1. YÖNETİM SÜREÇLERİ

Sağlık tesisimiz teşhis tedavi hizmetlerinde; yasal mevzuat şartların karşılanmasından, hizmet sunumunda hasta ihtiyaç ve beklentilerine cevap verecek şekilde gerçekleşmesinden sorumludur. Hasta kayıtları, tanı ve tedavi bilgileri radyoloji görüntüleri, laboratuvar sonuçları, ameliyat bilgileri, ücretlendirmeler gibi tüm bilgiler HBYS ortamında kaydedilmekte ve veri tabanında saklanmaktadır.

AMAÇ:

a. Faaliyetlerimizin ticari, mali ve diğer iç ve dış baskılardan ve etkilerden uzak tutulmasını,
b. Hasta ve hak sahiplerine ait gizli bilgilerin ve tescilli hakların korunmasını,
c. Teşhis ve tedavi sonuçlarının uygun şartlarda muhafaza edilmesini ve iletilmesini,
d. Yeterlilik, tarafsızlık, karar verme ve çalışmalarda güveni azaltacak herhangi bir faaliyette bulunmamayı,
e. Sağlık hizmeti sunarken beklenen kalite seviyesinin sağlanmasını,
f. Vereceğimiz hizmetin belirlenen standartlar çerçevesinde gerçekleştirilmesini,
g. Söz konusu bilgileri hasta onayı dışında ya da yasal bir yükümlülük altında bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ve kuruluş ile paylaşmamayı taahhüt eder. Kurum olarak gizliliğin önemli olduğuna inanırız. Bu politika hastanemizde sunulan tüm sağlık hizmetleri için geçerlidir.
h. Hastanemiz Hasta Hakları, güvenlik, veri bütünlüğü, erişim ve uygulama ile ilgili gizlilik ilkelerine bağlıdır.

KAPSAM:

a. Sağladığınız bilgiler; hastanemize teşhis ve tedavi için başvurduğunda hastalarımızdan kişisel bilgiler (ad, soyad, hastalık bilgileriniz, T.C Kimlik numarası, adres, telefon bilgileri, vb..) istenmektedir.
b. Hastanemiz yalnızca, Hasta Bilgi Güvenliği Politikası ve/veya belirli hizmetlere ilişkin gizlilik uyarısında açıklanan amaçlarla kişisel bilgileri kullanır.
c. Bilgi güvenliğini sağlamak amacıyla Bilgi Güvenliği gizlilik sözleşmesi tüm personele imzalatılmaktadır.
d. Bu doküman kurumumuz bilgi yönetimi işlemleri, genel HBYS kullanımı, erişim kuralları ile bilgi güvenliği konularını kapsar.

2. BİLGİ GÜVENLİĞİ

BYS ile ilgili politikaların oluşturulması, BYS'ye ilişkinfaaliyetlerin yürütülmesi ve koordinasyonunun sağlanması, bilgi güvenliği ile ilgili hususlarda gerekli çalışmaların yapılması amacıyla sorumlular ve sorumluluklar ilgili görev tanımlarında belirtilmiştir.

2.1. Bilgi Yönetimi ve Güvenliği Hedefleri

Bilgi güvenliği hedefleri aşağıdaki gibi sıralanmıştır:

- Kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak
- Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak

Amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi yönetimi ve güvenliğini sağlamayı hedefler.

Hizmet sunumu sürecinde yer alan tüm bilgi sistemlerini, bilişim kaynaklarını, fiziksel bilgi varlıklarını, bilişim ağları ve altyapısını, uygulama yazılımlarını, veri tabanı sistemlerini, tüm bilgi işlenen platform ve süreçleri ve bu süreçlerde görev yapan personel ve tedarikçiler de dâhil tüm paydaşları kapsar.

Bilgi güvenliği ve kişisel verilerin korunması konusunda çalışanlara yılda en az bir kez farkındalık eğitimi, ayrıca bilgi yönetim sisteminin etkin kullanılabilmesine ilişkin bilgi yönetim sistemi uygulamaları hakkında eğitim verilmektedir.

