



**KIRIKKALE ÜNİVERSİTESİ**  
**DİŞ HEKİMLİĞİ FAKÜLTESİ**  
**BİLGİ YÖNETİMİ RİSK ANALİZİ**



**Kodu: DBY.YD.02    Yayın Tarihi: 02.01.2019    Revizyon Tarihi:    Revizyon No:    Sayfa no/Sayfa Sayısı:1/2**

TANIMLAR				TEHLİKE TANIMLAMA			RİSK DEĞERLENDİRME				MEVCUT/DÜZELTİCİ ÖNLEYİCİ FAALİYET			
SIRA NO	Faaliyet Alanı	Alan Sorumlusu	Faaliyet Tanımı	Tehlike ( Kök-Neden)	Risk	Oluşum Sonucu / Kayıp	Olasılık	Şiddet	Ö. D.	Önem	Mevcut Tedbirler	Düzeltilici ve Önleyici Faaliyet	Planlanan Tarih	
							1	2	3					Önem öncelik sırası
<b>ENFEKSİYON RİSKİ</b>														
1	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Veritabanı Yönetimi ve Güvenliği	Veritabanına yetkisiz erişimler	Kritik bilgilerin silinmesi veya değiştirilmesi Hatalı işlemler	Maddi kayıp, Kurum İtibarının Zedelenmesi, Hatalı sonuç	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Kurumdan ayrılan personelin kullanıcı adı ve şifresi Bilgi İşlem Dairesine bildirilerek iptali sağlanır.		
2	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Veritabanı Yönetimi ve Güvenliği	Yetersiz veritabanı performansı	İşlem hızlarında düşüşler	Zaman kaybı	2	3	6	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Veritabanının yıllık bakımı sağlanır.		
3	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Veritabanı Yönetimi ve Güvenliği	Veritabanlarında aktif durumda olan firma kullanıcılarının bulunması.	Firma kullanıcıları gizli bilgileri görebilir, silip, değişiklik yapabilirler	Maddi kayıp, Kurum İtibarının Zedelenmesi, Hatalı sonuç	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Firma ile gizlilik sözleşmesi imzalanır. Uzaktan erişimler bilgi işlem personeli bilgisi ve gözetimi altında sağlanır.		
4	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Veritabanı Yönetimi ve Güvenliği	Veritabanlarında birden fazla kişinin kullanabildiği ortak kullanıcılarının bulunması	Usulsüz işlemlerin hangi kullanıcı tarafından yapıldığının tespit edilememesi	Denetim eksikliği	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Veritabanları için birden fazla kişinin kullanabileceği ortak kullanıcı hesabı mevcut değildir. Veritabanlarının bulunduğu odaya erişim sınırlıdır.		
5	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Veritabanı Yönetimi ve Güvenliği	Kullanıcılara gereğinden fazla rol ve yetkiler verilmesi	Yetkisi dışında veri silme, değiştirme, veritabanından kritik bilgilerin çekilmesi	Denetim eksikliği, Bilgi hırsızlığı,	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Bilgi Yönetim Sistemine ilişkin rol grupları ve yetkileri belirlenmiştir.		
6	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Veritabanı Yönetimi ve Güvenliği	Veri tabanı kullanıcı işlemlerinin loglanması.	İşlemlerin kim tarafından ne zaman yapıldığının tespit edilememesi	Denetim eksikliği, Bilgi hırsızlığı,	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Log kayıtları Bilgi İşlem Dairesi tarafından tutulur.		
7	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Veritabanı Yönetimi ve Güvenliği	Uygulama öncesi yetersiz test	Kullanım aşamasında sistem arızası	Zaman kaybı, Sistem aksaklığı	1	3	3	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Güncellemeler test edildikten sonra tüm hastane bilgisayarlarına aktarılır.		
8	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Değişiklik & Konfigürasyon	Yetkisiz değişikliklerin yapılması	Kullanım aşamasında sistem arızası	Zaman kaybı, Sistem aksaklığı	1	3	3	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Bilgi işlem personeli dışında değişiklik yapma yetkisi bulunmamaktadır.		
