BİLGİ YÖNETİMİ RİSK DEĞERLENDİRME PLANI

DÖK.NO:BY.PL.02 | YAY.TAR.: 16.11.2022 | REV.TAR.: 00 | REV.NO: - | SAYFA:1/1

OLASILIK	OLASILIK TANIMI	ETKİ	ETKİ TANIMI
Yüksek	Tehdit kaynağı çok kabiliyetli ve motivasyonu yüksektir,	Yüksek	Açıklığın gerçeklenmesi durumunda: Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur. Kurumun çıkarları,
Orta	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın	Orta	Açıklığın gerçeklenmesi durumunda: Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar.
Düşük	Tehdit kaynağı daha az kabiliyetli ve motivasyonu	Düşük	Açıklığın gerçeklenmesi durumunda: Kurumun bazı varlıkları etkilenir

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	
B: İnsan Kaynaklı	
K: İnsan Kaynaklı	
D: Doğal	
Ç: Çevresel	

RİSK DERECELERİNİN TANIMI	
Risk Derecesi	Düzeltici önlemlerin alınması
Yüksek	şarttır. Mevcut sistem
Orta	Düzeltici önlemlerin alınması gerekmektedir. Hangi
Düşük	Önlem alınıp alınmayacağı

Sıra	Tarih	Açıklık	Tehdidin	Tehdit	Tehdit	Olasılık	Etki	Risk	Hedef	Alınması Gereken Önlemler	Kontrol	Sonuç
1		Binada yeterli fiziksel güvenliğin bulunmaması	Altyapı ve Çevre	Hırsızlık	B	Düşük	Orta	Düşük		Yetkisiz erişimin engellenmesi		
2		Binalara ve odalara girişlerde yetersiz fiziksel kontrol		Kasten zarar verme	B	Düşük	Orta	Düşük		Kapı güvenliğini sağlamak ve Yetkisiz erişimin		
3		Eski güç kaynakları		Güç dalgalanmaları	Ç	Düşük	Düşük	Düşük		Elektrik hattının kontrol edilmesi ve regülatör ile		
4		Deprem bölgesinde bulunan yapılar		Deprem	D	Orta	Orta	Orta		Veritabanı yedeklenmesi ve faklı alanlarda		
5		Herkesin erişebildiği kablosuz ağlar		Hassas bilginin açığa çıkması, yetkisiz erişim	B	Düşük	Düşük	Düşük		Şifre güvenliği ve yetki seviyelerinin belirlenmesi		
6		Dış kaynak kullanımında işletilen prosedür ve		Yetkisiz erişim	B	Düşük	Orta	Düşük		Şifre güvenliği ve yetki seviyelerinin belirlenmesi		
7		Periyodik yenilemenin yapılmaması	Donanım	Saklama ortamlarınıneskimesi, donanımların bozulması nedeniyle erişimin	K	Düşük	Orta	Düşük		Veritabanı yedeklerinin birden fazla alanda		
8		Voltaj değişikliklerine, ısıya, neme, toza duyarlılık		Güç dalgalanmaları, erişim güçlükleri	D,Ç	Düşük	Orta	Düşük		Upslerin periyodik süreçlerde akü bakımının		
9		Periyodik bakım eksikliği		Bakım hataları	B,K	Düşük	Düşük	Düşük		Periyodik bakımların yazılı olarak tarihlerinin cihaz		
10		Değişim yönetimi eksikliği		Kullanıcı hataları	B,K	Düşük	Orta	Düşük		Yapılan güncelleme ve değişikliklerin birimlere		
11		Yama yönetimi eksikliği/yetersizliği	Yazılım	Yetkisiz erişim, hassas bilginin açığa çıkması	B	Düşük	Orta	Düşük		Birimlerin sistem üzerinde eksikleri belirleyip bilgi		
12		Kayıt yönetimi eksikliği/ yetersizliği		yetkisiz erişim	B	Düşük	Orta	Düşük		Kayıtların eksiksiz ve tam olmasıyla ilgili		
13		Kimlik tanımlama ve doğrulama eksiklikleri		yetkisiz erişim, başkalarının kimliğine bürünme	B	Düşük	Orta	Düşük		Kayıtların eksiksiz ve tam olmasıyla ilgili		
