	BİLGİ İŞLEM DAİRE BAŞKANLIĞI İYİLEŞTİRME EYLEM PLANI	Doküman No	**PL.009**
		İlk Yayın Tarihi	**22.07.2025**
		Revizyon Tarihi	**-**
		Revizyon No	**0**
		Sayfa	**1/4**

İyileştirilecek Durum*	Planlanan Eylemler	Eylem Uygulama Tarih Aralığı	Sonuç ve Açıklamalar
1. Kablolu ve kablosuz ağ kapsama alanı, kapasite ve bağlantı sürekliliğinin geliştirilmesi	Kampüs genelinde kapsama ve performans ölçümleri yapılacak; zayıf noktalar tespit edilerek erişim noktası, switch, omurga ve kablolama ihtiyaçları planlanacaktır. Kritik noktalarda ağ yedekliliği ve kapasite artışı sağlanacaktır.	Sürekli / 6 aylık gözden geçirme	Kapsama sorunlarının, bağlantı kesintilerinin ve yoğunluk kaynaklı performans kayıplarının azaltılması; ağ hizmet kalitesinin ölçülebilir verilerle izlenmesi hedeflenmektedir.
2. Kurumsal web sayfalarının güncelliği, erişilebilirliği ve kullanıcı deneyiminin iyileştirilmesi	Web sayfaları içerik güncelliği, bağlantı bütünlüğü, mobil uyumluluk, erişilebilirlik ve kullanıcı deneyimi açısından periyodik olarak kontrol edilecek; birimlerden güncel içerik akışı düzenli hâle getirilecektir.	Sürekli / 3 aylık içerik kontrolü	Doğru ve güncel bilgiye daha hızlı erişim sağlanması; hatalı veya güncelliğini yitirmiş içeriklerin azaltılması ve kullanıcı deneyiminin iyileştirilmesi hedeflenmektedir.
3. Bilgi güvenliği ve KVKK farkındalığının artırılması	Personel ve kullanıcılar için bilgi güvenliği, kişisel verilerin korunması, güçlü parola kullanımı, sosyal mühendislik ve oltalama saldırıları konularında farkındalık eğitimleri ve bilgilendirme çalışmaları yürütülecektir.	Yılda en az 1 kez / Sürekli bilgilendirme	Bilgi güvenliği kaynaklı kullanıcı hatalarının azaltılması ve kişisel verilerin korunmasına ilişkin kurumsal farkındalığın sürdürülebilir şekilde artırılması hedeflenmektedir.
4. Lisanssız veya yetkisiz yazılım ve uygulamaların kurumsal bilgisayarlara yüklenmesinin önlenmesi	Kurumsal bilgisayarlarda yazılım kurulum yetkileri kontrol altına alınacak; lisans envanteri düzenli takip edilecek ve ihtiyaç dışı/yetkisiz uygulamaların kurulmasını engelleyecek teknik ve idari kontroller uygulanacaktır.	Sürekli / 6 aylık kontrol	Lisans uyumsuzluğu, zararlı yazılım ve yetkisiz uygulama kaynaklı güvenlik risklerinin azaltılması; kurumsal cihazlarda standart yazılım yapısının korunması hedeflenmektedir.
5. Fiyat teklifi ve piyasa araştırması süreçlerinde firma geri dönüşlerinden kaynaklanan gecikmelerin azaltılması	Teklif talepleri standartlaştırılmış kayıtlarla takip edilecek; talep tarihi, son yanıt tarihi ve firma geri dönüşleri izlenecek, gerektiğinde alternatif tedarikçi havuzu kullanılacaktır.	Sürekli	Teklif toplama süresinin kısaltılması, satın alma işlemlerinin zamanında sonuçlandırılması ve piyasa araştırmasının izlenebilirliğinin artırılması hedeflenmektedir.
6. Birime iletilen satın alma taleplerinin öncelik ve aciliyet durumuna göre etkin takibinin sağlanması	Satın alma talepleri ihtiyaç, aciliyet, hizmet etkisi ve bütçe durumu dikkate alınarak sınıflandırılacak; işlem aşamaları kayıt altına alınacak ve periyodik olarak izlenecektir.	Sürekli	Acil ve kritik ihtiyaçların zamanında karşılanması, iş yükünün dengeli dağıtılması ve satın alma süreçlerinin daha etkin yürütülmesi hedeflenmektedir.
