1. AMAÇ

Bu politikanın amacı; Karadeniz Teknik Üniversitesi Farabi Hastanesinde meydana gelebilecek bilgi güvenliği olaylarının zamanında tespit edilmesi, raporlanması, analiz edilmesi ve etkilerinin en aza indirilerek kontrol altına alınmasına ilişkin usul ve esasları 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 altyapısı ve uç nokta sistemlerini,
- Fiziki ve mantıksal güvenlik olaylarını,
- Bilgi güvenliği olaylarının yönetiminde görev alan tüm personeli

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 Güvenliği Olayı:** Bilgi varlıklarının gizlilik, bütünlük veya erişilebilirliğini tehdit eden her türlü durum
- **Olay Bildirimi:** Bilgi güvenliği olayının yetkili birimlere iletilmesi
- **Olay Müdahalesi:** Bilgi güvenliği olayının etkilerini azaltmaya yönelik faaliyetler
- **Olay Kaydı:** Bilgi güvenliği olayına ilişkin tutulan resmî kayıt

---

5. GENEL İLKELER

- Tüm bilgi güvenliği olayları ciddiyetle ele alınır.
- Olaylar zamanında tespit edilir ve gecikmeksizin bildirilir.
- Olay yönetimi süreci kayıt altına alınır.
- Olaylara müdahale yetkili personel tarafından gerçekleştirilir.

---

6. BİLGİ GÜVENLİĞİ OLAY TÜRLERİ

Bilgi güvenliği olayları aşağıdakileri kapsar ancak bunlarla sınırlı değildir:

- Yetkisiz erişim girişimleri
- Zararlı yazılım bulaşmaları
- Veri kaybı veya veri sızıntısı
- Hizmet kesintileri
- Fiziksel güvenlik ihlalleri
- Kullanıcı kaynaklı hatalar

---

7. OLAY BİLDİRİMİ

- Bilgi güvenliği olayları derhal Bilgi İşlem Birimine bildirilir.
- Olay bildirimleri belirlenen formlar aracılığıyla yapılır.
- Bildirimlerde olayın türü, zamanı ve etkileri açıkça belirtilir.
- Bildirimler geciktirilmeden kayıt altına alınır.

---

8. OLAY MÜDAHALESİ VE YÖNETİMİ

- Olaylara müdahale Bilgi İşlem Birimi koordinasyonunda yürütülür.
- Olayın kapsamı ve etkisi analiz edilir.
- Gerekli teknik ve idari önlemler alınır.
- Olayın yayılması önlenir ve sistemler güvenli hâle getirilir.

---

9. OLAY KAYITLARI VE RAPORLAMA

- Tüm bilgi güvenliği olayları kayıt altına alınır.
- Olaylara ilişkin raporlar hazırlanır.
- Gerekli durumlarda üst yönetime bilgi verilir.
- KVKK kapsamında bildirim gerektiren durumlarda ilgili mercilere bildirim yapılır.

---

10. DÜZELTİCİ VE ÖNLEYİCİ FAALİYETLER

- Olay sonrası kök neden analizi yapılır.
- Benzer olayların tekrarını önlemek için önlemler alınır.
- Uygulanan faaliyetler kayıt altına alınır.

---

11. EĞİTİM VE FARKINDALIK

- Personel bilgi güvenliği olayları konusunda bilgilendirilir.
- Olay bildirim süreçleri personele 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.