2.2. Bilgi Yönetimi ve Güvenliği İlkeleri

Hizmet politikası gereği ilkemiz Tekirdağ Şehir Hastanesi'nde kurulan sistemde Hastane Bilgi Yönetim Sistemi'ni etkin ve verimli yöneterek, çalışanlarımızın, tedarikçilerimizin, hizmet verdiğimiz tüm kurum ve kişilerin memnuniyetini sürekli arttırmaktır. Prosedürde belirtildiği üzere HBYS Uygulama ve İşletim Hizmetinin sunumu Turkcell tarafından gerçekleştirmektedir.

Bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kesinlikle kullanılmaz.

Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:

- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
- Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
- Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı, risk analizi; yazılım ve donanımla ilgili sorunlar, bilgi güvenliği, bilgi mahremiyeti, kullanıcı hatalarını içerir. Tespit edilen riskler doğrultusunda iyileştirme çalışmaları yapılır.

Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3. kişilere iletilemez.

Bilgi güvenliği konusunda tüm çalışanlara "Yıllık Eğitim Planı"nda belirlenen zamanlarda ve uyum eğitimi kapsamında işe başlarken bilgi güvenliği ve kişisel verilerin korunması konusunda farkındalık eğitimi verilir.

Şifre kullanımı ile ilgili detaylar "Şifrelendirme Prosedürü"nde belirtilmiştir. Bilgi yönetim sisteminde kullanılan parolalar, Bakanlık parola politikaları ile uyumludur.

Bilgi yönetim sistemi sorumluları ve kullanıcılarına "Personel Gizlilik Sözleşmesi" imzalatılır.

Bilgi Güvenliği ve kişisel verilerin korunması ile ilgili hususlar:

- Erişim ve Yetki Kontrolü
- Fiziksel ve Çevresel Güvenlik Yönetimi
- İletişim Güvenliği
- Bilgi Güvenliği İhlal Olayı Yönetimi
- Kişisel Verilerin Korunması

2.3. Erişim ve Yetki Kontrolü

Erişim ve yetki kontrolü aktif dizin üzerinde bulunan güvenlik grupları ile sağlanır. Bilgilerin güvenliği için tüm kullanıcılara kendi yetkilerine göre her kademede yetkilendirme yapılmıştır. Tüm personel kendi alanı ile ilgili, ancak yetkilendirilmiş olduğu işlemleri gerçekleştirilebilir. Erişimler HBYS Uygulama ve İşletim Hizmetleri tarafından "Bilgi Sistemleri Yetkilendirme Prosedürü" doğrultusunda gerçekleştirilir.

Bilgilerin bütünlüğü ve güvenliği kurulmuş olan bilgisayar yazılım programlarında yetkilendirilmiş girişler ile korumaya alınmıştır.

2.4. Fiziksel ve Çevresel Güvenlik Yönetimi

Güvenlik önlemleri kapsamında tüm bilgisayarlar ve yazıcıların güç kabloları kullanıcıların temas mesafesinden uzak ve dağınık olmayacak bir şekildedir. Ayrıca tüm yazıcılar bulundukları masalara sabitlenmiş durumdadır.

2.5. İletişim Güvenliği

2.5.1. İnternet Erişimi ve Kullanımı

İnternet erişimi FW (Güvenlik Duvan) üzerinden Sağlık Bakanlığına (SB-Net) yönlendirilerek yapılır.

İnternet erişimi, kullanımı ve kısıtlamalar Sağlık Bakanlığı Kamu Hastaneler Birliği (KHB) tarafından belirlenen yetki çerçevesinde sağlanır. Bunun haricinde tüm bilgisayarlardan resmi sitelere erişim sağlanmaz.

Bilgi İşlem Sorumlu sadece İdare ve İşletme tarafından gelen, internet erişim ve kullanım taleplerini karşılar.

İnternet erişimi ve e-posta kullanım bağlantıları firewall cihazı tarafından kontrol edilir. İnternet kullanımında giriş yapılabilecek sayfalar ve internet uygulamaları firewall üzerinden yetkiye dayalı olarak belirlenmiştir.

Kişisel ve elektronik iletişimde üçüncü taraflarla yapılan bilgi alışverişinde kuruma ait bilgilerin gizliliği sağlanır.

