**1. AMAÇ:**

Bilgi yönetim sistemi kurum politikasına tüm çalışanları katmaktır.

**2. KAPSAM:** Bu talimat, SAÜ Diş Hekimliği Fakültesi Ağız ve Diş Sağlığı Merkezi Bilgi Yönetim Sistemi Politikası’na ait süreçleri kapsar.

**3.SORUMLULAR:** Bu talimatın uygulanmasından Ağız ve Diş Sağlığı Merkezi’nde çalışan tüm Otomasyon Sistemi kullanıcıları ve Otomasyon Bilgi İşlem Birimi, denetiminden ise Otomasyon Bilgi İşlem Birimi ve Başhekim sorumludur.

**4.1 BİLGİ YÖNETİM SİSTEMİ POLİTİKAMIZ**

1. Kurumumuz; teşhis ve tedavi hizmetlerinin sunumunda, hasta ihtiyaç ve beklentilerinin karşılanmasına yasal mevzuatlar doğrultusunda cevap vermekten sorumludur. Bu sorumluluk kapsamında Sağlık bakanlığı tarafından gizliliğin öneminin bilinci ile ilgili bilgi güvenliği politikaları oluşturulmuştur. Kurumumuz Sağlık bakanlığı tarafından oluşturulan bu politikalar doğrultusunda bilgi güvenliğini sağlamaktadır.
2. Kurumumuza teşhis ve tedavi için başvuran tüm hastalardan kayıtlar için gerekli kişisel bilgiler istenir. Bunlar; adı soyadı, hastalık bilgileri, T.C Kimlik numarası, adres, telefon bilgileri ve benzeri bilgilerdir.
3. Kurumumuza teşhis ve tedavi için başvuran hastalardan toplanan tüm bu bilgileri içeren verilerin güvenliği ile ilgili üç temel prensip söz konusudur. Bunlar;
* Gizlilik
* Bütünlük
* Erişilebilirliktir.
1. Sağlık kayıt bilgileri hastaya aittir. Bu bilgilere üçüncü taraflar veya yetkisi olmayan kişilerin ulaşabilmesi ve bilgilerin amaçları dışında kullanımını engelleyecek uygulamalar geliştirilir. Bu uygulamalar;
* Kurumuzda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmıştır.
* Yetkilendirilmiş çalışanlar ancak kendilerine kayıtlı hastaların bilgilerine ulaşabilir.
* Verilerin yetkisiz şekilde değiştirilmelerine, açıklanmalarına veya imha edilmelerine karşı korumak için gerekli dahili güvenlik önlemleri ile kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemleri alınmıştır.
* Hastalarla ilgili her türlü kaydın kim tarafından, hangi tarihte girildiği, ulaşma, değiştirme, silme bilgisi kurum bilgi işlem programında kayıt altında tutulmaktadır.
* Hiçbir hasta kaydı elektronik veya basılı ortamda (Sağlık Bakanlığının bu konularda çıkardığı genelgeler hariç) hiçbir kuruma veya üçüncü şahıslara sözlü veya yazılı olarak teslim edilmez.
* Hasta dosyaları üçüncü kişilerin ulaşabileceği ortamda bırakılmaz, bilgisayar ekranları bilgileri başkalarının okuyabileceği şekilde bırakılmaz.
* Hasta ile ilgili mahrem bilgiler üçüncü kişilere telefonla verilmez.
* Hastaların ismi ve kendileri tarif edilerek yapılacak bilgi paylaşımları genel ortamlarda ve başkalarının bulunduğu alanlarda yapılmaz.
* Bütün hasta kayıtları kurum arşivinde güvenli bir şekilde saklanır ve korunur.
* Elektronik hasta kayıtlarına internet ortamında ulaşılabilmesi engellenmiştir.

**5. YÖNETİM SÜREÇLERİ**

* 1. **Disiplinler arası Yetkilendirme:**

Disiplinler arası yetkilendirme aşağıdaki gibidir:

**5.1.1**  **Başhekim:**Kurumdaki tüm bilgilere ulaşır.

**5.1.2 Dişhekimi:**Kendi hastalarına ait tedavi ile ilgili bilgilerin tümüne erişebilir. Elektronik ortamda kayıtlı olması gereken hastaya ait tüm bilgileri girebilir. Onaylanmadan önce kendilerine ait raporlar üzerinde silme ve değişiklik yapabilir.

