1. AMAÇ

Bu politikanın amacı; Karadeniz Teknik Üniversitesi Farabi Hastanesinde üretilen, işlenen, saklanan ve iletilen tüm bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak, bilgi güvenliği risklerini yönetmek ve bilgi güvenliği yönetim sistemine ilişkin temel kuralları belirlemektir.

---

2. KAPSAM

Bu politika;

- Farabi Hastanesi Bilgi İşlem Birimini,
- Hastanede kullanılan tüm bilgi sistemlerini (HBYS, PACS, LIS, Oracle veritabanı ve diğer yazılımlar),
- Sunucuları, ağ altyapısını, bilgisayarları ve ağa bağlı tıbbi cihazları,
- Fiziki ortamları (sunucu odaları, sistem odaları, ofis alanları),
- Hastane bünyesinde bilgi sistemlerini kullanan tüm personel, akademik personel, öğrenciler, stajyerler ve yetkilendirilmiş üçüncü tarafları

kapsar.

---

3. DAYANAK

Bu politika aşağıdaki mevzuat ve standartlar esas alınarak hazırlanmıştır:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 5651 sayılı Kanun
- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
- Sağlık Bakanlığı bilgi güvenliği düzenlemeleri
- Karadeniz Teknik Üniversitesi ilgili yönerge ve talimatları

---

4. TANIMLAR

- **Bilgi:** Kurum faaliyetleri kapsamında üretilen her türlü veri
- **Bilgi Varlığı:** Bilgiyi işleyen, saklayan veya ileten her türlü donanım, yazılım, insan ve fiziki ortam
- **BGYS:** Bilgi Güvenliği Yönetim Sistemi
- **Kullanıcı:** Bilgi sistemlerine erişim yetkisi verilen kişi

---

5. BİLGİ GÜVENLİĞİ POLİTİKASININ HEDEFLERİ

Farabi Hastanesinde bilgi güvenliği kapsamında aşağıdaki hedefler benimsenir:

- Kişisel ve özel nitelikli sağlık verilerinin korunması
- Yetkisiz erişimlerin önlenmesi
- Bilgi sistemlerinin sürekliliğinin sağlanması
- Bilgi güvenliği ihlallerinin azaltılması
- Yasal ve düzenleyici gerekliliklere tam uyum sağlanması

---

6. ORGANİZASYON VE SORUMLULUKLAR

6.1 Üst Yönetim

- Bilgi güvenliği politikasını onaylar.
- Bilgi güvenliği faaliyetleri için gerekli kaynakları sağlar.

6.2 Bilgi Güvenliği Sorumlusu

- Bilgi Güvenliği Sorumlusu, Bilgi İşlem Birimi Amiridir.
- Bilgi güvenliği faaliyetlerini koordine eder.
- Bilgi güvenliği ihlallerini yönetir ve raporlar.

6.3 Bilgi İşlem Birimi

- Bilgi güvenliği kontrollerini uygular.
- Teknik ve idari tedbirleri hayata geçirir.
- Bilgi sistemlerinin güvenli ve kesintisiz çalışmasını sağlar.

6.4 Kullanıcılar

- Bilgi güvenliği politika ve talimatlarına uymakla yükümlüdür.
- Kendilerine verilen yetkiler dışında işlem yapamaz.
- Güvenlik ihlallerini derhal Bilgi İşlem Birimine bildirir.

---

7. BİLGİ GÜVENLİĞİ TEMEL İLKELERİ

7.1 Gizlilik

- Bilgiler yalnızca yetkili kişiler tarafından erişilebilir.
- Kişisel ve sağlık verileri özel olarak korunur.

7.2 Bütünlük

- Bilgilerin doğruluğu ve güncelliği korunur.
- Yetkisiz değişiklikler engellenir.

7.3 Erişilebilirlik

- Bilgi sistemleri yetkili kullanıcılar için erişilebilir tutulur.
- Sistem kesintilerine karşı gerekli önlemler alınır.

8. RİSK YÖNETİMİ

- Bilgi varlıkları için düzenli risk analizleri yapılır.
- Riskler değerlendirilir ve işleme alınır.
- Yüksek riskler için önleyici ve düzeltici faaliyetler uygulanır.
- Risk analizleri periyodik olarak güncellenir.

---

9. BİLGİ GÜVENLİĞİ İHLALLERİ

- Bilgi güvenliği ihlalleri kayıt altına alınır.
- İhlaller Bilgi Güvenliği Sorumlusuna bildirilir.
- Gerekli durumlarda KVKK kapsamında bildirim yapılır.
- İhlaller sonrası düzeltici ve önleyici faaliyetler yürütülür.

---

10. EĞİTİM VE FARKINDALIK

- Tüm kullanıcılara bilgi güvenliği farkındalık eğitimi verilir.
- Yeni başlayan personele bilgilendirme yapılır.
- Eğitim faaliyetleri kayıt altına alınır.

---

11. DENETİM VE İZLEME

- Bilgi güvenliği uygulamaları düzenli olarak izlenir.
- İç denetimler gerçekleştirilir.
- Tespit edilen uygunsuzluklar için düzeltici faaliyetler uygulanır.

---

12. YAPTIRIMLAR

Bu politika hükümlerine aykırı davranışlar hakkında ilgili mevzuat, disiplin hükümleri ve yasal düzenlemeler uygulanır.

---

13. YÜRÜRLÜK VE GÜNCELLEME

Bu politika, Hastane Başhekimlik onayı ile yürürlüğe girer.
Politika yılda en az bir kez gözden geçirilir ve gerekli durumlarda güncellenir.
Güncelleme yetkisi Bilgi İşlem Birimi Amirindedir.