RİSK YÖNETİMİ PROSEDÜRÜ

1.AMAÇ

Bu prosedür Hatay İl Sağlık Müdürlüğü, İl Ambulans Servisi Başhekimliği, İlçe Sağlık Müdürlüğü bünyesinde kurulacak olan TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin (BGYS) kapsamına giren hizmetlerin uygulanması sırasında kullanılan ve kazanılan bilgilerin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine yönelik risklerin değerlendirilmesi için kullanılan metodoloji prosedür ve sorumluları tanımlar.

2.KAPSAM

Hatay İl Sağlık Müdürlüğü, İl Ambulans Servisi Başhekimliği, İlçe Sağlık Müdürlüğü bünyesinde belirlenen kapsam dâhilinde uygulanacaktır.

3.SORUMLULAR

3.1. Bu prosedürün sorumluluğu BGYS komisyonuna aittir. Bu komisyon TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı bağlamında yılda 1 kez toplanarak Risk Analizi Tablosu 'nu gözden geçirilmesi planlanan kontrollerin gerçekleştirilip gerçekleştirilmediğinin tespiti, oluşabilecek yeni risk değerlerinin belirlenmesi, kararlarının alınması, artık Risk Analizi Tablosunda yer alan risklerin değerlendirilmesi, risk işleme ve risk izleme tablolarının güncellenmesi gibi konuları görüşür.

3.2. Bu toplantı sonucunda Risk Yönetimi ile ilgili çıkan raporlar ve BGYS komisyonu toplantı tutanağı YGG (Yönetim Gözden Geçirme) toplantısı için birer girdi olacaktır.

3.3.BGYS komisyonu kapsamda ve işlemde önemli bir değişiklik olduğunda veya önemli bir güvenlik ihlal olayında toplanacaktır. Bununla ilgili çalışmalar BGYS Forumu Toplantı Prosedürüne göre düzenlenir.

3.4.BGYS komisyonu BGYS kapsamında belirtilen üretilen, gerçekleştirilen ve kazanılan bilgilere yönelik risklerin yönetilebilmesi için, gerekli politika, prosedür, talimatlar vb. oluşturur ve yayınlar.

3.5.İşlemlerden sorumlu tüm personel politika ve prosedürlere uygun davranırlar ve olay raporlama sistemini kullanarak sapmaları veya olayları BGYS Birimine bildirme görevleri vardır.

3.6. Karar alma sürecinde önemli olabilecek tüm bilgileri BGYS birimine sunmak tüm Hatay İl Sağlık Müdürlüğü, İl Ambulans Servisi Başhekimliği, İlçe Sağlık Müdürlüğü çalışanlarının görevidir.

3.7. Bu, var olan ya da önerilen kontrolleri/karşı önlemleri ve mümkünse farklı güvence derecelerine alternatifleri veya seçenekleri içerebilir.

4. UYGULAMA

4.1.RİSK YÖNETİMİ

4.1.1. Hatay İl Sağlık Müdürlüğü, İl Ambulans Servisi Başhekimliği, İlçe Sağlık Müdürlüğü verimli ve ekonomik faaliyet göstermesi gereklidir ve bu yüzden bir ürünün/hizmetin teslimatını etkileyebilecek kuruma ait bilgilerini tehlikeye atacak bir olayın olasılığına karşı alınacak güvenlik önlemlerinin zaman ve maliyet sonuçlarını dengeleyen yönetim kararları verilmektedir.

4.1.2.BGYS komisyonu, bir riskin yönetiminde kabul edilebilir risk derecelerini değerlendirirken aşağıdaki hususları dikkate alır:

4.1.3. Kurumun fiziksel konumu yangın, arıza, su baskını gibi kaza niteliğindeki hasardan oluşacak olası risklere etki eder.