**5.1.3 Müdür:** İdari ve mali işlemlerle ilgili tüm bilgilere erişebilir.

**5.1.4 Fatura Birimi:** Ay içerisinde başvuran tüm hastaların faturalamasını ve anlaşmalı kurumlara teslimatı yapar. Başhekim ve İdari ve Mali İşler Müdürü kurumlara yapılan faturaların tutarlarını ve yapılan işlemleri görebilir inceleyebilir.

**5.1.5 Hemşire ve Diş Klink Yrd. :** Birimindeki Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Kendilerinin girmiş oldukları işlemleri Silme ve değiştirme yetkileri vardır. Kendi işlerine ait laboratuvar ve  hasta bilgilerini, hastaya ait sarf ve işlem girişlerini yetkileri dahilinde yapabilirler.

**5.1.6 Laboratuar:** Doktorların hastaları için, yaptığı protez istemlerini alır, işlemlerin otomasyon üzerinden takibini yapar. Bu işlemler barkotlu sistem ile çalışır.

**5.1.7 Veri Giriş Personeli:** Hatalı yaptığı işlemleri sorumlularına bildirirler. Sorumluların düzeltemediği işlemleri Sorumlular Yazılım firmasına bildirir.

**5.1.8 Özlük Birimi:** Kadrolu personelin özlük bilgilerine ulaşabilir, mesai, izin, sevk, rotasyon gibi kadrolu personelin tüm işleyişini otomasyon üzerinden gerçekleştirir.

**5.1.9 Radyoloji:** Hastaların radyolojik işlemlerini yapar. Tetkik işlemlerinin sonuçlarını otomasyon üzerinden kliniklere gönderir.

**5.1.10 Hasta Kabul:** Hastaların gelişte otomasyon programına kayıtlarını yapar. Hastaları kliniklere sevk eder.

**5.1.11. Yazılım Firması Çalışanları:**

* **Yazılım Kurma ve Silme İşlemleri:**

Ağız ve Diş Sağlığı Merkezi bünyesinde kullanılma kararı alınmış otomasyon sistemi dahilinde ki her türlü yazılımın kurma, silme ve düzenleme işlemleri ile işletim sistemi ayarlarının yapılması ve değiştirilmesi Yazılım firması yetkisindedir. Yazılım firması bilgisi dışında herhangi bir yazılım kurma ve silme işlemi ve işletim sistemi ayarları yetkilendirilmemiş bir işlem olarak değerlendirilecektir ve tamamen ilgili cihazın kullanıcısının sorumluluğundadır.

* **Otomasyon sistemi İşlemleri:**

Bilgi yönetim sistemi işlemleri, Yazılım firmasının onayladığı şartlar kapsamında saptanan çalışanın yetkisinde olacaktır. Verilen standart yetkiler dışında istenilen bir yetki, bağlı bulunduğu yöneticinin onayından sonra, uygun görüldüğü seviyede Yazılım firması tarafından verilir.

* **Bilgi Sistemleri Yöneticisine Açık Bilgi Yönetim Sistemi İşlemleri:**
* Aşağıda belirtilen ve otomasyon sistemi üzerinde normal kullanıcı şifreleri ile yapılamayan işlemler Yazılım firmasının yetkisinde olacaktır. Bu işlemlerin yapılabilmesi için gereken şifreler Yazılım firması tarafından verilecek ve gerektiğinde değiştirilecektir.
* Otomasyon sistemi üzerinde rutin kullanım yolları ile ancak yanlış olarak girilmiş ve aynı yollarla değiştirilmesi mümkün olmayan bilgilerin düzeltilmesi.
* Doğru olarak girilmekle beraber kullanıcıların kontrolü dışında yanlış sonuçlar doğuran ve aynı yollarla değiştirilmesi mümkün olmayan bilgilerin düzeltilmesi.
* Yetkilendirmeye uygun olmayan bilgi sistemi işlemlerinin hangi operatörler tarafından ve ne zaman yapıldığının sistem kayıtlarından açığa çıkarılması Yazılım firması bünyesinde çözülmektedir.