2.5.2 E-Posta Kullanımı

İşe alınan tüm çalışanlara e-posta adresi ve şifresi bağlı çalıştıkları firmalar ve kamu çalışanlarına İdare tarafından verilir. Kişilere mail adresleri verildikten sonra Bilgi İşlem Sorumlusu tarafından gerekli e-posta programları ve yapılandırmalar gerçekleştirilir.

2.5.2. Bilgi Güvenliği İhlal Olayları Yönetimi

Bilgi yönetim sistemine ilişkin olası yazılımsal ve donanımsal sorunların, ihlal ve hataların nasıl bildirileceği ve hatalara nasıl müdahale edileceği belirlenmiş olup; hatalar giderilinceye kadar işlerin aksamamasına yönelik yapılması gerekenler bölüm bazında belirlenmiştir.

Karşılaşılan hatalar, çözüm süreçleri, ne kadar sürede hatanın çözüldüğü gibi bilgiler kayıt altına alınır, benzer hataların gerçekleşmesi durumunda bu kayıtlar izlenebilir.

Hata bildirimine ve çözüm sürecine yönelik düzenlemeler:

Kuruma destek hizmeti veren firmanın dış ortamdan iç ortama Bilgi yönetim sistemine ilişkin yazılımsal ve donanımsal oluşacak sistem hatalarında, kurum iş ve işleyişe özgü özel bir değişiklik yapılmasını istenmesi halinde yazılım firmasına sistem üzerinden talep oluşturulur. Bu talepler sistem üzerinde kayıt edilip, yapılacak değişikler için firma personeli bilgimiz dâhilinde bağlanarak gerekli düzenlemeleri yapmaktadır. Merkezimize HBYS yazılım firması tarafından belirlenmiş olan, Veri Tabanı ve diğer ağ bileşenlerine uzaktan erişim ile yetkili personel listesi yer almaktadır. Ayrıca Dış Ortamdan İç Ortama Erişim Formu **(DBY.FR.008)** ve yazılım firması tarafından kullanılan ve merkezimiz bilgisayarlarına kurmuş olduğu uzak bağlantı programı "NETSUPPORT" programı ile kayıt altına alınmaktadır.

Bildirilen hata ve ihlal olayları ile ilgili aşağıdaki bilgiler kayıt altına alınır:

- Hatanın oluştuğu tarih ve saat
- Bildirimin yapıldığı tarih ve saat
- Hatanın içeriği

- Hatanın giderildiği tarih ve saat

8.3.1. Bilgi güvenliği ile ilgili olaylar derhal rapor edilmelidir. Raporun verileceği ve bilgi sunulacak bölümler tabloda belirtilmiştir.

8.3.2. Kurum politikalarına uymayan her tür davranış, kurum bilgi güvenliği prensipleri ve talimatlarına aykırı her tür bilgi paylaşımı, uygunsuz PC/Laptop kullanımı, yetkisiz girişler, uygun olmayan yerde yetkisiz personelin görülmesi, bilgisayar varlıkları ile ilgili arıza, hırsızlık, kaybolma vb. olumsuzluklar bilgi güvenliği olayı kapsamına girmektedir.

8.3.3. Olay halinde müdahaleyi ilgili/yetkili birimler yaparlar. Olayı raporlayan kişinin müdahale etmemesi ve uzmanların müdahalesi için hiçbir şeye dokunmaması gerekmektedir.

2.6. Kişisel Verilerin Korunması

"6698 Sayılı Kişisel Verilerin Korunması Kanunu"na göre hizmet verilir. Kişisel verilerin depoladığı sistemler yetkisiz erişime karşı korunur.

Çalışanların ve hastalann kişisel bilgilerine erişim, sadece bilgilere ulaşma yetkisi bulunan çalışanlar ile sınırlı tutulur ve bu kişiler gizliliği koruma yükümlülüklerini bilerek çalışır. Çalışanların ve hastaların bilgilerine yetkili olmayan kişilerin ulaşımına / kullanımına izin verilmez.

Kullanıcılar SBYS veya Windows ortamına aktif dizin hesaplan ve parola politikasına uygun güçlü şifreleri ile giriş sağlar. Ek olarak tüm cihazlarda aktif ve güncel çalışan (merkezi yönetilen) antivirüs yazılımı bulunur. Bu sayede kişisel verilere tehdit oluşturan dış etkenlere karşı koruma sağlanır.

