	HASSASGÖREVTESPİT FORMU	Doküman No	FR-0514
		İlk Yayın Tarihi	24.09.2025
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa	1/1

***Harcama Birimi:** BİLGİ İŞLEM DAİRE BAŞKANLIĞI

Sıra No	Hassas Görev/İş**	***Riskler	Risk Düzeyi****	Alınması Gereken Önlemler/Kontroller	Görevi Yürütecek Personelde Aranacak Kriterler
1	**Dış Kaynaklı Yazılım Temini ve Koordinasyonun Sağlanması** 1- İç kaynak ile karşılanamayan ihtiyaçların giderilmesi için dış kaynaklı yazılımların tercih edilmesi.	1-Hizmetlerin erişilebilirliğinin sekteye uğraması riski. 2- Dış kaynak paydaşın el değiştirmesi ve/veya faaliyetine son vermesi halinde alınan yazılım sağlama/bakım/destek hizmetinin sürdürülemez duruma gelmesi riski. 3- Birimlerin iş süreçlerinin sekteye uğraması riski. 4-Kişisel verilerin hukuka aykırı olarak işlenmesi ve erişilmesi riski.	Orta	1- Yazılımların ihtiyaçları karşılayıp karşılamadığının teknik olarak denetlenmesi. 2- Satın alma, yenileme ve yükseltme vb. süreçlerin takip edilmesi ve gerçekleştirilmesi. 3- 6698 sayılı ve 5651 sayılı Kanunlar ve ikincil mevzuatlar kapsamında gizliliği ve mahremiyeti sağlamak üzere ilgili taraflarla gizlilik sözleşmelerin yapılması	1-Kamu İhale Kanunu ve ilgili mevzuata hakim olmak. 2-Yazılım ve lisanslama modelleri (SaaS, On-Premise vb.) hakkında bilgi sahibi olmak. 3-Teknik şartname analizi ve değerlendirme yetkinliğine sahip olmak. 4-Firma ve paydaşlarla etkili iletişim ve koordinasyon becerisine sahip olmak. 5- Kişisel Verilerin Korunması Kanunu (KVKK) hakkında temel bilgi sahibi olmak.
2	**Bilişim Alanında Teknik Şartname Desteğinin Sağlanması**	1- Alınacak mal ve hizmet işinin nitelik ve nicelik bakımından eksik ya da yetersiz yapılması riski.	Düşük	1- Yasal mevzuatlar çerçevesinde süreçlerin yürütülmesi. 2- Resmi yazışma kurallarına uygun ve hızlı bir şekilde yazıların oluşturulması. 3- Kurumun ihtiyaçlarının eksiksiz ve yanlış anlaşılmaya meydan vermeden belirlenmesi. 4- Kurumun ihtiyaçlarına göre tüm piyasa araştırılarak en uygun teknolojiye göre şartların belirlenmesi. 5-Alınan yazılım ve donanımlar teknik şartnameye uygunluğu kontrol edilmeli.	1-Donanım, yazılım ve bilişim altyapısı konularında ileri düzeyde teknik bilgiye sahip olmak. 2- Piyasa araştırması yapma ve güncel teknolojileri takip etme becerisine sahip olmak. 3- İhtiyaç analizi yapabilme ve bu ihtiyaçları teknik dile doğru bir şekilde aktarabilme yeteneğine sahip olmak.

	HASSASGÖREVTESPİT FORMU	Doküman No	FR-0514
		İlk Yayın Tarihi	24.09.2025
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa	1/1

