(Logonuz Burada)

Demo Sağlık Tesisi (Prokalite.Com)
BİLGİ GÜVENLİĞİ RİSK ANALİZ FORMU

Risk Kaynağı	Tehlikenin Tanımı	Riskin Tanımı	Risk Puanı			Etkilenen	Alınması gereken Önlem /Faliyetler	Risk Puanı			Termin/ gün	Sorumlu Kişi	Tehlikenin Bulunduğu Yer /Faaliyet	Plan	Faaliyet Sonucu
			Olasılık	Şiddet	Risk			olasılık	Şiddet	Risk					
Fiziksel Güvenlik	Güç kesintisi	İş sürecinin gerçekleşmemesi, geç gerçekleşmesi	**1**	**2**	**2**	Kurum, çalışanlar, hastalar	Sistemin güç kaynaklarıyla desteklenmesi	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Ups mevcut	**
Sistem Odası Güvenliği	Havalandırma sisteminin arızası	Yüksek ısıya bağlı Server cihazının arızalanması	**4**	**4**	**16**	Kurum, çalışanlar, hastalar	Isı nem takibi, klima santral bakımı, mevcut klimanın kontrolü ve bakımı	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*Yedekli klima mevcut, takipler yapılmakta	**
Sunucu Güvenliği	Donanım arızaları Bakım hataları eksiklikleri	İş sürecinin gerçekleşmemesi, geç gerçekleşmesi	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	Peryodik yenilemenin yapılmaması, saklama ortamlarının eskimesine bağlı donanımların bozulması nedeniyle erişimin durmasına yönelik tedbirlerin alınması, bakımların peryodik yapılması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*	**
Sunucu Güvenliği	Güç dalgalanmaları Elektrostatik boşalma	İş sürecinin gerçekleşmemesi, geç gerçekleşmesi	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	Eski güç kaynaklarının kullanılmaması, voltaj değişikliklerinde gerekli müdahalenin yapılması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*2021 de UPS yenilendi.	**
Sunucu Güvenliği	Tozlanma	Cihaz Arızası	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	Tozlanma karşı donanımların belli periyotlarda bakımlarının yapılması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Kontroller yapılmakta	**
Sunucu Güvenliği	İletim hatlarının hasar görmesi	İş sürecinin gerçekleşmemesi, geç gerçekleşmesi	**2**	**1**	**2**	Kurum, çalışanlar, hastalar	Swicth kontrollerinin yapılması, IP Yapılandırılmasının Kontrollerinin yapılandırılması Testlerle kablo kontrollerinin yapılması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*	**

Risk Kaynağı	Tehlikenin Tanımı	Riskin Tanımı	Risk Puanı			Etkilenen	Alınması gereken Önlem /Faliyetler	Risk Puanı			Termin/ gün	Sorumlu Kişi	Tehlikenin Bulunduğu Yer /Faaliyet	Plan	Faaliyet Sonucu
			Olasılık	Şiddet	Risk			olasılık	Şiddet	Risk					
Fiziksel Güvenlik	Hırsızlık Binada yeterli fiziksel güvenliğin bulunmaması	Maddi kayıp, bilgi kaybı, imaj kaybı	**4**	**4**	**16**	Kurum, çalışanlar, hastalar	Binada yeterli fiziksel güvenliğin bulunmasının sağlanması	**1**	**4**	**4**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Kameralar mevcut, sunucular kilitli.	**
Fiziksel Güvenlik	Saklama ortamının izinsiz kullanılması	Maddi kayıp, bilgi kaybı, imaj kaybı	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	Yetkisiz kişililerin erişiminin engellenmesi	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Erişimler kontrollü	**
Fiziksel Güvenlik	Saklama ortamlarının eskiyip kullanılmaz duruma gelmesi	Maddi kayıp, bilgi kaybı, imaj kaybı	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	İki ayrı sunucuda, dört ayrı storage da ve ofline konumda saklanması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Online ve offline saklama ve veri kurtarma yapılıyor.	**
Sunucu Güvenliği	Lisanssız yazılım kullanımı	Bilgi kaybı, imaj kaybı	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	Lisanslı yazılımların kullanımının sağlanması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Son oracle lisanslı sunucular.	**
Sunucu Güvenliği	Bilgisayar /Yazılımların yetkisiz kullanımı	Yetkisiz erişim, başkalarının kimliğine bürünme Maddi kayıp, bilgi kaybı, imaj kaybı	**4**	**4**	**16**	Kurum, çalışanlar, hastalar	Bilgi yönetimine ilişkin rol grupları ve Yetkilendirme işlemlerinin güncel olması, İşletim sisteminin güncel olması, İşletim sistemine yüklü yetkilendirilmemiş programların kullanılmasının engellenmesi, bilgisayarların merkezi olarak yönetilmesinin sağlanması, güvenlik duvarının aktif olması, yazılımların yeterli test edilmesi	**1**	**4**	**4**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Güncel kaspersky lisans mevcut, ek duvar, fortinet vs. güvenlik önlemlerimiz alınmakta.	**

