AMAÇ: Veri tabanı sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik standartların tanımlanması, sunucularının temel güvenlik yapılandırmaları için standart belirlenmesi, fakültemize başvuruda bulunan kişilere ait bilgilerin ve kurumsal bilgilerin bulunduğu sistemlerin yetkisiz erişime karşı korunması, fiziksel güvenlik önlemleri alınması ve önlemlerin devamlılığının sağlanması için izlenecek yolun belirlenmesidir.

2.KAPSAM: Tüm Birimleri kapsar.

3.KISALTMALAR:

SDY: Sorumlu Dekan Yardımcısı, SY: Sistem Yöneticileri, BİL: Bilgi İşlem Birimi, PDR: Poliklinik Doktoru, TP: Tüm Personel

4.TANIMLAR:

5.SORUMLULAR:

Md. No.	SÜREÇ ADIMLARI / SORUMLULAR	SDY	SY	BİL	PDR	TP
3.1	Sunucuların Güvenliği		X			
3.2	Verilerin Yedeklenmesi		X	X		
3.3	Kişisel Sağlık Kayıtlarının Güvenliği	X		X		X
3.4	Bilgi Verilmesi Uygun Olmayan Ve Tedbir Alınması Gereken Hallerle İlgili Bilginin Verilmesi				X	
3.5	İnternet Erişimi ve Kullanımı					X
3.6	Elektronik Posta Kullanımı					X
3.7	Şifre Kullanımı					X
3.8	Uzaktan Erişim		X	X		
3.9	Kablosuz Erişim			X		

SDY: Sorumlu Dekan Yardımcısı, SY: Sistem Yöneticileri, BİL: Bilgi İşlem Birimi, PDR: Poliklinik Doktoru, TP: Tüm Personel

6.FAALİYET AKIŞI

Sunucuların Güvenliği

1. **Fakültemizde bulunan** sunucuların yönetiminden sistem yöneticileri sorumludur. Sunucuların yeri, şifreleri, ana görevleri ve üzerinde çalışan uygulamalara dair tüm bilgiler sistem yöneticileri tarafından yönetilir ve muhafaza edilir.
2. **İşletim** sistemi yapılandırmaları (konfigürasyonları) sunucunun yapacağı işin amacına göre sistem yöneticileri tarafından yapılır. Kullanılmayan servisler ve uygulamalar kapatılır. Veritabanına erişim tarihi, saati ve üzerinde yapılan işlemler kaydedilir.
3. Sunucu üzerinde çalışan işletim sistemlerinin, yazılımlarının, anti-virüs vb. güvenlik amaçlı yazılımların sürekli güncel olması sağlanır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılır. Ancak otomatik yazılımlar da sistem yöneticileri tarafından bir test ve onay sürecinden geçirildikten sonra uygulanır.
4. Sistem yöneticileri gerekli olduğu durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır.
5. Sunucu üzerindeki her türlü yazılım, işletim sistemi, veritabanı, anlaşmalı yazılım firması personelleri tarafından, bilgi işlem birimi denetiminde yapılır.
6. Anlaşmalı yazılım firması, sözleşme sırasında, hastaneye ve hastaneye başvuran hastalara ait bilgilerin güvenliği konusunda alınacak tedbirleri ve yükümlülükleri bildikleri ve kabul ettiklerine dair "**Anlaşmalı Kurumlar İçin Bilgi Güvenliği Taahhütnamesi**"ni imzalarlar. Taahhütname sistem yöneticileri tarafından dosyalanır ve süresiz olarak saklanır.
7. Uzaktan bağlantılar güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılır.
8. Kritik sistemlerde oluşan güvenlikle ilgili bütün olaylar gerektiğinde kullanmak veya geri çevirmek amacıyla kaydedilir. Kayıtlar minimum 1 hafta saklanır.
9. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri bakımından elverişli sunucu odalarında işletilir. Yedekli çalışan iki klima ile sıcaklık 18-22 ^{0}C; nem % 30 - % 50 arasında olması sağlanır.
10. Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, bakım sözleşmelerine uygun olarak yapılır.
11. Sistem odasının elektrik hattı kat panolarından bağımsız olarak direkt ana girişten beslenir.
12. Sistem odalarına yetkisiz kişiler giremezler, sorumluluk sistem yöneticilerindedir.
13. Sunucular sanal ortamdaki saldırılara karşı güvenlik duvarı (Firewall) ile korunmaktadır. Sunucu işletim sistemi mimarisi WINDOWS tabanlı olup ve sunucu üzerindeki kullanıcı hesapları karmaşık şifrelerle korunur.

