1. AMAÇ: Bu talimatın amacı, hastalara ve tüm hastane çalışanlarına ait bilgilerin doğru olarak toplanmasını, depolanmasını, güvenliği sağlanmış bilgisayar sisteminde ve arşivlerde uygun koşullarda saklanmasını ve hastanenin bilgi güvenliğini sağlamaya yönelik düzenleme yaparak bilgi işlem ağındaki bilgilerin güvenliğini, gizliliğini, erişilebilirliğini ve kişisel mahremiyetinin korunması amacıyla standart kuralları belirlemektir.

2. KAPSAM: Bu talimat hastanemizde Bilgi İşlem Biriminin yürüttüğü tüm faaliyetlerde bilgilerinin güvenliğini ve korunmasını kapsar.

3. TANIMLAR:

HBYS: Hastane Bilgi Yönetim Sistemi

4. SORUMLULAR: Bu talimatın uygulanmasından bilgi işlem altyapısını kullanmakta olan tüm birimler, bilgi sistemlerine erişen tüm kullanıcılar ve Bilgi İşlem Birimi sorumludur.

5. FAALİYET AKIŞI

a- Hastanemizde bilgi güvenliği konusunda *gizlilik, bütünlük ve erişebilirlik* olmak üzere 3 temel prensip göz önünde bulundurulmaktadır. Bilgi güvenliğine yönelik gerekli tüm önlemler Bilgi İşlem Birimi tarafından alınır.

b- Hastanemizde bilgi yönetim sisteminin kesintisiz ve güvenli çalışabilmesi için Bilgi İşlem Birimi oluşturulmuştur. Bilgi İşlem Koordinatörü ekibin başkanıdır.

c- Bilgisayar uygulamalarında ve veri tabanı sunucularında donanım ve yazılıma ait problemler ortaya çıktığında, bilgi güvenliği ile ilgili acil bir durum oluştuğunda ve yerel / uzaktan sisteme bağlanarak çalışmaların devam ettirilmesi gerektiğinde Bilgi İşlem Koordinatörü durumdan haberdar edilir.

d- Hastanemizde bilgi yönetim sistemi ile ilgili olarak oluşan durumlara yönelik tüm kararlar Bilgi İşlem Koordinatörü tarafından alınır ve gerekli ise Bilgi İşlem Birimi durumdan haberdar edilir.

e- Hastanemiz bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kesinlikle kullanılmaz.

f- Hastanemize destek hizmeti veren firmaların dış ortamdan iç ortama hangi durumlarda erişim yapacağı hastanemiz ile firmalar arasında imzalanan ve her iki tarafın da onayladığı teknik şartname ve hizmet alım sözleşmelerine göre kayıt altına alınmıştır.

5.1. HASTALARIN VE ÇALIŞANLARIN KAYITLARININ GÜVENLİĞİ

a- Hastalara ve çalışanlara ait bilgilerin güvenliğinin sağlanması amacıyla öncelikle sisteme kayıt edilen veriler doğru olarak toplanır, depolanır ve bilgilerin kullanımına yönelik uygulamalar ve güvenlik önlemleri belirli periyotlarla gözden geçirilir.

b- Tüm hasta bilgilerinin girişi HBYS'de tanımlanan alanlara yapılmaktadır.

c- Kişisel verilerin depolandığı sistemler yetkisiz erişime karşı korunmaktadır.

d- Hasta ve çalışanların kişisel bilgilerine erişim, yetkilendirme İşleyişi doğrultusunda, sadece bilgilere ulaşma yetkisi bulunan hastane çalışanları ile sınırlı tutulur ve bu kişiler gizliliği koruma yükümlülüklerini bilerek çalışır. Hasta ve çalışanların bilgilerine yetkili olmayan kişilerin ulaşımına / kullanımına izin verilmez. Hasta bilgilerinin güvenliği için tüm kullanıcılara kendi yetkilerine göre her kademede yetkilendirme yapılmıştır. Hastane personeli ancak yetkilendirilmiş olduğu işlemleri gerçekleştirilebilir.

e- Hastanemizde hasta ile ilgili bilgilerin bütünlüğü ve güvenliği kurulmuş olan bilgisayar yazılım programlarında yetkilendirilmiş girişler ile korumaya alınmıştır.

f- Bilgi İşlem Birimi tarafından ilgili mevzuat hükümleri saklı kalmak kaydıyla, hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemektedir.

g- Elektronik ortamdaki verilerin güvenliği sağlanmaktadır.