* **Üst Yönetime Açık Bilgi Yönetim Sistemi İşlemleri:**

Üst Yönetiminin kurum planlaması, tıbbi, işletme, mali değerlendirmeler ve benzeri amaçlar ile otomasyon sistemi üzerinden alacakları raporlar Yazılım firması tarafından yapılır.

**6. HBYS'YE İLİŞKİN YAZIMSAL SÜREÇLER**

**6.1.Yazımsal Süreçler:**

* Kurum çalışanları yaptıkları işle ilgili düzeltme, güncelleme, değişiklik gibi işlemleri bilgi işlem personeline iletir.
* Bilgi işlem personeli kullanıcı ile birlikte sorunu tespit eder ve yazılımsal değişikliğe gerek olan durum varsa yazılım şirketine ait olan internet ortamındaki istek bilgilerini sisteme yazılımsal isteği kaydeder.
* Yazılım şirketi isteği değerlendirip 48 saat içerisinde planlamaya alır. Planlamaya alınan istekler bilgi işlem sorumlusu tarafından kritik derecesi belirlenir. İsteklerin kritik derecesi;

**ÇOK KRİTİK:** 3 iş günü içerisinde (Y eni çıkan tebliğ, yönetmelik güncellemeleri)

**KRİTİK:** 5 iş gün içerisinde (Bir bölümün işletmesini aksatacak istekler)

**NORMAL:** 30 iş günü içerisinde herhangi bir işleve etki etmeyecek, yazılımda düzeltme yapılacak istekler.

* İstekler yukarıda belirtilen süreler dışına çıkmış ise sözleşmesinde belirtilen cezai işlemler devreye girer.
* Normal sürelerde yapılan istekler ise bilgi işlem sorumlusu ve isteği yapan kullanıcı tarafından onaylanarak, sistem üzerinden kapatılır.

**6.2.Sorunların Çözümü**

* Kurum iç hat telefon numarası EBYS üzerinden arza istek ve değişiklik formu doldurularak bilgi işlem servisi çalışanlarıyla irtibat kurulur.
* İlgili sorun çözüldüğünde çözen bilgi işlem personeli tarafından EBYS kayıt edilir

 **7. SİSTEM ALT YAPISINA İLİŞKİN SÜREÇLER:**

 **7.1. Network Donanım Cihazlarının;**

* Ana  omurgayı  (Merkez Switch)  taşıyan cihazın, değişen  şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.
* Ağ cihaz ve yazılımlarını kurar, internet ve intranet bağlantılarını yönetir.
* Kenar switch cihazlarının, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.
* Routerların, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.
* Güvenlik cihazlarının, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.
* Kablolu (ADSL, GSHDSL, Metro Ethernet) ve kablosuz iletişim cihazlarının (wireless cihazlar, Optik Laser Hat, Wimax..) iletişim cihazlarının yapılandırılmalarını, yönetimini gerçekleştirir.
* Bilgisayar sistemlerinin fiziksel güvenliğinin ötesinde yazılımsal güvenlini de sağlamak.
* Elektronik ortamda sisteme olabilecek saldırıları (virus, worm, rootkit, backdoor, trojan, hacker keyloger, spyware v.b.) engellemek,
* Sistem odasındaki cihazların bakım ve onarımlarını yapar/yaptırır.
* Tüm bilgisayar sisteminin sağlıklı çalışmasını sağlayan antivirus sunucularını, kurar, günceller, bakımını yapar, sistemin virüs saldırıları nedeni ile kesintiye uğramaması için tedbirler alır. Yeni çıkan virüslere yönelik güncelleştirmeleri sisteme yükler.
* Tüm bilgisayarların donanımsal ve yazılımsal arızalarını giderir. Son çıkan güncellemeleri takip eder ve kurum sistemindeki tüm bilgisayarlara yükler.