Verilerin Yedeklenmesi

1. Sunucular ve veri depolama üniteleri (storage) yedekli olarak çalışmaktadır.
2. Veriler ağ ortamında online olarak farklı depolama ünitelerinde yedeklenir.
3. Ana sunucu üzerinde her gün mesai bitiminde otomatik yedek klasörü oluşturulur.
4. Yedek klasörüne alınan veriler bilgi işlemdeki yetkili personel tarafından ayrıca harici bilgisayar üzerine alınarak manuel yedeklenir. Yapılan yedeklemeler offline olarak BluRay ortamına yazdırılır.*Günde 4 defa sistem otamatik olarak yedekleme yapmakta ve gün sonunda diş ortam hard-diske aktarılmaktatır.*
5. BluRay ortamında yapılan *günlük yedeklemeler üç ayda bir* tutanakla Dekanlığa teslim edilir.
6. Yapılan tüm yedeklemelerin bir yedeği ayrıca bilgi işlem biriminde muhafaza edilir.

Kişisel Sağlık Kayıtlarının Güvenliği

1. Kişisel sağlık kaydı kapsamına; hasta ile ilgili sözlü ya da yazılı bilgiler, tıbbi müdahaleler, ön tanı, teşhisler, grafik imajları ve fatura gibi konular girmektedir.
2. Bilgi güvenliği konusunda üç temel prensip olan gizlilik, bütünlük ve erişebilirlik esas alınır.
3. Fakültemizde hasta bilgilerinin girişi HBYS' nde tanımlanan alanlara ve hasta dosyalarına yapılmaktadır.
4. Fakültemizde belirli görevde çalışanlar, belirli verilere ulaşacağı tanımlanmış, şifreler kişilere özel verilmiştir. Görev bazlı yetkilendirme yapılmış, yetkisiz kişilerin sağlık kayıtlarına erişmesi engellenmiştir. Yetkilendirme kayıtları bilgi işlem personelleri tarafından kaydedilir ve her yıl ilgili başhekim yardımcısı tarafından kontrol edilir.
5. Fakültemizde hizmet alan hastaların rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara (bakanlık genelgeleri hariç) iletemez. (Bkz: **Veri Güvenliği Hakkında Genelge 2005/153**)
6. Yürürlükteki genelgelere göre hasta sağlık bilgilerini Sosyal Güvenlik Kurumu'na verilebilir. Özel sigorta kurumları hastanın sağlık bilgilerini elde edemez. Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara verilmez. Hastanın kullandığı ilaçlar, diyet programları vb. buna dahildir. (Bkz: **Veri Güvenliği Hakkında Genelge 2005/153**)
7. Kişisel bilgilere erişim hizmetlerini işletmek veya geliştirmek için bilgilere ulaşması gereken hastane çalışanları, hastalara ait bilgilerin mahremiyeti konusunda uyulması gereken kuralları bildiğini ve hasta bilgilerini üçüncü şahıslarla paylaşmayacağını taahhüt eden **"Çalışan İçin Bilgi Güvenliği Taahhütnamesi"**ni göreve başlamadan önce imzalarlar. İmzalı **"Çalışan İçin Bilgi Güvenliği Taahhütnamesi"** kişilerin özlük dosyalarında süresiz olarak saklanır. Yükümlülüklere uymamaları durumunda, işlerine son verilmesi, disiplin cezası veya yasal işlemler başlatılır.

8. Hastanın dosyasının izlenmemesi için gerekli tedbirler alınır. (Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi)
9. Sağlık hizmetlerinin devamlılığını sağlamak veya geliştirmek için bilgilerin doğru, tam ve geçerli olmasını sağlamak amacıyla kişisel bilgileri güncellemeleri gerektiğinde hastalara başvurulur.
10. Hastanemizde personelin yılda bir kez bilgi güvenliği eğitimi alarak, gereken hassasiyeti göstermeleri sağlanır.

