



T.C.
TRABZON ÜNİVERSİTESİ
Bilgi İşlem Daire Başkanlığı

HASSAS GÖREV FORMU

Doküman No: KYS-FR/DB-BID/08
İlk Yayın Tarihi: 21.10.2026
Rev. No/Tar.: 00/...
Sayfa: 1 / 5

BİRİM ADI: BİLGİ İŞLEM DAİRE BAŞKANLIĞI

Sıra No	Hassas Görev	Riskler	Risk Düzeyi (Yüksek-Orta-Düşük)	Gerekli Kontroller Tedbirler
1.	Sanal Sunucular	Kurumumuzda kullanılan tüm sistemlerin zarar görmesi.	Yüksek	Yedekten geri yüklenmesi ve sistemlerin yeni yapılarda çalıştırılması
2.	Depolama Üniteleri	Kurumda barındırılan dijital verilerin zarar görmesi	Yüksek	Yedekli Sistem Yöneticisi
3.	Web Hizmeti Veren Sunucular	Siber saldırılar	Yüksek	Sunucuların web güvenlik duvarı arkasına alınması
4.	Güvenlik Duvarı (Firewall), IPS/IDS ve Ağ Güvenliği	Kurum ağının dış ve iç trafik kurallarının, güvenlik duvarı (Firewall) politikalarının, VPN ve saldırı tespit/önleme sistemlerinin (IPS/IDS) yapılandırılması	Yüksek	Yapılan kural değişikliklerinin loglanması, düzenli sızma testleri (pentest) ve ulusal siber güvenlik (USOM / Üniversite SOME) koordinasyonu
5.	Sistem Odası (Datacenter) Erişimi ve Fiziksel Güvenlik	Sunucu, storage (depolama) ve network kabinlerinin bulunduğu ana sistem odasına fiziksel giriş ve acil müdahale yetkisi	Yüksek	Sistem odasına geçişlerin kartlı/biyometrik geçiş sistemleri ile kayıt altına alınması, mesai dışı erişimlerde Daire Başkanından onay alınması ve kamera izleme sistemleri
6.	Veri Yedekleme ve Felaket Kurtarma	Donanım arızası, siber saldırı (fidye yazılımı vb.) veya insan hatası durumunda verilerin geri getirilememesi ve hizmetlerin durması	Yüksek	Düzenli otomatik yedekleme planları, yedeklerin farklı(kısmen) fiziksel/bulut ortamlarda (off-site backup) saklanması ve periyodik geri yükleme (restore) tatbikatları
7.	ÜBYS, OBS, EBYS ve PBS sistemlerinin sürekliliğinin sağlanması	Sistem kesintileri nedeniyle akademik ve idari işlerin aksaması	Yüksek	Sistemlerin düzenli izlenmesi, arıza kayıtlarının tutulması, hizmet sağlayıcı ile koordinasyon kurulması ve kesinti durumunda gerekli



T.C.
TRABZON ÜNİVERSİTESİ
Bilgi İşlem Daire Başkanlığı

HASSAS GÖREV FORMU

Doküman No: KYS-FR/DB-BID/08
İlk Yayın Tarihi: 21.10.2026
Rev. No/Tar.: 00/...
Sayfa: 2 / 5

				müdahalelerin yapılması
8.	Kullanıcı hesapları ve erişim yetkilerinin yönetilmesi	Yetkisiz erişim, kişisel verilerin açığa çıkması ve yetki ihlalleri	Yüksek	Yetkilerin görev ve sorumluluklara göre tanımlanması, yetki taleplerinin kontrol edilmesi ve kullanıcı yetkilerinin periyodik olarak gözden geçirilmesi
9.	Kurumsal verilerin doğruluğunun ve bütünlüğünün korunması	Hatalı veya eksik veri nedeniyle raporların ve kurumsal kayıtların yanlış oluşması	Yüksek	Veri kontrollerinin yapılması, hatalı kayıtların incelenmesi, gerekli düzeltmelerin yetkili kişilerce gerçekleştirilmesi
10.	ÜBYS servisleri üzerinden veri alınması ve raporların hazırlanması	Yanlış, eksik veya tutarsız veriler nedeniyle hatalı karar alınması	Orta	Servislerden alınan verilerin doğrulanması, raporların kontrol edilmesi ve veri tutarlılığı incelemelerinin yapılması
11.	Sistem hatalarının tespiti ve hizmet sağlayıcıya iletilmesi	Hataların giderilmesinde gecikme ve iş süreçlerinin aksaması	Orta	Hataların kayıt altına alınması, önem derecesine göre sınıflandırılması, İKÇÜ'ye iletilmesi ve çözüm sürecinin takip edilmesi
12.	Yeni modül ve yazılım geliştirme taleplerinin yönetilmesi	İhtiyaçların yanlış analiz edilmesi veya geliştirmelerin iş süreçlerini karşılamaması	Orta	Birim taleplerinin analiz edilmesi, gereksinimlerin yazılı olarak belirlenmesi, testlerin yapılması ve kullanıcı onayının alınması
13.	Bilgi güvenliği ve kişisel verilerin korunmasına yönelik işlemler	Kişisel verilerin yetkisiz kişilerce erişilmesi, paylaşılması veya kaybolması	Yüksek	Erişim kontrollerinin uygulanması, bilgi güvenliği kurallarına uyulması, kayıtların izlenmesi ve gerekli güvenlik tedbirlerinin alınması