2.7. Uzaktan ve Kablolu Erişimlerde (Dış Ortamdan İç Ortama Erişim) Güvenlik Tedbirleri

Sisteme erişim ve yetkilendirme Hastane İdaresi tarafından, İşletme ve HBYS Uygulama İşletim Hizmetleri firma tarafından belirlenmiş olan esaslara göre düzenlenir.

Sisteme erişim kontrolü Hastane Yöneticisi ve Bilgi İşlem Sorumlusu tarafından ilgili kişilerin yetki ve sorumlulukları dikkate alınarak düzenlenir.

Sistemde herhangi bir arıza durumunda, HBYS Ekibi uzaktan erişimle arızaya müdahalede bulunur.

Hastane Yöneticisi ve Bilgi İşlem Sorumlusu bilgisi dışında bilgisayarlar üzerindeki ağ ayarlarında, kullanıcı tanımlarında, kaynak profillerinde vb. uygulamalar üzerinde mevcut yapılan düzenlemeler hiçbir suretle değiştirilemez. Bakanlığın bilgi güvenlik politikası gereği domain yapısı oluşturulmuş, tüm bilgisayarlar domain yapısına login durumda çalışmaktadır. Domaine bağlı olmayan bilgisayarlar yerel ağdan çıkarılmış, yerel ağdaki cihazlar arasında bilgi alışverişi yapılmamaktadır.

Bu tedbirler güvenlik duvarı, anti virüs programı ve şifreleme ile sağlanır. Dış ortamdan iç ortama erişebilme koşulları ve erişim sağlayabilecek kişiler belirlenmiştir. Dış ortamdan iç ortama yapılan erişimler "Dış Ortamdan İç Ortama Erişim Formu" doğrultusunda yapılır ve dış ortamdan iç ortama yapılan erişimler kayıt altına alınır.

Hizmet alımı kapsamında merkezimiz verilerine fiziksel veya bilgi sistemleri vasıtası ile erişim sağlayabilen tüm kişilere

personel gizlilik sözleşmesi imzalatılır. (DBY.YD.003)

2.8. Virüs ve Saldırganlardan Korunma

Bilgisayarları virüslerden ve saldırılardan korumak için gerekli alt yapıyı sağlamak Bilgi İşlem Biriminin, bilgisayarları virüslerden koruma sorumluluğu ise kullanıcılara aittir.

Sorumlular tarafından virüs ve saldırılardan korunma için gerekli donanım ve yazılım İdare ve İşletme'ye bildirilerek firewall, kullanıcı yetkileri gerekli tedbirler alınmaktadır.

Bu tedbirler, güncel anti virüs yazılımları ve firewall gibi donanımsal ve yazılımsal uygulamaları içeren asgari şartlardan oluşur.

Bu yazılımların güncellenmesini zamanında gerçekleştirmek de Bilgi İşlem Sorumlusunun sorumluluğundadır. Güncellenme zamanlarında İdare ve İşletme konu ile ilgili bilgilendirilir.

2.9. Dosya Sunucusu

Çalışanlar ağ üzerinde bulunan dosya sunucusu üzerinde yetkilendirildikleri alanlara erişebilirler.

2.4-Destek Birimi

1. Kurumumuzda bilgi yönetiminden sorumlu ekibi mevcuttur. Yazılım-Donanım Teknik Destek Ekibi, Bilgi Güvenliğinden Sorumlu İdari ve Mali İşler Müdür Yardımcısı'na bağlı olarak çalışır. HBYS yazılımının desteğini sağlayan firma personeli de ekipte görev almaktadır. Yazılım-Donanım Teknik Destek Ekibindeki personeller 7/24 teknik desteğin sağlanmasıyla görevlidirler. Gerek duyulması durumunda firma yetkilileri aranarak yaşanan soruna müdahale etmeleri sağlanmaktadır. Yazılım-Donanım Teknik Destek personellerinin listesi ve gerekli iletişim bilgileri (DBY.FR.002) **HBYS İLETİŞİM BİLGİ FORMU** dokümanında belirtilir ve bu listenin güncel hali santralde ve nöbetçi personelde bulunur.