4.1.4. Mevcut güvenlik - Mevcut fiziksel, mantıksal ve personel güvenlik önlemleri.

4.1.5. Saldırgan sayısı – Saldırgan sayısı ne kadar yüksekse, maruz kalma/nüfuz edilme riski o kadar fazladır. Potansiyel saldırgan sayısının, bilginin algılanan değeriyle orantılı olduğu düşünülmektedir.

4.1.6. Kullanılan araçlar - Bir saldırganın kullanabildiği araçlar ne kadar gelişkinse, saldırının başarı olasılığı o kadar yüksektir. Bu, saldırganın uzmanlığını da içerir.

4.1.7. Toplam fırsat - Fark edilmeden önce saldırganın saldırı için kullanabildiği zaman (ve en önemlisi, karşı önlem alma süresi) veya deneme sayısı riske önemli ölçüde etki eder.

4.1.8. Tanınmışlık seviyesi - 'Bilinmesi gerekli' mantığı. Bir sistemin/bilginin varlığı veya nerede olduğu ya da hangi şekilde olduğu genel olarak bilinmiyorsa saldırılar (saldırganın) arama becerisine veya şansına dayanır ve spekülatif olur.

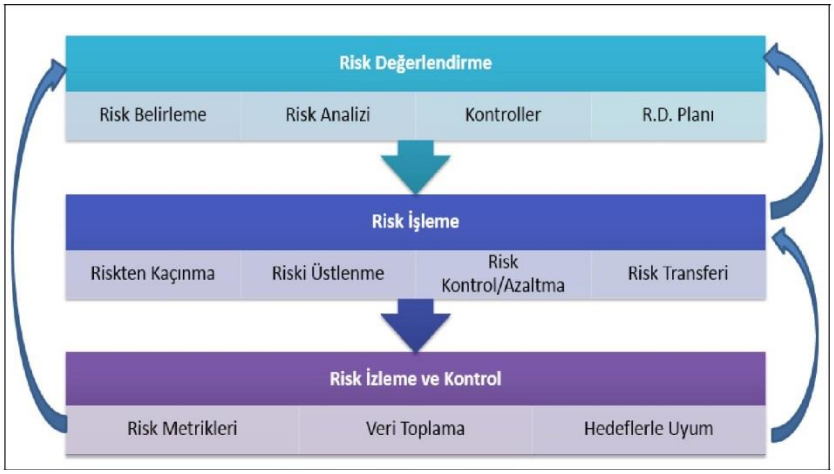
4.1.9.İş devamlılığı planlaması - Bir olayla baş etmek için mevcut iş devamlılığı önlemlerinin ve devam planlamasının becerisi.

4.1.10. Risk analizi sonucunda, sistemi etkileyebilecek tehditler ve oluşturdukları riskler bulunur. Risk analizinin son kısmında bulunan risk değerlerini gösteren tablo kullanılarak risk yönetimi yapılır. Tabloda bulunan risk puanları sistemin hâlihazırdaki durumunda var olan taban risk değerleridir. Yapılacak olan çalışmalar Risk Değerlendirme Prosedürüne uygun olarak yapılır.

4.1.11. Kabul edilebilir (istenen) risk değeri, kurumun varlıkları için, öngördüğü ve kabul ettiği risk miktarıdır. Kabul edilebilir risk seviyesine, Kurum çalışanları ve üst yönetim ile konuşulduktan sonra karar verilir. Kabul edilebilir risk seviyesinin belirlenmesi, risk yönetiminin çekirdeğini oluşturur. Çünkü gerçek risk seviyesinden, kabul edilebilir risk seviyesinin çıkarılması ile bulunan değer, karşı önlemin alınma önceliğini belirler. Risk yönetiminde sistemde var olan kabul edilebilir risk seviyesinin üzerinde riski olan varlıklar işaretlenir aldığı değere göre varlık üzerinde işlem kararı alınır.

4.1.12. Belirlenen risklere karşı alınacak önlemlere karar verilmesi risk yönetiminin asıl amacıdır. Sonuç ayrıntılı olarak kurumun en üst yöneticisine raporlanır. Yönetim tarafında onaylandıktan sonra, karşı önlemler alınır.

