BİLGİ YÖNETİM SİSTEMİ RİSK ANALİZİ

BY.YD.005	Yayın Tarihi: 2021 ARALIK	Revizyon Tarihi: 2019 ŞUBAT	Revizyon No:0 1

2019 YILI RİSK ANALİZİ

KAPSAM: SEYHAN DEVLET HASTANESİ

SORUMLULAR: HASTANE YÖNETİCİSİ, İDARİ VE MALİ İŞLER MÜDÜRÜ, BİLGİ GÜVENLİĞİ SORUMLUSU, ÇALIŞANLAR

	NO	Risk Tanımı	Tehlike	Risk Puanı			Etkilenen	Alınması gereken Önlem/Faliyetler	Yönetilebilir Risk Puanı			Termin/Gün	Sorumlu Kişi
				Olasılık	Şiddet	Risk			YönetilebilirOlasılık	Yönetilebilir Etki	Yönetilebilir Risk Değeri		
Genel	1	Bilgi Güvenliği İhlali	Sisteme yetkisiz erişim / sızma	3	5	15	Kurum, çalışanlar, hastalar	Kullanıcı adı ve parolaların 3.şahıslarla paylaşılmaması	1	3	3	Sürekli	Tüm Kullanıcılar
	2	Bilgi Güvenliği İhlali	Basit şifre belirlenmesi	3	4	12	Kurum, çalışanlar, hastalar	Kullanıcı şifreleri şifre politikasına göre karmaşık bir şekilde oluşturulmalı	2	2	4	Sürekli	Tüm Kullanıcılar
	3	Bilgi Güvenliği İhlali	Ekran koruyucu zaman aşımı devreye girene kadar cihazlara yetkisiz müdahale	2	3	6	Kurum çalışanları	Kullanıcıları bilgisayar başından ayrılırken Windows+L tuşuyla bilgisayarı kilitlemeye devam etmesi gerektiği eğitiminin ara ara kullanıcılara hatırlatılması	1	2	2	Sürekli	Tüm Kullanıcılar
	4	Bilgi Güvenliği İhlali	Ekran koruyucunun olmaması	1	2	2	Kurum çalışanları	Bilgisayara 10 dk müdahale edilmediği takdirde ekran koruyucunun devreye girmesi.	1	2	2	Sürekli	Bilgisayar Destek Birimi
	5	Bilgi Güvenliği İhlali	İşten ayrılan personelin tüm kullanıcı adı ve şifrelerinin iptal edilmesi	1	3	3	Kurum çalışanları	İşten ayrılan personelin ilgili birimlere uğramasının sağlanması	1	2	2	Sürekli	Bilgisayar Destek Birimi,Bilgi İşlem ve İnsan Kaynakları
	6	Bilgi Güvenliği İhlali	İşyeri e-posta kullanılmaması.	4	2	8	Kurum, çalışanlar	Elektronik ortamda iş ile ilgili bilgi ve belge alışverişlerinin saglik.gov.tr uzantılı kişisel veya kurumsal e-posta hesaplarıyla yapılması.	3	2	6	Sürekli	Tüm Kullanıcılar
	7	Bilgi Güvenliği İhlali	Tanımlanmayan yerlerden gelen e-postaların ve eklerin açılması, içeriğindeki şüpheli linklere girilmesi	3	4	12	Kurum	Bilgi Güvenliği ile ilgili farkındalık eğitimlerinde kullanıcıların bilgilendirilmesi, kullanıcıların da bu eğitimlerdeki gerekli hususlara uyması.	2	3	6	Sürekli	BGYS Komisyonu, Tüm Kullanıcılar
	8	Bilgi Güvenliği İhlali	Kablosuz ağlarda filtreleme yapılmaması.	4	4	16	Kurum	Kablosuz yayın yapan wireless cihazların MAC filtreleme özelliğini etkinleştirerek istenilen cihazların kablosuz bağlantıyı kullanması sağlanmalı.	2	3	6	Sürekli	Bilgisayar Destek Birimi
	9	Bilgi Güvenliği İhlali	İnternette sakıncalı sitelere girilmesi	3	3	9	Kurum	Güvenlik duvarı kullanılması ve bu güvenlik duvarında gerekli internet kısıtlamalarının yapılması	2	2	4	Sürekli	Bilgisayar Destek Birimi, Bilgi İşlem
	10	Bilgi Güvenliği İhlali	İnternetten içeriği bilinmeyen dosyaların indirilmesi	3	4	12	Kurum	Güvenlik duvarı kullanılması ve bu güvenlik duvarında gerekli internet kısıtlamalarının yapılması,antivirüs programı kullanılarak gerekli güvenlik ayarlarının yapılması.	2	3	6	Sürekli	Bilgisayar Destek Birimi, Bilgi İşlem
	11	Bilgi Güvenliği İhlali	Sunuculara ve kullanıcıların cihazlarına yetkisiz erişim	2	5	10	Kurum, çalışanlar, hastalar	Yetkili kullanıcı adı ve parolalar kimseyle paylaşılmamalı.	1	2	2	Sürekli	Tüm Kullanıcılar
	12	Bilgi Güvenliği İhlali	Yanlış yetki tanımlanması	2	4	8	Kurum, çalışanlar, hastalar	Yetkilendirme grup tablosu tanımlanmalı ve bu tabloya göre işlem yapılmalı	2	2	4	Sürekli	Bilgi İşlem Birimi
