HASTANEMİZDE BİLGİ GÜVENLİĞİ ÇALIŞMALARI

Bilgi İşlem Biriminin koordinesinde Bilgi Güvenliği Ekibi kurulmuş ve çalışmalarına devam etmektedir.

Bu ekibin en önemli görevleri arasında hastanemiz çalışanlarının bilgi güvenliği konusunda bilgilendirilmesini ve bilinçlendirilmesini sağlamaktır.

Ayrıca mevcut durum Bilgi Güvenliği açısından analiz edilerek risklerin belirlenmesini sağlamak ve bu konuda gerekli tedbirlerin alınması için hastane yönetimine önerilerde bulunmaktır.

Bilgi Güvenliği Ekibine Bilgi İşlem sorumlusu vasıtasıyla ulaşabilirsiniz.

Hastanemizin Bilgi Yönetimi Prosedürü hazırlanmış bu konudaki işleyişler açıkça tarif edilmiştir.

Bu işleyiş kapsamında

- Bilgisayar açma kullanma
- İnternet erişim izni verilmesi
- USB-CD kullanım izni verilmesi
- HBYS modül kullanım yetkisi verilmesi
- HBYS'nin hizmet vermediği durumlarda yapılacak işlemler
- HBYS'nin hizmet vermediği durumlarda tetkik istemleri

Bilgi güvenliği politikasına ve formlarına hastanemizin lokal internet sayfasından veya

http://10.61.0.18/index.php/kalite-yonetim-birimi-h-k-s-dokumanlari/viewcategory/967-31-bilgi-yonetim-sistemi

adresinden ulaşabilirsiniz.

HASTANEMİZDE BİLGİ GÜVENLİĞİ İHLALİ

HBYS şifrenizin başkası tarafından kullanıldığını, sizin kullanıcınız ile başkaları tarafından işlem yapıldığını Bilgi Güvenliği ihlaline uğradığınızı düşünüyorsanız,Lütfen aşağıdaki adresten bildirminizi yapınız

https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir

ÖNEMLİ İNTERNET ADRESLERİ

http://www.bilgiguvenligi.gov.tr/
http://www.bilgiguvenligi.saglik.gov.tr/
http://www.bilgimikoruyorum.org.tr/

LOKAL İNTERNET ADRESİ

http://10.61.0.18/index.php/kalite-yonetim-birimi-h-k-s-dokumanlari/viewcategory/967-31-bilgi-yonetim-sistemi

GÜÇLÜ PAROLA GÜÇLÜ GÜVENLİK

ŞİFRENİZİ KİMSEYLE PAYLAŞMAYINIZ

YETKİSİZ KİŞİLERE HASTA BİLGİSİ VERMEYİNİZ

Bilgi Güvenliği Ekibi:
Dr.Ali ÇELİK
Halit KAHVECİ (Müdür)
Ali RIza ALTUNTAŞ (Md. Yrd)
Öner KARSLI (Md. Yrd.)
Hüseyin ARSLANOĞLU (BİM Sorumlusu)

Bilgi Güvenliği

KANUNİ EĞİTİM VE ARAŞTIRMA HASTANESİ-TRABZON

2019

Merhaba

Bu broşür personelimizin Bilgi Güvenliği konusunda bilinçlendirmek amacıyla “Bilgi Güvenliği Ekibi” tarafından hazırlanmıştır.

Broşürü dikkatle okuyunuz, önerilere mutlaka uyunuz. Bilgi Güvenliği Ekibi olarak çalışmalarınızda başarılar diliyoruz.

HBYS KULLANIMI

1. HBYS program girişlerinizi kendi kullanıcı kodunuz ve şifreniz ile giriş yapınız. Başka kullanıcıya ait şifre ile giriş yapılması suç teşkil etmektedir.
2. HBYS ve bilgisayar-yazıcı gibi donanımlar ile ilgili problemlerinizi HBYS ana giriş ekranındaki “ARIZA BİLDİR” butonuna tıklayarak bildiriniz. Telefon ile yapılan bildirimler acil olmadığı sürece kabul edilmeyecektir.
3. Şifrenizi başkasına göstermeyiniz ve vermeyiniz. HBYS üzerinde yapılan tüm veri girişi ve işlemlerin sorumlusu kullanıcı kişiye aittir.
4. Bilgi işlem tarafından verilen şifreyi ilk program girişinde mutlaka değiştiriniz. Yeni şifre oluşturma yöntemi hakkında broşürde yer alan “Şifre Oluşturma Yöntemi” bölümünü okuyunuz.
5. Kullanıcıların HBYS işlemleri kayıt altına alınmakta olup, işlem bazlı logları tutulmaktadır.
6. Kısa süreli de olsa bilgisayardan ayrıldığınızda mutlaka HBYS programınızı kapatınız.
7. Yaptığınız görevin haricinde yetki kullanımı (görevi haricindeki modüller) yapmayınız. Gereksiz yetkilerinizi bilgi işleme bildirerek iptal ettiriniz.
8. Hasta bilgilerini hastanın istemi dışında kimseyle paylaşmayınız.
9. Hasta mahremiyet ilkelerine lütfen uyunuz.
10. Görev değişikliğinde gereksiz modül ve yetkilerinizi iptal ettiriniz.
11. Görevlendirildiğiniz ve yetkilendirildiğiniz modül veya birimle ilgili işlemleri yapınız. Görev ve yetki dışı işlemler yapmayınız.