2. Bilgi Güvenliği Birimi ve Yazılım-Donanım Teknik Destek Ekibi yetkilerin güncel durumunu izler ve gerektiğinde HBYS' deki yetkilendirmeleri yapar.

3. Bilgilerinin güncelliğini sağlar. Yetkilendirme düzeylerinde herhangi bir değişiklik olduğunda ilgili kullanıcılara yapılan değişikliklerle ilgili gerekli bilgiyi vermekle de yükümlüdür.

Bilgi Yönetim Sisteminde kullanılabilirlik açısından gerekli düzenlemeler:

Bilgi Yönetim Sisteminde kullanılabilirlik açısından gerekli düzenlemeler HBYS'de kullanılabilirlik açısından incelenebilecek unsurlardan bazıları aşağıda verilmiştir:

- Kullanım Kolaylığı
- Öğrenilebilirlik
- Verimlilik
- Hataların Azlığı
- Memnuniyet
- Esneklik
- Sekmelere Kolay Erişilebilirlik

gibi konularda talepler arıza talep- modülü kullanılarak yapılmaktadır. Ayrıca whatsapp gurubu üzerinden fikir alışverişi yapılabilmekte ve aynı yazılım firmasını kullanan ADSM ler ile de istişare edilerek sistem üzerinde kullanılabilirlik sağlanabilmektedir.

3. BİLGİ YÖNETİM SİSTEMİNİ OLUŞTURAN ALT SİSTEMLER

Topraklık Ağız ve Diş Sağlığı Merkezin 'de SBYS ile entegre olarak PACS (Picture Archiving Communication Systems) sistemleri bulunmaktadır.

4. SAĞLIK BİLGİ YÖNETİM SİSTEMİ İŞLETİM VE DEĞİŞİKLİK YÖNETİM SÜREÇLERİ

Hastanemizde kullanılan SBYS kullanıcı dostudur. Sistem ara yüzü tüm kullanıcıların kolaylıkla kullanılabileceği bir şekilde dizayn edilmiştir. SBYS tarafından tarih kontrolleri yapılır. SBYS üzerinde kullanıcılar için kısayollar oluşturulmuştur. Tüm kısayollar sistematiktir. Kısayollar "HBYS Kısayol Listesi"nde belirtilmiştir. Bilgi Yönetim Sisteminin etkin kullanılabilmesi amacıyla ilgili tüm çalışanlara işe girişten itibaren ve ihtiyaç durumunda eğitimler verilir. Eğitimler "Eğitime Katılım Formu" ile kayıt altına alınır. SBYS'nin muayene ekranlarından ulusal sağlık veri tabanına (e-nabız) entegrasyon sağlanmıştır. Hastaların aynı hastanedeki geçmiş tıbbi kayıtlarına SBYS üzerinden erişim sağlanabilir. SBYS, T.C. Sağlık Bakanlığı Kayıt Tescil Birimi tarafından tescil edilmiştir. SBYS tescil durumu T.C. Sağlık Bakanlığı https://kayittescil.saglik.gov.tr/TR,54929/aktif-hbys-listesi.html adresinden teyit edilebilmektedir.

5. BİLGİ SİTEM DONANIM ALTYAPI, YÖNETİM VE TALEP SÜREÇLERİ

5.5.1. Sahip Olma ve Sorumluluklar

a. Firma tarafından hazırlanan HBYS yazılımı sunucular vasıtasıyla sağlık tesisimizde hasta kayıt işlemi, laboratuvar tektik işlemleri, PACS işlemleri için kullanılan uç kullanıcılara(bilgisayarlara) ulaştırılmaktadır.

b. Fiziki güvenlikleri için sunucular; girişi çıkışı kontrol altında tutulan sistem odalarında muhafaza edilmektedir

c. Kurum bünyesindeki bütün dahili sunucuların yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılır.

d. Bütün sunucular (kurumun sahip olduğu) ilgili kurumun yönetim sistemine kayıtlıdır. Bu işlemde **HBYS Sunucu bilgi formu (DBY.FR.010)**kullanılarak sunucu bilgileri kayıt altına alınır. Sunuculardan ve veri tabanından sorumlu kişilerin iletişim bilgileri **HBYS İLETİŞİM BİLGİ FORMU** dokümanında bulunur.

e. Sunucu odasına Teknik Destek Ekibi dışındaki personelin girmesi yasaktır, şifreli kapıyla kontrolü sağlanır.

f. Bütün bilgiler tek bir merkezde güncel olarak tutulur.

