1. AMAÇ

Bu politikanın amacı; Karadeniz Teknik Üniversitesi Farabi Hastanesine ait bilgi sistemlerinin, donanımların, sunucuların ve bilgi varlıklarının bulunduğu fiziki ortamların yetkisiz erişim, sabotaj, hırsızlık, yangın ve çevresel tehditlere karşı korunmasına ilişkin usul ve esasları belirlemektir.

---

2. KAPSAM

Bu politika;

- Farabi Hastanesi Bilgi İşlem Birimini,
- Sunucu odaları, sistem odaları ve ağ dolaplarını,
- Bilgi İşlem ofislerini,
- Bilgi sistemlerinin bulunduğu tüm fiziki alanları,
- Bu alanlara erişimi bulunan tüm personeli ve yetkilendirilmiş üçüncü tarafları

kapsar.

---

3. DAYANAK

Bu politika aşağıdaki mevzuat ve standartlara dayanılarak 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

- **Fiziksel Güvenlik:** Bilgi varlıklarının bulunduğu alanların fiziki tehditlere karşı korunması
- **Sunucu Odası:** Kritik bilgi sistemlerinin bulunduğu özel alan
- **Yetkili Personel:** Fiziki alanlara erişim izni bulunan personel

---

5. GENEL İLKELER

- Fiziki alanlara erişim yetki esasına göre sağlanır.
- Kritik alanlara yalnızca yetkilendirilmiş personel girebilir.

- Fiziksel güvenlik önlemleri sürekli olarak izlenir ve kontrol edilir.
- Fiziki erişimler kayıt altına alınır.

---

6. SUNUCU VE SİSTEM ODALARI GÜVENLİĞİ

- Sunucu odalarına girişler sınırlandırılmıştır.
- Sunucu odalarında kamera sistemi bulunmaktadır.
- Sunucu odaları anahtarlı giriş sistemi ile korunmaktadır.
- Yetkisiz kişilerin sunucu odalarına girmesi yasaktır.
- Sunucu odalarında ısı ve nem kontrol sistemleri bulunmaktadır.
- Yangın algılama ve söndürme sistemleri mevcuttur.
- Sunucular kesintisiz güç kaynakları ile korunmaktadır.

---

7. BİLGİ İŞLEM OFİSLERİ VE SİSTEM DOLAPLARI

- Bilgi İşlem ofisleri yalnızca yetkili personel tarafından kullanılır.
- Sistem dolapları kilitli tutulur.
- Yetkisiz donanım bağlantısına izin verilmez.
- Fiziki ekipmanların yer değişikliği kayıt altına alınır.

---

8. ZİYARETÇİ VE ÜÇÜNCÜ TARAF ERİŞİMLERİ

- Ziyaretçiler fiziki alanlara yetkili personel eşliğinde alınır.
- Üçüncü tarafların erişimleri önceden planlanır ve sınırlandırılır.
- Ziyaretçi erişimleri kayıt altına alınır.

---

9. ÇEVRESEL TEHDİTLER VE ÖNLEMLER

- Yangın, su baskını ve aşırı ısınma gibi risklere karşı önlemler alınır.
- Fiziki güvenlik sistemlerinin bakımları periyodik olarak yapılır.
- Çevresel riskler düzenli olarak değerlendirilir.

---

10. FİZİKSEL GÜVENLİK İHLALLERİ

- Fiziksel güvenlik ihlalleri derhal Bilgi İşlem Birimine bildirilir.
- İhlaller kayıt altına alınır ve incelenir.
- Gerekli durumlarda disiplin ve yasal süreçler başlatılır.

---

11. EĞİTİM VE FARKINDALIK

- Yetkili personele fiziki güvenlik konusunda bilgilendirme yapılır.
- Fiziksel güvenlik kuralları düzenli olarak hatırlatılır.

---

12. YAPTIRIMLAR

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

---

13. YÜRÜRLÜK VE GÜNCELLEME

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