YAKIN DOĞU ÜNİVERSİTESİ HASTANESİ

BİLGİ İŞLEM MÜDÜRLÜĞÜ BİLGİ GÜVENLİĞİ PROSEDÜRÜ				
Doküman No:	İlk Yayın Tarihi:	Revizyon Tarihi:	Revizyon No:	Toplam Sayfa Sayısı:
BIS_P_02	02.01.2023	-	-	4

REVİZYON DURUMU

“Revizyon Tarihi”	“Açıklama”	“Revizyon No”

Hazırlayan	Kontrol Eden	Onaylayan
Bilgi İşlem Müdürlüğü	Kalite Koordinatörü	Hastaneler Yönetim Kurulu Başkanı

1. AMAÇ: Hastanelerdeki bilgilerin yönetilmesini, korunmasını dağıtımını ve önemli işlemlerin korunmasını sağlamak.

2. KAPSAM: Prosedür bilgi sistemleri bilgi güvenliği sürecine ilişkin faaliyetlerini kapsar.

3. KISALTMALAR: -

4. TANIMLAR:

4.1. Bilgi: Diğer önemli varlıkları gibi, kurum için değeri olan ve bu nedenle uygun olarak korunması gereken varlıktır. Bilgi birçok biçimde bulunabilir. Kâğıt üzerine yazılmış ve basılmış olabilir, elektronik olarak saklanmış olabilir, posta yoluyla veya elektronik imkânlar kullanılarak gönderilebilir, sunularda/filmlerde gösterilebilir veya karşılıklı konuşma sırasında sözlü olarak ifade edilmiş olabilir.

4.2. Bilgi Güvenliği: Bilgiyi; sürekliliği sağlamak, maddi ve/veya manevi kayıpları en aza indirmek ve maddi ve/veya manevi fırsatların ve yatırımların dönüşünü en üst seviyeye çıkartmak için, geniş tehlike ve tehdit alanlarından korumaktır.

4.3. Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması, kullanıcılardan gizlilik sözleşmesi alınır.

4.4. Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması,

4.5. Kullanılabilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması.

5. SORUMLULAR: Kurumumuz sağlık hizmetlerinin büyük bölümünü Elektronik ortamda gerçekleştirmektedir. Bu yönetmelik, kurum Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarının sorumluluğundadır.

6. UYGULAMA:

Bilgi Güvenliği Hedefleri:

6.1. Hastanede bilgi güvenliği hedefleri aşağıdaki gibi sıralanmıştır.

a) Kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak,

b) Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,

c) Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

d) Bilgi güvenliği konusunda tüm kullanıcılara farkındalık eğitimi ayrıca etkin kullanım, bilgi yönetim sistemi uygulamaları yılda bir kez verilir ve tüm güncellemelerde eğitim verilir.

6.2. Bilgi Güvenliği İlkeleri

6.2.1. Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:

- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
- Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli. Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,
- Verilerin gizliliği, güvenliği veya bütünlüğünü ihlal eden olaylar takip edilerek raporlamalı ve Bilgi İşlem Müdürlüğü'ne bildirmeli ve ilgili müdürlük bu ihlalleri engelleyecek önlemleri almalıdır.

6.2.2. Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3. kişilere iletilemez.

6.2.3. Kurum bilişim kaynakları, K.K.T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.

6.2.4. Hastanede bünyesinde bilgi güvenliğine yönelik olarak aşağıdaki uygulamalar gerçekleştirilmektedir:

6.2.4.1. Hastane Bilgi Yönetim sisteminin etkinliği ve sürekliliği için gerekli teknik ve destek alt yapıları oluşturulur.

6.2.4.2. Donanım birimi 24 saat ulaşılabilir durumdadır. İletişim bilgileri, santral ve birimde her ay güncellenir. Olası sorunlarda tüm kullanıcılar bu listeye göre irtibat geçebilir.

6.2.4.3. Hastane bilgi yönetim sisteminin devre dışı kaldığı durumlar İnovasyon Merkezine bağlı personel tarafından kayıt altına alınır.

6.2.4.4. Aksaklık meydana gelirse, iyileştirme çalışmaları yapılır. Her bölümün sorumluluğunda ve revizyonu bölüm sorumlusuna ait olan kısayollarda HBYS acil durum klasörleri bulunmaktadır.

6.2.4.5. Sunucuların güvenliğine ilişkin düzenlemeler, "**Bilgi Sistemleri Sunucu ve Sistem Odası Güvenliği Prosedürü"**nde tanımlanmıştır.

6.2.4.6. Yedeklemeye ilişkin düzenlemeler, **Bilgi Sistemleri Yedekleme Prosedürü**'nde tanımlanmıştır. Her yıl en az bir kez "**Bilgi Sistemleri Yedekten Dönme Tatbikat Formu"** kullanılarak yedeklenen verilerin güvenliği test edilir.

6.3. Veri Bütünlüğü ve İş Sürekliliğinin Sağlanması

6.3.1. Hastane veri sistemlerinin planlı ya da plansız bir şekilde devre dışı kalması ya da çökmesi durumlarında bilgi güvenliğinin sağlanarak klinik ve diğer destek süreçlerinin aksamadan sürdürülmesi amacıyla "**Bilgi Sistemleri Hizmet Dışı Kalma Durumları İçin Acil Durum Planı"** doğrultusunda hareket edilir.

6.3.2. Veri sistemlerinin çökmesi/devre dışı kalması durumlarında hastane işleyişinin sorunsuz bir şekilde sağlanabilmesi amacıyla "**Bilgi Sistemleri Hizmet Dışı Kalma Durumları İçin Acil Durum Planı"** doğrultusunda tüm çalışanlara eğitim verilir.

7. İLGİLİ DOKÜMANLAR:

7.1. Bilgi Sistemleri Haberleşme Prosedürü

7.2. Bilgi Sistemleri Yedekleme Prosedürü

7.3. Bilgi Sistemleri Sunucu ve Sistem Odası Güvenliği Prosedürü

7.5. Bilgi Sistemleri Yedekleme Prosedürü

7.6. Bilgi Sistemleri Yedekten Dönme Tatbikat Formu

7.9. Bilgi Sistemleri Hizmet Dışı Kalma Durumları İçin Acil Durum Planı