**1. AMAÇ:**

Bu prosedürün amacı SAÜ Diş Hekimliği Fakültesi Uygulama ve Araştırma Merkezi’nin tüm birimlerinde çalışan ya da hastalara ait tıbbi ve kişisel bilgilerin doğru ve düzenli olarak toplanması, depolanması, değerlendirilmesi ve korunması, kayıtların mahremiyetinin sağlanması ile ilgili uyulması gereken kuralların ve bilgi güvenliğinin sağlanmasının tanımlanmasıdır.

**2. KAPSAM:**

Bu prosedür SAÜ Diş Hekimliği Fakültesi Uygulama ve Araştırma Merkezi’nin bütün birim ve çalışanları ile kurum bilgi işlem hizmetlerini yürüten firma sahibi, yetkilileri ve çalışanlarını kapsar.

**3. SORUMLULAR:**

Bu prosedürden sorumlu olanlar; Başhekim,, Bilgi İşlem Sorumlusu, Hizmet Satın Alınan Firma Yöneticisi, firma sorumluları, tüm bilgi işlem firma elemanları, Hastane Bilgi Yönetimi Sistemini kullanan tüm çalışanlardır.

**5. UYGULAMA**

 **1. SUNUCULARIN GÜVENLİĞİ**

* 1. Kurum bünyesindeki bütün sunucuların yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılacaktır.
	2. Kurumda bulunan bütün sunucuların kayıtları tutulmalıdır. Bu kayıtlar en az aşağıdaki bilgileri içermelidir;
	+ Sunucuların yeri,
	+ Sorumlu kişisi,
	+ Donanım,
	+ İşletim sistemi,
	+ İşletim sistemi üzerinde çalışan uygulama bilgileri.
	1. Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.
	2. Sunucu yedekleri talimata uygun olarak düzenli şekilde alınmalıdır.
	3. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse yama ve anti-virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır.
	4. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
	5. Sistem yöneticileri gerekli olmadığı durumlar dışında “Administrator”, “Root” gibi genel yönetici hesapları kullanılmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Gerekli olduğunda kendi hesapları ile log-on olup sonra genel yönetici hesabına geçiş yapılmalıdır.
	6. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
	7. Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır, yetkisiz girişler engellenmelidir.
	8. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
	9. Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar yapılmalıdır.

**1.12.** Sunucular güvenlik duvarının arkasında bulunur.

**2. YEDEKLEME**

Bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekir.

* 1. **Yedekleme Planı:**
* **Yedekleme sorumlulukları:** Yedekleme planının sahibi Bilgi İşlem Birim Sorumlusudur. Planı uygulamaktan sorumlu personel Bilgi İşlem Otomasyon Sorumlusudur. Bilgi İşlem Birim Sorumlusu yedekleme işlemlerinin politikaya uygun olarak gerçekleştirilmesinden, Bilgi İşlem Otomasyon Sorumlusu planda yazılı işlemlerin yerine getirilmesinden sorumludur.
* **Yedekleme işleri:**
	+ Her gün saat 12:00, 00:00 ve 02:00 olmak üzere 3 kez server tarafından otomatik olarak yedek alınır.

**3. KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ**Kurumumuzda kayıtlı olan hasta sağlık bilgisinin mahremiyeti hususunda uyulması gereken kuralları tanımlamaktadır. Hasta kaydı bilgisi kapsamına, hasta ile ilgili sözlü bilgi, yazılı bilgi, tıbbi müdahaleler, ön tanı, teşhisler, görüntüleme filmleri ve faturalama gibi bilgiler girmektedir.