3	**Başkanlığımız Yazı İşlerinin Yürütülmesi**	1- Hizmetlerin erişilebilirliğinin sekteye uğraması riski.	Düşük	1- Yasal mevzuatlar çerçevesinde süreçlerin yürütülmesi. 2- Resmi yazışma kurallarına uygun ve hızlı bir şekilde yazıların oluşturulması. 3-Evrakların dosyalanmasında Standart Dosya Planına uyulması.	1- Resmi yazışma kurallarına ve kurumsal dil kullanımına hâkim olmak. 2- Elektronik Belge Yönetim Sistemi (EBYS) ve ofis yazılımlarını etkin kullanabilmek. 3- Dosyalama, arşivleme ve süreç takibi konularında titiz ve düzenli olmak.
4	**Birim Faaliyet Raporunun Hazırlanması**	1- Şeffaflık ve hesap verme sorumluluğunun yerine getirilememesi riski.	Düşük	1-Faaliyet raporunun performans programı baz alınarak hazırlanmasının sağlanması, bu konuda ilgili kişilere gerekli bilgilendirmelerin yapılması. 2-İlgili mevzuatında belirtilen tarihler dikkate alınarak çalışma takviminin belirlenmesi.	1- Veri toplama, analiz etme ve raporlama yeteneğine sahip olmak. 2- Üst yönetime sunulacak formatta rapor ve sunum hazırlama becerisine sahip olmak. 3- Başkanlığın genel işleyişi ve hedefleri hakkında bilgi sahibi olmak.
5	**Birim İç Kontrol Süreçlerinin Yürütülmesi**	1- Üniversitemizin amaç ve hedeflerine ulaşmasını engelleyecek muhtemel risklerin gözden kaçırılması.	Düşük	1-İç kontrolün sadece bir mali kontrol değil bir yönetim şekli olduğunun birime benimsetilmesine ve eylem planlarının bu temelde gerçekleştirilmesine özen gösterilmesi. 2-Bilgi paylaşım toplantılarının yapılması. 3-Birim bazında faaliyetlerin takip edilerek geri bildirim yapılması.	1- Kamu İç Kontrol Standartları hakkında bilgi sahibi olmak. 2- Risk analizi ve değerlendirme metodolojilerine hâkim olmak. 3- Süreç analizi ve iyileştirme yetkinliğine sahip olmak. 4- Analitik düşünme ve problem çözme becerisine sahip olmak.
6	**Satın Alma Süreçlerinin Yürütülmesi**	1- Zamanında alınmayan yazılım, lisans ve hizmetlerin, üniversite işleyişinde yavaşlamaya ve aksamaya neden olması riski. 2- Depoda ki malzemenin tükenmesi ve zamanında temin edilememesi sonucu Üniversitenin işlerinin yavaşlaması veya aksaması riski	Orta	1- Satın alınan yazılım ve lisanslardan Bilgi İşlem Daire Başkanlığı sorumluluğunda olanlarının garanti sürelerinin takip edilerek ihtiyaç durumunda yenilemelerinin yapılması, sorumluluğunda olmayanlar için ilgili birimden gelen taleplere göre işlemlerin hızlı şekilde yerine getirilmesi. 2- Bilgi İşlem Daire	1- Kamu İhale Kanunu ve ilgili satın alma mevzuatına hâkim olmak. 2- Tedarikçi ilişkileri yönetimi ve müzakere becerilerine sahip olmak. 3- Stok ve talep yönetimi konusunda bilgi sahibi olmak.

	HASSASGÖREVTESPİT FORMU	Doküman No	FR-0514
		İlk Yayın Tarihi	24.09.2025
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa	1/1