Bilgi Verilmesi Uygun Olmayan Ve Tedbir Alınması Gereken Hallerle İlgili Bilginin Verilmesi

1. Kurumumuzda hasta ile ilgili tüm tıbbi bilgiler her gün klinik doktoru tarafından hastaya veya hasta yakınına anlatılarak durumu hakkında bilgilendirme yapılır. Konulan teşhisin hastaya söylenmesinin doğuracağı olumsuz etkiler göz önünde bulundurularak hastalığının artması ihtimalinin bulunması veya hastalığın seyrinin ve sonucunun vahim görülmesi hallerinde, teşhis hastadan saklanabilir. Ancak hastanın yasal temsilcisine tüm bilgiler verilerek birlikte karar verilir.
2. Yasal konular dışında, hasta, sağlık durumu hakkında kendisine veya yakınlarına bilgi verilmemesini isteyebilir. Hasta veya hasta yakını bilgi almak istediği alanları ve sınırları hekimine bildirmelidir.

İnternet Erişimi Ve Kullanımı

1. Çalışanlar fakültemizde internete erişebilmek için bilgi işlem birimine başvurarak bilgisayarlarını sisteme tanıtmalıdırlar.
2. Tanıtma işlemi sırasında çalışanı bilgilendirmek ve kayıt almak amacıyla "**İnternet Kullanım Kuralları Bilgilendirme ve Kayıt Formu"** kullanıcıya imzalatılır.
3. İmzalı formlar bilgi işlem biriminde muhafaza edilir. Kullanıcı işten ayrıldıktan 1 yıl sonra imha edilir.

Elektronik Posta Kullanımı

1. E-posta kaynakları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır. Fakültemizde e-posta kaynaklarının kişisel kullanımına kısıtlı olarak izin verilmektedir.
2. Kullanıcılar kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur.
3. Kurum e-posta kaynakları hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez, normal operasyon ve iş aktivitelerini engelleyemez.
4. Kurum e-posta kaynakları; "zincir e-postalar", reklam gibi istenmeyen mesajlar (SPAM) göndermek için kullanılamaz.

5. Kullanıcılar e-posta yazılımının gönderenin kimliğini gizleyecek özelliklerini kullanamazlar.
6. Kullanıcılar e-posta yazılımının otomatik mesaj iletme özelliklerini kullanamazlar.

Şifre Kullanımı

1. Bütün kullanıcı şifreleri (otomasyon şifresi, e-posta şifresi, masaüstü bilgisayar şifresi gibi) her iki ayda bir değiştirilmelidir.
2. Şifreler;
3. En az altı adet harf ve numara karışımı karaktere sahip olmalıdır.
4. Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
5. Aile bireylerinin isimleri, doğum tarihi, telefon numarası gibi kolay tahmin edilebilir olmamalıdır.
6. Başkalarıyla paylaşılmamalı, e-posta iletilerine, herhangi bir elektronik forma, kağıtlara ya da elektronik ortamlara yazılmamalıdır.

İşten uzakta olunan zamanlarda iş arkadaşlarına verilmemelidir.

Uzaktan Erişim

1. Fakültemizde sunucuların yerinde çözülmesi zor olan durumlar için veya dışarıdan yetkili bir kişi veya kuruluştan yardım almak için sunuculara uzaktan erişim yoluyla bağlantı sağlanabilir.
2. Uzaktan erişim yapacak kullanıcılar için belirlenen bilgisayar üzerinde güvenli bir yazılımla bağlantı yapılmaktadır.
3. Uzaktan bağlantı yapılan tarih ve yapılan işlemler kayıt altına alınmaktadır.
4. Bağlantı şifreleri uzaktan bağlantı yapacak kişiler haricinde başka kullanıcılara verilmez.

Kablosuz Erişim

1. Fakültemizde kablosuz olarak internete bağlanmak veya ağa erişmek isteyen kullanıcılar, bilgi işlem biriminde bilgisayarlarının güvenlik yapılandırmasını yaptırmaları gerekmektedir.
2. Kullanıcı işlemlerini kaydetmek ve izleyebilmek amacıyla kablosuz erişim cihazları mac-ip eşleştirme yöntemiyle statik ip kullanmaktadır.