YÜREĞİR DEVLET HASTANESİ
BİLGİ YÖNETİMİ RİSK DEĞERLENDİRME PLANI

DOKÜMAN NO : BY.PL.03	YAYIN TARİHİ	6.12.2019	REVİZYON TARİHİ : 02/06/2021	REVİZYON NO : 01	SAYFA NO : 1/2

OLASILIK SEVİYESİ	OLASILIK TANIMI	ETKİ DERECESİ	ETKİ TANIMI
Yüksek	Tehdit kaynağı çok kabiliyetli ve motivasyonu yüksektir, açıklığın gerçeklenmesini engelleyecek kontroller bulunmamaktadır veya etkisizdir	Yüksek	Açıklığın gerçeklenmesi durumunda: Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur. Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir. İnsan hayatı kaybı veya ciddi yaralanmalar gerçekleşebilir.
Orta	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın gerçeklenmesine engel olacak kontroller mevcuttur.	Orta	Açıklığın gerçeklenmesi durumunda: Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar. Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir.Yaralanmalar gerçekleşebilir.
Düşük	Tehdit kaynağı daha az kabiliyetli ve motivasyonu daha düşüktür, açıklığın gerçeklenmesini engelleyecek veya çok zorlaştıracak kontroller mevcuttur.	Düşük	Açıklığın gerçeklenmesi durumunda: Kurumun bazı varlıkları etkilenir Kurumun çıkarları, misyonu ve prestiji etkilenebilir.

RİSK DERECELENDİRME MATRİSİ				
3x3 Matris Risk Değerlendirme		ETKİ SEVİYESİ		
		Düşük	Orta	Yüksek
OLMA OLASILIĞI	Düşük	Düşük	Düşük	Düşük
	Orta	Düşük	Orta	Orta
	Yüksek	Düşük	Orta	Yüksek

TEHDİT KAYNAKLARI	RİSK DERECELERİNİN TANIMI	
	Risk Derecesi (OlasılıkxEtki)	
B: İnsan Kaynaklı ve Bilerek	Yüksek	Düzeltici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve olabildiğince çabuk uygulanmalıdır.
K: İnsan Kaynaklı ve Kazayla	Orta	Düzeltici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içerisinde hazırlanmalı ve uygulanmaya başlanmalıdır.
D: Doğal		
Ç: Çevresel	Düşük	Önlem alınıp alınmayacağı sistem sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