				Başkanlığı deposundaki mal ve malzemelerin takibi yapılarak olası ihtiyaçlara karşı hazırlıklı olunması ve gerektiği durumlarda yeni alımların yapılması. 3- Kurum bilişim ihtiyaçları tespit edilerek alımların yapılması ya da alım için gerekli taleplerin oluşturulması	
7	**Birim Bütçe Planlamasının Yapılması**	1- Üniversite bünyesinde ihtiyaç duyulan bilişim kaynaklarının karşılanamaması riski. 2-Kamu zararına sebebiyet verme riski.	Yüksek	1- Üniversite içinde kullanılan bilişim kaynaklarının bakım ve güncelleme ihtiyaçlarının belirlenmesi. 2- Üniversite için temin edilmesi gereken bilişim sistemlerinin belirlenmesi ve ön çalışmaların yapılması. 3- Kurum hedef ve amaçları doğrultusunda tüm ihtiyaçların belirlenerek yıllık bütçe planlamasının yapılması.	1- Kamu mali yönetimi ve bütçe mevzuatına hakim olmak. 2- Stratejik planlama ve bütçeleme teknikleri konusunda bilgi sahibi olmak. 3- Finansal analiz ve raporlama yeteneğine sahip olmak.
8	**Bilgisayar Bakım ve Onarım Hizmetinin Sağlanması** 1- Birimlerin kullandığı bilgisayarlara, Üniversitemizin lisanslı programlarını kurmak. 2- Birimlerden gelen bilgisayarların bakım ve onarımını yapmak. 3- Telefonda destek vermek. 4- Birimlere istendiğinde yerinde servis hizmeti vermek. 5- Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik ve fiziki nedenlerle alınış amaçları doğrultusunda kullanılması imkânı kalmayan ya da tamiri mümkün veya ekonomik olmayan arızalar nedeniyle kullanılmasında yarar görülmeyecek bilgisayar ve bilişim malzemelerinin tespit edip, hurdaya ayrılması için görüş	1- Lisanssız program kullanma sonucunda kurumun yaptırımlara maruz kalması riski. 2- Arızaların zamanında giderilememesi durumunda iş akışının sekteye uğraması riski. 3-Kamu zararına sebebiyet verme riski.	Düşük	1- Bilgisayar envanteri çıkartacak ortamların oluşturulması ve kurum bilgisayarlarının yazılım ve donanım takibinin yapılması. 2- Müdahale edilebilecek arızalara en hızlı şekilde iç kaynak ile müdahale edilmesi. 3- Müdahale edilemeyecek arızalarla ilgili dış kaynaklı hizmet yönlendirmesi yapılması ve alınacak aksiyonla ilgili görüş bildirilmesi. 4- Depo takibinin yapılarak ihtiyaç halinde parça temininde sorun yaşanmamasının sağlanması	1- Bilgisayar donanımı ve yazılımı arızalarının tespiti ve çözümü konusunda ileri düzeyde teknik bilgiye sahip olmak. 2- İşletim sistemleri (Windows, Linux vb.) kurulumu, yapılandırması ve yönetimi konusunda deneyimli olmak. 3- Yazılım lisanslama esasları hakkında bilgi sahibi olmak. 4- Problem çözme ve kullanıcıya teknik destek verme becerisine sahip olmak.