* 1. **Genel Kurallar**

Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mali vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

* + Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir; bunlar veri gizliliğinin, değiştirilmediğinin (bütünlüğünün) ve erişilebilirliğinin sağlanmasıdır.
	+ Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.
	+ Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar (hastanın tedavisinden sorumlu sağlık personeli) ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidir. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilirler.
	+ Hasta dosyasının bir kopyası hastaya teslim edilebilir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir.
	+ Hastanın rızası olmadan hiçbir çalışan yazılı veya sözlü olarak hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.
	+ Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara ve kurumlara iletilemez Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.
	+ Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi.
	+ Telefonda konuşurken hastanın mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.
	+ Bütün hasta sağlık kayıtları (online bilgi veya yedek medya) fiziksel olarak korunmuş mekanlarda saklanmalıdır.
	+ Elektronik sağlık kayıtlarına internet ortamından erişim, ancak yetkilendirilmiş kullanıcılara güvenli erişim sağlandığında mümkün olabilir.
	+ Hasta sağlık bilgileri kurum tarafından veya Sağlık Bakanlığının Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir.
	+ Sağlık kayıt dosyalarının saklandığı kağıt veya elektronik medyalar (kartuş,CD,DVD, Flash disk, HDD, vb.) güvenli bir ortamda saklanmalıdır.
	+ Kurum, kritik bilgiye erişim hakkı olan çalışanlar ve firmalar ile gizlilik anlaşması imzalamalıdır.
	+ Yetkiler, "görevler ayrımı" ve "en az ayrıcalık' esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılması ile ilgilidir. Bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığını azaltılır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.
	+ Sağlık kayıt dosyalarına erişecek kurum çalışanları belirlenmiş olmalıdır. Bu çalışanlar dosyaların güvenliğinden ve her türlü hareketinden sorumlu olmalıdır.
	+ Sağlık kaydı arşivi en az 30 (Otuz) yıl süre ile saklanmalıdır.
	1. **Sistem Güvenliği**
* Kurum bünyesinde hasta tanımlayıcı olarak TC Kimlik numarası baz alınacaktır. Hastanın sağlık kaydına erişimde özel olarak atanan protokol numarası kullanılabilir.
* Bilgi siteminde güvenlik veriye erişim bazında olacaktır. Bunun için bu sistemin özellikle yazılım ve veritabanı erişim katmanlarında özel uygulamalar oluşturulacaktır.
* Gerektiğinde saat ve/veya gün bazında belirlenen bir süre için bazı kullanıcı ve istemci makinelerin sisteme oturum açmalarına kısıtlama getirilebilmelidir.
* Sadece yetkisi olan kullanıcılar için veri girişi ve/veya verinin elde edilmesi için erişim izni verilmelidir. Birçok kullanıcının veri tabanında sadece belirli bir veri setine erişim yetkisinin denetlenebilmesini sağlamak için çok katmanlı denetim mekanizmaları olmalıdır.
* Veri tabanında tutulacak verilerin tutarlılığı tam ve kesin bir şekilde sağlanmalıdır. Bunu sağlamak için en azından, veri onay (validation), çapraz sorgulama (cross-checking) ve mükerrer kayıt önleme gibi ölçütler uygulanmalıdır.
* Yönetimsel analizler yapmak için veri tabanındaki veriler bir yerden başka bir yere
aktarılırken, kayıtlarda bulunan kişisel kimlik tanımlayıcıları kayıtlardan çıkartılmalı ve analizler hasta ile hastalık bilgilerini eşleştirmeden yapılmalıdır.
* Kullanıcı aktiviteleri (yapılan tüm işlemler ve erişimler) izlenebilmelidir. Veri tabanı üzerinde yapılan şüpheli işler denetlenebilmelidir. Sistemin hem etkin bir şekilde yönetilmesi hem de yetkisiz erişimlerin engellenmesi ve izlenmesi anlamında gelişmiş bir kontrol mekanizması olmalıdır. Sistem, hangi kullanıcının sistemin hangi kısmına ne zaman ve nereden eriştiğine dair (zaman damgası-date stamp, işlem, kullanılan istemci bilgisayar tanımı gibi bilgileri de içeren) kayıt tutmalıdır.
* Firma, CD, kartuş, kağıt vb. ortamında Kuruma ilettiği bilgileri tutanakla teslim edecektir.
* Sertifika tabanlı kimlik doğrulama yapılamadığı durumlarda password ve hash tabanlı kimlik doğrulama yapılacaktır.
* Kurum ile başka ağlar arasındaki tüm haberleşme şifreli yapılmalıdır.

