	T.C. **SAĞLIK BAKANLIĞI** **ARDAHAN İL SAĞLIK MÜDÜRLÜĞÜ** **İç Tetkik Prosedürü**	

Kodu	Yayın Tarihi	Revizyon No	Revizyon Tarihi	Sayfa Sayısı / Num.
BY.PR.18	29.10.2018	2	03.07.2019	1/5

1. **AMAÇ**

Bu prosedürün amacı, T.C. Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü faaliyetlerinin belirlenen politika, prosedür ve diğer bilgi güvenliği gereklilikleri çerçevesinde yürütülmesini, ayrıca Bilgi Güvenliği Yönetim Sistemi (BGYS)' nin sürekli iyileştirilmesini sağlamak ve belirlenen hedeflere ulaşmak için uygun yapıda ve işlevsellikte olup olmadığının tespitini sağlamaktır.

2. **KAPSAM**

Bu prosedür, BGYS iç denetim planlama, yürütme, raporlama ve takibi faaliyetlerini kapsar.

3. **GÖREV ve SORUMLULUKLAR**

3.1. Bilgi Güvenliği Yönetim Temsilcisi

3.1.1. Bilgi Güvenliği Yönetim Temsilcisi ve Denetim ekibinin atamasını yapar.

3.1.2. Bilgi Güvenliği Yönetim Temsilcisi ile birlikte Düzeltici Faaliyetleri gözden geçirir ve iç tetkik raporunu inceler.

3.2. Bilgi Güvenliği Yönetim Temsilcisi

3.2.1. Denetim Planını hazırlar, denetim hakkında bilgi notu oluşturarak ilgililere duyurulmasını gerçekleştirir.

3.2.2. BGYS İç Tetkik faaliyetlerini yürütür.

3.2.3. İlgili Birim ve Birim Sorumluları ile Denetim Programını hazırlar.

3.2.4. Denetimi planlar, denetim ekibi için çalışma dokümanı ve notlarını hazırlar.

3.2.5. Tüm denetim bulguları ve gözlemleri birleştirir ve iç denetim raporunu denetimden sonra 1 hafta içinde hazırlar.

3.2.6. Denetlenen kritik uygunsuzlukları ivedilikle rapor eder. 3.2.7. Denetlenen denetim sonuçlarını açıkça ve gecikmeden rapor eder.

3.2.8. Açılış ve kapanış toplantısı yapar.

3.3. Denetim Ekibi Üyesi

3.3.1. Bilgi Güvenliği Yönetim Temsilcisi faaliyetlerine yardımcı olur.

3.3.2. Denetim kontrol listesi kullanarak denetim gerçekleştirir.

3.3.3. Uygunsuzlukları raporlar ve düzeltici faaliyet önerilerinde bulunur.

3.3.4. Denetim bulgularının gizliliğinin korunmasından sorumludur.

3.4. Denetlenen

3.4.1. Denetim raporunu alır, değerlendirir, itirazı varsa istişare edilir, yoksa imzalar.

3.4.2. Varsa alınacak düzeltici önlemler için kaynak belirler ve gerçekleştirilmesini sağlar.

4. UYGULAMA

4.1. Genel Kurallar

4.1.1. BGYS denetim programı, tüm takvim yılı için kesin takvimine karar verilmiş ve takvimi planlanmış tüm denetimleri içerecek şekilde yıllık olarak hazırlanır.

4.1.2. İç tetkik yılda bir kez yapılacak şekilde planlanır, ihtiyaç duyulduğunda tekrarı gerçekleştirilir.

4.1.3. İç Tetkik, denetim yapılacak birimden tamamen bağımsız ve yetkin, Ardahan İl Sağlık Müdürlüğü personeli, dış kaynaklı iç tetkikçi veya bir eğitim kuruluşundan İç Tetkik sertifikası almış denetçi tarafından gerçekleştirilir.

4.1.4. İç Tetkik Denetim üyeleri, BGYS birimi tarafından Üst Yönetime tavsiye edilir. Üst yönetim onayından sonra denetim ekibi en az 1 Bilgi Güvenliği Yönetim Temsilcisi ve denetçiler olarak BGYS Temsilcisi tarafından atanır.

4.1.5. Bilgi Güvenliği Yönetim Temsilcisi Denetim Ekibinin çalışmalarını denetler.

4.1.6. Denetim Bildirim notu, denetleme yapılacak olan birime en az 7 gün önceden e-posta veya resmi yazı ile gönderilir.

