İÇİNDEKİLER

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

1. AMAÇ

Bu prosedürün amacı, EGE Üniversitesi Hastanesi BİDB tarafından sahip oluna veya koruması üstlenilen varlıklara yönelik risk değerlendirme sürecinin ve metodolojisinin tanımlanmasıdır.

2. KAPSAM

EGE Üniversitesi Hastanesi BİDB tarafından sahip olunan veya koruması üstlenilen tüm süreçler bunlar için geçerli olan riskler bu prosedür kapsamındadır.

3. TANIMLAR VE KISALTMALAR

-

4. SORUMLULAR

Bu prosedürün hazırlanmasından BGYS Yönetim Temsilcisi sorumludur. Prosedürün uygulanmasından, BGYS risklerinin çıkarılıp takip edilmesinden BGYS Yöneticisi sorumludur.

5. UYGULAMA

5.1 RİSK YÖNETİM SÜRECİ İLE İLGİLİ TANIMLAMALAR

Bilgi varlıklarının karşılaşabilecekleri risklerin, bu risklerin kabul edilebilir düzeyde tutulması için alınması gereken önlemlerin değerlendirildiği çalışmalar "Risk Analizi" olarak adlandırılır.

Risk analizleri Bilgi Güvenliği Ekibi tarafından gerçekleştirilir ve yıllık olarak Bilgi Güvenliği ekibi tarafından gözden geçirilir.

Risk analizi; BGYS kapsamındaki süreçler, bu süreçlerin sahipleri, bu süreçlere yönelik tehditler gizlilik, bütünlük ve erişilebilirlik açısından süreçler üzerinde oluşturabileceği etkiler değerlendirilerek yapılır**.**

Öngörülen risklerin kabul edilebilir düzeyde tutulabilmesi için alınması gereken önlemler belirlenir.

Risk Analizi Tablosu aşağıdaki başlıkları içerir;

Sıra: Tanımlanan risklerin sıra numarasını belirtir.

Süreç: İlgili departmanın tanımlanmış iş süreci.

Risk: Süreçler üzerindeki olabilecek tehdit/zayıflık.

Risk Sahibi: Tanımlanan risklerin firmadaki sorumlusu/varlık sahibi.

Süreç Değeri: Sürecin Gizlilik, Bütünlük ve Erişilebilirlik bakımından değeri.

Olasılık: Riskin gerçekleşme olasılığı. (Bkz. Tablo – 1)

Şiddet: Riskin gerçekleşmesi durumunda Gizlilik, Bütünlük veya Erişilebilirlik açından kuruma etkisi. (Bkz. Tablo – 2)

Toplam Risk: Süreç üzerindeki riskin Gizlilik, Bütünlük ve Erişilebilirlik bakımından toplam değeri.

5.2 TEHDİTLERİN VE ZAYIFLIKLARIN BELİRLENMESİ

Varlık Listesi üzerinde bulunan tüm süreçler için personelden alınan bilgiler ışığında süreçlerin üzerindeki tehdit ve zayıflıklar belirlenir.

Tehditler belirlendikten sonra her tehdit için sürecin değeri, sürece ait tehdidin gerçekleşme ihtimali ve gerçekleştiği zaman firmaya verebileceği zarar (Gizlilik – Bütünlük – Erişilebilirlik) üzerinden bir risk değerlendirmesi yapılır.

Yeni bir tehdit belirlendiğinde tehdit belirleyen personel mail ile (ilgili tehdidi (Riski) Bilgi Güvenliği Ekibine bildirir, risk değerlendirme yapıldıktan sonra tabloya eklenir ve risk yönetim süreci devreye girer. Her yıl iç denetimlerden önce risk analizleri gözden geçirilir ve yeni riskler için aksiyon alınır.

5.3 RİSK METODOLOJİSİ

BGYS'yi etkileyen bütün alanlarda riskler analiz edilerek alınacak tavır belirlenir. Bunun için Varlık Envanter Listesi ve Risk Analizi Tablosu kullanılır. Tablo üzerinde yer alan tanımlamalar ayrıca bir talimata gerek bırakmayacak şekilde hazırlanmıştır.

Öngörülen risklerin kabul edilebilir düzeyde tutulabilmesi için alınması gereken önlemler aynı tablo üzerinden takip edilir.

Bilgi Güvenliği Ekibi, belli bir riskin yönetiminde gereken kabul edilebilir risk derecelerini değerlendirirken aşağıdaki hususları dikkate alır:

BİR OLAYIN GERÇEKLEŞME OLASILIĞI		
OLASILIK		**DERECELENDİRME BASAMAKLARI**
1	**ÇOK KÜÇÜK**	**HEMEN HEMEN HİÇ**
2	**KÜÇÜK**	**ÇOK AZ (YILDA 1 KEZ), SADECE ANORMAL DURUMLARDA**
3	**ORTA**	**AZ (YILDA BİR KAÇ KEZ)**
4	**YÜKSEK**	**SIKLIKLA (AYDA BİR)**
5	**ÇOK YÜKSEK**	**ÇOK SIKLIKLA (HERGÜN, HAFTADA BİR) NORMAL ÇALIŞMA ŞARTLARINDA**