**4.İNTERNET ERİŞİM VE KULLANIMI**

Kurum içinde güvenli internet erişimi için sahip olması gereken standartları belirlemektedir. İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeden bu türden olumsuzluklara neden olunmaması; internetin kurallarına, etiğe ve yasalara uygun kullanılmasının sağlanmasını amaçlamaktadır. Bütün kullanıcılar ve Bilgi İşlem yöneticileri aşağıdaki internet erişim ve kullanım kurallarına uymalıdır.

* 1. Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkacaktır. Ağ güvenlik duvarı (fortigate), 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 sağlayabilmelidir.
	2. Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografik, oyun, kumar, şiddet içeren vs) yasaklanabilmelidir.
	3. Anti-virus gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik (smtp, pop3, ayrıca mümkünse http ve ftp vs) virüslere karşı taranmalıdır.
	4. Ancak Yetkilendirilmiş Sistem Yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir. Bunlar;[www, ftp, telnet](http://www.ftp.telnet), ping, traceroute vs.
	5. Hiçbir kullanıcı peer-to-peer bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örnek; KaZaA, iMesh, eDonkey2000, Gnutella, Napster, Aimster, Madster, FastTrack, Audiogalaxy, MFTP, eMule, Overnet, NeoModus, Direct Connect, Acquisition, BearShare! Gnucleus, GTK-Gnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, XoLoX, OpenNap, WinMX. v.b.)
	6. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ, MIRC, Messenger v.b. mesajlaşma ve sohbet programları gibi chat programları kullanılmamalıdır. Bu chat programları üzerinden dosya alışverişinde bulunulmamalıdır.
	7. Hiçbir kullanıcı internet üzerinden Multimedia Streaming yapamayacaktır.( Streaming media, ses, video ve diğer multimedia dosyalarının internette veya kurumsal internetlerde bilgisayara yüklemeden ve sabit disk içerisinde yer kaplamadan on-line izlenmesini sağlayan, tamamen ses ve görüntü dosyalarından oluşan bir sistemdir. “Streaming” sistemi sayesinde seslere ve görüntülere, veriyi bilgisayarınıza “indirmeyi” beklemeden ulaşabilirsiniz. Streaming media teknolojisinin kullanıcı, kullanıcı bilgisayarı, kullanıcı yazılımı, Internet bağlantısı, ağ altyapısı, sunucu alt yapısı gibi kalite belirleyici kriterleri vardır)
	8. Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinmek yasaktır.
	9. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve
	dosya indirilmeişlemi yapılmamalıdır.
	10. İş ile ilgili olmayan (müzik, video dosyaları ) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download etmek) yasaktır.
	11. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz. Kurumsal işlevlere yönelik yazılım ihtiyaçları için ilgili prosedürler dahilinde ilgili Bilgi İşlem sorumlularına müracaat edilmesi gerekmektedir.
	12. Üçüncü şahısların kurum internetini kullanmaları Bilgi İşlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilir.

**5. E-POSTA KULLANIMI**E-posta kurumun önemli iletişim araçlarından biridir ve bu kanalın kullanılması kaçınılmazdır. Kurumda oluşturulan e-postalar resmi bir kimlik taşımaktadır. E-posta basitliği ve hızı ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır. Bu düzenleme e-postaların doğru kullanımını içermektedir.

