında paylaşılmasıdır.

Anti-virüs Programı: Hastane otomasyon sistemine dışarıdan ve içeriden gelebilecek tehditlere ve kötü amaçlı yazılımlara karşı koruma amaçlı bir programdır.

Uzaktan Erişim: Başka bir yerdeki bir bilgisayara IP adresi yordamıyla bağlanma çeşididir.

İnternet: Tüm dünyaya yayılmış, birbirleri ile bağlantılı, yani birbirleri ile "konuşabilen" yüz binlerce bilgisayardan oluşan bir ağdır.

Bellek: Bilgi depolama ünitesidir.

Log-on: Oturum açmak

HBYS: Hastane Bilgi Yönetim Sistemi

Spam: İstek dışında gönderilen reklam içerikli mail.

Junk: Gereksiz (çöp)

Firmware: Donanımların veya cihazın işlevlerini nasıl yerine getireceklerini bildiren ve genellikle tekrar yazılabilir olan ufak kodlar.
SSID (Hizmet Seti Kimliği): Bir kablosuz ağı tanımlayan addır.

Reset: İlk duruma getirmek, sıfırlamak.

5- BILGİ YÖNETİM SİSTEMİ (BYS) YÖNETİM SÜRECİ

a. Bilgi Güvenliği Komisyonu

AD SOYAD	UNVAN
Sevgi ÖZYEĞEN ARSLAN	Başhekim Yardımcısı
Yaşar AŞIK	İdari Mali İşler Müdürü
Nuray ŞANLI	Müdür Yardımcısı
Selda DOĞAN	Bilgi İşlem Sorumlusu
Coşkun ÇELEN	Bilgi İşlem Çalışanı

b. Bilgi Güvenliği Komisyonunun Görev, Yetki ve Sorumlulukları

- Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde Bilgi Güvenliği Politikaları Yönergesine bağlı olarak çalışma grupları tarafından hazırlanacak olan kılavuzlarla ilgili yenilenme kararlarını verir,
- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlar,

BİLGİ GÜVENLİĞİ

<u>İnsan Kaynakları ve Zafiyetleri Yönetimi</u>

a. Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
b. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
c. ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kâğıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
d. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
e. İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kâğıt kesme makinasında imha edilmelidir.
f. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
g. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
h. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
i. Göreve yeni başlayan ve ayrılan personeller **"Bilgi Güvenliği İşe Başlama ve İşten Ayrılma Süreç Prosedürü"**nde belirtildiği şekilde **"İşe Başlama ve İşten Ayrılma Formları"**nı doldurarak gerekli tanımlamaları yapılmalıdır.

Kişisel sağlık kayıtlarının güvenliği

a. Bolu Fizik Tedavi ve Rehabilitasyon Hastanesi'nde göreve başlayan tüm personeller **" Personel Gizlilik Sözleşmesi "** ni okuyarak imzalamalıdır.
b. Gizlilik sözleşmesinde belirtilen yükümlülüklerin bir veya birkaçına uyulmaması durumunda hukuki ve cezai yaptırım uygulanır.
c. Bilgi Yönetim Sistemine ait verilen tüm yetkiler, yetki talep eden kişilerin ve birim sorumlusunun imzası ile kayıt altına alınarak verilmelidir.
d. Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletmez.
e. Hastanın sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programlar vs. buna dâhildir.
f. Hasta dosyasının bir kopyası hastaya teslim edilir. Hiçbir hasta kaydı, elektronik veya kâğıt ortamında (Bakanlığın bu konuda çıkardığı genelgeler hariç) hiçbir kuruma veya üçüncü şahıslara sözlü veya yazılı olarak teslim edilemez.
g. Hastanın dosyası izlenmeli, gelişigüzel ortada bırakılmamalı, bilgisayar ekranında başkalarınca okunabilecek şekilde bırakılmamaktadır.
h. Telefonla konuşurken hasta ile ilgili özel, mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen gösterilmelidir.
i. Bütün hasta sağlık kayıtları fiziksel olarak korunmuş mekânlarda saklanmaktadır.
j. Yönetimsel analizler yapmak için veri tabanındaki veriler bir yerden başka bir yere aktarılırken, kayıtlarda bulunan kişisel kimlik tanımlayıcıları kayıttan çıkartılmakta ve analizler hasta ile hastalık bilgisi eşleştirmeden yapılmaktadır.