Sıra	Tarih	Açıklık	Tehdidin Çeşidi	Tehdit	Tehdit Kaynağı	Olasılık	Etki	Risk	SONUÇ	Alınması Gereken Önlemler
1		Binada yeterli fiziksel güvenliğin bulunmaması	Altyapı ve Çevre	Hırsızlık	B	Düşük	Orta	Düşük	X	Yetkisiz erişimin engellenmesi
2		Binalara ve odalara girişlerde yetersiz fiziksel kontrol		Kasten zarar verme	B	Düşük	Orta	Düşük	X	Kapı güvenliğini sağlamak ve Yetkisiz erişimin engellenmesi
3		Eski güç kaynakları		Güç dalgalanmaları	Ç	Düşük	Düşük	Düşük	X	Elektrik hattının kontrol edilmesi ve regülatör ile beslenmesini sağlamak
4		Deprem bölgesinde bulunan yapılar		Deprem	D	Orta	Orta	Orta	X	Veritabanı yedeklenmesi ve faklı alanlarda muhafazası
5		Herkesin erişebildiği kablosuz ağlar		Hassas bilginin açığa çıkması, yetkisiz erişim	B	Düşük	Düşük	Düşük	X	Şifre güvenliği ve yetki seviyelerinin belirlenmesi
6		Dış kaynak kullanımında işletilen prosedür ve yönetmeliklerin veya şartnamelerin eksikliği/yetersizliği		Yetkisiz erişim	B	Düşük	Orta	Düşük	X	Şifre güvenliği ve yetki seviyelerinin belirlenmesi
7		Periyodik yenilemenin yapılmaması	Donanım	Saklama ortamlarınınneskimesi, donanımların bozulması nedeniyle erişimin durması	K	Düşük	Orta	Düşük	X	Veritabanı yedeklerinin birden fazla alanda saklanması ve bakımlarının periyodik süreçlerde yapılması
8		Voltaj değişikliklerine, ısıya, neme, toza duyarlılık		Güç dalgalanmaları, erişim güçlükleri	D,Ç	Düşük	Orta	Düşük	X	Upslerin periyodik süreçlerde akü bakımının sağlanması ve ısı-nem yalıtımının sağlamansı
9		Periyodik bakım eksikliği		Bakım hataları	B,K	Düşük	Düşük	Düşük	X	Periyodik bakımların yazılı olarak tarihlerinin cihaz özelliğine göre belirlenmesi
10		Değişim yönetimi eksikliği		Kullanıcı hataları	B,K	Düşük	Orta	Düşük	X	Yapılan güncelleme ve değişikliklerin birimlere yazılı olarak duyurulmasıı ve eğitim verilmesi
11		Yama yönetimi eksikliği/yetersizliği	Yazılım	Yetkisiz erişim, hassas bilginin açığa çıkması	B	Düşük	Orta	Düşük	X	Birimlerin sistem üzerinde eksikleri belirleyip bilgi işlem sorumlusuyla birlikte kordineli çalışmasını sağlamak
12		Kayıt yönetimi eksikliği/ yetersizliği		yetkisiz erişim	B	Düşük	Orta	Düşük	X	Kayıtların eksiksiz ve tam olmasıyla ilgili farkındalık eğitimi düzenlemek günlük kayıt kontrolünü sağlamak
13		Kimlik tanımlama ve doğrulama eksiklikleri		yetkisiz erişim, başkalarının kimliğine bürünme	B	Düşük	Orta	Düşük	X	Kayıtların eksiksiz ve tam olmasıyla ilgili farkındalık eğitimi düzenlemek günlük kayıt kontrolünü sağlamak
14		Şifre yönetimi yetersizliği		yetkisiz erişim, başkalarının kimliğine bürünme	B	Düşük	Orta	Düşük	X	Şifre güvenliği politikasının belirlenmesi ve uyulması
15		Şifre veritabanlarının korunmaması		yetkisiz erişim, başkalarının kimliğine bürünme	B	Düşük	Orta	Düşük	X	Şifre güvenliği politikasının belirlenmesi ve uyulması