	bildirmek. 6- Üniversitemize alınacak donanımlara teknik şartname hazırlamak.				
9	**IP Telefon/Telefon Hizmetinin Sağlanması** 1- Telefon ağı yapısal kablolama mantığına uygun bir biçimde üniversitemizin tüm birimlerinin telefon ve santral altyapısının planlanması. 2- Tüm birimlerin kurum içi ve kurum dışı sesli iletişim problemlerinin çözümüne destek verilmesi. 3- Dâhili telefon numaralarının dağıtımı ve yönetilmesi. 4- Kurum için IP yönetiminin yapılması.	1- İletişim altyapısının sekteye uğraması veya durması riski	Düşük	1- IP telefon hizmeti için gerekli alımların yapılması ve lisans takibinin yapılması. 2- Sistemlerin güncel tutulmasının ve yetkilerinin kontrol edilmesinin sağlanması. 3- Olası arızalarda hızlı bir şekilde iletişime geçilmesi ve sürecin takibinin yapılması. 4- Son kullanıcılara olası sorunlarda en hızlı şekilde destek verilmesi	1- IP santral (PBX) ve VoIP teknolojileri yönetimi konusunda bilgi ve tecrübe sahibi olmak. 2- Yapısal kablolama ve network altyapısı hakkında bilgi sahibi olmak. 3- IP adresi ve ağ yönetimi konularına hakim olmak.
10	**Bilişim Altyapı Hizmetlerinin Sağlanması** 1-Şebeke Elektriği 2-UPS 3-İklimlendirme Sistemi 4-Ortam İzleme Sistemi 5-Yangın Söndürme Sistemi	1- Aktif cihazlarda kalıcı hasar oluşması. 2- Hizmetlerin erişilebilirliğinin sekteye uğraması. 3- Veri kayıplarının oluşması	Yüksek	1-Aktif cihazların düzenli olarak takip edilip izlenmesi, bakım ve onarımlarının yapılması, gerekli ortamın sağlanması. 2-Mevcut personele cihazları manuel olarak aktif/pasif hale getirebilecek yetkinliğin kazandırılması için gerekli olan eğitimlerin verilmesi. 3-Mevcut cihazlarla ilgili bilgi ve eğitim verilmesi dahil her türlü tedbirin alınması.	1-Veri merkezi altyapı bileşenleri (UPS, iklimlendirme, yangın söndürme, ortam izleme) hakkında teknik bilgi sahibi olmak. 2- Elektrik ve elektronik sistemler konusunda temel yetkinliğe sahip olmak. 3- Kriz anında hızlı ve doğru karar verebilme becerisine sahip olmak.
11	**Sunucu Kaynaklarının Yönetilmesi** 1- Sunucularının yapılandırılması. 2- Sunucuların sağlıklı işlemesinin sağlanması. 3- Sanallaştırma altyapısı.	1- Üniversite faaliyetlerinin aksamasına sebebiyet verme riski. 2- Hizmetlerin erişilebilirliğinin sekteye uğraması riski.	Yüksek	1- Sunucu ve üzerinde kurulu olan uygulamalardaki driver, firmware, versiyon, lisans vb. güncellemelerin düzenli aralıklarda yapılması. 2- Sunucuların yedekli bir yapıda konumlandırılmasının sağlanması. 3- Sunucuların izlenebilir olmasının sağlanması. 4- Sanallaştırma altyapısı, storage, sunucular ile çevresel	1- Sunucu işletim sistemleri (Windows Server, Linux) yönetimi konusunda ileri düzeyde bilgi sahibi olmak. 2- Sanallaştırma platformları (VMware, Hyper-V vb.) yönetimi konusunda deneyimli olmak. 3- Sunucu donanımları ve konfigürasyonları hakkında yetkin olmak.

				birimler ve sistemlerinin bakımının düzenli olarak yapılmasının sağlanması. 5- Kaynaklara erişimlerin kontrol edilmesi ve güvenlik tedbirlerinin alınması. 6- Fiziki ve sanal ortamlar için alarm üretilmesi ve en hızlı şekilde aksiyon alınabilmesi için süreçlerin belirlenmesi. 7- Sunucu ve lisansların yenileme prosedürünün hazırlanması ve uygulamaya konulması.	
12	**Yedekleme Süreçlerinin Yönetilmesi** 1-Sanal ortam yedekleri. 2-Fiziksel ortam yedekleri.	1- Üniversite faaliyetlerinin aksamasına sebebiyet verme riski. 2- Kurum genelinde veri kaybı yaşanması riski.	Düşük	1- Yedekleme yazılımlarının güncelliğinin sağlanması. 2- Yedek alınan cihazlarının güvenilir ve kesintisiz erişiminin sağlanması. 3- Kritiklik seviyelerine göre yedekleme planlarının oluşturulması. 4- Yedekten geri dönüş testleri ile yedeklerin doğruluklarının test edilmesi. 5-Farklı lokasyonlarda ve formatlarda yedeklerinin tutulmasına yönelik önlemlerin alınması.	1- Yedekleme yazılımları, teknolojileri ve stratejileri konusunda bilgi ve tecrübe sahibi olmak. 2- Veri kurtarma (disaster recovery) ve iş sürekliliği planlaması hakkında bilgi sahibi olmak. 3- Sorumluluk sahibi, planlı ve titiz çalışma disiplinine sahip olmak.
13	**Siber Güvenlik Tedbirlerin Sağlanması** 1- Sistem ve network güvenliğinin düzenlenmesi. 2- Kullanıcı erişiminin denetlenmesi ve yetkilendirilmesi. 3- Yeni teknolojileri takip etmek ve uygulanabilirliği olan ürün/sistemler için satın alma aşamasına geçmek.	1-Siber saldırılara maruz kalma riski. 2- Üniversite faaliyetlerinin aksamasına sebebiyet verme riski. 3- Bilişim kaynaklarının yetkisiz kişilerce kullanılması, suç unsurunda kişinin tespit edilememesi riski. 4- Kurumsal imajın zarar görme riski. 5-Kurum genelinde veri kaybı yaşanması riski	Yüksek	1- Ağ ve sistem güvenlik önlemlerinin alınması. 2- Güvenlik cihazlarının kuruma özel ayarlarının yapılması ve takiplerinin sağlanması. 3- Mümkün olduğu ölçüde sürekli denetimlerle zafiyet ve tehditlerin tespit edilmesi ve giderilmesi. 4- Yeterli seviyede yetkilendirmeler ile kişilerin sadece ilgili oldukları alanlara	1- Güvenlik duvarı (Firewall), IDS/IPS, SIEM gibi siber güvenlik ürünlerinin yönetimi konusunda deneyimli olmak. 2- Ağ ve sistem güvenliği prensiplerine hakim olmak. 3- Güncel siber tehditler, zafiyetler ve saldırı türleri hakkında bilgi sahibi olmak ve sürekli kendini güncellemek. 4- KVKK ve 5651 sayılı kanun gibi yasal düzenlemelerin teknik gerekliliklerine hakim olmak.

