1.AMAÇ: Kurumun otomasyon üzerindeki tüm bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kuralları ve uygulamaları belirlemeyi amaçlar.

2.**KAPSAM**: Bu talimat, kurum Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

3.TANIMLAR: HBYS; Hastane bilgi yönetim sistemi

4. İŞLEM:

4.1. Bilgi işlem merkezi bünyesinde Yazılım-donanım destek birimi bulunur. Yazılım- donanım destek birimi 24 saat kesintisiz hizmet sunar. Yazılım - donanım destek birimi çalışanlarının güncel iletişim bilgileri santralde bulunur.

4.2. 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. HBYS de Hasta Kayıt, Yatış, Poliklinik, Klinik, Eczane, Depo, Satınalma, Ayniyat, Laboratuvar, Vezne, Faturalandırma, Radyoloji, Mutemetlik, Personel modülü ve diğer modüller bulunur.

4.3. Bölümlerin malzeme ve demirbaş istemlerinin yapılması, onaylanması, satın alınması, depoya teslim edilmesi, bölümler tarafından teslim alınması HBYS üzerinden gerçekleştirilir.

4.4. Personel bilgi modülünde çalışanların; fotoğrafı, çalıştığı bölüm, kan grubu, iletişim bilgileri, izin ve rapor bilgileri, eğitim durumu, sertifikaları, hizmet içi eğitimleri, yabancı dil bilgisi güncel olarak yer alır.

4.5. Tüm bilgisayarların donanım ve yazılımlarının güncel envanteri oluşturulur. Envanterde; Bulunduğu bölüm, marka, model, seri no, demirbaş numarası, donanım ve yazılım adı, İşletim sistemi, ek aksamlar, alınma tarihi, varsa garanti süresi bulunur.

4.6. Hastanemizde bilgi güvenliğini sağlamaya yönelik olarak aşağıdaki uygulamalar yapılmaktadır;

4.6.1. Hasta bilgilerinin girişi HBYS' de tanımlanan alanlara yapılmaktadır.

4.6.2. Hasta bilgilerinin güvenliği için, tüm kullanıcılara her kademede yetkilendirme yapılır ve kontrol edilir. Çalışanlar yetki düzeyleri ile ilgili olarak bilgilendirilir.

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

4.6.4. Sunucu üzerindeki her türlü yazılım, işletim sistemi, veritabanı, Yazılım Firması elemanları Tarafından Bilgi İşlem Bölümü denetiminde yapılır.

4.6.5. Tüm modem üniteleri ile haberleşme ve İnternet erişim yazılımlarının kurulması ve Ayarları Hastane Bilgi İşlem Bölümünün yetkisinde olur.

4.6.6. Veri yedekleme işlemi bilgi işlem işletimini yapan HBYS Sistem Destek Elemanlarınca online bağlanılarak yapılır. Firma elemanı her gün yedekleme alıp yedeklenen verileri kendi üzerinde bulunan başka bir diske ve hastanede başka bir odada bulunan yedek bilgisayar üzerine yedekleme işlemini yapar. Bu bilgilere Bilgi İşlem Sorumlusu ve HBYS Sistem Destek Elemanları ulaşabilir.

4.6.7. Hastalarımıza ait bilgilerin güvenliği açısından hastanemiz sistem ve internet altyapısı en güvenilir seviyede tutularak gerekli önlemler alınır.

4.6.8. Kişilere ait bilgilerin güvenliğinin sağlanması için öncelikle verilerin doğru olarak toplanması, depolanması ve kullanılmasına ilişkin uygulamalarımızın ve güvenlik önlemlerimizin dâhili olarak gözden geçirilmesi ve kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemlerinin alınmasını içerir.

4.6.9. Kişisel bilgilere erişim hizmetlerimizi işletmek, geliştirmek ve iyileştirmek için onları bilmeleri gereken hastane çalışanları, yüklenicileri ve aracılarıyla sınırlı tutulur. Bu bireyler gizliliği koruma yükümlülükleri altında çalışırlar.

4.6.10. Hastanemizde hasta ile ilgili bilgilerin bütünlüğü ve güvenliği kurulmuş olan bilgisayar yazılım programlarında yetkilendirilmiş girişler ile korumaya alınmıştır. Elektronik ortamdaki verilerin güvenliği sağlanmaktadır. Hasta bilgilerine yetkili olmayan kişilerin ulaşımına / kullanımına izin verilmez.

4.6.11. Hastanemizde internet erişimi ve kullanımı Başhekim tarafından onay verilen Bilgisayarlarda kullanılmaktadır. Bunun haricinde tüm pc lerden resmi sitelere erişim sağlanmaktadır. E-posta kullanımı sadece yetkili personeller resmi e-postaları kullanabilirler. İnternet erişimi ve e-posta kullanım bağlantıları Genel Sekreterliğimizde bulunan firewall cihazı tarafından kontrol edilmektedir.

4.6.12. Her yetkili kullanıcı kendi şifresi ile işlem yapar. Başkalarına şifresini söylemez, görünür, ulaşılabilir alanlara yazılı olarak bırakılmaz. Güvenli bir bilgi sistemine erişmek için yetkisiz bir kullanıcıdan yardım istenmez.

4.6.13. Başka bir kişinin kullanıcı kimliği, parola veya diğer güvenlik kodları kullanılmamalıdır.

4.6.14. Çalışanlar gizliliği koruma yükümlülükleri altında çalışırlar

4.6.15. Kullanıcı yetkisi olan yetkili çalışanlar, bilgisayar kullanımı bitince, odadan ayrıldığında, mesai ve nöbet bitiminde şifresini kapatmalıdır. Kişinin çalışmadığı veya bulunmadığı zamanlarda şifresi kullanılarak yapılan işlemlerden kurum sorumlu değildir.