İnternet erişim ve kullanımı

a. Bilgisayar ağı erişim ve içerik denetimi yapan bir güvenlik duvarı üzerinden internete çıkmaktadır.
b. Hastanemizde içerik filtreleme sistemi kullanılmaktadır. İstenmeyen siteler (pornografik, oyun, kumar vs.) yasaklanmıştır.
c. Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgisi olmayan sitelerde gezinmek yasaktır.
d. İş ile ilgisi olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek ve indirmek yasaktır.
e. İnternet üzerinden, kurumun yetkili birimlerinden onay alınmaksızın kurum adına elektronik işlem yapılamaz.
f. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez.
g. Bütün kurum bilgisayarları anti-virüs yazılımına sahiptir.
h. Anti-virüs güncellemeleri sunucular vasıtası ile yapılmaktadır. Sunucuların internete bağlantısı olup otomatik olarak veritabanlarını güncellemektedir.
i. Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmaktadır.
j. Zararlı programları (virüs, solucan, Truva atı…) hastanemiz bünyesinde oluşturmak ve dağıtmak yasaktır.

k. Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramaz.
l. Bilinmeyen kaynaklardan gelen cd-rom ve dvd-rom lar anti-virüs programı tarafından taraması otomatik olarak yapılmaktadır.
m. Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
n. Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

Kablosuz erişim:

a. Erişim cihazlarında ki güncellemeler sunucu tarafından düzenli olarak taranmakta ve Bilgi işlem Birimi tarafından güncellemeler yapılmalıdır.
b. Erişim cihazlarına kolayca erişilebilir olmaması için tavana monte edilmelidir.
c. Cihaza erişim için güçlü bir şifre kullanılmaktadır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır.

E-posta kullanımı

a. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
b. Bakanlık ile ilgisi olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğelerde dâhildir.
c. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
d. Kurum işlevleri dışında, kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
e. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalı ve Bilgi İşlem Yazılım Birimine haber verilmektedir.
f. Kullanıcıların kullanıcı kodu, şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal Bilgi işlem şubesine bilgi verilmelidir.
g. Çalışanlar e-posta ile uygun olmayan içerik (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb) paylaşmamalıdır.
h. Kurum çalışanları mesajlarını düzenli olarak kontrol etmekte ve kurumsal mesajlar cevaplandırılmalıdır.
i. Kurum çalışanları e-postaların kurum dışında ki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludur.
j. İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.
k. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
l. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.
m. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.
n. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.
o. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.

Son Kullanıcı Güvenliği

a. Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir.
b. Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı loglanarak kayıt altına alınmalıdır.
c. Güvenlik zafiyetlerine karşı, son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır.
d. Son kullanıcılar bilgisayarlarında ki ve sorumlusu oldukları cihazlarda ki bilgilerin düzenli olarak yedeklerini almalıdır.
e. Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.
f. Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde hastaneye ait olmayan USB flash bellek ve/veya harici hard disk gibi taşınabilir medya kullanmamalıdır.

HBYS' YE İLİŞKİN YAZILIMSAL SÜREÇLER

Şifre güvenliği

a. HBYS kullanıcıları programın zorunlu bırakması nedeniyle şifrelerini 6 ayda bir değiştirmek zorundadır.
b. Şifreler en az 6 hane olmalıdır.
c. Şifrelerde harf ve rakam kullanılmalıdır.
d. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
e. Şifreler başkası ile paylaşılmamalı, kağıtlara ya da elektronik ortamlara yazılmamalıdır.
f. Şifre, kullanıcı adı ile aynı olmamalıdır.
g. Şifre ardışık rakamlardan oluşmamalıdır.
h. Herhangi bir kişiye telefonda şifre verilmemelidir.
i. Şifreler aile bireyleriyle paylaşılmamalıdır.
j. Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.