7. BİDB personelinin mesleki bilgi ve yetkinliklerinin artırılması	Şube ve görev alanları bazında yıllık eğitim ihtiyaçları belirlenecek; teknik eğitim, sertifika programı, kurum içi bilgi paylaşımı ve deneyim aktarım toplantıları planlanacaktır.	Yıllık eğitim planı / Sürekli	Personelin güncel teknolojilere uyumunun, teknik uzmanlığının ve birimler arası bilgi paylaşımının artırılması hedeflenmektedir.
8. Personel çalışma alanlarının kapasite ve ergonomi açısından iyileştirilmesi	Personel sayısı ve görev ihtiyaçları dikkate alınarak çalışma alanları gözden geçirilecek; oda, masa, teknik çalışma alanı ve ergonomik düzenlemelere ilişkin ihtiyaçlar planlanacaktır.	İhtiyaç ve bütçe imkânları doğrultusunda	Daha düzenli, güvenli ve verimli bir çalışma ortamının oluşturulması; yoğun çalışma alanlarından kaynaklanan verim kaybının azaltılması hedeflenmektedir.
9. Risk Kontrol Eylem Planında yer alan eylemlerin takibinde yaşanabilecek aksaklıkların önlenmesi	Risk Kontrol Eylem Planındaki faaliyetler BİDB iş takvimine işlenecek; sorumlular, hedef tarihler ve gerçekleşme durumları belirli periyotlarda kontrol edilerek geciken eylemler için takip mekanizması işletilecektir.	3 aylık izleme / Sürekli	Risklerin zamanında ele alınması, geciken faaliyetlerin görünür hâle getirilmesi ve iç kontrol sürecinin izlenebilirliğinin artırılması hedeflenmektedir.
10. Etkinlik ve organizasyonlara ilişkin teknik destek taleplerinin geç veya eksik bildirilmesinden kaynaklanan aksaklıkların azaltılması	Etkinlik teknik destek taleplerinin standart bir başvuru/randevu yapısı üzerinden alınması; tarih, yer, ihtiyaç duyulan cihaz ve hizmet bilgilerinin önceden bildirilmesi sağlanacaktır.	Sürekli	Teknik ekip ve ekipman planlamasının önceden yapılması, çakışmaların azaltılması ve etkinliklerde kesintisiz teknik destek sağlanması hedeflenmektedir.

Hazırlayan	Sistem Onayı	Yürürlük Onayı
Bölüm Kalite Sorumlusu	Kalite Koordinatörü	Üst Yönetici

İyileştirilecek Durum*	Planlanan Eylemler	Eylem Uygulama Tarih Aralığı	Sonuç ve Açıklamalar
11. Gelişen teknoloji ve kurumsal ihtiyaçlar doğrultusunda mevcut yazılımların güncel tutulması ve ihtiyaç duyulan çözümlerin planlanması	Kurumsal uygulamalar için ihtiyaç analizi ve yıllık geliştirme/yenileme planı hazırlanacak; kullanım dışı, yetersiz veya mükerrer çözümler gözden geçirilecek ve gerekli yazılım geliştirme ya da tedarik faaliyetleri önceliklendirilecektir.	Yıllık planlama / Sürekli	Kurumsal süreçlerde yazılım kaynaklı aksamaların azaltılması, kullanıcı ihtiyaçlarına daha hızlı cevap verilmesi ve kaynakların etkin kullanılması hedeflenmektedir.
12. Eskiyen donanım ve yazılımlardan kaynaklanan hizmet kesintilerinin azaltılması	Donanım ve yazılım varlıkları yaşam döngüsü, üretici destek süresi ve arıza sıklığı açısından izlenecek; yenileme öncelikleri belirlenerek yıllık yatırım planlarına dâhil edilecektir.	Yıllık envanter değerlendirmesi / Sürekli	Kritik arızaların ve plansız kesintilerin azaltılması; ekonomik ömrünü tamamlayan cihaz ve yazılımların kontrollü biçimde yenilenmesi hedeflenmektedir.
13. Üniversite personelinin bilgi teknolojileri kullanımından kaynaklanan hata ve veri kaybı risklerinin azaltılması	Kullanıcılara yönelik kısa rehberler, sık sorulan sorular, resmî bilgilendirmeler ve uygulamalı eğitimler hazırlanacak; güvenli kullanım, veri saklama ve temel sorun giderme konularında farkındalık artırılacaktır.	Sürekli / Yılda en az 1 bilgilendirme	Kullanıcı kaynaklı arıza, veri kaybı ve destek taleplerinin azaltılması; öz hizmet ve bilinçli kullanım oranının artırılması hedeflenmektedir.