5.2. İNTERNET ERİŞİM VE KULLANIMI

a- İnternet erişimi ve e-posta kullanım bağlantıları üniversitemizde bulunan güvenlik duvarı cihazı tarafından kontrol edilmektedir. İnternet kullanımında giriş yapılabilecek sayfalar ve internet uygulamaları güvenlik duvarı üzerinden yetkiye dayalı olarak belirlenmiştir.

b- Kişisel ve elektronik iletişimde üçüncü taraflarla yapılan bilgi alışverişinde kuruma ait bilgilerin gizli tutulması esastır**.**

c- Her bilgisayarın MAC adresleri güvenlik duvarı üzerine kaydedilmiş olup alacakları IP Adresleri sabitlenmiştir.

d- Her bilgisayarın internet kullanımı loglama yazılımı ile kayıt altına alınmaktadır.

5.3. ŞİFRE KULLANIMI

a- Hastanemizin bütün sistem seviyeli şifreleri (örnek, root, administrator, admin, vs) gerek duyulduğunda değiştirilmektedir.

b- Sistem yöneticileri her sistem için farklı şifreler kullanmakta; şifreler asla e-posta iletilerine veya herhangi bir elektronik forma eklenmemektedir.

c- Üst yönetimin gerek gördüğü hallerde kullanıcıların HBYS üzerindeki tüm yetkilendirmeleri yeniden düzenlenebilir.

d- Her yetkili kullanıcı kendi şifresi ile işlem yapar. Başkalarına şifresini söylemez, görünür/ ulaşılabilir alanlara (kâğıtlara ya da elektronik ortamlara yazmaması) yazılı olarak bırakılmaması tavsiye edilir. Başka bir kişinin kullanıcı kimliği, parola veya diğer güvenlik kodları bir başkası tarafından kullanılmamalıdır.

e- Kullanıcı yetkisi olan çalışanlar, bilgisayar kullanımı bitince, odadan ayrılırken, mesai ve nöbet bitiminde şifresini kapatır. Kişinin çalışmadığı veya bulunmadığı zamanlarda şifresi kullanılarak yapılan işlemlerden şifre sahibi sorumludur.

f- Kullanıcılar, herkesin kendi kişisel şifresini başkasıyla paylaşmaması, paylaşmaları durumunda yükümlükleri, görünür/ulaşılabilir alanlara (kâğıtlara ya da elektronik ortamlara yazmaması) yazılı olarak bırakmamaları, kullanıcı adı ve kodunun çalışanlara yüklemiş olduğu sorumluluklar konusunda eğitilmektedir.

5.4. UZAKTAN VE KABLOLU ERİŞİM

a- Sisteme erişim kontrolü Bilgi İşlem Koordinatörü tarafından kişilerin yetki ve sorumlulukları dikkate alınarak düzenlenir. Bu şartlar uzaktan erişim için de geçerlidir. Sistemde herhangi bir arıza durumunda yazılım firmaları ve Bilgi İşlem Personelleri tarafından uzaktan bakım için bağlantı hakkı 6 aylık süreler için verilir. Bu bağlantı VPN ve Proxy yazılımları ile yapılır.

b- Sisteme erişim ve yetkilendirme Üniversite tarafından belirlenmiş uzaktan erişim esaslarına göre düzenlenir.

c- Bilgi İşlem Koordinatörü bilgisi dışında "Active Directory" sistemine dâhil olan bilgisayarlar üzerindeki ağ ayarlarında, kullanıcı tanımlarında, kaynak profillerinde vb. uygulamalar üzerinde mevcut yapılan düzenlemeler hiçbir suretle değiştirilemez.

d- Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulamaz ve kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilmemesi esastır.

5.5. VİRÜS VE ZARARLI YAZILIMLARDAN KORUNMA

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

b- Hastanemizde sorumlular tarafından virüs ve saldırılardan korunma için gerekli donanım ve yazılım üst yönetime bildirilerek güvenlik duvarı, kullanıcı yetkileri vb. gerekli tedbirler alınmaktadır.

c- Bu tedbirler, anti virüs yazılımları ve güvenlik duvarı gibi donanımsal ve yazılımsal uygulamaları içeren Üniversitemizce istenen asgari şartlardan oluşur.

d- Bu yazılımların güncellenmesini zamanında gerçekleştirmek de Bilgi İşlem Biriminin sorumluluğundadır. Güncellenme zamanlarında üst yönetim konu ile ilgili bilgilendirilir.

5.6. DÜZELTİCİ ÖNLEYİCİ FAALİYETLERİN PLANLANMASI

a- Bilgi güvenliği ihlalleri raporlanır ve Bilgi İşlem Birimine bildirilir ve bu ihlalleri engelleyecek önlemler alınır.

b- Yaşanan acil durumlar sonrası işleyiş ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmektedir.

6. İLGİLİ DOKÜMANLAR