9	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Servis Sürekliliği	Veri kurtarma işleminin yetersiz yapılması	Arıza, kayıp, afet durumunda verilere ulaşamama	Maddi kayıp, Hukuki problemler	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Otomasyon sistemi serverları yedekli olarak çalışmaktadır. Yılda bir defa veri kurtarma testi yapılmaktadır.	Hastane ortamı dışında verilerin yedeklenmesi için Bilgi İşlem Dairesi ile görüşme yapılmıştır.	
10	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Servis Sürekliliği	Kurtarma merkezindeki kritik verilerin arşivlenmesi	Arıza, kayıp, afet durumunda verilere ulaşamama	Maddi kayıp, Hukuki problemler	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Otomasyon sistemi serverları yedekli olarak çalışmaktadır. Yılda bir defa veri kurtarma testi yapılmaktadır.	Hastane ortamı dışında verilerin yedeklenmesi için Bilgi İşlem Dairesi ile görüşme yapılmıştır.	
11	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Servis Sürekliliği	İş kesintisini gidermede yetersizlik	Hizmet üretiminde zaman kaybı, Hasta muayene ve tetkik sürelerinin uzaması	Maddi kayıp, Hukuki problemler	2	3	6	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Servis kesintileri Metasistem üzerinden HBYS sistem sağlayıcısına bildirmekte ve kayıtları tutulmaktadır.		
12	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Problem Çözüm Yönetimi	Olay sonrası problemler için zamanında aksiyon alınmaması	Hizmet üretiminde zaman kaybı, Hasta muayene ve tetkik sürelerinin uzaması	Maddi kayıp, Hukuki problemler	2	3	6	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Servis aksaklıkları Metasistem üzerinden HBYS sistem sağlayıcısına bildirilmekte ve kayıtları tutulmaktadır.		
13	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Kayıt, Olay ve Alarm Yönetimi	Yetersiz kapasite planlaması	Arşivleyememe, Kayıt tutamama	Maddi kayıp, Hukuki problemler	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Server sistemi kapasitesi 6 aylık dönemlerle gözden geçirilmekte ve ihtiyaç halinde kapasite artırımı yapılmaktadır.	Serverların yedekleri temin edilmiş ve kapasiteleri artırılmıştır.	
14	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Hizmet	Hizmet kesintisi	Sağlık hizmeti kayıtlarını yapamama,	Maddi kayıp, Hukuki problemler	2	3	6	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Servis kesintileri Metasistem üzerinden HBYS sistem sağlayıcısına bildirilmektedir. Acil durumlarda direk iletişim kurularak gerekli durumlarda bilgi işlem personeli denetiminde uzaktan erişim sağlanmaktadır.		
15	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Operasyon	Lisanssız ve uygun olmayan yazılım kullanımı	Yazılım şirketleri tarafından dava edilme, Hizmet sunumunun aksaması	Maddi kayıp, Hukuki problemler	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Fakültemizde kullanılan bütün yazılımlar bilgi işlem dairesi tarafından temin edilmektedir. Ayrıca hastanede kullanılan bütün cihazlar lisanslı olarak alınmıştır.		
16	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Operasyon	IP adres planlaması ve IP dağıtımının yapılmaması	Yasal takip veya inceleme durumunda hangi IP den işlemin kim tarafından yapıldığının tespit edilememesi	Maddi kayıp, Hukuki problemler	2	3	6	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	İp dağıtımı ve kayıtları bilgi işlem dairesi tarafından planlanmaktadır.		
17	Bilgi İşlem Birimi	Bilgi İşlem Birimi	Operasyon	Kablosuz ağ erişim noktalarında düşük seviyede güvenlik uygulanması	Kablosuz ağ üzerinden yerel alan ağ kaynaklarına yetkisiz erişimlerin yapılabilmesi	Denetim eksikliği, Bilgi hırsızlığı,	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Yerel alan ağ kaynaklarına kablosuz ağ üzerinden (misafir kullanıcı) erişim sınırlandırılmıştır.		