5.5.2. Genel Konfigürasyon Kuralları

a. İşletim sistemi konfigürasyonları Kurumumuzun Bilgi Güvenliği ve Teknik Destek Ekibi'nin talimatlarına göre yapılır.

b. Kullanılmayan servisler ve uygulamalar kapatılır.

c. Servislere erişimler logların ve erişim kontrol metotlarıyla koruma sağlanır.

d. 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 yapılır, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanır.

e. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "roof" gibi genel kullanıcı hesapları kullanmaz, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanırlar. Genel yönetici hesapları yeniden adlandırılmıştır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yaparlar.

f. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılır.

g. Sunucular fiziksel olarak korunmuş sistem odalarında bulunur.

h. Sunucu odasının sıcaklık değeri 18-22 °C; nem değeri % 30 - % 50 arasında olmalıdır. Sunucu odasının sıcaklık nem kaydı **Isı Nem Takip Formu (SİY.FR.009)** kullanılarak, sabah ve akşam olmak üzere günde 2 defa kaydedilir.

6. VARLIK YÖNETİMİ

Bilgisayarlara Yönelik Düzenleme Bilgi Yönetim Sisteminde kullanılan tüm bilgisayaralar hastane etki alanına dahil edilir. Bilgisayarlarda lisanssız program kullanımına izin verilmez. Tüm bilgisayarlarda merkezi sunucu tarafından kontrol edilebilen antivirüs yazılımları bulunur. Ayrıca tüm bilgisayarlara yönelik güncel envanter oluşturulur. Bilgisayar donanım ve yazılım envanterinde aşağıdaki bilgiler bulunur:

- Bulunduğu bölüm
- Marka
- Model
- Seri No
- Demirbaş numarası
- Donanım ve yazılım adı
- İşletim sistemi
- Ek aksamlar
- Alınma tarihi
- Varsa garanti süresi

Kullanıcı bilgisayarlarındaki virüs yazılımları ve virüs tarama dosyaları ile işletim sistemi ve güvenlik yamalarının güncellenmeleri merkezi bir sunucu vasıtası ile otomatik olarak yapılır. Bilgi güvenliği amacıyla kablosuz ağ bağlantıları için farklı VLAN bağlantıları oluşturulur. Misafir kullanıcıların bağlandığı kablosuz ağ bağlantıları için farklı vlan oluşturulur.

7. İŞ SÜREKLİLİĞİ YÖNETİMİ

Bilgi Yönetim Sistemi Risk Yönetimi Bilgi Yönetim Sistemine yönelik olarak fiziksel tehlikeler, yazılım ve donanımla ilgili sorunlar, bilgi güvenliği, bilgi mahremiyeti, kullanıcı hataları, kişisel verilerin korunması gibi konularda "Bilgi

Yönetimi Risk Analizi Planı" ile risk analizi yapılarak riskler tespit edilir. Tespit edilen risklerin ortadan kaldırılması amacıyla iyileştirme çalışmaları yapılır.

8. YEDEKLEME

a) Bilgi sisteminde oluşabilecek hatalar karşısında; sistemin kesinti süresini ve olası bilgi kayıplarını en aza indirmek için sistem üzerindeki konfigürasyon, sistem bilgileri ve kurumsal veriler "Yedekleme Politikası" nde belirlenen ilkeler doğrultusunda düzenli olarak yedeklenmektedir.

b) Yedekleme ile ilgili süreçler, verinin depolanması ve korunmasına yönelik dikkat edilmesi gereken hususlar ve veri kurtarma testi planlarını kapsayacak şekilde tanımlanmıştır.

c) Veri yedekleme standardı, yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı ne koşullarda ve hangi aşamalarda yedeklerin yükleneceği "**Yedekleme Politikası**"nde belirtilmiştir.

d) Uygulamalarda herhangi bir değişiklik olması durumunda "**Yedekleme Politikası**"nün işlerliği ve güncelliği gözden geçirilir.