	13	Kullanıcı	Kullanıcının kötü niyetli olması,sabotaj	3	4	12	Kurum,çalışanlar	Tespit edilen kullanıcı sistemden çıkarılması	2	3	6	Sürekli	Tüm Kullanıcılar
	14	Kullanıcı	Eğitimsiz ve bilinçsiz kullanıcı	3	3	9	Kurum,çalışanlar	Bilgi Güvenliği ile ilgili farkındalık eğitimlerinde kullanıcıların bilgilendirilmesi, kullanıcıların da bu eğitimlerdeki gerekli hususlara uyması.	2	2	4	Sürekli	BGYS Komisyonu, Tüm Kullanıcılar
	15	Kullanıcı	Şifrenin paylaşılması,kötü niyetli kişilerin eline geçmesi	4	5	20	Kurum,çalışanlar	Bilgi Güvenliği ile ilgili farkındalık eğitimlerinde kullanıcıların bilgilendirilmesi,şifre paylaşımının ne gibi durumlara yol açacağının anlatılması	3	2	6	Sürekli	BGYS Komisyonu, Tüm Kullanıcılar
	16	Donanım	Network cihazlarının çalınması	3	4	12	Kurum, kurum çalışanları	Hastane giriş çıkışlarında güvenliğinin sağlanması	1	2	2	Sürekli	Tüm Kullanıcılar
	17	Donanım	Sunucuların çökmesi	3	5	15	Kurum, çalışanlar, hastalar	Alternatif sunucu bulundurma	1	3	3	150	Bilgi İşlem Birimi, İdari ve Mali İşler
	18	Donanım	Kurumda yetersiz bilgisayar,sunucu ve storage olması	3	5	15	Kurum,çalışanlar	Kurumun gerekli donanımı alması	2	2	4	150	Kurum
	19	Donanım (Sunucu,storage)	Elektrik kesintisi	1	5	5	Kurum, çalışanlar, hastalar	Sunucu odasındaki UPS' in akülerinin çalışır halde tutulması ve ömrü dolan akülerin yenisiyle değiştirilmesi.	1	2	2	Sürekli	Bilgisayar Destek Birimi
	20	Donanım	Bilgisayarlara virüs bulaşması	3	3	9	Kurum,çalışanlar	Bilgisayarlara antivirüs yazılımının yüklenmesi	2	2	4	Sürekli	Bilgisayar Destek Birimi
	21	Sistem Odası	Yetkisiz personelin sistem odasına girmesi	1	5	5	Kurum	Sunucu sistem odalarında sadece yetkili personelin giriş yapabileceği şifreli kapı girişi yapılması	1	2	2	200	Bilgisayar Destek Birimi, Bilgi İşlem
	22	Bilgisayarlar ve Çevre Donanımları	Elektrik kesintisi	3	3	9	Kurum, çalışanlar, hastalar	Birimlere kurululan bilgisayarların ve çevre birimlerinin elektrik kablolarının, duvardaki UPS prizlerine takılması.	2	3	6		Bilgisayar Destek Birimi
	23	Bilgisayarlar	Bilgisayarlara virüslü USB Bellek takılması.	3	3	9	Kurum, çalışanlar	Birimlerde kullanılan bilgisayarlara rastgele USB Bellek takılmaması, USB Belleklerin anti virüs programlarıyla taratılması.	2	2	4	Sürekli	Tüm Kullanıcılar
	24	Yazılım	Backupların bütünlüğünün bozulması	2	4	8	Kurum, çalışanlar, hastalar	Yedekleme yazılımının alınması	1	2	2	120	Bilgi İşlem Birimi, İdari ve Mali İşler
	25	Yazılım	Sunuculara ve kullanıcıların cihazlarına virüs bulaşması	3	4	12	Kurum,kurum çalışanları	Tüm bilgisayarlara antivirüs programının yüklü olması ve sürekli güncelliğinin sağlanması.	1	2	2	Sürekli	Bilgisayar Destek Birimi
	26	Veritabanı-Yetkilendirme	Kişilere veri tabanı ile ilgili geniş yetki verilmesi	2	5	10	Kurum	Veritabanı bilgilerinin sadece firma merkezindeki kişilerde bulunması	1	3	3	Sürekli	HBYS Firması
	27	Veritabanı-Yedekleme	Veritabanı yedeklerinin düzenli alınmaması ,olası bir sıkıntıda veri kaybının yaşanması	1	5	5	Kurum	VTYS Yedeklerin günde 3 defa düzenli alınması	2	2	4	20	HBYS Firması
	28	Veritabanı-Lisanssız Yazılım	Yazılımların lisansız olması ve güncelleme yamalarını almaması	2	4	8	Kurum	Gerekli lisansların alınması	1	2	2	Sürekli	Bilgisayar Destek Birimi
	29	Uygulama Yazılımı	İhtiyaçların eksik belirlenmesi	3	3	9	Kurum,çalışanlar,hastalar	İhtiyaçların belirlenip hbys firmasına iletilmesi	2	1	2	Sürekli	HBYS Firması