4.6.16. Sisteme erişim kontrolü ilgili başhekim yardımcısı ve bilgi işlem sorumlusu tarafından kişilerin yetki ve sorumlulukları dikkate alınarak düzenlenir. Bu şartlar uzaktan erişim içinde geçerlidir. Sistemde herhangi bir arıza durumunda HBYS firması tarafından uzaktan bakım için bağlantı verilir. Bu bağlantı ekstra programlar aracığı ile yapılır ve her bağlantıdan sonra program kapatılır.

4.6.17. Sisteme erişim ve yetkilendirme sağlık bakanlığı tarafından belirlenmiş olan esaslara göre düzenlenir.

4.6.18. Birimden sorumlu başhekim yardımcısı ve ilgili teknik personelin bilgisi dışında bilgisayarlar
üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb üzerinde mevcut yapılan düzenlemelerin hiçbir suretle değiştirilemez.

4.6.19. Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulamaz

4.6.20. Bakanlığın bilgi güvenliği politikası gereği çalışmalar yürütülmektedir.

4.6.21. Virüs ve saldırganlardan korunma sorumluluğu ilgili başhekim yardımcısı 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.

4.6.22. Hastanemizde bilgi güvenliğinden sorumlu bir ekip oluşturulmuştur. Hastane üst yönetiminden Başhekim Yardımcısı ekibe başkanlık eder. Müdür Yardımcısı, Bilgi işlem Sorumlusu, Kalite Yönetim Direktörü ve Bilgi İşlem Teknik Elemanı bu ekibin üyeleridir. Ekip; Bilgi güvenliği ile ilgili mevcut durumu tespit etmekle, bilgi güvenliği için olası riskleri belirlemekle, tanımlı kullanıcılar için yapılan yetki değişikliklerini izlemekle, gerektiğinde düzeltici önleyici faaliyet

4.7. Sunucu odalarının güvenliği sağlanması için;

4.7.1. Sadece sunuculara tahsis edilmiş bağımsız bir oda mevcuttur.

4.7.2. Sunucu odasına yetkisiz personelin girişi engellenmiştir.

4.7.3. Suya karşı yalıtım yapılmış, alttan ve üstten su akmalarına karşı gerekli önlemler alınmıştır.

4.7.4. Hastanedeki diğer kesintisiz güç kaynaklarından bağımsız bir kesintisiz güç kaynağına bağlanmıştır.

4.7.5. Oda ısı takipleri günlük olarak yapılır. Sıcaklığın 18-22 °C; nemin % 30 - % 50 arasında olmasına dikkat edilir.

4.7.6. Hastane merkezi klima sistemi dışında yedekli klima sistemiyle odanın iklimlendirilmesi sağlanır.

4.8. 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 yapılır.

4.9. Veritabanı güvenliğini sağlamaya yönelik tedbirler alınır. Veritabanı sistem logları tutulur ve gerektiğinde idare tarafından izlenebilir. Veritabanı ile ilgili sorumlu kişilerin iletişim bilgileri santralde ve birimde bulunmaktadır. Kullanıcıların ara yüze bağlanmak için kullandıkları şifreler şifreli bir şekilde saklanmaktadır. Veritabanı üzerinde tüm işlemler loglanır. Kullanıcılar veritabanına yapılacak müdahale (yama ve güncelleme vb.) öncesinde bilgilendirilir.

4.10. Hastaneye destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında hastane tarafından onaylanmış gizlilik sözleşmesi mevcuttur. Dış ortamdan iç ortama yapılan erişimler kayıt altına alınır.

4.11. Yedeklemeler aracılığı ile yılda bir kez veri kurtarma testi uygulanır, Yedeklemeden geri dönüşün sağlanıp sağlanmadığı ve veri kaybının olup olmadığı kontrol edilir, Test kayıt altına alınır, gerektiğinde düzeltici önleyici faaliyet başlatılır.

4.12. HBYS üzerinde yapılan işlemler izlenebilir niteliktedir. Salt okunur özellikte ayrı bir veritabanı ya da tablo mevcuttur. Veritabanı ya da tablolarda sisteme giriş yapan kullanıcılar, gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalar ile ilgili veriler kayıt altına alınır. Veritabanı ya da tablolara sadece bilgi sisteminde yönetici olarak yetkilendirilmiş kişiler ulaşabilir.

4.13. HBYS' de oluşan sorunların çözümüne yönelik 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.SORUMLULAR: Bu talimatın uygulanmasından Bilgi İşlemden Sorumlu Başhekim Yardımcısı, Müdür Yardımcısı, Bilgi İşlem Sorumlusu, Bilgi İşlem Çalışanları, HBYS Sistem Destek Elemanları ve hastanedeki tüm kullanıcılar sorumludur.

6-EKLER:

BİLGİ GÜVENLİĞİ POLİTİKAMIZ

- Hastalarımız ve çalışanlarımıza ait kişisel bilgilerinin güvenliği açısından Hastanemiz internet ve sistem altyapısını en güvenilir seviyede tutmak.
- Hastalarımıza ait sağlık bilgilerine yetkili olmayan kişilerin erişimini engellemek.
- Hastanemiz söz konusu bilgileri, hastaların ve çalışanların onayı olmaksızın yasal bir yükümlülük bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ve kuruluş ile paylaşmamak.
- Hastalarımız ve çalışanlarımızın şahsi yazılı istekleri dahilinde istenen bilgi ve belgelere ulaşmasını sağlamak.