* 1. Kurumun e-posta sistemi, taciz, suistimal 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.
	2. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
	3. Kurum ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dahildir.
	4. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
	5. Kişisel kullanım için Internet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
	6. Spam zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
	7. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
	8. Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyası propaganda, fikri mülkiyet içeren malzeme, vb) gönderemezler.
	9. Kurum personeli tarafından internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında, e-posta iletisinin içeriğinden ve niteliğinden kurumun sorumlu tutulamayacağı gibi açıklamalar içermelidir.
	10. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu sebeple şifre kullanılmalı ve e-posta erişimi için kullanılan donanım ve yazılıma yetkisiz erişimi engellemelidirler.
	11. Gizli ve hassas bilgi içeren e-postalar kriptolanarak iletilmelidir.
	12. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
	13. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
	14. Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
	15. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.
	16. Virüs, solucan, Truva Atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslerle bulaşmış e-postalar Anti-virus sistemleri tarafından analiz edilip temizlenmelidir.

**6. ŞİFRE KULLANIMI**Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Kurum çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifreleme yapmakla sorumludurlar.

* 1. Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her dört ayda birdir.
	2. Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
	3. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
	4. Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.
	5. Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
	6. Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.

**7. UZAKTAN ERİŞİM**

Bu düzenleme herhangi bir yerden kurumun bilgisayar ağına erişilmesine ilişkin standartları belirlemektedir. Bu standartlar kaynakların yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları (hassas bilgilerin kaybı, prestij kaybı, içerideki sistemlerde meydana gelebilecek zararlar vs.) minimize etmek için tasarlanmıştır.

* 1. Uzaktan erişim için yetkilendirilmiş kullanıcılar kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.
	2. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar Windows Uzak Masaüstü Bağlantısıve Kablosuz Wireless Bağlantı teknolojisini kullanacaklardır. Semt poliklinikleri,ilçe hastaneleri de bu kapsam içerisindedir. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır.
	3. Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Bağlantı güçlü bir şifre ile sağlanmalıdır.
	4. Kurum çalışanları hiç bir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.
	5. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.
	6. Çalışanlar Kurum ile ilgili yazışmalarında Kurumun dışındaki e-posta hesaplarını (örnek, hotmail, yahoo, mynet vs) kullanamazlar. Bunun için sağlık bakanlığı tarafından oluşturulmuş kişisel ve kurumsal mail adresleri kullanacaklardır.
	7. Uzaktan erişim yöntemi ile kuruma erişen bütün bilgisayarlar en son güncellenmiş anti­virus yazılımına sahip olmalıdırlar.
	8. Kurum ağına standart dışı eğitim isteğinde bulunan organizasyon veya kişiler Bilgi İşlem biriminin özel izni ile geçici olarak izin verilebilir.
	9. Periyodik olarak yapılan kontrollerde kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

**8.KABLOSUZ ERİŞİM**

Bu bağlamda kurumda kurumsal bir kablosuz ağ olmamakla birlikte Türk Telekom TTNET erişim noktaları kuruludur. Yasal veya hukuki kurumu ilgilendiren hiçbir konu mevcut değildir.

**9.ANTİVİRÜS YAZILIMI**

Merkezimizde merkezi sunucu tarafından kontrol edilebilen antivirüs yazılımı mevcuttur ve günceldir. (01.05.05.03)Ayrıca Frewall (Güvenlik Duvarı) mevcuttur.

**10. BİLGİ GÜVENLİĞİ İÇİN YAPILAN DİĞER UYGULAMALAR**

* Merkezimizde merkezi sunucu tarafından kontrol edilebilen antivirüs yazılımı mevcuttur ve günceldir. (01.05.05.03)Ayrıca Frewall (Güvenlik Duvarı) mevcuttur.
* Merkezimizde Bilgi güvenliği konusunda çalışanlara yılda bir kez eğitim verilmektedir.
* Kurumda bulunan bütün sunucuların Sunucunun yeri, Sorumlu kişisi, Donanım, İşletim sistemi üzerinde çalışan uygulama bilgilerinin yer aldığı kayıtlar bilgiişlem ve ayniyat biriminde mevcuttur. Bilgi İşlem Merkezinde bulunan; sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs gibi koruma amaçlı yazılımlar günceldir.

