



T.C.
SAĞLIK BAKANLIĞI
KEMALPAŞA DEVLET HASTANESİ
BİLGİ GÜVENLİĞİ POLİTİKASI REHBERİ

DÖK.KODU : BY.RH.01

YAY.TRH: 29.02.2016

REV.TRH : 23.05.2019

REV.NO : 03

S.NO : 1/1

1. Bilgi Güvenliği Politikası Rehberi: Kemalpaşa Devlet Hastanesi bünyesinde yürütülen bilgi güvenliği çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu rehberde tüm birimleri ilgilendiren maddeler olduğu gibi sadece bazı birimleri ilgilendiren maddelerde bulunmaktadır. Bu rehberde genel bilgi güvenliği kuralları tanımlanmıştır. Kurumda çalışan tüm personel bu dokümanlarda belirtilen kurallara uymakla sorumludur.

2. AMAÇ: Bilgi Güvenliği Politikası Rehberi'nin amacı hastanemizdeki tüm bilgi varlıklarının gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişebilirliğini sağlamaktır.

Bilgi güvenliği bir kurumda yalnızca bilgi işlem biriminin konusu değil, tüm birimlerin katılımı ile başarılabilir bir konudur. Buna bağlı olarak bilgi güvenliği sadece bilgi teknolojileri alanındaki teknik önlemler ile sağlanamaz. İnsan kaynakları ve zafiyetleri yönetimi, parola güvenliği, bilgi kaynakları, atık ve imha yönetimi, internet ve elektronik posta güvenliği, bilgi güvenliği ihlal bildirim ve yönetimi gibi bir çok konudaki bilgi güvenliği çalışmalarımızın genel özeti bu rehberde verilmektedir. Uygulama detay bilgileri için ilgili prosedürlere bakılmaktadır. Bu rehber, bilgi güvenliği prosedürlerini kapsayan bir üst dokümandır.

Bilgi Güvenliği Politikası Rehberimiz hastane yönetimi tarafından onaylanarak yayınlanmıştır. Yönetim tarafından düzenli olarak gözden geçirilmektedir.

3. KAPSAM: Bilgi Güvenliği Politikası Rehberi hastanemiz tüm birimlerini kapsamaktadır.

4. TANIMLAMALAR VE KISALTMALAR:

4.1. Veri: Sayısal ve mantıksal her bir değere (sayı, rakam, sembol) veri denir. Örneğin: Ali, İzmir, 1925.

4.2. Bilgi: Verinin işlenmiş haline bilgi denir. Örneğin: Ali 1925'te İzmir'de doğdu.

4.3. Gizlilik: Bilgiye yalnızca yetkili kişilerin, varlıkların ve süreçlerin erişebilmesidir.

4.4. Bütünlük: Bilginin doğruluk, bütünlük ve kendisine has özelliklerinin korunmasıdır.

4.5. Erişilebilirlik: Bilginin yetkili kişiler, varlıklar ve süreçler tarafından istenildiğinde ulaşılabilir ve kullanılabilir olmasıdır.

4.6. Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkar edememe ve güvenilirlik gibi diğer özellikleride kapsar.

5. BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

5.1. Bilgi Güvenliği Takımı ve Yetkileri

T.C.Sağlık Bakanlığının Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzu gereği hastanemiz bünyesinde bu rehberin 2.maddesinde yer alan kapsam dahilinde bilgi güvenliği gerekliliklerini yürütmek üzere bilgi güvenliği yetkilileri belirlenmiş ve bilgi güvenliği komisyonu oluşturulmuştur.



T.C.
SAĞLIK BAKANLIĞI
KEMALPAŞA DEVLET HASTANESİ
BİLGİ GÜVENLİĞİ POLİTİKASI REHBERİ

DÖK.KODU : BY.RH.01

YAY.TRH: 29.02.2016

REV.TRH : 23.05.2019

REV.NO : 03

S.NO : 2/1

5.2. Bilgi Güvenliği Yetkilileri

Bilgi Güvenliği Yetkilisi İdari ve Mali Hizmetler Müdürü tarafından belirlenir. Başhekimlik tarafından onaylanır. Hastanemiz Bilgi Güvenliği Yetkilileri olarak V.H.K.İ Ragıp ERDUHAN ve Bilgi İşlem Sorumlusu İbrahim BİBER belirlenmiştir.

5.3. Bilgi Güvenliği Komisyonu

Bilgi Güvenliği komisyonu Hastane Yöneticisi Başhekim Yardımcısı tarafından oluşturulur. Başhekim tarafından onaylanır. Komisyon Başkanı Hastane Yöneticisi Başhekim Yardımcısıdır. Hastanemiz Bilgi Güvenliği Komisyonu; Sağlık Bakım Hizmetler Müdür Yardımcısı, Satın Alma Birimi Sorumlusu, Kalite Yönetim Direktörü, Tıbbi Sekreterden oluşur.

6. ORGANİZASYON ŞEMASI

6.1. Bilgi Güvenliği Üst Yönetim Görev, Yetki ve Sorumluluklar:

- 6.1.1. Bilgi Güvenliği Komisyonu tarafından bilgi güvenliği konularında geliştirilen politika ve prosedürleri uygulamak üzere gerekli alt yapıyı oluşturmak için hazırlanmış projelere gerekli kaynağı sağlamak.
- 6.1.2. Bilgi Güvenliği Komisyonu tarafından oluşturulan Bilgi Güvenliği Politikası Rehberini ve prosedürlerini onaylamak.
- 6.1.3. Çalışmaların yürütülebilmesi için yatırım kararlarına, hastanemizde Bilgi Güvenliği Komisyonu tarafından yapılması önerilen çalışma süreçleri, usul ve esaslara dair değişiklikleri onaylamak.
- 6.1.4. Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanları (yüklenici firma personeli dahil) bilgi güvenliği farkındalığının artırılmasına yönelik planlanan çalışmaların etkinliğinin artırılması için teşvik edici faaliyetleri onaylamak.

6.2. Bilgi Güvenliği Yönetim Sistemi Yetkilisi Görev, Yetki ve Sorumlulukları:

- 6.2.1. Bilgi Güvenliği konularının alt yapısını oluşturacak projeler hazırlanmasını sağlamak.
- 6.2.2. Hastanemizde yürütülen Bilgi Güvenliği faaliyetlerinin T.C. Sağlık Bakanlığının Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzu'na uygun şekilde yürütülmesi için gerekli çalışmaları yapmak.
- 6.2.3. Bilgi Güvenliği dökümanları'nın hazırlanmasına rehberlik etmek ve hazırlanan dökümanları onaylamak.
- 6.2.4. Üst Yönetim onayı gerektiren dökümanların üst yönetim tarafından onaylanmasını sağlamak.
- 6.2.5. Projelerin yürütülebilmesi için gerekli olan ihtiyaçların temin edilmesini sağlamak.