4.1.13. Karşı önlemler alındıktan sonra ikinci bir risk analizi yapılır. Böylece, alınan güvenlik önlemleri sonucunda, sistemde kalan risk miktarı bulunur. Kalan risk miktarının, kabul edilebilir risk miktarı ile aynı ya da taşınabilir risk miktarından düşük olması gerekir.



(Kurum ismi yazılacaktır. ÖRN: ….Genel Müdürlüğü , ….Hastanesi vb.) kapsamı dahilinde Risk yönetim süreci yukarıda gösterildiği gibidir. Risk Yönetimini üç adımda gerçekleştirilecektir. İş bu yönetim sürecinin detayları Risk Değerlendirme Prosedüründe anlatılmıştır.

4.2.1.Uzman Tavsiyesi

Gerekli olduğu tespit edilen durumlarda bilgi güvenliğine ilişkin uzman tavsiyesi için Bilgi Güvenliği Yönetim Temsilcisine başvurulur. Yönetim Temsilcisi uzmanlık alanı dışında kalan durumlarda gerekli görüldüğü takdirde dışarıdan uzman görevlendirilmesini "Harici Hizmet Yönetim Prosedürü" ne uygun olarak yapar.

4.2.2.Bağımsız Gözden Geçirme

Bilgi Güvenliği politika ve sorumluluklarının uygulanabilir ve etkili olduğuna dair güven sağlamak için bağımsız olarak gözden geçirme yılda bir kez "İç Tetkik Prosedürü" ne uygun olarak yapılır.

5-Kayıtlar

5.1. Bir riski yönetmek için önlem almak gerektiğinde, yönetim kararları YGG toplantı notlarında dokümante edilir ve kontrolün/karşı önlemin uygulanması için BGYS Komisyonu ve üst yönetim onayından sonra ilgili birim yöneticilerine iletilir. Bu tür kararlar yeni bir politika bildirisi veya mevcut politikanın değiştirilmesini gerektirebilir.

5.2.Risk tanımlandığında, ancak mali, çevresel, teknolojik, kültürel, zamanla ilgili veya başka nedenler dolayısıyla kontrolün/karşı önlemlerin uygulanması uygun olmadığında, karar BGYS toplantısı notlarının parçası olarak kaydedilir ve kararın geçerliliğini korumak için düzenli olarak gözden geçirilir.

5.1. Uygulanabilirlik Bildirgesi

5.1.1.BGYS için yönetim yapısının parçası olarak seçilen kontrol hedeflerini, kontrolleri ve karşı önlemleri listeleyen bir Uygulanabilirlik Bildirgesi (SOA) üretilir. SOA'nın özü, Risk Analiz Tablosu'nda tanımlanan 'Risk Değerlendirmesinden Tespit Edilen Kontroller Başlığında' tanımlanmıştır. Bu belge, risk değerlendirme sürecinin bir sonucu olarak seçilen ISO 27001 kontrollerini özetler. Uygulanabilirlik Bildirgesi, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardında seçilmeyen kontrol hedeflerini ve kontrolleri de hariç tutulma nedenleriyle birlikte listeler. SOA

ISO 27001 kontrol hedeflerine ve kontrollere ek olarak, yasal, nizami, kurumsal veya sözleşmeyle ilgili şartlar nedeniyle gereken başka ek kontrolleri de listeler.

6. YAPTIRIM

Kurum ismi yazılacaktır. (ÖRN: ….Genel Müdürlüğü , ….Hastanesi vb.) kapsamında uygulanacak olan risk yönetimi prosedürü gerekliliklerine uyulmadığı takdirde bu prosedür sorumluları BGYS Disiplin Prosedürü ne uygun olarak değerlendirilir.

7. İLGİLİ DOKÜMANLAR

7.1.1. BGYS TOPLANTI FORMU
7.1.2. İÇ TETKİK PROSEDÜRÜ
7.1.3. RİSK DEĞERLENDİRME PROSEDÜRÜ