4.2. Denetimin Planlanması ve Hazırlanması

4.2.1. Yıllık BGYS İç Tetkik programı, Bilgi Güvenliği Yönetim Temsilcisi tarafından hazırlanır, Üst Yönetim tarafından onaylanır. Yıl içerisinde iş önceliklerinde ya da programda oluşabilecek herhangi bir değişiklik durumunda, güncel durum yansıtılarak revize edilir.

4.2.2. Denetim programına dayanarak, Bilgi Güvenliği Yönetim Temsilcisi ilgili denetim planını hazırlar.

4.2.3. Denetim Planı, Bilgi Güvenliği Yönetim Temsilcisi tarafından hazırlanır, BGYS Yönetim Temsilcisi tarafından gözden geçirilerek onaylanır. İç Tetkik Planı işlenir. Denetim sırasında toplanan bilgilere dayanarak değişikliklere izin verecek şekilde tasarlanır. Denetim planı en az şu bilgileri içerir:

4.2.3.1. Denetim hedef, kapsam ve yaklaşımı

4.2.3.2. Birimler ve görevdeki sorumlu kişiler

4.2.3.3. Denetim ekibi üyeleri, denetlenecek birim iş süreci büyüklüğüne bağlı olarak denetçi sayısı

4.2.3.4. Denetlenecek denetim sisteminin türü

4.2.3.5. Denetimin tarihi, yeri, zamanı ve denetim raporunun iletim tarihi

4.3. Denetim Öncesi Yapılacaklar

4.3.1. BGYS Birimi, denetim için gerekli olabilecek tüm kaynak ve lojistiğin hazırlanması için denetlenecek bölüme ve denetim görevlilerine denetim tarihini bildirir.

4.3.2. BGYS Birimi denetlenecek bölümler için denetim personelini belirleyerek İç Tetkik Rapor Formuna işler.

4.3.3. Denetçiler, denetim öncesinde denetimin gerçekleştirileceği bölüm ile ilgili İç Tetkik Soru Listesinin altına varsa ilave soruları işlerler. Birimlerin yürüttükleri iş ve işlemler ile ilgili birimlere ayrı ayrı soruların yer alacağı soru listeleri hazırlanır.

4.3.4. BGYS Birim sorumlusu tarafından denetimin kapsamı ve denetim planı kontrol edilir.

4.4. İç Tetkik Açılış Toplantısı Bilgi Güvenliği Yönetim Temsilcisi tarafından denetimden önce, denetimin amacı ve kapsamı, denetim planının teyidi ve denetimden önce varsa açıklığa kavuşturulması gereken hususlar ele alınarak yapılır.

4.5. Denetimin Yürütülmesi

4.5.1. Denetçiler iç denetim kontrol listesi ve gözlem formunu kullanarak denetimi gerçekleştirir. İç Tetkik Soru Listesi ISO/IEC 27001 EK A maddeleri, ISO/IEC 27002 ve gözlem öğeleri doğrultusunda hazırlanır. Gözlem formu, denetlenecek birime spesifik öğeleri içerir, bu formu kullanarak da denetim sorularını üretir.

4.5.2. Denetim bulguları, görüşmeler yoluyla toplanan belgeler, zafiyet alanlarında gösterilen faaliyet ve önlemler, gözlem muayene sonuçları, İç Tetkik Soru Listesi üzerine yazılır. Denetim bulgularından elde edilen sonuçlara göre uygunsuzluklar, Düzeltici Faaliyet Prosedürü' ne uygun

olarak değerlendirilir ve Düzeltici Faaliyet İstek Formu'na işlenir. Kontrol listesi kapsamında olmayan ancak BGYS üzerinde olumlu / olumsuz etkileri olacağı saptanan objektif kanıtlara dayanan diğer bulgular da denetim listesine işlenir.

