07/10/2005 Tarih ve 45 sayılı makam oluru ile Sağlık Bakanlığının bütün kurum ve kuruluşlarında Bilgi Sistemleri ile ilgili uyulması gereken bilgi güvenliği hususları ve bu hususlardan sorumlu olacak kişiler ile ilgili politikalar T.C. Sağlık Bakanlığı Bilgi Güvenliği Politikasının dokümanında belirlenmiştir.

Bu kapsamda hastanemiz çalışanı olarak, bulunduğunuz servis sorumlusuna dağıtılmış olan T.C. Sağlık Bakanlığı Bilgi Güvenliği Politikası dokümanını okumanız ve buna uygun çalışmanız gerekmektedir. T.C. Sağlık Bakanlığı Bilgi Güvenliği Politikası dokümanına ve aşağıda size dokümanın özeti olarak belirtilen konulara özellikle dikkat etmeniz ve belirtilen maddelere uygun çalışmanız gerekmektedir.

Bilgi Güvenliği Politikasını okuduktan sonra Bilgi Güvenliği Politikası Onayı Formunu imzalayarak güvenlik politikası şartlarını kabul etmeniz gerekmektedir. Bu doküman içerisinde belirtilen güvenlik politikalarını ihlal eden kurum çalışanları hakkında mevcut yasalar çerçevesinde idari soruşturma açılacaktır.

A) ŞİFRE KORUMA STANDARTLARI:

1. Şifreler en az 6 ayda bir değiştirilmelidir.

2. Herhangi bir kişiye telefonda şifre verilmemelidir.

3. E –Posta mesajlarında şifre belirtilmemelidir.

4. Üst yöneticilere şifreler söylenmemelidir.

5. Başkaları önünde şifreler hakkında konuşulmamalıdır.

6. Aile isimleri şifre olarak kullanılmamalıdır.

7. Herhangi form üzerinde şifre belirtilmemelidir.

8. Şifreler aile bireyleri ile paylaşılmamalıdır.

9. Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirilmemelidir.

** Herhangi bir kimse şifre istediğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem Birimi yetkilisini aramasını söyleyiniz.

B) İNTERNET ERİŞİM VE KULLANIM POLİTİKASI:

1. Hiç bir kullanıcı internet üzerinden Multimedia Streaming (MSN) yapamayacaktır.

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

3. İş ile ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek ve indirmek (dawnload) etmek yasaktır.

4. İnternet üzerinden, kurumun yetkili birimlerinden yazılı onay alınmaksızın kurum adına elektronik işlem yapılamaz.

5. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve Sağlık Bakanlığı sistemleri üzerine bu yazılımlar kurulamaz. Kurumsal işlevlere yönelik yazılım ihtiyaçları için ilgili prosedürler dahilinde Sağlık Bakanlığı Bilgi İşlem Sorumlularına müracaat edilmesi gerekmektedir.

C) BİLGİ SİSTEMLERİNİN GENEL KULLANIM POLİTİKASI:

Uygunsuz Kullanım: Genel olarak aşağıdaki eylemler yasaklanmıştır. Sistem yöneticileri bu kapsamın dışında olabilir. Herhangi bir kullanıcı kurumun kaynaklarını kullanarak hiçbir şart altında herhangi bir yasadışı aktivitede bulunamaz.

Sistem Ve Ağ Aktiviteleri:

Aşağıdaki aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.

1. Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer şirket bilgileri, yazılım lisansları vs. haklarını çiğnemek.

2. Kitapların izinsiz kopyalanması, magazindeki fotoğrafların dijital formata dönüştürülmesi, lisan gerektiren yazılımların kopyalanması.

3. Zararlı programların (virus, solucan, truva atı, e- mail bombaları vs.) ağa veya sunuculara bulaştırılması.

4. Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırmak. Bu evden çalışırken aile bireylerini de kapsar.

5. Kurumun bilgisayarını kullanarak taciz veya yasadışı olaylara karışmak.

6. Ağ güvenliğini etkilemek.(bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi gibi) veya ağ haberleşmesini bozmak.

7. Port veya ağ taraması yapmak.

8. Kullanıcı kimlik tanıma yöntemlerinden kaçmak.

9. Program/script/komut kullanarak kullanıcının bağlantısını etkilemek.

10. Kurum bilgilerini kurum dışından üçüncü şahıslara iletmek.

11. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Şubesinin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapması.

12. Cihaz, yazılım ve verinin izinsiz olarak kurum dışına çıkarılması.

13. Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları (dergi cd leri veya internetten indirilen programlar vs) kurmak ve kullanmak yasaktır.

E-Mail Ve Haberleşme Aktiviteleri:

1. Kurum dışından web posta sistemini güvenliğinden emin olunmayan bir bilgisayardan kullanmak.

2. İstenilmeyen e- posta mesajlarının iletilmesi.

3. E-posta veya telefon vasıtası ile taciz etmek.

4. E-posta başlık bilgilerini yetkisiz kullanmak veya değiştirmek.

5. Zincir e-postaları oluşturmak veya iletmek.

6. İş ile alakası olmayan mesajları birçok haber gruplarına iletmek.

D) KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ POLİTİKASI:

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

1. Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; gizlilik, bütünlülük ve erişebilirliliktir.

2. Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalı, yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.

3. Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidir. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilirler.

4. Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.

5. Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.

6. Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programları, vs. buna dahildir.

7. Hiçbir hasta kaydı, elektronik veya kâğıt ortamında (Bakanlığımızın bu konularda çıkardığı genelgeler hariç) hiçbir kuruma veya üçüncü şahıslara sözlü veya yazılı olarak teslim edilemez.(Yürürlükteki genelgelere göre hasta sağlık bilgilerini Sosyal Güvence Kurumları (Bağ kur, SSK, ES, GSS) elde edebilir. Özel sigorta kurumları hastanın sağlık bilgilerini elde edemez.

8. Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır.(Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi.)

9. Telefon ile konuşurken hasta ile ilgili mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen gösterilmelidir.

10. Bütün hasta sağlık kayıtları fiziksel olarak korunmuş mekânlarda saklanmalıdır.

11. Elektronik hasta kayıtlarına internet ortamından erişim mümkün olmamalıdır.

12. Bu metne birim sorumlularından ya da web sitemiz (surmenedh.gov.tr) üzerinden (personel sekmesinden) ulaşabilirsiniz.

E) BİLGİ GÜVENLİĞİ POLİTİKASI ONAYI

Bu yazı Sağlık Bakanlığı Bilgi Güvenliği Politikasının okunduğu, anlaşıldığı ve kabul edildiğinin onaylandığı bir dokümandır.

F) İZLENECEK PROSEDÜR

Aşağıdaki adımlar takip edilmelidir.

1. Bilgi Güvenliği Politikasını okuyunuz.

2. Aşağıda bilgi güvenliği onay formunda belirtilen bölümlere tarih atınız ve imzalayınız.

G) YETKİLENDİRİLDİĞİNİZ BİRİMLER:

1. Yetkilendirildiğiniz birimler HBYS giriş ekranında bulunmaktadır.

H) ANLAŞMA

Bu metne imza atarak yukarıda yazılanları kabul etmiş oluyorum.

Sağlık Bakanlığı Bilgi Güvenliği Politikasını okudum ve anladım.

BİLGİ GÜVENLİĞİ POLİTİKASI SÖZLEŞME ONAY FORMU

ÇALIŞANIN ADI SOYADI	GÖREVİ	HBYS KULLANICI ADI	TARİH	ÇALIŞANIN İMZASI