BİLGİSAYAR KULLANIMI

1. Bilgisayarınızı yetkisiz kişilere kullandırmayınız, Şifrenizi vermeyiniz.
2. Mesai bitiminde bilgisayarınız ve bağlı cihazları mutlaka kapatınız. Bilgisayar başından kısa süreli ayrılmalarda “CTRL ALT DELETE tuşlarına birlikte basıp ENTER tuşu ile bilgisayarınızı kilitleyebilirsiniz. Açmak için aynı yolu deneyiniz.
3. Bilgisayarları sadece iş amacı için kullanınız. İş amacı dışında kullanmayınız. (oyun oynamak, müzik dinlemek, film izlemek, sistem performansını düşürecek programları kurmak vb.)
4. Bilgisayar ve yan donanımlarında meydana gelen arızalara müdahale etmeyiniz, bilgi işleme bildiriniz.
5. Yasadışı ya da lisansı olmayan program ve yazılımları kurmayınız.
6. Kullanıcı hatalarından dolayı meydana gelebilecek(donanım üzerine su, çay dökülmesi, yere düşüp kırılması vb.) hasarlardan kullanıcı sorumlu tutulmaktadır.
7. Bilgisayarda saklanılan kişisel dosya/verilerin yedeklemesi kullanıcıya aittir. Bilgi işlem çalışanı sorumlu tutulamaz. Lütfen belgelerinizin yedeğini alınız.

İNTERNET KULLANIMI

Hastanemizde network altyapısının imkânları ölçüsünde internet hizmeti verilmektedir. İnternet kullanımı kullanıcının görev pozisyonu göz önünde bulundurularak gruplandırma yapılmak suretiyle sağlanmaktadır.

Sistem ve Ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Kurumun bilgisayar ağı, kurumun birincil amaçlarına hizmet etmek üzere yapılmıştır. Ağ üzerindeki kişisel kullanımlar hiçbir zaman diğer kullanıcıların birincil ağ erişim gereksinimlerini yerine getirmelerine engel olmamalıdır.

Kurum İnternetini aşağıdaki amaçlarla kullanılması yasaklanmıştır.

1. Başka bir kullanıcının posta sunucusunu (mail sunucu), o kullanıcının açık izni olmadan mesaj gönderme amacıyla kullanılması;
2. Kullanım amaçlarına uygun olmayan, müstehcen, rahatsız edici materyalin üretilmesi ve dağıtılması;
3. Gerçek dışı, rahatsızlık verici, gereksiz yere sıkıntı ve korku yaratacak materyalin üretimi ve dağıtımı;
4. Başkalarının fikri haklarını ihlal edici mahiyette (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri ve benzeri konularda) dağıtımı;
5. Hastane İnternet Ağı üzerinden ulusal veya uluslararası hizmetlerin kasıtlı olarak yetkisiz kullanımı;
6. Başkalarının verilerinin tahrip edilmesi;
7. Başkalarına ait kişisel bilgilerine izinsiz erişilmesi;

Hastanemizde internet kullanım yetkisi bulunan kullanıcılar 5651 sayılı " İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" gereği internet üzerinden yapacağım tüm işlemlerin kayıt altına alınacağını bildiği her türlü sorumluluğu kabul ettiği var sayılmaktadır.

ŞİFRE OLUŞTURMA YÖNTEMİ

Kullanılacak şifrenin sizin adınıza sistem girişi sağlayacağını, bütün işlemlerin sorumluluğunu size yükleyeceğini unutmamalısınız. Bu amaçla uymanız gereken birkaç kuralla basit, güvenli, hatırlanabilir, sizi yansıtabilir güvenli şifreler oluşturabilirsiniz. Bu amaçla aşağıda belirtilen kurallara uyunuz:

1. Parola en az 8 karakterden oluşmalıdır.
2. Harflerin yanı sıra, rakam ve “ @, !, #, %, +, -, * ” gibi özel karakterler içermelidir.
3. Büyük, küçük harf ve rakamlardan oluşan bir kombinasyon kullanılmalıdır.
4. Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin; 12345678, doğum tarihiniz, çocuğunuzun ya da eşinizin adı, soyadı gibi)
5. Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
6. Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.
7. Basit bir kelimenin yanına benzer içerikte yerleştirilebilecek harf ve rakamlar parolanızı güçlü bir hale getirecektir.

Örneğin,

B yerine **8**	Z yerine **2**	Balıkçıl ➢ 8a11ç11 Kazak ➢ Ka2ak Solaryum ➢ 501aryum
I, i, L, yerine **1**	O yerine **0**	
S yerine **5** - G yerine **6**	G yerine **9**	