8.1. Temiz Masa

Çalışma saatleri dışında bilgisayarlar Merkezimizin belirlediği saatler de otomatik olarak kapanmaktadır.

8.2. Kişisel Sağlık Kayıtlarının Güvenliği

a. Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mâli vb.) güvenliğinin sağlanmasına dikkat edilir.

b. Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; veri gizliliği, bütünlüğü (değiştirilmemiş olması) ve erişilebilirliğidir.

c. Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmış olup yetkisiz kişiler hastanın sağlık kayıtlarına erişmez.

d. Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar (hastanın tedavisinden sorumlu sağlık personeli) ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilir. Ancak hastanın yazılı onayı, ve yasalarca belirlenmiş görevleri yerine getiren diğer sağlık çalışanları bu veriye erişebilirler.

e. Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.

f. Hasta dosyasının bir kopyası hastaya teslim edilir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmez."

g. Hastanın rızası olmadan hiçbir çalışan yazılı veya sözlü olarak hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.

h. Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara ve kurumlara iletilemez. Hastanın kullandığı ilaçlar, diyet programlan vs. buna dahildir.

i. Hastanın dosyasının izlenmemesi için gerekli tedbirler alınır. Hasta dosyaları gelişigüzel ortada bırakılmaz, bilgisayar ekranının başkalarınca okunmaması için gerekli tedbirler alınır.

j. Telefonda konuşurken hastanın mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen gösterilir.

k. Bütün hasta sağlık kayıtları (online bilgi veya yedek medya) fiziksel olarak korunmuş mekanlarda saklanır.

l. Elektronik sağlık kayıtlarına internet ortamından erişim, ancak yetkilendirilmiş kullanıcılara güvenli erişim sağlandığında mümkün olabilir.

m. Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya kurumumuzun Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir,

n. Kurum, kritik bilgiye erişim hakkı olan çalışanlar ve firmalar ile gizlilik anlaşması imzalar.

8.4. İnternet Erişim ve Kullanımı

Bütün kullanıcılar ve Bilgi İşlem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkar.

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 İnternet 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 sağlar.

b. Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılır. İstenilmeyen siteler (pornografik, oyun, kumar, şiddet içeren vs) yasaklanır.

c. Anti-virusgateaway sistemleri kullanılır. İnternete giden veya gelen bütün trafik (smtp, pop3, ayrıca mümkünse http ve ftp vs) virüslere karşı taranır.

d. İnternet erişimlerinde firewall, anti-virus, içerik kontrol vs. güvenlik kriterleri hayata geçirilmiştir.

e. Ancak Yetkilendirilmiş Sistem Yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir. Bunlar; www,ftp,telnet, ping, traceroute vs.

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

g. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemesi ve dosya indirimi yapılmaz.

h. İş ile ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır, internet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve Kurum sistemleri üzerine bu yazılımlar kurulamaz. Kurumsal işlevlere yönelik yazılım ihtiyaçları için ilgili prosedürler dahilinde ilgili Bilgi işlem sorumlularına müracaat edilmesi gerekmektedir.

i. Üçüncü şahısların kurum internetini kullanmaları Bilgi İşlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.

8.5. E-Posta Kullanımı

a. Yasaklanmış Kullanım

b. 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.

c. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

d. Kurum ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dahildir.

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

f. Kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

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

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

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

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

8.6. Kişisel Kullanım

a. 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. Bu bilgiler, e-posta iletisinin içeriğinden ve niteliğinden Kurum'un sorumlu tutulamayacağı gibi açıklamalar içermelidir.

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

c. Gizli ve hassas bilgi içeren elektronik postalar kriptolanarak iletilmelidir.

d. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

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

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

g. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

h. Elektronik postaların sık sık gözden geçirilmesi, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmaması ve bilgisayardaki kişisel klasöre (personel folder) çekilmelidir

i. 6 ay süreyle hiç kullanılmamış e-posta adresleri kullanıcıya haber vermeden kapatılabilir.