**7.2.İnternet Bağlantılarının;**

* Kurumun internet bağlantısını yönetir, izler yetkili kullanıcıların internete erişimine izin verir.
* Firewall  cihazının yönetimini  yapar, IP, port, yetkilendirmesi,  erişim kontrol listelerinin tanımlanmasını yapar VPN (sanal Özel Ağ) yapısını yönetir.
* Filtreleme cihazı aracılığı ile uygun olmayan içeriğe ulaşımı engeller, zararlı sitelerin kullanıcı bilgisayarlarını bozmasına engel olur. Yeni çıkan zararlı siteleri cihaz güncellemeleriyle engeller.
* İnternet kullanıcılarının kurum web sitesine ulaşmasını, Web Sunucusunun güvenli biçimde internet üzerinden internet yayını yapmasını sağlar.
* Elektronik posta sunucusunu kurar, işletir, kurum kullanıcılarının e-posta alıp göndermesini sağlar.
* Kurumsal   kullanıcıların   kendilerine verilen   yetkilendirmeler dâhilinde   sistem kaynaklarını kullanmasına izin verir.

**7.3.İşletim Sistemlerinin;**

* Yazılım güncelleştirmelerini, yamalarını, loglarını, performanslarını izlerler.
* İşletim sistemlerinin yapılandırma/konfigürasyonlarını yaparlar.
* İşletim sistemlerinin güvenlik ayarlarını yaparlar.
* İşletim sistemlerinin üzerinde çalıştığı fiziksel sunucuların çalışma düzenini kontrol ederler.
* Donanım kaynaklarının (Diski, Ram, Kontrol Kartları, Güç Kaynakları, İşlemciler) çalışırlığını izler ve kontrol ederler.

 **7.4.Veritabanlarının;**

* Veri tabanın performansını izlerler.
* Veri tabanının bakımını gerçekleştirir.
* Yedeklerinin alınmasını sağlar ve/veya gerçekleştirirler.
* Yedek alma ve arşivleme işlemi depolama cihazlarını ve kotaları yönetir,
* İlgili sistemlerde bulunan verilerin yedeğini uygun periyotlar da alır.
* Programlar her veri güncellemesinde yedeklenir ve DVD medyada arşivlenir.
* Kullanıcı bilgisayarlarındaki verilerin merkezi olarak yedeklenmesi ve arşivlenmesi teknoloji olarak mümkün olmakla birlikte hali hazırdaki birim imkânları ile gerçekleştirilemediğinden kullanıcılara ait veri yedekleme işlemi kullanıcıların kendileri tarafından müdürlük yedekleme talimatına uygun olarak yapılmaktadır.
* Yedekleme cihazlarını izler,
* Yedekleri güvenli yerlerde saklar.

❖ Belirli aralıklarla veri arşivleme çalışması yapar. Güvenli yerlerde muhafaza eder.

 **7.5 Yazılım Geliştirme**

* Kurumsal kullanıcılardan gelen merkezimiz hizmetlerine yönelik yazılım taleplerini değerlendirmek
* Bilgi işlem müdürlüğünce onaylanan yazılım talepleri ile analiz çalışmalarını yapmak.
* Programın çalışması için gerekli kaynakları belirlemek ve sistem yönetimine müdürün onayı sonrasında bildirmek
* Yazılım geliştirme  platformu ve temel  yazılım geliştirme mimarisi belirlenir.(clien-server/web tabanlı,lokal,Windows vb.)
* Veri tabanı belirlenir. Yazılım geliştirme dili seçilir.
* Analiz çalışmalarına dayalı olarak temel fonksiyonların yazımı gerçekleştirilir, menülerin yazılımına başlanır.
* Programın yazılımı sonrasında çalışma testleri yapılır. Testler sonrasında çıkan bugler düzeltilir.
* Son kontroller sonrasında veri tabanındaki test verileri silinir,programı yönetecek kişi için kullanıcı tanımlamaları yapılır.Program devreye alınır.
* Programın devreye alınması sonrasında program kullanıcılarından gelen programla ilgili sorunlar giderilir, kullanıcılara teknik destek verilir.
* Programın görsel tasarımı kurumsal kimlik standartlarına uygun olarak tasarlanır.

