1. AMAÇ

Bu politikanın amacı; Karadeniz Teknik Üniversitesi Farabi Hastanesinde kullanılan bilgi sistemlerine erişimin **yetkilendirilmiş kişilerle sınırlı** olmasını sağlamak, yetkisiz erişimleri önlemek ve erişimlerin güvenli, izlenebilir ve kontrol edilebilir şekilde yönetilmesine ilişkin esasları belirlemektir.

---

2. KAPSAM

Bu politika;

- Farabi Hastanesi Bilgi İşlem Birimini,
- Hastane bilgi sistemlerini (HBYS, PACS, LIS, Oracle veritabanı ve diğer tüm yazılımlar),
- Sunucuları, ağ altyapısını ve uç nokta cihazlarını,
- Kablolu ve kablosuz ağ erişimlerini,
- Tüm çalışanlar, akademik personel, öğrenciler, stajyerler 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

- **Erişim:** Bilgi sistemlerine giriş ve kullanım yetkisi
- **Yetkilendirme:** Kullanıcılara görevlerine uygun erişim haklarının tanımlanması
- **Kullanıcı:** Bilgi sistemlerine erişim yetkisi verilen kişi
- **Rol:** Kullanıcının görev tanımına karşılık gelen yetki seti

---

5. GENEL ERİŞİM ESASLARI

- Bilgi sistemlerine erişim **yetki esasına** dayanır.
- Her kullanıcıya **kişiye özel** kullanıcı adı ve şifre tanımlanır.
- Paylaşımlı kullanıcı hesapları kullanılmaz.
- Erişim yetkileri **asgari yetki prensibine** göre verilir.
- Tüm erişimler kayıt altına alınır ve izlenir.

---

6. KULLANICI HESAP YÖNETİMİ

6.1 Kullanıcı Hesabı Açılması

- Kullanıcı hesapları, resmi talep ve onay süreci tamamlandıktan sonra açılır.
- Hesap açma işlemleri Bilgi İşlem Birimi tarafından gerçekleştirilir.
- Öğrenci ve stajyer hesapları **süreli** olarak tanımlanır.

6.2 Kullanıcı Hesabı Değişikliği

- Görev değişikliği durumunda erişim yetkileri gözden geçirilir.
- Gereksiz yetkiler kaldırılır.
- Değişiklikler kayıt altına alınır.

6.3 Kullanıcı Hesabı Kapatılması

- Kurumdan ayrılma, görev bitimi veya yetki iptali durumunda kullanıcı hesabı kapatılır.
- Hesap kapatma işlemleri gecikmeksizin yapılır.

---

7. ROL VE YETKİ YÖNETİMİ

- Kullanıcılara verilen yetkiler görev tanımlarına uygun olmalıdır.
- Kritik sistemlerde (HBYS, PACS, LIS, Oracle) yetkiler ayrıca onay gerektirir.
- Yönetici yetkileri sınırlı sayıda personele verilir.
- Yetkiler periyodik olarak gözden geçirilir.

---

8. AĞ ERİŞİM KONTROLLERİ

- Kablolu ve kablosuz ağ erişimleri kontrol altındadır.
- Ağ bağlantılarında MAC kimlik doğrulama uygulanır.
- Misafir kullanıcılar için ayrı bir kablosuz ağ altyapısı kullanılır.
- Akademik ve idari personel için Eduroam altyapısı kullanılır.
- Yetkisiz cihazların ağa bağlanması engellenir.

---

9. UZAKTAN ERİŞİM

- Uzaktan erişim yalnızca yetkilendirilmiş kullanıcılar için sağlanır.
- Uzaktan erişimler kayıt altına alınır.
- Gerekli durumlarda ek güvenlik önlemleri uygulanır.

---

10. ERİŞİM KAYITLARI VE İZLEME

- Kullanıcı erişimleri ve yetkilendirme işlemleri loglanır.
- Log kayıtları yetkisiz erişime karşı korunur.
- Şüpheli erişimler incelenir ve gerekli aksiyonlar alınır.

---

11. İHLALLER VE YAPTIRIMLAR

- Yetkisiz erişim veya yetki ihlali tespit edildiğinde gerekli işlemler yapılır.
- Erişim ihlalleri Bilgi Güvenliği Sorumlusuna bildirilir.
- İhlaller disiplin ve yasal yaptırımlara tabidir.

---

12. EĞİTİM VE FARKINDALIK

- Kullanıcılara erişim güvenliği konusunda bilgilendirme yapılır.
- Erişim kontrol kuralları düzenli olarak duyurulur.

---

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.