Tablo 1

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

ŞİDDET TABLOSU				
DEĞER	**ANLAM**	**ANLAM**		
		GİZLİLİK	**BÜTÜNLÜK**	**ERİŞİLEBİLİRLİK**
1	**ÇOK HAFİF**	Gizli bilgiye erişim imkânı vermez	Bilgi bütünlüğü bozulmaz	Erişilebilirlik etkilenmez
2	**HAFİF**	Şirkete açık bilgiler şirket dışına çıkabilir	Bilgi bütünlüğü kısmen veya geri dönüşü kolay olacak şekilde bozulabilir	Erişilebilirlik kısmen veya KEKS dâhilinde gerçekleşebilir
3	**ORTA**	Gizli seviyeli bilgiler kısmen dışarı çıkabilir	Bilgi bütünlüğü KEVK dâhilinde bozulabilir	Kesinti KESK içinde giderilemez fakat MKEKS içerisinde kesinti son bulur
4	**CİDDİ**	Çok gizli bilgiler dışarı çıkabilir ve kontrol edilemez	Bilgi varlıkları kaybolmaya/yetkisiz biçimde değiştirilmeye açık hale gelir, kontrol edilemez	Erişilebilirlik kabul edilebilir seviyelerin üzerinde hasar görür, kontrol edilemez
5	**ÇOK CİDDİ**	Çok gizli direk bilgilere erişim verir, yıkıcı olur	Bilgi bütünlüğü geri dönülemez şekilde bozulur, yıkıcı olur	Sistem erişimi tamamen veya kabul edilemez bir süre durur, yıkıcı olur

Tablo 2

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

Süreç Değeri:

Varlık envanterindeki süreç; Kategori bölümünden gelmektedir. BGYS Ekibinin hazırlamış olduğu Varlık Envanteri Listesindeki Süreç Değerlerindeki personelden alınan bilgiler doğrultusunda iş akış derecesine göre 1-5 aralığında puanlanarak risk analizinde belirtilmiştir. Süreç değeri; risk analizini belirleyen Gizlilik- Bütünlük- Erişebilirlik bölümüne doğrudan etki etmektedir.

Risk Metodolojisi;

Risk Değerlendirme ve Risk İşlemede aşağıdaki formül kullanılır.

TOPLAM RİSK = Süreç Değeri * Olasılık * Şiddet (gizlilik/bütünlük/erişilebilirlik) formülü kullanılır.

Bu formüle göre teorik olarak elde edilebilecek en yüksek değer 100 puandır. {4*[5*(5)]}

Mevcut risk analiz çalışmaları neticesinde maksimum kabul edilebilir risk puanı 34 olarak belirlenmiştir.(Bkz. Tablo – 3)

İndirgenmiş risk puanının, kabul edilebilir seviye olan 34 puanın üzerine çıkması halinde Yönetim Temsilcisi tarafından üst yönetime veya ilgili birim müdürü risk durumu e-mail ile bildirilir. Riski yüksek çıkan süreçlerin hedefleri Risk İşleme tablosu üzerinden takip edilir.

Yönetim Temsilcisi ile yapılacak değerlendirme neticesinde; gerekli iyileştirme çalışmalarının başlatılması için onay verilir. Onay verilmesi halinde, ilgili varlık sahibi bölüm yönetimi öncülüğünde iyileştirici faaliyetler planlanarak hayata geçirilir.

İyileştirici faaliyet neticesinde risk değerlendirmesi tekrarlanır. Söz konusu risk puanın kabul edilebilir seviyenin üzerinde kalması durumunda aynı süreç tekrarlanır.

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı

Risk analizi sonucunda aynı varlık için, farklı tehditlere karşın farklı risk puanları oluşabilir. Dolayısıyla risk analizi sonucunda hangi varlığın ne kadar korunacağı değil, hangi varlığın, hangi tehdit karşısında ne kadar korunacağına dair sonuçlar oluşturulur.

Risk işleme planına dair yapılan çalışmalar Düzeltici Önleyici Faaliyet (DÖF) formları ile takip edilir.

SONUÇ	EYLEM
68-100	KABUL EDİLEMEZ RİSK Bu risklerle ilgili hemen çalışma yapılmalı
35-67	DİKKATE DEĞER RİSK Risklere mümkün olduğunca çabuk müdahale edilmeli
1-34	KABUL EDİLEBİLİR RİSK Acil tedbir gerekmeyebilir

Tablo 3

* Eylem matrisine göre değeri yüksek olan riskler öncelikli değerlendirilecektir, risk değeri eşit olanlar ise süreç/olasılık değeri yüksek olanlar önceliklendirilir.

5.4 ARTIK RİSK

Risk analizi tamamlandıktan sonra, risk değeri düşürülemeyen riskler artık risk olarak kabul edilir. YGG toplantılarında yönetim tarafında görülen artık riskler, risk sahibi yöneticilere sunularak kendilerine ait olduğu onaylatılır ve YGG toplantı tutanaklarına atılan imzalar ile kabullenilir.

6. İLGİLİ DOKÜMANLAR

FRM.027– Risk Analizi Formu

FRM.028– Risk Kabul Formu

HAZIRLAYAN	ONAYLAYAN
Şube Müdürü	B.İ. Daire Başkanı