

Sayfa No:
1/2**Doküman Kodu:**
PR.BİM.016**Yayın Tarihi:**
16.07.2020**Revizyon Tarihi:**
16.07.2020**Revizyon No:**
0

1. GENEL BAKIŞ

Bilgi Güvenliği; gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda hayati öneme sahip bilginin korunması, bütünlüğünün sağlanması, erişebilir ve ulaşılabilir olmasının sağlanması için alınan gerekli ve önemler ve tedbirlerdir.

- Gizlilik: Bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır.
- Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.
- Kullanılabilirlik: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

2. KAPSAM

Bu politika, Hisar Hastanesi'nin tüm çalışanları, stajyerleri ile dış kaynak çalışanlarını kapsar. Tüm kullanıcılar bu politika içeriğinde yer alan sorumluluk ve yasal zorunluluklarının bilincinde hareket etmek zorundadırlar.

3. HEDEF

Bu politikanın hedefi; kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak, üçüncü taraflarla yapılan sözleşmelerde uygunluğu sağlamak, kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devamlılığını sağlamaktır.

4. SORUMLULUK

Bilgi Güvenliği Yönetim Kurulu kapsam çerçevesinde şirket bilgi varlıklarına yönelik risklerin üst yönetim tarafından onaylanan kabul edilebilir seviyede tutulmasından sorumludur.

5. BİLGİ GÜVENLİĞİ İLKELERİ

- Gizli bilgilerin korunması ilkesi ile diğer politika ve dokümanlara öğrenmek ve bunlara uymak,
- Kişisel ve elektronik iletişimde şirkete ait bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak,
- Şirket içi bilgi kaynaklarını(doküman, duyuru vb.) yetkisiz olarak 3.kişiler ile paylaşılmaması,

Hazırlayan:
BİLGİ İŞLEM MÜDÜRÜ**Kontrol Eden:**
KALİTE DİREKTÖRÜ**Onaylayan:**
MESUL MÜDÜR

Sayfa No:
2/2**Doküman Kodu:**
PR.BİM.016**Yayın Tarihi:**
16.07.2020**Revizyon Tarihi:**
16.07.2020**Revizyon No:**
0

- Hisar Hastanesinin müşterileri, iş ortakları, tedarikçiler veya üçüncü kişilere ait bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak.
- Şirket bilgi sistemlerini altyapılarını mevzuata aykırı faaliyetler amacıyla kullanmamak,
- Bilgi Güvenliği ihlal olaylarını raporlamalı, bu ihlalleri önleyecek önlemler alınmalıdır.
- Bilgi Güvenliği politikasının uygulanabilirliği, koyulan kurallar ve alınan önlemlerin işleyişi sekteye uğratmaması adına belirli aralıklarla bu yapılar gözden geçirilmeli, sürekli geliştirilmesi yapılmalı ve aksiyon planları hazırlanmalıdır.
- Bilgi Güvenliğinin riskleri tanımlanmalı, değerlendirilmeli ve bunlara göre risk işleme planı hazırlamaktır.

6. KURALLARIN İHLALİ VE YAPTIRIMLAR

Bu politikanın ihlal edilmesi durumunda Hisar Hastanesi Bilgi Güvenliği ekibi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Bilgi Güvenliği politikasına, prosedürlerine ve talimatlarına uyulmaması halinde kurum uyarma, kınama, para cezası ve sözleşme feshi gibi aksiyonları uygulayabilir.

Hazırlayan:
BİLGİ İŞLEM MÜDÜRÜ**Kontrol Eden:**
KALİTE DİREKTÖRÜ**Onaylayan:**
MESUL MÜDÜR