YAKIN DOĞU ÜNİVERSİTESİ HASTANESİ

# BİLGİ İŞLEM MÜDÜRLÜĞÜ RİSK YÖNETİMİ PROSEDÜRÜ

| Doküman No: | İlk Yayın Tarihi: | Revizyon Tarihi: | Revizyon No: | Toplam Sayfa Sayısı: |
|---|---|---|---|---|
| BIS_P_03 | 02.01.2023 | - | - | 5 |

## REVİZYON DURUMU

| “Revizyon Tarihi” | “Açıklama” | “Revizyon No” |
|---|---|---|

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| Bilgi İşlem Müdürlüğü | Kalite Koordinatörü | Hastaneler Yönetim Kurulu Başkanı |

**1. AMAÇ:**

**1.1.** Bilgi İşlem Müdürlüğü yükümlülüğü kapsamında olan donanım ve yazılım sistemlerinin, herhangi bir şekilde arızalanma ya da faaliyetine devam edememe gibi durumlarda oluşacak risk yönetiminin uygulanmasını sağlamak,

**1.1.1.** İş süreçlerini olumsuz yönde etkileyecek şekilde otomasyon sisteminin, ağ veya diğer kritik Bilgi Teknoloji kaynaklarının kaybedilmemesi,

**1.1.2.** Risklerin başarılı bir şekilde belirlenmesi, analiz edilmesi ve izlenmesi için risk yönetim politikaları ve bu politikaları destekleyen dokümanlar oluşturmak,

**1.1.3.** Tüm kurum geneline uygun bir risk protokolü oluşturmak ve paylaşmak.

**2. KAPSAM**

Bu prosedür bilgi işlem müdürlüğünün risk yönetimi sürecine ilişkin faaliyetleri kapsar.

**3. KISALTMALAR: -**

**4. SORUMLULAR:**

Bu prosedür YDU Hastanesi Bilgi İşlem Müdürlüğü'nün sorumluluğunda olan bilişim hizmetlerinde meydana gelecek durumlar için risk yönetiminin etkin bir şekilde yürütülerek diğer birimlerine gereken alt yapı ve sistem desteğinin sağlanmasını sağlar.

**5. TANIMLAR:**

**5.1. YDU Hastanesi:** Yakın Doğu Üniversitesi Hastanesi

**5.2. Mücbir Sebep:** Doğal afet, deprem, sel, yıldırım düşmesi vb. gibi olaylar.

**5.3. ISP:** İnternet Servis Sağlayıcı

**5.4. Hack'leme**: İzinsiz olarak bir sisteme dâhil olma ve zarar verme

**5.5. E-dolandırıcılık:** İnternet aracılığı ile dolandırıcılık

**5.6. Konfigürasyon**: Bir cihaz veya Donanım' a ait Yazılım üzerinde yapılan değişiklikler

**5.7. Paydaş**: Bir cihazın çalışabilir hale getirilmesinde birden fazla birimin müdahale etmesi gereken durum.

**5.8. Network**: Bir veya birden fazla bilgisayarın; dosya ve veri alış verişi yapabilmesi için birbirine bağlanarak oluşturduğu yapıya denir.

**5.9.** **Switch**: Birden fazla cihazın (bilgisayar, ağ kartı kullanabilen cihazlar) birbirleri arasındaki bağlantıyı sağlamaya yarayan cihaz

## 6. UYGULAMA

**6.1.** Bilgi Güvenliği ekibi bu prosedür için çalışır. Bu ekipde bilgi işlem müdürü, bilgi işlem müdürlüğüne bağlı bir personel ve sözleşmeli olunan firma personeli bulunur.

### 6.2. Potansiyel Tehdit Sahalarının Belirlenmesi

**6.2.1.** Mücbir sebepler, organizasyonel eksiklikler (tam tanımlanmamış sorumluluklar vb.), insan hataları (şifreleri kâğıt üzerine yazma, yanlışlıkla dosya silme vb.), teknik hatalar (donanım arızaları, kısa devre, sabit disk arızalanması vb.), planlanmış eylemler (hack'leme, e-dolandırıcılık, zararlı kod kullanımı, hırsızlık vb.), İnternet hizmeti'nin durması (ISP kaynaklı sorunlar), Test ve görüntüleme cihazlarının network kaynaklı sorunlardan dolayı çalışamaması.

### 6.3. Risk Analizi

**6.3.1.** Bilgi işlem müdürlüğü değerlerine ilişkin riskler, nasıl kontrol edilecekleri ve yönetilecekleri belirlenmek üzere analiz edilir. Bu analiz sonucu sadece temel ve kalıcı riskler, uzatmalı veya artakalan riskler (konfigürasyon ve değişiklik kontrolleri veya süreçlerin kullanılmaması vb.) incelenir.

### 6.4. Paydaş Analizi

**6.4.1.** Bir cihazın çalışmasında birden çok birimin olması gerektiği durumlardır. Bilgi sistemlerinin, cihaz kurulumların da ve sonrasında cihazın çalışmasında cihaz teknisyeni kadar rol almaması fakat yardımcı olması gereken durumlar. Örneğin; MR sisteminin çalışması için gereken kablolama ve switch konfigürasyonunun yapılması. Yapı kurulduktan sonra doğabilecek riskler (switch portunun disable konuma gelebilecek olması, cihazın bulunduğu kat switch'inin konfigürasyon yedeği, kat switch'inin MR odasına olan mesafesinin doğruluğundan emin olmak, radyoaktif yayın switchleri olumsuz yönde etkiler ve data akışının olmamasına neden olur). Sisteme dahil edilen cihazlar sistemi olumsuz yönde etkileyebilir (Network'u karıştırabilir ya da uzun zaman harcamak gerektiğinde iş kaybına sebep olur). Dış firma destekli cihazların kurulumlarından sonra firma

teknik yetkilisi ile cihazların çalıştığına ve sonrasında oluşabilecek risklere karşı neler yapılabilir bilgisini içeren bir form doldurmak ve karşılıklı imzalamak.