8.7. Veri Tabanı Güvenliğini Sağlamaya Yönelik Tedbirler

Bilgi yönetim sisteminde kritik verilere ve tıbbi bilgilere ait değiştirme, düzeltme, silme, erişim işlemleri (veri tabanı ya da tablolarda sisteme giriş yapan kullanıcılar, gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalara ilişkin iz kayıtları) bir noktada loglanır.

Bu loglar veri tabanı içinde güvenli olarak kayıt altına alınmakta ve salt okunur bir şekilde saklanır.

Log kayıtlarına HBYS ve Bilgi İşlem Sorumluları izni olmadan kesinlikle hiçbir şekilde erişilemez, ihtiyaç durumunda HBYS ve Bilgi İşlem Sorumluları tarafından ancak hastane yönetimi onayı ile loglanan bilgilere ulaşılır.

Bilgi sisteminde veri tabanı sistem logları, gerektiğinde veya acil durumlarda izlenebilmek amacıyla 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"a uygun şekilde saklanır. Loglanan tüm bilgilerin geçmişe dönük olarak takibi yapılabilir.

Kullanıcıların arayüze bağlanmak için kullandıkları parolalar şifreli bir şekilde saklanmaktadır.

Veri tabanının güvenlik açıkları ve ihlalleri Bilgi İşlem Sorumluları tarafından tespit edilir ve tespit edilen açıklar, yazılım firmasına iletilerek çözümü sağlanır. Problemlerin çözümünden sonra güvenlik açıklarının ve ihlallerin giderilip giderilmediği Bilgi İşlem Sorumluları tarafından yapılan kontrol testleri ile teyit edilir.

HBYS Uygulama ve İşletim Hizmetleri'nde veri tabanı ile ilgili sorumlu kişilerin iletişim bilgileri bulunur. Veri tabanı ile ilgili sorumlu kişilerin iletişim bilgileri "Veri Tabanı İletişim Bilgi Formu"nda belirtilmiştir.

Veri tabanı üzerinde iz kaydı alınması gereken işlemler belirlenerek veri tabanında iz kaydı alınan işlemler listesi ile kayıt altına alınmıştır.

Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulur ve sonrasında ilgili uygulama kontrolleri gerçekleştirilir. Kullanıcılar veri tabanına yapılacak müdahale öncesinde, gerekli görülmesi durumunda hastane yönetiminin belirlediği zaman diliminde ile tüm client PC lere bilgi iletilir.

8.8. Kablosuz Erişim

Erişim Cihazları (Access Point) ve Kartların Kayıt Olunması Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ 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 ağına erişebilmelidir.

9. BİLGİ TEKNOLOJİLERİ İMHA YÖNETİMİ

HBYS Uygulama ve İşletim Hizmetleri yönetiminde olan cihaz ve ekipmanların arıza vb. durumlar sebebiyle kullanım dışı kalması durumunda ilgili cihaz ve ekipmanlar imha edilmez, garanti kapsamında anlaşmalı firmalara iade edilir ve firmalar tarafından değişimleri yapılır.

Topraklık Ağız ve Diş Sağlığı Merkezi 'nde HBYS Uygulama ve İşletim Hizmetleri bünyesindeki bilgi saklama ortamlarının nasıl yok edileceğini "**TAŞINABİLİR ORTAM CİHAZ İMHA FORMU**'' da belirtilmiştir.

İlgili Doküman

- **Personel Gizlilik Sözleşmesi (DBY.YD.002)**
- **HBYS iletişim bilgi formu (DBY.FR.002)**
- **Kurumsal gizlilik sözleşmesi (DBY.YD.003)**
- **Dış Ortamdan İç Ortama Erişim Formu (DBY.FR.008)**
- **HBYS Sunucu bilgi formu (DBY.FR.010)**
- **Isı Nem Takip Formu (SİY.FR.009)**
- **Yedekleme kontrol formu (DBY.FR.025)**

HAZIRLAYAN	KONTROL EDEN		ONAYLAYAN
BİLGİ İŞLEM SORUMLUSU	KALİTE YÖNETİM SORUMLUSU	BAŞHEKİM YARDIMCISI	BAŞHEKİM