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. Sorumlular:
3.1. Bilgi İşlem Sorumlusu

4. Uygulama:
4.1 **Sunucuların güvenliği**
4.1.1.Sadece sunuculara tahsis edilmiş bağımsız bir oda mevcuttur.
4.1.2.Sunucu odasına yetkisiz personel girişi engellenmiştir.
4.1.3.Hastanedeki diğer kesintisiz güç kaynaklarından bağımsız bir kesintisiz güç kaynağına bağlanmıştır.
4.1.4.Oda ısı takibi günlük olarak yapılır. sıcaklığın 18-22 ^{O}C ;nemin % 30-% 60 arasında olmasına dikkat edilir.
4.1.5.Hastane merkezi klima sistemi dışında yedekli klima sistemiyle odanın iklimlendirilmesi sağlanır.
4.2.Kurumda bulunan bütün sunucuların kayıtları tutulur.Bu kayıtlarda:sunucunun yeri,sorumlu kişisi,donanım,işletim üzerinde çalışan uygulama bilgileri yer alır. Sunucu üzeride çalışan işletim sistemleri, hizmet sunucu yazılımları ve anti virüs gibi koruma amaçlı yazılımların güncel olmalarına dikkat edilir.sunucuların yazılım ve donanım bakımları uygun sürelerde yapılır.

5. Veri Yedekleme:
5.1. Veri yedekleme işlemi Bilgi İşlem Sorumlusu tarafından yapılacaktır.
5.2. Bilgi İşlem Sorumlusu her gün akşam yedekleme alıp harici hard diske kaydeder.
5.3. Burada yedeklenen bir haftalık veriler haftanın son günü USB HDD ye kaydedilerek Hastane Müdürüne teslim edilir.

6.Kişisel Sağlık Kayıtların güvenliği:
6.1.Hastalarımıza ait bilgilerin güvenliği açısından hastanemiz sistem ve internet altyapısı en güvenilir seviyede tutularak gerekli önlemler alınır.
6.2.Kişilere ait bilgilerinin güvenliğinin sağlanması için öncelikle verilerin doğru olarak toplanması, depolanması ve kullanılmasına ilişkin uygulamalarımızın ve güvenlik önlemlerimizin dahili olarak gözden geçirilmesi ve kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemlerin alınmasını içerir.
6.3.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 çalışılırlar.
6.4.Hastanemizde hasta ile ilgili bilgilerin bütünlüğü ve güvenliği kurulmuş olan bilgisayar yazılım programlarında yetkilendirilmiş girişler ile korunmaya alınmıştır. Elektronik ortamdaki verilerin güvenliği sağlanmaktadır. Hasta bilgilerine yetkili olmayan kişilerin ulaşımına/kullanımına izin verilmez.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Bilgi İşlem Sorumlusu	Kalite Yönetim Direktörü	Hastane Müdürü

7.İnternet erişimi ve kullanımı

7.1.Hastanemizde internet erişimi ve kullanımı Hastane yönetimi tarafından onay verilen bilgisayarlarda kullanılmaktadır.

8.E.posta kullanımı

8.1.E-Posta kullanımı sadece idari personeller resmi e-postaları kullanabilirler internet erişimi ve e-posta kullanım bağlantıları hastanemizde bulunan Firewall cihazı tarafından kontrol edilmektedir.

9.Şifre kullanımı

9.1.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.
9.2.Başka bir kişinin kullanıcı kimliği,parola veya diğer kodları kullanılmamalıdır.
9.3.Çalışanlar gizliliği koruma yükümlülükleri altında çalışırlar.
9.4.Kullanıcı yetkisi olan yetkili çalışanlar.bilgisayar kullanımı bitince,odadan ayrıldığında,mesai ve nöbet bitiminde şifresini kapatmalıdır.Kişinin çalışmadığı ve bulunmadığı zamanlarda şifresi kullanılarak yapılan işlemlerden kurum sorumlu değildir.

10.Uzaktan erişim

10.1.Anti virüs programının yüklenmesi
10.2.Friwall/ Güvenlik duvarı donanım / Yazılımlarının kullanılması
10.3.Hesap şifrelerinin yüksek güvenlikli olması/ En az 8-10 Karakter olması
10.4.Şüpheli e-postaların,reklam ilan sayfalarını açılmaması.şüpheli bağlantıların ziyaret edilmemesi.

11.Kablosuz erişim

11.1.Modeme kablosuz bağlantı koyma .
11.2.Bilgisayar ile ADSL arasındaki iletişim şifrelenmesi.(WPA/WPA2)
11.3.Güvenlik duvarının aktif hale getirilmesi.
11.4.IP adres filtrelenmesi.
11.5.Gereksiz servislerin kapatılması

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Bilgi İşlem Sorumlusu	Kalite Yönetim Direktörü	Hastane Müdürü