KIRIKKALE ÜNİVERSİTESİ  
DİŞ HEKİMLİĞİ FAKÜLTESİ  
BİLGİ YÖNETİMİ RİSK ANALİZİ



Kodu: DBY.YD.02 Yayın Tarihi: 02.01.2019 Revizyon Tarihi: Revizyon No: Sayfa no/Sayfa Sayısı:2/2

Bilgi İşlem Birimi	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Sunucularda Lisanssız Yazılımların çalışması	Kullanıcılar ile etkileşimli çalışmama	Zaman kaybı, Maddi kayıp, Hukuki problemler	2	3	6	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Fakültemizde kullanılan bütün yazılımlar bilgi işlem dairesi tarafından temin edilmektedir. Ayrıca hastanede kullanılan bütün cihazlar lisanslı olarak alınmıştır.
19	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Sunucular için standart bir şifre politikasının bulunmaması	Yetkisiz erişim	Denetim eksikliği, Bilgi hırsızlığı,	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Sunuculara erişim için şifreler bilgi işlem personeline bulunmaktadır. Bilgi işlem personeli dışında sunuculara erişim mümkün değildir.
20	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Sunucularda uzaktan bağlantı sağlayacak servislerin açık olması	Kötü yazılım, Hacker saldırılarına maruz kalma	Maddi kayıp, Hukuki problemler, İtibar kaybı	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Uzaktan erişimler bilgi işlem personeli izni ve denetimi altında gerçekleştirilmektedir. Uzaktan erişimler kurum içinden izin verilmediği takdirde (güvenlik duvarından izin verilmesi) mümkün değildir. Ayrıca lisanslı virüs koruma programı kullanılmaktadır.
21	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Sunucu log kayıtlarının değiştirilebilir olması	Yetkisiz erişim Bilgi kaybı Bilgiye erişim işlemlerinin izlenememesi	Bilgi hırsızlığı	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Log kayıtlarına erişim yetkisi bilgi işlem dairesine aittir.
22	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Sunucuların yedeklenmemesi veya yedeklerin düzenli olarak test edilmemesi	Arşivleme problemleri	Maddi kayıp, Hukuki problemler, İtibar kaybı	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Sunucular düzenli olarak yedeklenmektedir. Yılda bir defa veri kurtarma testi yapılmaktadır.
23	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Veritabanlarında tanımlı kurum dışı (tedarikçi) kullanıcılarının işlemlerinin takip edilmemesi	Kötüye kullanma	Bilgi hırsızlığı, Hukuki problemler	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Bilgi işlem personeli uzaktan bağlantıya izin vermediği takdirde kurum dışı kullanıcılar sisteme bağlanamamaktadır.
24	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Bilgisayarlarda Anti virüs yazılımların bulunmaması	Kötü yazılım, Hacker saldırılarına maruz kalma, sistemi kullanamama	Maddi kayıp, Hukuki problemler, İtibar kaybı	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Lisanslı virüs koruma programı kullanılmaktadır.
25	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Bilgisayarların tüm internet sitelerine açık olması	Kötü yazılım, Hacker saldırılarına maruz kalma, hizmet üretiminde aksamalar,	Maddi kayıp, Hukuki problemler, İtibar kaybı	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Bilgisayarların yasaklı internet sitelerine girişi kapalıdır. Ayrıca log kayıtları tutulmaktadır.
26	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Serverların bulunduğu alanlara izinsiz girişlerin yapılması	Kötüye kullanma, server vs zarar verme,	Maddi kayıp, Hukuki problemler, İtibar kaybı	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Server odalarına giriş bilgi işlem personeli denetimindedir.
27	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Serverlerin Bulunduğu alanlarda yangına karşı önlem alınmaması	Yangın anında müdahale edememe	Maddi kayıp, Hukuki problemler, İtibar kaybı	1	5	5	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Server odalarına uygun yangın söndürme ekipmanları mevcuttur. Bakımları düzenli olarak yapılmaktadır.
28	Bilgi İşlem Birimi	Veritabanı İşletimi ve güvenliği	Serverların bulunduğu alanların üst, yan vb katlarında su tesisatlarının bulunması	Serverların su vb. sıvıya maruz kalması	Maddi kayıp, Hukuki problemler, İtibar kaybı	1	4	4	1	Kontrol altında tutulur 1 yılda bir gözden geçirilir	Serverların bulunduğu alanların üst, yan vb katlarında su tesisatları bulunmamaktadır.

RİSK PUANI	RİSK YOK (RY)
<b>RİSK FAKTÖRÜ:1 ANLAMSIZ RİSK</b>	<b>ANLAMSIZ RİSK (AR)</b>
<b>RİSK FAKTÖRÜ:2-6 DÜŞÜK RİSK</b>	<b>DÜŞÜK RİSK (DR)</b>
<b>RİSK FAKTÖRÜ:8-12 ORTA RİSK</b>	<b>ORTA RİSK (OR)</b>
<b>RİSK FAKTÖRÜ:15-20 YÜKSEK RİSK</b>	<b>YÜKSEK RİSK (YR)</b>
<b>RİSK FAKTÖRÜ:25 TOLERE EDİLEMEZ RİSK</b>	<b>TOLERE EDİLEMEZ (TE)</b>
<b>İHTİMAL</b>	<b>SKOR</b>
<b>COK KÜÇÜK= Hemen Hemen Hiç</b>	<b>1</b>
<b>KÜÇÜK= Çok Az Yılda bir kez</b>	<b>2</b>
<b>ORTA= Yılda birkaç kez</b>	<b>3</b>
<b>YÜKSEK=Sıklıkla avda bir kez</b>	<b>4</b>
<b>COK YÜKSEK= Çok sık haftada bir, her gün</b>	<b>5</b>
<b>ŞİDDETİ</b>	<b>SKOR</b>
<b>COK HAFİF=İş saati kaybı yok</b>	<b>1</b>
<b>HAFİF=İş günü kaybı yok</b>	<b>2</b>
<b>ORTA=İş günü kaybı var (1 gün)</b>	<b>3</b>
<b>CİDDİ=Uzun süreli iş günü kaybı (1gün - 1 hafta)</b>	<b>4</b>
<b>COK CİDDİ=Çok uzun süreli iş günü kaybı (1 haftadan uzun)</b>	<b>5</b>
<b>HAZIRLAYAN:</b> Bilgi İşlem Sorumlusu	<b>KONTROL EDEN:</b> Kalite Direktörü
	<b>ONAYLAYAN</b> Dekan

Bölümdeki her puan seviyesindeki risk önlem almayı gerektirir.  
Ancak öncelik sırası ile önlem alınmaya Risk puanı (zarar verme derecesi) yüksek olan riskler ile şiddet değeri yüksek (şiddet 4 puan ve 5 puan) olan risklerden başlanır. Şiddet puanı yüksek(4-5) seviyesindeki riskler için mevcut kontrollerin sürdürülmesi sağlanmalı ve zarar verme derecesinin daha düşük puan seviyesine düşürülmesi/yok edilmesi için önlemler alınmalıdır.