Yedekleme

a. Hastane verileri HBYS nin hiç kullanılmadığı ya da minimum düzeyde kullanıldığı saatlerde yedeklenmektedir.
b. HBYS verileri günde 3 defa yapılmaktadır. İşlem otomatik her gün sabah saat 05.00, öğlen 12.30, akşam 21.00 saatlerinde gerçekleştirilmektedir.
c. Yedekler sunucu odasında bulunan depolama ünitesi üzerine, ayrıca üniversite ünitesinde bulunan depolama ünitesine otomatik olarak yedek almaktadır.
d. Her 7 günde bir (Pazartesi günü) HBYS verilerinin tamamı DVD ortamına yedeklenmektedir.
e. DVD üzerine alınan yedekler Vezne biriminde bulunan kilitli kasa içerisinde süresiz olarak saklanmaktadır.
f. DVD üzerine verilerin yedeklendiğine dair tutanak hastane müdürü tarafından imzalanmakta ve tutanaklar bilgi işlem biriminde saklanmaktadır.
g. Yılda bir defa veri kurtarma testi yapılmalıdır.

Uzaktan erişim

a. HBYS firması yazılım destek elemanlarının, hangi durumlarda uzaktan erişimle, iç ortama erişim yapacağına dair hastane tarafından onaylanmış gizlilik sözleşmesi bulunmalıdır.
b. Yazılım destek elemanlarının yetersiz kaldığı durumlarda, yazılım bakım, güncelleme ve destek hizmetleri için bilgi yönetim sistemi firması yazılım destek elemanları, uzaktan erişim ile destek verebilir.
c. Sistemi kısmen veya bütünüyle çalışamaz hale getiren bir arıza durumunda bilgi yönetim sistemi firması uzaktan erişim ile destek verebilir.

d. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahiptir.
e. Kurum ağına uzaktan erişim ile erişen Bilgi Yönetim Sistemi firması çalışanları Bilgi İşlem Yazılım Biriminden izin almak zorundadır.
f. Uzaktan erişimler bağlanan kullanıcılar "Dış Ortamdan İç Ortama Bağlantı" formuna kaydedilerek hastane yönetimine onaylatılmalıdır.
g. Uzaktan erişim için tek kullanımlık şifre ve geçici süreli erişim hakkı verilir.
h. Periyodik yapılan kontrollerle gereksiz kullanıcı kimlikleri ve hesapları kaldırılmalıdır.
i. Uzak erişim için kullanılacak olan servisler ve protokoller güvenlik duvarında tanımlı olmalıdır.

SİSTEM ALT YAPISINA İLİŞKİN SÜREÇLERİ

Sunucu güvenliği

a) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.
b) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
c) Sunucuların elektrik kesintilerinden etkilenmemesi için hastane güç kaynağından bağımsız kesintisiz güç kaynağı bulunmalıdır.
d) Sunucuların oluşabilecek tehditlere karşı yer ile teması kesilerek, bir kabin içerisinde ve yükseltilmiş taban üzerinde muhafaza edilmelidir.
e) İklimlendirme şartlarının sağlanması için klima bulunmalıdır. Herhangi bir arıza anında ikinci bir yedek klima bulunmalıdır.
f) Sunucu odasına yetkisiz personel girişleri engellenmiştir. Sistem odası kapısında şifreli giriş sistemi bulunmalıdır.
g) Sunucu odasına girişler güvenlik kamerası ile izlenerek kayıt altına alınmalıdır.
h) Isı ve nem takibi çevrimiçi çalışan ısı nem cihazı ile her gün yarım saatte bir otomatik olarak yapılmaktadır. Isı ve nemlerde ki sapmalarda cihaz üzerinde ki alarm çalmakta ve sunucu odası sorumlularına e-posta ile bilgi mesajı gitmelidir.
i) Isı-nem cihazlarında ki anormal değerlerin her ay çıktısı alınarak analiz edilmelidir.
j) Sunucu üzerinde çalışan anti virüs ve diğer sunucu yazılımları güncel olarak çalışmalıdır.
k) Sunucuların yazılım bakımları hastanede faaliyet gösteren otomasyon firması tarafından sürekli olarak yapılmalı ve 6 ayda bir tutanak altına alınmalıdır.
l) Sunucu donanım bakımları yetkili firma tarafından 6 ayda bir yapılmalı ve tutanak altına alınmalıdır.
m) Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı ve kullanım politikasına aykırı bir kullanıma olanak verilmemelidir.

n) Sunucular üzerinde kesinlikle ticari amaç güden yazılımlar kurulmamalıdır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
BÖLÜM KALİTE SORUMLUSU	KALİTE YÖNETİM DİREKTÖRÜ	HASTANE YÖNETİCİSİ