Risk Kaynağı	Tehlikenin Tanımı	Riskin Tanımı	Risk Puanı			Etkilenen	Alınması gereken Önlem /Faliyetler	Risk Puanı			Termin/ gün	Sorumlu Kişi	Tehlikenin Bulunduğu Yer /Faaliyet	Plan	Faaliyet Sonucu
			Olasılık	Şiddet	Risk			olasılık	Şiddet	Risk					
Sunucu Güvenliği	Yetkisiz kişilerin ağa erişimi	Hassas bilginin açığa çıkması Maddi kayıp, bilgi kaybı, imaj kaybı	**1**	**4**	**4**	Kurum, çalışanlar, hastalar	Herkesin erişebildiği kablosuz ağların kullanımından kaçınma, erişim izinlerinin doğru verilmesi yanlış verilmemesi, şifre veri tabanlarının korunması, Ağ yönetiminin etkin yapılması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* İzinler ve ağ güvenliği için programlar mevcut.	**
Sunucu Güvenliği	Zararlı yazılımlar	Hassas bilginin açığa çıkması Maddi kayıp, bilgi kaybı, imaj kaybı	**4**	**4**	**16**	Kurum, çalışanlar, hastalar	Anti virüs programların kullanılması, güvenlik duvarının aktif olması, izinsiz yazılım yüklenmesi ve kullanılmasının engellenmesi	1	1	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Kaspersky lisanslı yazılım aktif	**
Donanım Güvenliği	Ağ cihazlarının arızalanması	İş sürecinin gerçekleşmemesi, geç gerçekleşmesi	**1**	**2**	**2**	Kurum, çalışanlar, hastalar	Cihazda arıza tespitinde Yedek swich lerin kullanılması	1	1	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*	**
HBYS Uygulaması Güvenliği	Hat kapasitelerinin yetersiz kalması	İş sürecinin gerçekleşmemesi, geç gerçekleşmesi	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	Hat kapasitesinin arttırılması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*	**
Sistem Odası Güvenliği	Server odasının güvenliğinin sağlanmaması	Hassas bilginin açığa çıkması Maddi kayıp, bilgi kaybı, imaj kaybı	**4**	**4**	**16**	Kurum, çalışanlar, hastalar	Server odasının iklemdirme, sıcaklık seviyelerinin standartlara uygun hale getirilmesi, fiziksel ortamın güvenliğinin sağlanması, yetkisiz kişlerin server odasına girişinin engellenmesi, yedeklemelerin yapılması ve ayrı bir alanda muhafaza edilmesi	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Server odası ısı nem izlemi ek muhafaza gibi önlemler mevcut.	**

