1. AMAÇ:

Bu prosedürün amacı D.Ü. Diş Hekimliği Fakültesi Hastanesi'nin tüm birimlerinde hasta sağlık bilgilerinin doğru ve düzenli olarak toplanması, depolanması, değerlendirilmesi ve korunması, hasta kayıtlarının mahremiyetinin sağlanması ile ilgili uyulması gereken kuralların ve bilgi güvenliğinin sağlanmasının tanımlanmasıdır.

2. KAPSAM:

Bu prosedür D.Ü. Diş Hekimliği Fakültesi Hastanesi'nin bütün birim ve çalışanları ile hastane bilgi işlem hizmetlerini yürüten firma sahibi, yetkilileri ve çalışanlarını kapsar.

3. KISALTMALAR
4. TANIMLAR
5. SORUMLULAR:

Bu prosedürden sorumlu olanlar; Hastane Yöneticisi, Başhekim, İdari ve Mali İşler Müdürü, Bilgi İşlemden Sorumlu Başhekim Yardımcısı, , Hizmet Satın Alınan Firma Yöneticisi, firma sorumluları, tüm bilgi işlem firma elemanları, Hastane Bilgi Yönetimi Sistemini kullanan tüm çalışanlardır.

6. FAALİYET AKIŞI:
6.1. Genel Kurallar:

a. Hastanemiz; teşhis ve tedavi hizmetlerinin sunumunda, hasta ihtiyaç ve beklentilerinin karşılanmasına yasal mevzuatlar doğrultusunda cevap verecek şekilde sorumludur. Bu sorumluluk kapsamında gizliliğin öneminin bilinci ile bilgi güvenliği politikaları oluşturulmuştur.

b. Hastanemize teşhis ve tedavi için başvuran tüm hastalardan kayıtlar için gerekli kişisel bilgiler istenir. Bunlar; ad soyadı, hastalık bilgileri, T.C Kimlik numarası, adres, telefon bilgileri ve benzeri bilgilerdir.

c. Hastanemize teşhis ve tedavi için başvuran hastalardan toplanan tüm bu bilgileri içeren verilerin güvenliği ile ilgili üç temel prensip söz konusudur. Bunlar;

- Gizlilik
- Bütünlük
- Erişilebilirliktir.

d. Sağlık kayıt bilgileri hastaya aittir. Bu bilgilere üçüncü taraflar veya yetkisi olmayan kişilerin ulaşabilmesi ve bilgilerin amaçları dışında kullanımını engelleyecek uygulamalar geliştirilir. Bu uygulamalar;

- Hastanemizde 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 hastane 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 hastane arşivinde güvenli bir şekilde saklanır ve korunur.

- Elektronik hasta kayıtlarına internet ortamında ulaşılabilmesi engellenmiştir.
- Hastaların sağlık harcamaları sadece faturalama birimi, vezne tarafından değerlendirilmektedir. Diğer sağlık çalışanları fiyat ve ödeme ile ilgili konularda görüş ve fiyat bildiremezler.

Bilgi güvenliğinin sağlanmasında;

6.2. SUNUCULARIN GÜVENLİĞİ

6.2.1. Kurum bünyesindeki bütün sunucuların yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılacaktır.

6.2.2. 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.

6.2.3. Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

6.2.4. Sunucu yedekleri talimata uygun olarak düzenli şekilde alınmalıdır.

6.2.5. 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.

6.2.6. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

6.2.7. 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.

6.2.8. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

6.2.9. Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır, yetkisiz girişler engellenmelidir.

6.2.10. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.

6.2.11. Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar yapılmalıdır.

6.3. 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.

6.3.1. 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 06:00'de 12:00'de ve 23:00' de server tarafından otomatik olarak günlük yedek alınır.
- ➢ Günlük yedekler her gün bilgi işlem personeli tarafından DVD 'ye kaydedilir.

➢ Günlük yedekler ve tam yedek bilgi işlem personeli tarafından her hafta cuma günü bina dışında bulunan güvenlik birimindeki çelik kasaya imza karşılığında teslim edilir.

✓ **Veri koruma süreleri:** Yedekleme DVD'si süresiz olarak saklanmak üzere güvenli bir ortamda (güvenlik birimindeki çelik kasa) arşivlenir.

6.4. KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ

Hastanemizde 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.

6.4.1. 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 taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez

✓ 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 ve 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.

6.4.2. 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.
Veriye erişecek kişiler aşağıdaki şekilde tanımlanmıştır.
✓ Hasta kendi verisine online olarak kurum tarafından kendisine verilen sadece ilgili vakayla ilişkili pin numarası ve şifre ile internetten erişebilir. Diğer taraftan Akıllı kart, elektronik imza, token vb. mekanizmalar kullanıldığı taktirde veriye tam erişim mümkün olabilir.
✓ Hastanedeki yetkilendirilmiş sağlık çalışanları ise, ancak hastanın giriş tarihinden, taburcu olana kadar geçen zaman içerisinde hastanın elektronik sağlık kayıtlarına erişebilirler.
✓ Gerektiğinde saat ve/veya gün bazında belirlenen bir sure için bazı kullanıcı ve istemci makinelerin sisteme oturum açmalarına kısıtlama getirilebilmelidir
✓ Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin verilmemelidir.
✓ 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.