BİLGİ YÖNETİM SİSTEMİ RİSK ANALİZİ

BY.YD.005	Yayın Tarihi: 2021 ARALIK	Revizyon Tarihi: 2019 ŞUBAT	Revizyon No:0 1

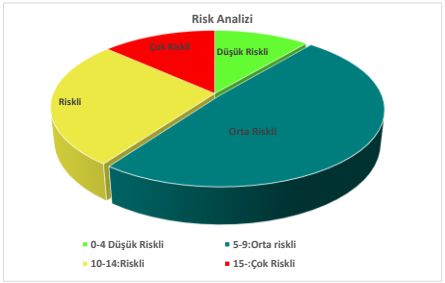
2019 YILI RİSK ANALİZİ

KAPSAM: SEYHAN DEVLET HASTANESİ

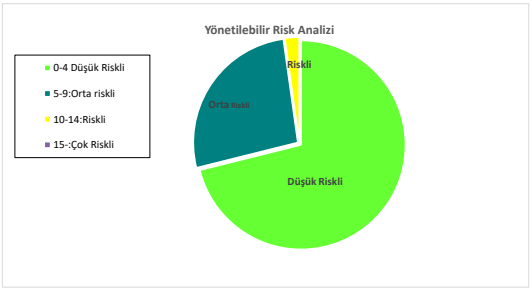
SORUMLULAR: HASTANE YÖNETİCİSİ, İDARİ VE MALİ İŞLER MÜDÜRÜ, BİLGİ GÜVENLİĞİ SORUMLUSU, ÇALIŞANLAR