	T.C. TRABZON ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı		
	HASSAS GÖREV FORMU		Doküman No: KYS-FR/DB-BID/08
			İlk Yayın Tarihi: 21.10.2026
			Rev. No/Tar.: 00/...
			Sayfa: 3 / 5

14.	Kullanıcılara teknik destek verilmesi ve eğitim sağlanması	Yanlış işlem yapılması, kullanıcı hataları ve hizmet süreçlerinde gecikmeler	Orta	Kullanıcı taleplerinin kayıt altına alınması, doğru işlem adımlarının aktarılması ve gerekli eğitimlerin verilmesi
15.	Kurumsal sistemlerde yapılan değişikliklerin yönetilmesi	Hatalı değişiklikler nedeniyle veri kaybı, erişim sorunları veya sistem kesintileri	Yüksek	Değişikliklerin değerlendirilmesi, test edilmesi, yetkilendirilmesi.
16.	Üniversite personeli ve öğrencilerinin e-posta hesaplarına ilişkin bildirilen teknik sorunların giderilmesi, hesap güvenliğinin sağlanması ve kurumsal e-posta hizmetlerinin kesintisiz yürütülmesi.	Yetkisiz erişim ve bilgi güvenliği ihlalleri, E-posta hizmetlerinde kesinti yaşanması, kişisel ve kurumsal verilerin kaybolması veya açığa çıkması, Teknik sorunlara geç müdahale edilmesi.	Yüksek	E-posta hesaplarına ilişkin taleplerin kayıt altına alınması, kullanıcı kimlik doğrulamasının yapılması, erişim yetkilerinin kontrol edilmesi, sistem güvenliği ve sürekliliğinin sağlanması, düzenli yedekleme yapılması ve teknik sorunların zamanında giderilmesine yönelik kontrollerin uygulanması.
17.	Hizmet alımları kapsamında gerçekleştirilen sözleşmelere ilişkin belgelerin hazırlanması ve kontrol edilmesi, kayıt ve onay işlemlerinin yürütülmesi, sözleşme hükümlerinin takibi ile ödeme aşamasına kadar olan iş ve işlemlerin ilgili mevzuata ve kurum prosedürlerine uygun şekilde yürütülmesini sağlamak.	Hizmet alımı sözleşmelerine ilişkin belge ve kayıt işlemlerinde hata veya eksiklik yapılması, mevzuata aykırı işlem gerçekleştirilmesi, ödeme süreçlerinde gecikme ya da hatalı ödeme oluşması ve sözleşme hükümlerinin takibinde yetersizlik nedeniyle idari ve mali risklerin ortaya çıkması.	Yüksek	Hizmet alımı sözleşmelerine ilişkin belgelerin mevzuata uygun, eksiksiz ve doğru hazırlanması; kayıt, onay ve ödeme süreçlerinin zamanında takip edilmesi; ödeme öncesi belge ve hizmet uygunluk kontrollerinin yapılması; işlemlerin kayıt altına alınması, belgelerin güvenli şekilde arşivlenmesi ve görev-yetki ayrımının sağlanması
18.	ISO 27001 Risk Analizi ve Değerlendirme Dokümanlarının Hazırlanması	Kurumsal bilgi güvenliği risklerinin yanlış hesaplanması veya eksik dokümanite edilmesi sonucu dış denetimlerde majör uygunsuzluk alınması ve belgenin tehlikeye girmesi.	Yüksek	Risk analiz formlarının (F.001 vb.) sistem/ağ yöneticileriyle koordineli ve kanıta dayalı doldurulması, periyodik risk gözden geçirme toplantılarının yapılması.