4.6. Denetim Raporlama

4.6.1. Denetçiler tarafından, denetimden kapalı değerlendirme toplantısı yapılır. Toplantı gündemi aşağıdaki maddeleri içerir:

4.6.1.1. Bulguların gözden geçirilmesi ve analizi

4.6.1.2. Bulguların gruplandırılıp, listelenerek birleştirilmesi

4.6.1.3. Bulguların sınıflandırılması

4.6.1.4. Uygunsuzluk ya da gözlem olarak rapor edilip edilmeyeceğine karar verilmesi

4.6.1.5. Önerilerin alınması ve denetim raporunun hazırlanması

4.6.2. Bilgi Güvenliği Yönetim Temsilcisi, denetim raporunu hazırlamak üzere tüm bulguları birleştirir.

4.6.3. Bulguların sınıflandırılması;

4.6.3.1. Majör Uygunsuzluk: BGYS' nde büyük bir eksiklik anlamına gelir. ISO 27001 Standardının bir ve / veya daha fazla maddesinin uygulanmaması durumudur. Bilgi varlıklarının gizlilik, bütünlük, erişilebilirlik durumunun korunmasında doğrudan etkili öğelerde önlem alınmadığını ifade eder.

4.6.3.2. Minör Uygunsuzluk: BGYS öğelerinin bir ve / veya daha fazla maddesine kısmen uyulması durumudur. Bilgi güvenliği önlemlerine dolaylı etkisi vardır. Majör ve minör uygunsuzluklar için uygun düzeltici faaliyetin dokümante edilmesi gerekir.

4.6.3.3. Gözlem: Denetlenen birimin iş sürecinin iyileştirilmesi için öneri niteliğindedir. Bilgi güvenliği zafiyetlerini ilgilendirmeyen konularda uygun koruyucu önlemlerin alınması için girdi oluşturur.

4.6.3.4. Pozitif Bulgular: Standart tarafından gerekli görülen önlemlerin üzerinde bulunan süreç ve sistemler.

4.6.4. Bilgi Güvenliği Yönetim Temsilcisi aşağıdaki bilgileri içeren İç Tetkik raporunu hazırlar:

4.6.4.1. Denetim Tarihi

4.6.4.2. Denetlenen Birim / Süreç adı

4.6.4.3. Denetçilerin isimleri

4.6.4.4. Kontrol maddeleri ve Bulgular

4.6.4.5. Tespit Edilen Düzeltici Faaliyetler ve Uygunsuzluklar

4.6.4.6. Rapor Özeti

4.6.5. Denetimden sonra bulgular denetçiler tarafından İç Tetkik Raporuna işlenir. Raporun aslı Yönetim Temsilcisine, kopyası ise denetimin yapıldığı bölüm yöneticisine iletilir.

4.7. İç Tetkik Kapanış Toplantısı

4.7.1 Bilgi Güvenliği Yönetim Temsilcisi, denetim ekibi ve denetlenenlerin katıldığı kapanış toplantısına başkanlık eder.

4.7.2. Denetçiler, somut bulgularını ve gözlemlerini, önce pozitif bulgularından başlayarak, uygunsuzlukları tartışırlar, özetleyerek raporlarlar.

4.8. Denetim Takip ve Kapatma

4.8.1. Denetlenen birimler uygunsuzlukları gidermekle sorumludur.

4.8.2. Onaylanmış düzeltici faaliyetler, denetçilerle mutabık kalınan zaman ölçeğine dayanacaktır. İlgili DF' in bitiş tarihinde makul sebeplerle kapatılmaması durumunda, ilave bir süre daha verilebilir. Ek sürede de kapanmaması durumunda, BGYS Yönetim Temsilcisi koordinasyonunda, sorun incelemeye alınarak Üst Yönetimin görüşüne sunulur.

4.8.3. Düzenleyici Faaliyet(DF)' ler, Düzeltici Faaliyet Takip Listesinden elektronik ortamda izlenebilir.

4.8.4. Tüm düzeltme önlemleri başarılı bir şekilde uygulanana kadar denetim tamamlanmış ve kapanmış sayılmaz.

4.8.5. Tüm iç denetim bulguları Yönetim Gözden Geçirme Toplantıları'nda prosedüre uygun olarak gündemde yer alır ve toplantı için girdi oluşturur.

5. DOKÜMANLAR

- Düzeltici Faaliyet Prosedürü
- Düzeltici Faaliyet İstek Formu
- İç Tetkik Rapor Formu
- İç Tetkik Soru Listesi
- Düzeltici Faaliyet Takip Listesi
- İç Tetkik Planı

Hazırlayan	Kontrol Eden	Onaylayan
Oğuz KARABAĞ Bilgi Güvenliği Yetkilisi	Uz. Dr. Nejat AKIN Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Op. Dr. Erkan ÖZDEMİR İl Sağlık Müdürü