1. AMAÇ

Bu politika, T.C. Sağlık Bakanlığı KİLİS DEVLET HASTANESİ tesisindeki kâğıtlar, taşınabilir depolama ortamları ve kişisel bilgisayar için mesai saatleri içinde ve dışında bilgiye yetkisiz erişim ve bilginin hasar görmesi gibi riskleri azaltmak amacıyla gerekli olan şartları tanımlamak amacıyla hazırlanmıştır.

1. KAPSAM

Bu politika, T.C. Sağlık Bakanlığı KİLİS DEVLET HASTANESİ bünyesinde ve bağlı tesislerinde çalışan tüm personeli kapsamaktadır.

1. POLİTİKA

3.1 Kuruma ait uygulamalarda kullanılan parolalar iş arkadaşları da dâhilolmaküzere kimse ilepaylaşılmamalı, parolalar yazılı olarak post-it ya da not kâğıtlarına yazılarak pano, bilgisayar ekranı, klavye gibi donanımlara yapıştırılmamalıdır.

3.2 Evrak ve dokümanların güvenliği için çalışma saatleri dışında ofis kapılarının kilitli tutulmasıgerekmektedir.

3.3 Evrak ve dokümanlarda ki bilgilerin farklı kişiler tarafından ele geçirilmemesi için klasörlerdesaklanmalıdır.

3.4 Hassas bilgi içeren evrak klasörleri ve kuruma aitbaşlıklı kâğıtlar kilitli dolaplarda saklanmalıdır.

3.5 Kâğıtların çöp kutularına atılması yerine, kâğıtimha makinalarında kırpılmasına dikkat edilmesigerekir.

3.6 Hassas ve kritik bilgi içeren evraklarağ üzerinden paylaşılamaz.

3.7 Masa üstü doküman sayısını artırmamak için mümkün olduğu kadar elektronik dokümanlarınyazıcıdan çıktılarının alınmamasına dikkat edilmelidir.

3.8 Masa üzerinde kartvizit kutuları, kişisel ajandalar, değerli bilgilere sahip dokümanlar bırakılmaz vebunların kilitli çekmecelerde muhafaza edilmesi gerekir.

3.9 Masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerindebırakılmamalıdır.

3.10 Kuruma ait kritik bilgi içeren dokümanlar başkaları tarafından fark edilmeyecek şekilde muhafazaedilmelidir.

3.11 Personelin kişisel gizli bilgileri maaş bordrosu gibi başkaları tarafından fark edilmeyecek şekildemuhafaza edilmelidir.

3.12 Personel telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranmalıdır.

3.13 Bilgi ve veri alışverişinden önce dış tarafların kimliklerinin tespit edilmesi gerekir.

3.14 Kurum bünyesinde kullanılan toplantı salonlarında gizli ve kritik bilgi içeren dokümanları toplantısonrasında ilgili salonlarda bırakmamalı ve salonlardaki tahtalara alınmış notlar silinmelidir.

3.15 Gizlilik içeren bilgilerin umumi yerlerde konuşulmaması gerekir.

3.16 Gizlilik içeren bilgiler, telefonlarda dışarıya ses açık olarak görüşülmemelidir. Faks yoluyla gizlilikiçeren herhangi bir bilgi gönderilmemelidir.

3.17 Bilgisayar gibi elektronik ortamlardabulunan bilginin korunması için çalışma saatleri dışında ofiskapılarının kilitli tutulması gerekir.

3.18 Kısa süreli ayrılmalarda dahi, cep telefonu,taşınabilirbellek, harici hard disk, CD, DVD gibi eşyalarçalışma masası üzerinde bırakılmamalıdır.

3.19 Bilgisayarlar gözetimsiz bırakıldığında kapatılmalı veya parola kullanılarak korunmalıdır.Ekrankoruyucusu aktif hale getirilmelidir.

3.20 Fotokopi cihazlarının yetkisiz kullanımı önlenmelidir.

3.21 Fotokopi cihazlarının belleğinde bulunan kritik vehassas bilgiler silinmelidir.

3.22 Hassas ve sınıflandırılmış bilgi içeren ortamlarda ki bilgiler yazıcıdan çıktı alındıktan sonra hemensilinmelidir.

3.23 Parolalar yazılı olarak saklanmamalı ve gizli tutulmalıdır.

3.24 Kullanılan parolalar tahmin edilebilir olmamalıdır. Parolayı oluşturan kişi ile ilgili bilgiler içermemelidir.Ardışık, tümü sayısal ya da tümü alfabetik karakterlerden oluşmamalıdır. Parola Yönetimi Politikası kurallarına göre belirlenmeli.

3.25 Personelbilgisayarındaki,Taşınabilir belleğindeki, harici diskte ve benzeri depolamanın mümkünolduğu ortamlarda ki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. Taşınabilir bellek veya harici diske gizli veya önemli veri konulması gerekiyorsa kriptolayarak korunması gerekmektedir.

3.26 Gizli belgelerin,parolaların, adreslerin, özellikle taşınabilirbellek, e-posta, sosyal medya gibi alanlardapaylaşılmamasına dikkat edilmelidir.

3.27 Bilinmeyen e-posta ve haber gruplarına üye olunmamalıdır.

3.28 Elektronik posta ortamında kişisel parola bilgileri paylaşılmamalıdır.

3.29 Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımdan sonra etkin yöntemler kullanılarak geridönülmeyecek şekilde silinmesi gerekir.

3.30 Kuruma ait yürütülen iş ve işlemlerdeT.C.Sağlık Bakanlığı e-posta*(@saglik.gov.tr*) adresikullanılmalıdır.

3.31 Kurumsal işlerin yapıldığı bilgisayarlar personelin kendi sorumluluğundadır. Kurum bilgisayarlarınıpersonel haricinde yetkisiz kullanıcılara teslim edilmemelidir.

4. YAPTIRIM

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla BGYS Disiplin Prosedürü Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.