 **7.6 Web Uygulamaları ve Web Tasarım Çalışmaları**

* Web uygulamaları geliştirme çalışmaları yapılır.

 **8. BİLGİ GÜVENLİĞİ UYGULAMALARIMIZ**

* Tüm hasta bilgilerinin girişi EBYS’ nde tanımlanan alanlara yapılmaktadır.
* Hasta bilgilerinin güvenliği için tüm kullanıcılar için her kademede yetkilendirme yapılmalı ve kontrol edilmelidir.
* Her kademedeki kurum personeli ancak yetkilendirilmiş olduğu işlemleri, diğer kurum prosedürlerine uygun olarak uygular.
* Sunucu üzerindeki her türlü yazılım, işletim sistemi, veritabanı, Yazılım Firması elemanları tarafından, Bilgi İşlem Bölümü denetiminde yapılır.
* Tüm fax-modem üniteleri ile haberleşme ve İnternet erişim yazılımlarının kurulması ve ayarları Bilgi İşlem Bölümünün yetkisinde olacaktır.
* Veri yedekleme işlemi bilgi işlem sorumlusu tarafından yapılmaktadır.
* Hastalarımıza ait bilgilerin güvenliği açısından kurumumuz sistem ve internet altyapısı en güvenilir seviyede tutularak gerekli önlemler alınmıştır.
* 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.
* Kişisel bilgilere erişim hizmetlerimizi işletmek, geliştirmek ve iyileştirmek için onları bilmeleri gereken kurum çalışanları, yüklenicileri ve aracılarıyla sınırlı tutulur. Bu bireyler gizliliği koruma yükümlülükleri altında çalışırlar.
* Kurumumuzda 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 verilmemektedir
* Kurumumuzda internet erişimi ve kullanımı Başhekim tarafından onay verilen bilgisayarlarda kullanılmaktadır. Bunun haricinde tüm bilgisayarlarda resmi sitelere erişim sağlanmaktadır. E-posta kullanımı sadece idari personeller resmi e-postaları kullanabilirler. İnternet erişimi ve e-posta kullanım bağlantıları kurumumuzda bulunan firewall cihazı tarafından kontrol edilmektedir.
* Her yetkili kullanıcı kendi şifresi ile işlem yapar. Başkalarına şifresini söylememeli görünür, ulaşılabilir alanlara yazılı olarak bırakılmamalıdır.
* Güvenli bir bilgi sistemine erişmek için yetkisiz bir kullanıcıdan yardım istenmemelidir.
* Başka bir kişinin kullanıcı kimliği, parola veya diğer güvenlik kodları kullanılmamalıdır.
* Çalışanlar gizliliği koruma yükümlülükleri altında çalışırlar.
* 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.
* 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 EBYS firması tarafından uzaktan bakım için bağlantı verilir. Bu bağlantı ekstra programlar aracığı ile yapılır ve her bağlantıdan sonra program kapatılır.
* Sisteme erişim ve yetkilendirme sağlık bakanlığı tarafından belirlenmiş olan esaslara göre düzenlenir (yöneticiler için bilgi güvenliği politikası).
* 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.
* Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulamaz.
* Bakanlığın bilgi güvenliği politikası gereği domain yapısı oluşturulmuş, tüm bilgisayarlar domain yapısına login durumda çalışmaktadır. Domaine bağlı olmayan bilgisayarlar Anti virüs programı ve Fortinet ile korumaya alınmış yerel ağdaki cihazlar arasında bilgi alışverişi yapılmaktadır.

**Virüs ve saldırganlardan korunma:**

 -Korunma sorumluluğu başhekim 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 ilgilileri sorumluluğundadır, zamanı geldiğinde üst yönetimin haberdar ederek güncellemeleri yaparlar.

|  |  |  |
| --- | --- | --- |
| **Hazırlayan Bilgi İşlem Birimi Sorumlusu** | **Kontrol Eden Kalite Yönetim Direktörü** | **Onaylayan Başhekim** |