**6.5.** Risk Değerlendirme

**6.5.1.** İş gücü kaybı – mücbir sebeplerden dolayı olsun ya da olmasın çözüm için harcanan zaman.

**6.5.2.** Çalışan personel iş kaybı – sorun olan birim çalışanlarının sorun esnasında veya sorun giderilme esnasında çalışamaz durumda olması.

**6.5.3.** Finansal kayıp – doğabilecek aksaklıklar da belirli bir harcama yapılması (dış firmadan saat ücreti olarak destek alınması, bilgi sistemleri tarafından alınması gereken donanım (power supply – Ethernet kartı vs.))

**6.5.4.** Güvenlik riski – bilgi değiştirilebilir, erişilebilir veya yetkisiz kişilerce kullanılması

**6.5.5.** Erişilebilirlik – bilgi veya uygulamalara bir sistem hatası veya doğal bir felaket sonucu erişilememesi

**6.5.6.** Erişim kısıtlama – Uzaktan destek veren firmalara VPN bağlantısı açıldıktan sonra işleri bittiğinde açılan hesapları kaldırmak, sisteme erişilemez duruma getirmek.

**6.5.7.** Geri Kazanılabilirlik – Sistem kaybı veya çökmesi sonrasında Sahip olunan Bilişim Teknoloji Sistemlerinin bilgiyi zamanında geri getirememesi

**6.5.8.** Performans riski – sistemler, uygulamalar veya personelin – veya tüm Bilişim Teknoloji Sistemlerinin – beklenenin altında performans göstermesi sonucu iş üretkenliği veya değerinin azalması

**6.5.9.** Ölçeklenebilirlik – Bilişim Teknoloji Sistemlerinin, organizasyonun değişen bilgi gereksinimlerini karşılaması için geliştirilememesi veya değiştirilememesi

**6.5.10.** Uyumluluk riski – bilgi tutma ve işleme, düzenlemelere ve Bilişim Teknolojileri veya iş politika gereksinimlerine uygun gerçekleştirilememesi

**6.6.** Riske Karşı Alınan Tedbirler

**6.6.1.** Hastanede Bilgi İşlem Müdürü, Bilgi İşlem Müdürlüğüne bağlı personel ve sözleşmeli firma personeli, oluşan risklere müdahale kararı ve aşağıda belirtilen format içinde yazılı olarak planını Bilgi Sistemleri Direktörü'ne sunar.

**6.6.2.** Risk planları kayıtlarında, risk numarası, alınacak aksiyon, görevin kime atandığı, tamamlanma zamanı, statüsü bulunur.

**6.6.3.** Bilgi İşlem Müdürlüğüne bağlı personel ve sözleşmeli firma personeli tarafından, riske müdahale edildikten sonra kalan riskler (artakalan risk) bağlı olunan yöneticiye yazılı olarak iletilir.

**6.7.** Risk Yönetimini İzleme

**6.7.1.** Bilgi İşlem Müdürlüğüne bağlı personel ve sözleşmeli firma personeli, risk belirleme aşamasında yapılacak izleme, değerine (yüksek-düşük) göre risk sayısının, risk kaydının varlığının/güncelliğinin, süreç sıklığının ve kalitesinin belirlenmesi ve tanımlanmamış riskleri tespit ederek, Bilgi İşlem Müdürüne, yeni risk oluşumları ve mevcut risklerin olabilirliğindeki artışı raporlar.

**6.7.2.** Bilgi İşlem Müdürlüğüne bağlı personel ve sözleşmeli firma personeli, Risk değerlendirmesi aşamasında yapılacak izleme ile yüksek ve orta dereceli risk sayısı, risk profili varlığı, önceliklendirmenin hangi sıklıkta gözden geçirildiği ve risk hesaplaması uygunluğunu inceleyerek. Bilgi İşlem Müdürüne, önceliği yüksek riskler, kabul edilen riskler, etkin olmayan kontroller ve azaltma gerektiren riskler, raporlar.

**6.7.3.** Bilgi İşlem Müdürlüğüne bağlı personel ve sözleşmeli firma personeli, riske müdahale aşamasında yapılacak izleme ile aksiyon planının varlığı ve güncelliği (kim atanmış, ne zaman tamamlanacak), planın işleyişinin uygunluğu ve riske karşı alınan aksiyonları Bilgi İşlem Müdürüne raporlayarak, izleme ve denetimlerin sağlanması ve “riske karşı alınacak aksiyonlar nelerdir” ve “uygun aksiyonlar alınmakta mıdır” bilgisini paylaşır.

**6.7.4.** HBYS’nin çalışmasını engelleyecek genel veya kısmi bir durum söz konusu ise sorun giderilinceye kadar işlerin aksamamasına yönelik tedbirlerin alınabilmesi için gerekli analizler Bilgi İşlem Müdürü tarafından yapılır ve sorunun çözüm süresi bölüm yöneticisine iletilir.

## 7. İLGİLİ DOKÜMANLAR:

**7.1.** Risk Değerlendirme Formu