1. AMAÇ

Bu politikanın amacı; Karadeniz Teknik Üniversitesi Farabi Hastanesinde kullanılan bilgi sistemlerine erişimde kullanılan şifrelerin ve kimlik doğrulama mekanizmalarının güvenliğini sağlamak, yetkisiz erişimleri önlemek ve kullanıcı kimlik doğrulama süreçlerine ilişkin kuralları belirlemektir.

---

2. KAPSAM

Bu politika;

- Farabi Hastanesi Bilgi İşlem Birimini,
- Hastanede kullanılan tüm bilgi sistemlerini (HBYS, PACS, LIS, Oracle veritabanı ve diğer yazılımlar),
- Sunucular, ağ cihazları ve uç nokta sistemlerini,
- Bilgi sistemlerine erişim yetkisi bulunan tüm kullanıcıları (doktor, sağlık personeli, idari personel, akademik personel, öğrenci, stajyer ve yetkilendirilmiş üçüncü taraflar)

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

- **Şifre:** Kullanıcının kimliğini doğrulamak için kullandığı gizli bilgi
- **Kimlik Doğrulama:** Kullanıcının iddia ettiği kimliğin doğrulanması süreci
- **Kullanıcı Hesabı:** Bilgi sistemlerine erişim için tanımlanan kişisel hesap
- **Çok Faktörlü Doğrulama:** Birden fazla doğrulama yöntemi kullanılan kimlik doğrulama

---

5. GENEL İLKELER

- Tüm kullanıcı hesapları kişiye özeldir.
- Şifreler gizlidir ve üçüncü kişilerle paylaşılmaz.
- Kimlik doğrulama mekanizmaları yetkisiz erişimi önleyecek şekilde yapılandırılır.
- Şifre ve kimlik doğrulama işlemleri kayıt altına alınır.

---

6. ŞİFRE OLUŞTURMA KURALLARI

- Şifreler en az **8 karakter** uzunluğunda olmalıdır.
- Şifreler büyük harf, küçük harf ve rakam içermelidir.
- Kolay tahmin edilebilir bilgiler (isim, doğum tarihi vb.) kullanılmaz.
- Varsayılan şifreler ilk girişte değiştirilir.
- Aynı şifre tekrar kullanılmaz.

---

7. ŞİFRE DEĞİŞTİRME VE GEÇERLİLİK

- Şifreler belirli periyotlarda değiştirilir.
- Şifre değişiklikleri kullanıcı tarafından yapılır.
- Şüpheli durumlarda şifreler derhal sıfırlanır.

---

8. KİMLİK DOĞRULAMA UYGULAMALARI

- Bilgi sistemlerine erişim kullanıcı adı ve şifre ile sağlanır.
- Kritik sistemlerde ek güvenlik önlemleri uygulanabilir.
- Yanlış şifre denemeleri belirli sayıda kilitlenir.
- Uzaktan erişimlerde ilave doğrulama mekanizmaları kullanılabilir.

---

9. ŞİFRELERİN KORUNMASI

- Şifreler açık metin olarak saklanmaz.
- Şifreler e-posta veya mesaj yoluyla paylaşılmaz.
- Şifrelerin yazılı olarak saklanması önerilmez.

---

10. İHLALLER VE OLAY YÖNETİMİ

- Şifre güvenliği ihlalleri Bilgi İşlem Birimine bildirilir.
- İhlaller kayıt altına alınır.
- Gerekli durumlarda kullanıcı hesapları askıya alınır.
- İhlaller sonrası düzeltici ve önleyici faaliyetler uygulanır.

11. EĞİTİM VE FARKINDALIK

- Kullanıcılara şifre güvenliği konusunda bilgilendirme yapılır.
- Kimlik doğrulama kuralları periyodik olarak duyurulur.

---

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.