6.5. İNTERNET ERİŞİM VE KULLANIMI

Kurum içinde güvenli internet erişimi için sahip olması gereken standartları belirlemektedir. İnternet'in 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 ne internet'in kurallarına, etiğe ve yasalara uygun kullanılmasının sağlanmasını amaçlamaktadır. Bütün kullanıcılar ve Bilgi İşlem yöneticileri aşağıdaki internet erişim ve kullanım kurallarına uymalıdır.

6.5.1. Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkacaktır. Ağ güvenlik duvarı (firewall), 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.

6.5.2. Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografik, oyun, kumar, şiddet içeren vs) yasaklanabilmelidir.

6.5.3. Anti-virus gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik (smtp, pop3, ayrıca mümkünse http ve ftp vs) virüslere karşı taranmalıdır.

6.5.4. Ancak Yetkilendirilmiş Sistem Yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir. Bunlar; www, ftp, telnet, ping, traceroute vs.

6.5.5. 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.)

6.5.6. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ, MIRC, Messenger v.b. mesajlaşma ve sohbet programları gibi chat programlarının kullanılmaması. Bu chat programları üzerinden dosya alışverişinde bulunulmamalıdır.

6.5.7. Hiçbir kullanıcı internet üzerinden Multimedia Streaming yapamayacaktır.(Streaming media, ses, video ve diğer multimedia dosyalarının İnternet'te veya kurumsal intranetlerde 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)

6.5.8. Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.

6.5.9. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemesi ve dosya indirimi yapılmamalıdır.

6.5.10. İş ile ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download etmek) yasaktır.

6.5.11. 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.

6.5.12. Üçüncü şahısların kurum internetini kullanmaları Bilgi İşlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilir.

6.6. E-POSTA KULLANIMI

E-posta kurumun önemli iletişim araçlarından biridir ve bu kanalın kullanılması kaçınılmazdır. Kurum'da 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.

6.6.1. 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.
6.6.2. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
6.6.3. Kurum ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dahildir.
6.6.4. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
6.6.5. Kişisel kullanım için Internet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
6.6.6. Spam zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
6.6.7. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

6.6.8. Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyası propaganda, fikri mülkiyet içeren malzeme, vb) gönderemezler.
6.6.9. Kurum personeli tarafından internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında, e-posta iletisinin içeriğinden ve niteliğinden Kurum'un sorumlu tutulamayacağı gibi açıklamalar içermelidir.
6.6.10. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu sebeple şifre kullanılmalı ve e-posta erişimi için kullanılan donanım ve yazılıma yetkisiz erişimi engellemelidirler.
6.6.11. Gizli ve hassas bilgi içeren e-postalar kriptolanarak iletilmelidir.
6.6.12. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
6.6.13. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
6.6.14. Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
6.6.15. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.
6.6.16. 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.

6.7. 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.

6.7.1. Bütün sistem seviyeli şifreler (örnek, root, administrator vs) en az üç ayda bir değiştirilmelidir.

6.7.2. 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.

6.7.3. Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

6.7.4. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

6.7.5. Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.

6.7.6. Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

6.7.7. Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.

6.8. 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.

6.8.1. Uzaktan erişim için yetkilendirilmiş kullanıcılar kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.
6.8.2. Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar Windows Uzak Masaüstü Bağlantısı ve 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.
6.8.3. Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Bağlantı güçlü bir şifre ile sağlanmalıdır. Daha fazla bilgi için Şifreleme Politikası'na bakınız.
6.8.4. Kurum çalışanları hiç bir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.
6.8.5. 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.

6.8.6. 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.
6.8.7. Uzaktan erişim yöntemi ile kuruma erişen bütün bilgisayarlar en son güncellenmiş antivirus yazılımına sahip olmalıdırlar.
6.8.8. Kurum ağına standart dışı eğitim isteğinde bulunan organizasyon veya kişiler Bilgi İşlem biriminin özel izni ile geçici olarak izin verilebilir.
6.8.9. Periyodik olarak yapılan kontrollerde kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

6.9. KABLOSUZ ERİŞİM

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

6.10. SERVER ODASINA GİRİŞ ve YETKİLENDİRME

Server odası girişleri yetkilendirilmiş personel harici girişin engellenmesi amacıyla kullanıcı tanımlı giriş kartları veya Bilgi İşlem Birim sorumlusunda bulunan anahtar ile yapılabilmektedir. Uygulama sırasında odaya girecek personele Bilgi İşlem Sorumlusu tarafından giriş yetkisine sahip giriş kart kartları teslim edilir. Server odasına kart sahiplerinden başkasının girmesi yasaktır.

Görev değişikli, tayin vb. durumlarda yetkilendirilen personelde değişiklik olması durumunda giriş kartı yetkilendirmesi yapmak amacıyla kullanılan master kart yardımı ile bütün kullanıcı yetkileri sıfırlanır. Yeni yetkilendirilen personel ve görevi devam eden personel giriş kartları tekrar tanımlanır. Yetkilendirme yapmada kullanılan master kart server yedeklerinin saklandığı Güvenlik Birimindeki çelik kasada saklanmaktadır.