YÜREĞİR DEVLET HASTANESİ
BİLGİ YÖNETİMİ RİSK DEĞERLENDİRME PLANI

DOKÜMAN NO : BY.PL.03	YAYIN TARİHİ	6.12.2019	REVİZYON TARİHİ : 00	REVİZYON NO : 00	SAYFA NO : 2/2

16		Erişim izinlerinin yanlış verilmesi	Yazılım	yetkisiz erişim	B	Düşük	Orta	Düşük	X	Yetki düzeylerinin periyodik sürelerle kontrol edilmesi
17		İzinsiz yazılım yüklenmesi ve kullanılması		zararlı yazılımlar, yasal gerekliliklere uyum	B	Düşük	Orta	Düşük	X	Birimlerdeki eksik yazılımların belirlenip admin kullanıcı tarafından yapılmasını sağlamak, yükleme ve silme işlemlerini şifrelemek
18		Saklama ortamlarının doğru silinmemesi ve imha edilmemesi		Hassas bilginin açığa çıkması, yetkisiz erişim	B	Düşük	Orta	Düşük	X	Saklama sürelerinin belirlenmesi ve bilgi işlem sorumlusu tarafından tutanak altına alınarak imha edilmesi
19		Dokümantasyon eksikliği/yetersizliği		Kullanıcı hataları	K	Düşük	Düşük	Düşük	X	Kurumca belirlenen dökümanların belirlenerek şifre zorunluluğu getirlip eksiksiz olmasını sağlamak
20		Yazılım gereksinimlerinin yanlış veya eksik belirlenmesi		yazılım hataları	K	Düşük	Düşük	Düşük	X	Biirimlerdeki kullanıcıların sistem üzerindeki eksikleri bilgi işlem sorumlusuyla tam ve doğru şekilde belirlemesi
21		Yazılımların yeterli test edilmemesi		yetkisiz erişim, yazılımların yetersiz kullanımı	B	Düşük	Düşük	Düşük	X	Periyodik sürelerde veri kurtarma testi ve eksiklerin belirlenmesi
22		Korunmayan haberleşme hatları	Haberleşme	haberleşmenin dinlenmesi	B	Düşük	Düşük	Düşük	X	Bilgi güvenliği ve gizliliği ile ilgili farkındalık eğitimlerinin sıklaştırılması
23		Hat üzerinden şifrelerin açık olarak iletilmesi		yetkisiz erişim	B	Düşük	Orta	Düşük	X	Şifre güvenliği politikasının belirlenmesi ve uyulması
24		Telefon hatlarıyla kurum ağına erişim		yetkisiz erişim	B	Düşük	Düşük	Düşük	X	Güvenlik duvarının güçlendirilmesi ve dışarıdan erişimi şifrelemek bilgi güveniğini sağlamak
25		Ağ yönetimi yetersizliği/eksikliği		trafiğin aşırı yüklenmesi	K	Düşük	Orta	Düşük	X	Ağ trafiğini meşgul edecek herhangi bir işlem veya sayfaya girmeyi engellemek
26		Dokümanların güvensiz saklanması	Doküman	Hırsızlık	B	Düşük	Orta	Düşük	X	Bilgi güvenliği ve gizliliği ile ilgili farkındalık eğitimlerinin sıklaştırılması
27		Dokümanların kontrolsüz çoğaltılması		Hırsızlık	B	Düşük	Orta	Düşük	X	Yetki seviyelerinin belirlenmesi ve dökümanların ekleme, silme ve çoğaltma yetkilerini birimlerce belirlemek ve kontrolünü sağlamak
28		Dokümanların imha edilmemesi		Hırsızlık, hassas bilginin açığa çıkması	B	Düşük	Orta	Düşük	X	Dökümanların özelliğine göre imha sürelerinin yasal süreçlerinin belirlenerek imha edilmesini sağlamak
29		Eğitimi eksikliği	Personel	personel hataları	K	Düşük	Düşük	Düşük	X	Donanım ve yazılımlarla ilgili eğitim düzenlenmesi
30		Güvenlik farkındalığı eksikliği		Kullanıcı hataları	K	Düşük	Orta	Düşük	X	Kullanıcıların şifre güvenlliği ve gizliliği ile ilgli bilgilendirilmesi
31		Donanımların veya yazılımların yanlış kullanılması		personel hataları	K	Düşük	Orta	Düşük	X	Donanım ve yazılımlarla ilgili eğitim düzenlenmesi
32		İletişim ve mesajlaşma ortamların kullanımını düzenleyen politikanın eksikliği/yetersizliği		yetkisiz erişim	B	Düşük	Orta	Düşük	X	İletişim ve mesajlaşmayla ilgili olarak politika belirlenmesi ve çalışanların bilgilendirilmesi
33		İşe alımda yetersiz özgeçmiş incelemesi ve doğrulaması		Kasten zarar verme	K	Orta	Orta	Orta	X	Birimlerin yetkinlik düzeylerinin yazılı olarak belirlenmesi ve İnsan kaynakları departmanının güvenlik soruşturması yaparak alım sürecini başlatması

Hazırlayan	Kontrol Eden	Onaylayan
	KALİTE YÖNETİM DİREKTÖRÜ	BAŞHEKİM