Risk Kaynağı	Tehlikenin Tanımı	Riskin Tanımı	Risk Puanı			Etkilenen	Alınması gereken Önlem /Faliyetler	Risk Puanı			Termin/ gün	Sorumlu Kişi	Tehlikenin Bulunduğu Yer /Faaliyet	Plan	Faaliyet Sonucu
			Olasılık	Şiddet	Risk			olasılık	Şiddet	Risk					
Veri Tabanı Güvenliği	Veri kaybı	Maddi kayıp, bilgi kaybı, imaj kaybı	**1**	**4**	**4**	Kurum, çalışanlar, hastalar	Firma değişimlerinde % 100 veri aktarımının sağlanması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Yılda 2 kez kurtarma testi yapılıyor.	**
Sunucu Güvenliği	Yazılım hataları	Hassas bilginin açığa çıkması Maddi kayıp, bilgi kaybı, imaj kaybı	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	Kimlik doğrulama ve tanımlama eksikliklerinin tespiti, Dış kaynak kullanımında işletilen prosedür ve yönetmeliklerin veye şartnamelerin eksiksiz ve yeterli hazırlanması, yetkisiz erişimlerin engellenmesi, yazılım gereksinimlerinin doğru ve tam belirlenmesi, sorunun tespitinde gerekli müdahalenin yapılması	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*	**
Sunucu Güvenliği	Ağ trafiğinin yetkisiz kişilerce dinlenmesi İletişimin dinlenmesi	Gizlilik, bütünlük ve süreklilik ilkelerinin ihlal edilmemesi, Hassas bilginin açığa çıkması Maddi kayıp, bilgi kaybı, imaj kaybı	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	HBYS firmasının sunuculara düzenli bakım ve güncelleme çalışmaları planlaması, tespit edilen açıkların giderilmesi faaliyetleri	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*	**
İnsan Kaynakları Güvenliği	Personel yetersizliği	İş sürecinin gerçekleşmemesi, geç gerçekleşmesi	**5**	**3**	**15**	Kurum, çalışanlar, hastalar	Kurumda yeterli seviyede Bilgi güvenliği eğitimi almış personel bulundurulması.	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*	**

Risk Kaynağı	Tehlikenin Tanımı	Riskin Tanımı	Risk Puanı			Etkilenen	Alınması gereken Önlem /Faliyetler	Risk Puanı			Termin/ gün	Sorumlu Kişi	Tehlikenin Bulunduğu Yer /Faaliyet	Plan	Faaliyet Sonucu
			Olasılık	Şiddet	Risk			olasılık	Şiddet	Risk					
HBYS Uygulaması Güvenliği	Web uygulaması nın yetkisiz kişilerce ele geçirilmesi Hastalara ait bilgilerin yetkisiz kişilerle paylaşımı	Gizlilik, bütünlük ve süreklilik ilkelerinin ihlal edilmemesi, Hassas bilginin açığa çıkması	**1**	**4**	**4**	Kurum, çalışanlar, hastalar	HBYS firmasının sunuculara düzenli bakım ve güncelleme çalışmaları planlaması, tespit edilen açıkların giderilmesi faaliyetleri	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*	**
İnsan Kaynakları Güvenliği	Kimlik doğrulamanın yanlış yapılması	Maddi kayıp, bilgi Gizlilik, bütünlük ve süreklilik ilkelerinin ihlal edilmemesi	**1**	**1**	**1**	Kurum, çalışanlar, hastalar	Bilgi sistemlerine ilişkin Bilgi Güvenliği eğitimlerinin verilmesi	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	* Eğitimler düzenli aralıklarla egmod ve gerektiğinde bilgi işlem tarafından veriliyor.	**
İnsan Kaynakları Güvenliği	Hasta kimliğinin gizlenmesi istendiğind e işlemin kullanıcı tarafından bilinmemesi	Gizlilik, bütünlük ve süreklilik ilkelerinin ihlal edilmemesi,	**2**	**1**	**2**	Kurum, çalışanlar, hastalar	Bilgi sistemlerine ilişkin Bilgi Güvenliği eğitimlerinin verilmesi	**1**	**1**	**1**	Faaliyet Süresince	Bilgi İşlem Sorumlusu	Kurum Bilgi İşlem Ağı	*Eğitimler düzenli aralıklarla egmod ve gerektiğinde bilgi işlem tarafından veriliyor.	**

* Bilgi yönetimi Risk analiz planı doğrultusunda gözden geçirilir. Gerektiğinde faaliyetler planlanır.

** Yapılmış faaliyetlere ilişkin döf numaraları bu sutuna işlenir.