**Veritabanı güvenliğini sağlamaya yönelik;**

* Veri tabanına girmek için öncelikle servera giriş yapılmalıdır.(Şifrelidir) Daha sonra veri tabanına giriş yapılır bu girişlerde şifrelidir.
* Yetkisiz personel dışında giriş yapılamaz.
* Veritabanı sistem logları tutulmakta ve gerektiğinde idare tarafından izlenmektedir.
* Yazılım-donanım destek birimi 24 (yirmidört) saat kesintisiz hizmet sunar ve bu birimde çalışanların güncel iletişim bilgileri santralde mevcuttur.
* Kullanıcıların ara yüze bağlanmak için kullandıkları şifreler şifreli bir şekilde saklanmaktadır.
* Veritabanı üzerinde loglanması gereken işlemler (Fatura Birimi kayıtları, Klinikte hasta dosyası, hasta dosyasına girilen işlemler, Mutemetlik Birimi kayıtları) otomasyon firması tarafından belirlenmiştir. Veritabanına yapılacak müdahale (yama ve güncelleme vb.) öncesinde kullanıcılar Bilgi İşlem tarafından bilgilendirilmektedir. (01.05.08.00)
* Kullanıcılar veri tabanına yapılacak müdahale öncesinde bilgilendirilir.

**Dış ortamdan iç ortama erişimlerde güvenlik tedbirler;**

* Yazılım firmasının kullanmış olduğu yardım programı kullanılmaktadır.
* Program şifrelidir ve belli sürelerde şifreleri değiştirmektedirler. Ayrıca merkezimizde güvenlik duvarı bulunduğundan merkezimiz istemediği sürece dış ortamdan iç ortama erişim yapılamaz.
* SAÜ'ye destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında kurum tarafından onaylanmış gizlilik sözleşmesi Satın alma biriminde bulunmaktadır.
* Yedeklemeler aracılığı ile yılda bir kez veri kurtarmatesti uygulanmaktadır. Uygulanan testte yedeklemeden geri dönüşün sağlanıp sağlanmadığı ve veri kaybının olup olmadığı kontrol edilmektedir ve test kayıt altına alınmaktadır. Gerektiğinde düzeltici önleyici faaliyet başlatılmaktadır.
* ADSM bilgi sisteminde yetkilendirme yapılmış olup her kullanıcının veri tabanında hangi bilgilere erişebileceği tablo ortamında tanımlanmıştır.
* Aynı görevi icra eden çalışanlar aynı yetki gruplarına sahiptir.
* HBYS üzerinden yapılan işlemler Bilgi İşlem ve İdare tarafından izlenmektedir.Salt okunur özellikte tablo mevcuttur. Tabloda sisteme giriş yapan kullanıcılar, gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalar ile ilgili kayıtlar yer almaktadır. Bu tabloya sadece bilgi sisteminde yönetici olarak yetkilendirilmişkişiler ulaşabilmektedir
* HBYS ile ilgili sorunlarda çalışanlar Bilgi İşlem merkezi ile irtibata geçmektedirler.
* Kliniklerde oluşan sorunlarda kayıtlı olan hastaya bakılmaya devam edilir en yakın hekimin bilgisayarından ya da klinik sekreterinin bilgisayarından veri girişi sağlanır.
* HBYS ile ilgili sorunlar ve çözümler sorunun oluştuğu tarih ve saat, bildirimin yapıldığı tarih ve saat, sorunun çözüldüğü tarih ve saatin bulunduğu form ile HBYS’de kayıt altına alınmaktadır.
* Bilgi İşlem tarafından sorunlar ile ilgili aylık istatistiksel çalışma yapılmaktadır.

9. **İLGİLİ DÖKÜMANLAR**

Sağlık Bakanlığı Bilgi Güvenliği Politikası Yönergesi

|  |  |  |
| --- | --- | --- |
| **Hazırlayan****Kalite Birim Sorumlusu** | **Kontrol Eden Kalite Yönetim Direktörü** | **Onaylayan Dekan** |
|  |  |  |