**AMAÇ:** Şanlıurfa Suruç Devlet Hastanesi’ne başvuruda bulunan kişilere ait bilgilerin güvenliğinin sağlanması amaçlı öncelikle verilerin doğru olarak toplanması, depolanması ve kullanılmasına ilişki uygulamalarımızı ve güvenlik önlemlerimizi dahili olarak gözden geçirmek ve kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemlerini almak ve bunun devamlılığını sağlamaktır. Bu prosedürün amacı, hastaya ait bilgilerin mahremiyeti konusunda uyulması gereken kuralları tanımlamaktır.

**KAPSAM:** Suruç Devlet Hastanesi’ne başvuruda bulunan kişilere ait bilgilerin güvenliği ile ilgili hususları kapsar.

**TANIMLAR:**

**HBYS:** Hastane Bilgi Yönetim Sistemi

Hastanemiz teşhis ve tedavi hizmetlerinde; yasal mevzuat şartlarının karşılanmasından, hizmet sunumunda hasta ihtiyaç ve beklentilerine cevap verecek şekilde gerçekleşmesinden sorumludur. Bu amaçla kurulan Bilgi İşlem Birimi yazılım ve donanım açısından 24 saat kesintisiz hizmet sunmakta olup, bu birimde çalışmakta olan sorumlu personelin güncel iletişim bilgileri hastane santralinde bulunmaktadır. Hastane Bilgi Yönetim Sistemi (HBYS)’de yer alan temel modüllerin tümü aktif olarak kullanılmaktadır.

**Bu amaçla kurumumuz;**

* Faaliyetlerimizin ticari, mali ve diğer iç ve dış baskılardan ve etkilerden uzak tutulmasını,
* Hasta ve hak sahiplerine ait gizli bilgilerin ve tescilli hakların korunmasını,
* Teşhis ve tedavi sonuçlarının uygun şartlarda muhafaza edilmesini ve iletilmesini,
* Yeterlilik, tarafsızlık, karar verme ve çalışmalarda güveni azaltacak herhangi bir faaliyette bulunmamayı,
* Sağlık hizmeti sunarken beklenen kalite seviyesinin sağlanmasını,
* Vereceğimiz hizmetin belirlenen standartlar çerçevesinde gerçekleştirilmesini,
* Söz konusu bilgileri hasta onayı dışında ya da yasal bir yükümlülük altında bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ve kuruluş ile paylaşmamayı taahhüt eder.

Kurum olarak gizliliğin önemli olduğuna inanırız. Bu politika, hastanemizde sunulan tüm sağlık hizmetleri için geçerlidir.

Hastanemiz Hasta Hakları, güvenlik, veri bütünlüğü, erişim ve uygulama ile ilgili gizlilik ilkelerine bağlıdır.

**Topladığımız Bilgiler ve Onları Nasıl Kullandığımız:**

* Sağladığımız bilgiler; Hastanemize teşhis ve tedavi için başvurduğunda hastalarımızdan kişisel bilgiler (ad, soyad, hastalık bilgileri, T.C. Kimlik Numarası, adres, telefon bilgileri vb.) istenmektedir.
* Hastanemiz yalnızca Hasta Bilgi Güvenliği Politikası ve/veya belirli hizmetlere ilişkin gizlilik uyarısında açıklanan amaçlarla kişisel bilgileri kullanır.
* Otomasyon kullanan tüm hastane personeli eğitimden geçirilmekte, Bilgi Güvenliği Gizlilik Sözleşmesi tüm personele imzalatılmaktadır. Aksi davrananlar hakkında gerekli yasal işlemler yapılmaktadır.

**Sunucu Güvenliği:**

Hastanemizde bulunan sunucular bilgi işlem ünitesi içerisinde ayrı bir bölümde izinsiz erişimin engellendiği alanda çalışmaktadır. Ancak yetkili kişilerce ilgili birime girilmektedir. Sunucuların bulunduğu alan su basması, yangına karşı her türlü önlemi alınmış ve klima sistemi ile soğutulmakta olup ayrıca sıcaklık ve nem bilgileri de düzenli olarak kayıt altına alınmaktadır.

Sıcaklık değerleri 18-22 °C, nem %45-70 arasında olması sağlanmaktadır. Bunun yanında yedekli güç kaynakları (UPS) mevcut olup, periyodik bakımları yapılmaktadır.

**E-Posta Kullanım Kuralları:**

* Kurumun e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
* Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
* Kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
* Spam zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
* Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
* Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.
* Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılması ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
* Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
* Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.
* Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodlar içerebilirler.
* Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.
* Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre (personel folder) çekilmelidir.
* Hastanemiz çalışanları gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Yasadışı ve hakaret edici e-posta haberleşmesi yapılması durumunda yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilir ve kullanıcı hakkında yasal ve idari işlemler başlatabilir.
* Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerin kırıldığının fark ettikleri andan itibaren yetkililerle temasa geçip durumu haber vermekle yükümlüdürler.