	T.C. TRABZON ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı		
	HASSAS GÖREV FORMU		Doküman No: KYS-FR/DB-BID/08
			İlk Yayın Tarihi: 21.10.2026
			Rev. No/Tar.: 00/...
			Sayfa: 4 / 5

19.	Kalite Yönetimi ve BGYS Dokümantasyonunun (Prosedür, Talimat vb.) Oluşturulması ve Güncellenmesi	Dokümanların güncel standartlara (ISO 27001, YÖKAK) uymaması, eski versiyonların sistemde kalarak süreçlerin hatalı yürütülmesine neden olması.	Yüksek	Doküman versiyon takibinin (revizyon numarası/tarihi) titizlikle yapılması, onaylı dokümanların kontrollü dağıtılması ve eski dokümanların arşive kaldırılması.
20.	İç/Dış Denetim ve Sızma Testi (Pentest) Bulgularının Muhafazası	Kurumsal zafiyetleri barındıran hassas raporlara veya denetim bulgularına yetkisiz kişilerin erişmesi sonucu gizlilik ihlali oluşması.	Yüksek	Kalite ve güvenlik dokümanlarının barındırıldığı klasörlere yetkisiz erişimlerin engellenmesi ve dosyaların şifrlenmesi.
21.	Yazılım ihtiyaçlarının belirlenmesi ve gereksinim analizinin yapılması	İhtiyaçların yanlış belirlenmesi, iş süreçlerinin aksamaması ve kaynak kaybı.	Orta	Gereksinimler ilgili birimlerle doğrulanmalı, mutabık kalınan ihtiyaçlar kayıt altına alınmalıdır.
22.	Web siteleri ve yazılım uygulamalarının geliştirilmesi, güncellenmesi ve bakımının yapılması	Yazılım hataları, hizmet kesintisi, veri kaybı ve iş süreçlerinin aksamaması.	Orta	Kod incelemesi ve testler yapılmalı, değişiklikler kayıt altına alınmalı ve mevcut sistemlerin çalışması kontrol edilmelidir.
23.	Yazılımların canlı ortama alınması ve sürüm yönetiminin yürütülmesi	Hatalı yayın, hizmet kesintisi ve veri kaybı.	Yüksek	Yayın öncesi test ve yedekleme yapılmalı, geri dönüş planı hazırlanmalı ve yayın sonrası kontroller gerçekleştirilmelidir.
24.	Yazılım uygulamalarında kullanıcı ve birim yetkilerinin yönetilmesi	Yetkisiz erişim, veri ihlali ve yetkilerin kötüye kullanılması.	Yüksek	Yetkiler onaylı talepler doğrultusunda, görev ve sorumluluklarla sınırlı olarak tanımlanmalı ve periyodik olarak gözden geçirilmelidir.
25.	Yazılım geliştirme, bakım ve hata giderme taleplerinin yönetilmesi	Taleplerin kaybolması, gecikmesi, yanlış yönlendirilmesi ve hizmet kalitesinin düşmesi.	Orta	Talepler kayıt altına alınmalı, önceliklendirilmeli, ilgili ekiplere yönlendirilmeli ve sonuçları takip edilmelidir.

	T.C. TRABZON ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı	
	HASSAS GÖREV FORMU	Doküman No: KYS-FR/DB-BID/08
		İlk Yayın Tarihi: 21.10.2026
		Rev. No/Tar.: 00/...
		Sayfa: 5 / 5

26.	Web sitelerinin oluşturulması, içeriklerinin güncellenmesi ve bilgi güvenliği tedbirlerinin uygulanması	Hatalı veya yetkisiz içerik yayını, erişim sorunları, kişisel verilerin ihlali ve kurumsal itibar kaybı.	Yüksek	Yayın öncesi içerik ve erişim kontrolleri yapılmalı; güvenli yazılım geliştirme ilkeleri, kişisel verilerin korunması ve bilgi güvenliği tedbirleri uygulanmalıdır.
-----	---	--	--------	---