1. AMAÇ

Gemerek Devlet Hastanesi bünyesinde yürütülen TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı uygunluğunun ve etkinliğinin periyodik olarak doğrulanması, uygunsuzluklar için düzeltici ve önleyici faaliyetlerin belirlenmesi ve iyileştirme alanlarının tespit edilmesi amaçlanmıştır.

2. KAPSAM

Bu politikanın uygulamaları Bilgi Güvenliği Yönetim Sisteminin uygulandığı tüm fonksiyonları kapsar.

3. TANIMLAR VE KISALTMALAR

BGYS : TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı

4. UYGULAMA

Yıllık Denetim Programı

1. Her yıl en az bir kez BGYS Birimi tarafından yıllık İç Denetim Programı hazırlanır.

2. Hangi bölümlerin ne zaman denetleneceği Yönetimin onayından sonra bölümlere dağıtılır.

Denetçilerin Seçimi

3. Denetim, dış kaynaklı iç tetkikçiler veya kurum içinden teknik personeller tarafından uygulanır.

4. Yapılacak denetim, tarih saat ve departman bazında **İç Denetim Programına** işlenir. Programda ayrıca denetimi kimlerin yapacağı bilgisi yer almalıdır.

Denetimlerin Programı

5. BGYS Birimi, denetlenecek bölüme ve denetim görevlilerine denetim tarihini en az 7 gün önceden e-posta veya resmi yazı ile bildirir.

6. BGYS Birimi denetlenecek bölümler için denetim personelini belirleyerek **İç Denetim Raporuna** işler.

7. Denetçiler, denetim öncesinde denetimin gerçekleştirileceği bölüm ile ilgili **İç Denetim Soru Listesinin** Altına varsa ilave soruları işlerler.

Denetimin Yürütülmesi

8. Denetimler programa uygun yürütülerek varsa uygunsuzluklar **Düzeltici ve Önleyici Faaliyet İstek Formu** işlenir ve **DÖF Politikalarına** uygun olarak işlemler gerçekleştirilir.

9. Denetimden sonra bulgular denetçiler tarafından **İç Denetim Raporuna** işlenir. Raporun aslı Bilgi **Güvenliği Yetkilisine**, kopyası ise denetimin yapıldığı bölüm yöneticisine iletilir.

10. BGYS kapsamında ki tüm fonksiyonlar yılda en az 1 defa olmak üzere iç denetimden geçirilir.

11. İlgili DÖF'ün bitiş tarihine de makul sebeplerle kapatılmaması durumunda, ilave bir süre daha verilebilir. Ek sürede de kapanmaması durumunda, Entegre Yönetimin Temsilcisi koordinasyonunda, sorun incelemeye alınarak üst yönetime götürülür.

12. DÖF'ler, Takip Listesinden elektronik ortamda izlenebilir.

13. Tüm iç denetim bulguları Yönetimi Gözden Geçirme Toplantıları'nda Politikalara uygun olarak gündemde yer alır.