**Şifre Kullanım Kuralları:**

* Bütün kullanıcı seviyeli şifreler (örnek; e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her üç ayda birdir.
* Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
* Şifreler başkası ile paylaşılmamalı, kağıtlara ya da elektronik ortamlara yazılmamalıdır.
* Şifrelemede, küçük ve büyük karakterlere (örnek: a-z, A-Z), hem digit hem de noktalama karakterleri ve ayrıca harflere (örnek, 0-9. “’><+%&/()\_;\*) sahip olmalıdır.
* En az sekiz adet alfa nümerik karaktere sahiptir.
* Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
* Aile isimleri kullanılmamalıdır.
* Herhangi bir kişiye telefonda şifre verilmemelidir.
* E-posta mesajlarında şifre yazılmamalıdır.
* Şifreler aile bireyleriyle paylaşılmamalıdır.
* Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
* Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.
* Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

**Antivirüs Politikası:**

* Bütün bilgisayarda kurumun lisanslı Antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.
* Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem birimine haber verilmelidir.
* Zararlı programları (örneğin, virüsler, solucanlar, Truva atı, e-mail bombaları vb.) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.
* Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını sisteme kuramaz.

**İnternet Kullanım Politikası:**

* Hiçbir kullanıcı peer-to peer bağlantı yoluyla internetteki servisleri kullanamayacaktır. (Örneğin; KaZaA, iMesh, eDonkey, Gnutella, Napster, Aimster, Madster, FastTrak, Audiogalaxy, MFTP, eMuel, Overnet, NeoModus, Direckt Connect, Asquisition, BearShare, Gnucleus, GTK-Gnutella, LimeWier, Mactella, Morpheus, Phex, Otella, Shareaza, XoLoX, OpenNap, WinMX vb.)
* Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ, MIRC, Messenger vb. mesajlaşma ve sohbet programları gibi chat programlarının kullanılmaması. Bu chat programları üzerinden dosya alışverişinde bulunulmamalıdır.
* Hiçbir kullanıcı internet üzerinden Multimedia Streamingi (Video, mp3 yayını ve iletişimi) yapamayacaktır.
* Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.
* İş ile ilgili olmayan (Müzik video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır.
* İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.
* Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
* Bilgisayar İşletim Sistemlerine zarar verdiği için internet üzerinden ekran koruyucu, yamalar, masaüstü resimleri, yardımcı tamir edici program olduğu belirtilen araçlar gibi her türlü dosya ve programların indirilmesi ve/veya kurulması yasaktır.
* Üçüncü şahısların kurum içerisinden interneti kullanmaları Bilgi İşlem sorumlusunun izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.
* Bilgi İşlem Birimi iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir.

**Genel Kullanım Politikası:**

* Bütün PC ve laptoplar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.
* Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
* Kurumda domain yapısında mutlaka login olunmalıdır. Bu durumda, domaine bağlı olmayan bilgisayarların yere ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır. **(Domain var)**
* Laptop bilgisayarların çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimi’ne haber verilmelidir.
* Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur.
* Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.
* Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişilmemelidir.
* Port veya ağ taraması yapılmamalıdır.
* Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-networt taramışı vb. yapılmamalıdır.
* Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması yapılmamalıdır.
* Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.
* Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
* Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.
* Kurumun kullanmakta olduğu yazılımlar hariç, kaynağı belirsiz olan programları (Dergi, CD’leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.
* Yetkisi olmayan personelin, kurumdaki gizli ve hassa bilgileri görmesi veya elde etmesi yasaktır.
* Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, hastanemizin bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilemez.
* Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak farklı ortamlara (CD, DVD, USB, External Harddisk vb.) yedeklenmesinden sorumludur.
* Bilgi İşlem Birimi tarafından atanan yetkili kişiler kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel kişisel bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.
* Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/kopyalanmamalıdır.
* Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
* Kurumda Bilgi İşlem biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-Post Servisi vb.) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.
* Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.
* Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.
* Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
* Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir. Kuralların uygulanmasından birim amirleri sorumlu olup, şahısların yapmış olduğu kural ihlallerinde ilgili sistem kullanıcısından başlamak üzere silsile yolu ile sorumludurlar.