				erişimlerinin sağlanması. 5-Görev ayrılığı ilkesinin uygulanması	
14	**İz Kayıtlarının (Loglama) Yönetilmesi** 1- Sistemlerin iz kayıtlarını toplamak, izlemek, yedeklemek. 2- İz kayıtlarından kritiklik derecelerine göre alarmlar üretmek.	1- Herhangi bir suç unsurunda kişinin belirlenememesi riski.	Düşük	1- Merkezi log sunucusunun kurulması ve lokal log kayıtlarının düzenlenmesi. 2- Log verilerinin 5651 sayılı Kanunla belirlenen kurallara göre tutulmasının sağlanması. 3- Kritik sistemlerin loglarının merkezi log sunucusuna aktarılması	1- Log yönetimi ve analizi araçlarını (SIEM vb.) kullanma tecrübesine sahip olmak. 2- 5651 sayılı kanun ve ilgili mevzuat gerekliliklerini bilmek. 3- Anomali tespiti ve olay müdahale süreçleri hakkında bilgi sahibi olmak.
15	**Bilişim Altyapılarında Son Kullanıcı Güvenliğinin Sağlanması** 1- Antivirüs programının sağlanması. 2- Son kullanıcı aktivitelerinin sınırlanması.	1- Kişisel veri kayıplarının yaşanması riski. 2- Zararlı yazılımların kurum ağına yayılabilmesi riski. 3- Kurumsal veri kayıplarının yaşanması riski.	Yüksek	1- Lisanslı program kullanılması ve düzenli aralıklarla güncellenmesi. 2- Yazılımın otomatik olarak tarama modunda çalıştırılması. 3- Otomatik olarak tüm cihazlara kurulması ve kullanıcı tarafından kaldırılmasının iptal edilmesi. 4-Kurumsal antivirüs yazılımının kullandırılması.	1- Antivirüs, EDR gibi uç nokta güvenlik çözümlerinin merkezi yönetimi konusunda deneyimli olmak. 2- Active Directory, Group Policy gibi merkezi kullanıcı yönetimi ve kısıtlama politikalarına hakim olmak. 3- Kullanıcı kaynaklı güvenlik riskleri hakkında bilgi sahibi olmak.
16	**Web Servis Hizmetlerinin Yönetimi** 1- Sistemler arası entegrasyonun sağlanması. 2- İnsan hatasını en aza indirmek için otomatik süreçler tasarlanması.	1- Bilişim sistemlerinin entegre çalışmalarının sağlanamaması riski. 2- Hizmetlerin erişilebilirliğinin sekteye uğraması riski. 3-Kontrolsüz ve yetkisiz erişimlerin oluşması riski.	Düşük	1- Web servis entegrasyonlarının kontrollerinin yapılması. 2- Entegre edilecek sistemler için senaryonun oluşturulması ve uygulamasının testlerinin yapılması veya ilgili birimlere yaptırılması. 3- İlgili birimlerin bilgilendirmelerinin sağlanması. 4- Daha entegre ve otonom sistemler için ihtiyaç duyulan servislerin ve entegrasyonların tespit edilip, gerçekleştirilmesinin	1- API, REST, SOAP gibi web servis teknolojileri hakkında bilgi sahibi olmak. 2- Sistem entegrasyonu ve otomasyon konularında deneyimli olmak. 3- Kimlik doğrulama ve yetkilendirme mekanizmaları hakkında bilgi sahibi olmak.