14		Şifre yönetimi yetersizliği		yetkisiz erişim, başkalarının kimliğine bürünme	B	Düşük	Orta	Düşük		Şifre güvenliği politikasının belirlenmesi ve		
15		Şifre veritabanlarının korunmaması		yetkisiz erişim, başkalarının kimliğine bürünme	B	Düşük	Orta	Düşük		Şifre güvenliği politikasının belirlenmesi ve		
16		Erişim izinlerinin yanlış verilmesi		yetkisiz erişim	B	Düşük	Orta	Düşük		Yetki düzeylerinin periyodik sürelerle kontrol		
17		İzinsiz yazılım yüklenmesi ve kullanılması		zararlı yazılımlar, yasal gerekliliklere uyum	B	Düşük	Orta	Düşük		Birimlerdeki eksik yazılımların belirlenip admin		
18		Saklama ortamlarının doğru silinmemesi ve imha		Hassas bilginin açığa çıkması, yetkisiz erişim	B	Düşük	Orta	Düşük		Saklama sürelerinin belirlenmesi ve bilgi işlem		
19		Dokümantasyon eksikliği/yetersizliği		Kullanıcı hataları	K	Düşük	Düşük	Düşük		Kurumca belirlenen dökümanların belirlenerek		
20		Yazılım gereksinimlerinin yanlış veya eksik belirlenme		yazılım hataları	K	Düşük	Düşük	Düşük		Biirimlerdeki kullanıcıların sistem üzerindeki		
21		Yazılımların yeterli test edilmemesi		yetkisiz erişim, yazılımların yetersiz kullanımı	B	Düşük	Düşük	Düşük		Periyodik sürelerde veri kurtarma testi ve		
22		Korunmayan haberleşme hatları	Haberleşme	haberleşmenin dinlenmesi	B	Düşük	Düşük	Düşük		Bilgi güvenliği ve gizliliği ile ilgili farkındalık		
23		Hat üzerinden şifrelerin açık olarak iletilmesi		yetkisiz erişim	B	Düşük	Orta	Düşük		Şifre güvenliği politikasının belirlenmesi ve		
24		Telefon hatlarıyla kurum ağına erişim		yetkisiz erişim	B	Düşük	Düşük	Düşük		Güvenlik duvarının güçlendirilmesi ve dışarıdan		
25		Ağ yönetimi yetersizliği/eksikliği		trafiğin aşırı yüklenmesi	K	Düşük	Orta	Düşük		Ağ trafiğini meşgul edecek herhangi bir işlem veya		
26		Dokümanların güvensiz saklanması	Doküman	Hırsızlık	B	Düşük	Orta	Düşük		Bilgi güvenliği ve gizliliği ile ilgili farkındalık		
27		Dokümanların kontrolsüz çoğaltılması		Hırsızlık	B	Düşük	Orta	Düşük		Yetki seviyelerinin belirlenmesi ve dökümanların		
28		Dokümanların imha edilmemesi		Hırsızlık, hassas bilginin açığa çıkması	B	Düşük	Orta	Düşük		Dökümanların özelliğine göre imha sürelerinin		
29		Eğitimi eksikliği	Personel	personel hataları	K	Düşük	Düşük	Düşük		Donanım ve yazılımlarla ilgili eğitim düzenlenmesi		
30		Güvenlik farkındalığı eksikliği		Kullanıcı hataları	K	Düşük	Orta	Düşük		Kullanıcıların şifre güvenlliği ve gizliliği ile ilgli		
31		Donanımların veya yazılımların yanlış kullanılması		personel hataları	K	Düşük	Orta	Düşük		Donanım ve yazılımlarla ilgili eğitim düzenlenmesi		
32		İletişim ve mesajlaşma ortamların kullanımını		yetkisiz erişim	B	Düşük	Orta	Düşük		İletişim ve mesajlaşmayla ilgili olarak politika		
33		İşe alımda yetersiz özgeçmiş incelemesi ve doğrulam		Kasten zarar verme	K	Orta	Orta	Orta		Birimlerin yetkinlik düzeylerinin yazılı olarak		