NO	Risk Tanımı	Tehlike	Risk Puanı			Etkilenen	Alınması gereken Önlem/Faliyetler	Yönetilebilir Risk Puanı			Termin/Gün	Sorumlu Kişi
			Olasılık	Şiddet	Risk			YönetilebilirOlasılık	Yönetilebilir Etki	Yönetilebilir Risk Değeri		
30	Uygulama Yazılımı	Kötü HBYS yazılımı	2	3	6	Kurum,çalışanlar,hastalar	Yazılımın iyileştirilmesi	3	3	9	Sürekli	HBYS Firması,Kontrol Komisyonu
31	Uygulama Yazılımı	Kullanıcılara yanlış veya geniş yetki tanımlanması	2	3	6	Kurum,çalışanlar,hastalar	Yetkilendirme grup tablosu tanımlanmalı ve bu tabloya göre işlem yapılmalı	1	2	2	Sürekli	HBYS Firması
32	Uygulama Yazılımı	Yavaşlık	3	3	9	Kurum,çalışanlar,hastalar	Yazılımın iyileştirilmesi,eksik donanım olmaması	2	3	6	Sürekli	HBYS Firması,Bilgisayar Destek Birimi
33	Dış Etkenler	Afetler,terörist saldırıları	2	5	10	Kurum,çalışanlar,hastalar	Kurumun felaket kurtarma senaryosunun ve merkezinin olması	2	3	6	200	Kurum, Bilgisayar Destek Birimi
34	Dış Etkenler	Su basması, yangın, deprem	2	5	10	Kurum, çalışanlar, hastalar	Sunucu odası ilgili yönetmeliğe göre dizayn edilmeli	2	2	4	180	İdari ve Mali İşler
35	Ağ (Network)	Network sistem uzmanı eksikliği	3	3	9	Kurum	Konunun uzmanı kişilerin kurumlarda istihdam edilmesi,	1	2	2	sürekli	Kurum,HBYS Firması
36	Ağ (Network)	Kurumda internet çıkışlarını filtreleyen güvenlik duvarının olmaması, lisansız olması	1	5	5	Kurum, çalışanlar	Güvenlik duvarı temin edilmesi	2	1	2	Sürekli	Kurum,İl Sağlık Müdürlüğü
37	Ağ (Network)	Altyapı eksiklikleri	3	3	9	Kurum ,çalışanlar,hastalar	Gerekli kablolama vb .işlemlerin yapılarak altyapı eksikliklerinin giderilmesi	2	2	4	Sürekli	HBYS Firması,Bilgisayar Destek Birimi
38	Ağ (Network)	Uzaktan Erişim	2	4	8	Kurum,çalışanlar	Yetkisiz kullanıcıların sisteme uzaktan erişiminin engellenmesi	2	2	4	Sürekli	İl Sağlık Müdürlüğü
39	Ağ (Network)	Network hattındaki yoğunluktan ötürü sistemin yavaşlaması	4	3	12	Kurum,çalışanlar,hastalar	Yük dengelemesi yapılması,yoğunluğun giderilmesi	2	2	4	Sürekli	HBYS Firması,Bilgisayar Destek Birimi
40	Ağ (Network)	WAN (hattın) kesilmesi	2	5	10	Kurum, çalışanlar, hastalar	İl Sağlık Müdürlüğü tarafından gerekli iyileştirmelerin yapılıp kurum magduriyetinin giderilmesi	2	5	10	sürekli	İl Sağlık Müdürlüğü
41	Ağ (Network)	İnternetin Kesilmesi ve internet bazlı süreçlerin durması	1	3	3	Kurum, çalışanlar, hastalar	Mevcut durumun korunması sağlanmalı	2	4	8	sürekli	Tüm çalışanlar
42	Ağ (Network)	Sisteme izinsiz modem vb cihaz takılması	3	5	15	Kurum,çalışanlar,hastalar	IP dağıtan izinsiz cihaz takılmasının engellenmesi,bilgisayar destek birimine haber verilmesi	2	3	6	Sürekli	Tüm çalışanlar
43	Dış Kaynaklar (gizlilik)	Hizmet alımı yapılan firmalar ile gizlilik sözleşmelerinin olmaması	1	3	3	Kurum	Hizmet alımı yapılan firmalar ile gizlilik sözleşmeleri yapılması	1	2	2	Sürekli	Hastane Yönetimi
44	Etki Alanı(Active Directory)	Kullanıcıların bilgisayarlarını kendi kullanıcı adı ve şifreleri ile açmaması	1	3	3	Kurum,çalışanlar	Tüm kullanıcıların etki alanına dahil edilmesi	1	2	2	Sürekli	HBYS Firması,Bilgisayar Destek Birimi
45	İlgisiz Yönetim	Yöneticilerin bilgi güvenliğine gerekli özeni göstermemesi	2	4	8	Kurum,çalışanlar	Yöneticilerin bilgi güvenliğine önem vermesi, önderlik etmesi	2	2	4	Sürekli	Kurum

Risk Değeri	
0-4 Düşük Riskli	5
5-9:Orta riskli	22
10-14:Riskli	12
15-:Çok Riskli	6



Yönetilebilir Risk Puanı	
0-4 Düşük Riskli	32
5-9:Orta riskli	12
10-14:Riskli	1
15-:Çok Riskli	0



Hazırlayan: Bilgi Güvenliği Sorumlusu	Kontrol Eden: Kalite Direktörü	Onaylayan:Başhekim