	HASSASGÖREVTESPİT FORMU	Doküman No	FR-0514
		İlk Yayın Tarihi	24.09.2025
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa	1/1

				sağlanması.	
17	**Web Sitesi Yönetimi** 1- Web sayfaların oluşturulması ve İYS yetkililerinin atanması. 2- Eğitimlerin verilmesi.	1- Gerekli bilgileri dış dünyayla paylaşılamaması riski. 2- Kurumsal imajın zarar görme riski. 3-Şifrelerin 3.şahısların eline geçmesi riski.	Düşük	1- Gelen taleplere göre yetkilendirmelerin yapılması ve ilgili kişilere İYS eğitimlerinin verilmesi. 2- Web sitesinin 7/24 sürekliliğinin sağlanması. 3- İçerik girişlerinin güncel ve doğru olması. 4- Alınması gereken güvenlik önlemlerinin sunucu ve uygulama katmanında alınması.	1- İçerik Yönetim Sistemlerini (CMS) etkin bir şekilde kullanabilmek. 2- Temel web teknolojileri (HTML, CSS) hakkında bilgi sahibi olmak. 3- Kullanıcı yetki yönetimi ve web güvenliği en iyi uygulamaları hakkında bilgi sahibi olmak.
18	**Elektronik Belge Yönetim Sistemine Teknik Destek Sağlanması** 1- Karşılaşılan problemlere teknik destek sağlanması ve firma ile koordinasyonun sağlanması.	1-İhtiyacın düzgün tespit edilememesi nedeniyle iş ihtiyaçlarının karşılanamaması riski. 2-EBYS ile ilgili aksaklıklar yaşanması riski. 3- Hizmetlerin erişilebilirliğinin sekteye uğraması riski.	Orta	1- Bilgi İşlem Daire Başkanlığı tarafından çözülebilecek teknik problemlerle ilgili hızlı ve pratik çözümlerin üretilmesi ve sunulması. 2- Gerektiği durumda firma ile hızlı şekilde iletişime geçerek problemin çözümlenmesinin sağlanması	1- Kurumda kullanılan EBYS yazılımının teknik mimarisi ve işleyişi hakkında bilgi sahibi olmak. 2- Kullanıcı desteği ve problem çözme becerilerine sahip olmak. 3- Yazılım firması ile teknik konularda etkin iletişim kurabilme yeteneğine sahip olmak.
Hazırlayan Abdulkadir GÖNÜLALGAK Büro Personeli				**Onaylayan (*Birim Amiri*)** Halis BOZKURT Bilgi İşlem Daire Başkanı	

Bubölüme,...Birimadıyazılacaktır.

***** Bubölümde,faaliyetlerinyürütülmesiamacıylabirimtarafındanbelirlenenhassasgörev tanımlanacaktır.***

****Bubölüme...HassasGörevriskleriyazılacaktır.***

*****HassasGörev/İş'inriskdüzeyieklenecektir.(Yüksek-Orta-Düşük)***