**Sisteme Erişim:**

* Hastanedeki tüm bilgisayarlar otomasyon sistemine bağlı olup ayrıca güvenlik duvarı koruması altında bu bilgisayarların internete erişimi sağlanmaktadır. İnternete erişim bilgi işlem ünitesinin kontrolü altında kısıtlı olarak sağlanmaktadır.
* E-Posta erişimine internet üzerinden kullanımına izin verilmekte olup, sakıncalı iletiler güvenlik duvarı tarafından engellenmektedir.
* Uzaktan Erişim: Bilgi işlemden sorumlu personel tarafından gerekli görülen durumlarda güvenlik duvarı tarafından korumalı olarak erişim sağlanmaktadır.
* Kablosuz Erişim: Hastane içerisinde kablosuz erişim mevcut olup, otomasyon ile bağlantıyı sağlayacak olan cihazların MAC (fiziksel) adresleri modem üzerinde kayıtlıdır. İzinsiz olarak dışarıdan girişlere kapalıdır.
* Şifre Kullanımı: Otomasyon erişimi verilen personellerin kullanıcı adı ve şifreleri bilgi işlem tarafından verilmekte olup, bu şifrelerin kısa süre içerisinde ilgili personel tarafından belirli zaman aralıklarında değiştirilmesi istenmektedir. Şifre değişikliği yapılmadan sisteme erişim sağlanmamaktadır. Personelin değiştirmiş olduğu şifreler otomasyon üzerinden hiçbir şekilde görülmemektedir.

**Bilgi Güvenliği:**

* Verileri yetkisiz erişime, yetkisiz şekilde değiştirilmelerine, açıklanmalarına veya imha edilmelerine karşı korumak için uygun önlemleri alırız. Hastanın özlük bilgileri ve kurum bilgileri sadece Hasta Kabul-Kayıt tarafından değiştirilebilir. Bilgisayar sekreterlerinin bilgileri silme yetkileri yoktur.
* Hastalarla ilgili her türlü kaydın kim tarafından, hangi tarihte girildiği, ulaşma, değiştirme bilgisi hastane bilgi işlem programı log kayıtları altında tutulmaktadır.
* Hastaların klinik kayıtlarına yalnızca konu ile ilgili yetkilendirilmiş kişinin giriş yaptığ hastane bilgi işlem programında “Veri Giriş Kontrol” adı altında izlenebilmektedir.

Veri tabanı üzerinde Hasta kayıt loğları, Hasta Hizmet loğları, Hasta Fatura loğları, Hasta Poliklinik loğları, Tanımlama loğları, Hasta Dosya loğları, Veri Tabanı oturum loğları, Sağlık kurulu kayıt loğları kayıt altına alınmaktadır.

Kullanıcıların ara yüze bağlanmak için kullandıkları şifreler, şifreli biçimde veri tabanında saklanmaktadır. Veri tabanı sistem loğları gerektiğinde idare tarafından yazılımcı firmadan istenerek izlenmektedir.

Kullanıcılar veri tabanına yapılacak müdahale (yama, güncelleme vb.l) öncesinde otomasyon sistemi üzerinden bilgilendirilmektedir. Hastaneye destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında hastane tarafından onaylanmış gizlilik sözleşmesi mevcut olup, dış ortamdan iç ortama erişimler yazılım hizmeti veren firma tarafından kayıt altına alınmaktadır.

Her kullanıcının veri tabanında hangi bilgilere erişebileceği bilgi işlem biriminde sorumlular tarafından belirlenmektedir. Ayrıca bu kişilerin hangi yetkilere sahip olduğu HBYS üzerinden takip edilebilmekte ve rapor edilebilmektedir.

**HBYS’de Oluşan Sorunların Çözümünde Uyulması Gereken Kurallar:**

* Konu ile ilgili bilgi işleme sistem sorumluları ile telefon veya HBYS modülü üzerinde online mesajlaşarak irtibat kurulmaktadır.
* HBYS ile ilgili sorunlar ve çözümler sorunun oluştuğu tarih ve saat bildirimin yapıldığı tarih ve saat kayıt altına alınmaktadır. Bu kayıtlar HBYS modülü üzerinden izlenebilmektedir.
* Sorunlar ile ilgili aylık istatistiksel çalışmalar yapılmakta olup, sorunlarla ilgili gerekli düzeltici önleyici faaliyet başlatılmaktadır.

**Bilgi Paylaşımı:**

* İleri tetkik ve tedavi yöntemleri için başka hastane veya özel merkezler sevk sırasında hastaya ait bilgiler ilgili mevzuatın gereklerine uygun belgeler ile hastanın kendisi tarafından iletilmektedir.
* Hasta sağlık bilgileri hastanemiz tarafından veya Sağlık Bakanlığının bilgi yönetim sistemleri tarafından araştırma, istatistik ve karar destek sistemleri için kullanırlar.

**Yedekleme:**

* Bütün hasta kayıtları ve yedeklenmiş hasta bilgileri fiziksel olarak korunmuş mekanlarda saklanmaktadır.
* Hasta kayıtlarının yedeklenmesi Bilgi İşlem tarafından yapılmaktadır. Yedekler, harici belleklere backup yapılan yedeklemeler, Harici Bellek ortamında Bilgi İşlem odasında saklanmaktadır. Bu harici disk dolduğu zaman arşive teslim edilir.

**İLGİLİ DOKÜMANLAR:**

* Otomasyon Arıza Bildirim Formu