14. Sistem odalarında altyapı, enerji, iklimlendirme ve fiziksel güvenlik koşullarının iyileştirilmesi	Sunucu ve sistem odalarında sıcaklık/nem takibi, UPS ve enerji altyapısı, iklimlendirme, yangın algılama/söndürme, kablolama düzeni ve fiziksel erişim kontrolleri periyodik olarak gözden geçirilecek ve gerekli yenilemeler planlanacaktır.	Sürekli / Periyodik bakım	Kritik bilişim altyapısının güvenliği ve sürekliliğinin artırılması; çevresel ve fiziksel risklerden kaynaklanan hizmet kesintilerinin azaltılması hedeflenmektedir.
15. BİDB bünyesinde yürütülen iş ve işlemlerin standardizasyonunun artırılması	Tekrarlanan işler için süreç akışları, görev tanımları, kontrol listeleri, talimatlar ve uygulama prosedürleri hazırlanacak; dokümanlar versiyon kontrollü olarak güncel tutulacaktır.	Sürekli / Yıllık gözden geçirme	İşlerin kişiye bağımlılığının azaltılması, görev devrinin kolaylaştırılması, işlem sürelerinin standartlaştırılması ve kurumsal hafızanın güçlendirilmesi hedeflenmektedir.
16. Kritik bilişim sistemlerinin merkezi izlenmesi ve arızalara erken müdahale kapasitesinin geliştirilmesi	Sunucu, ağ cihazı, servis, disk, kaynak kullanımı ve erişilebilirlik göstergeleri merkezi izleme sistemi üzerinden takip edilecek; kritik eşikler için alarm mekanizmaları ve sorumlu bildirimleri tanımlanacaktır.	7/24 izleme / Aylık değerlendirme	Arızaların kullanıcı bildiriminden önce tespit edilmesi, müdahale süresinin kısaltılması ve hizmet sürekliliğinin ölçülebilir göstergelerle izlenmesi hedeflenmektedir.
17. Yedekleme ve felaket kurtarma süreçlerinin güçlendirilmesi	Kritik sistemler için yedekleme sıklığı, saklama süresi ve farklı konumda yedek bulundurma esasları tanımlanacak; yedeklerden geri dönüş testleri ve felaket kurtarma senaryoları periyodik olarak uygulanacaktır.	Sürekli / En az 6 ayda 1 geri dönüş testi	Yedeklerin yalnızca alınmasının değil, ihtiyaç hâlinde kullanılabilirliğinin de doğrulanması; veri kaybı ve uzun süreli hizmet kesintisi riskinin azaltılması hedeflenmektedir.
18. Kritik ağ, sunucu ve depolama bileşenlerinde tek hata noktasının azaltılması	Kritik hizmetlerde ağ bağlantısı, güç kaynağı, sunucu, sanallaştırma, depolama ve temel ağ servisleri açısından yedeklilik ihtiyacı analiz edilecek; uygun bileşenlerde yüksek erişilebilirlik ve alternatif çalışma senaryoları oluşturulacaktır.	Yıllık değerlendirme / Büyük değişiklikler sonrası	Tek bir cihaz veya bağlantı arızasının geniş çaplı hizmet kesintisine dönüşme olasılığının azaltılması hedeflenmektedir.
19. İşletim sistemi, sunucu, ağ cihazı ve uygulamalarda güvenlik güncellemelerinin sistematik yönetilmesi	Varlıklar için yama/güncelleme takvimi oluşturulacak; kritik güvenlik güncellemeleri önceliklendirilecek, mümkün olan sistemlerde test ve geri dönüş planı sonrasında üretim ortamına uygulanacaktır.	Aylık / Kritik güncellemelerde öncelikli	Bilinen güvenlik açıklarından kaynaklanan risklerin azaltılması ve sistemlerin desteklenen sürümlerde tutulması hedeflenmektedir.

İyileştirilecek Durum*	Planlanan Eylemler	Eylem Uygulama Tarih Aralığı	Sonuç ve Açıklamalar
20. Kullanıcı hesapları, yetkiler ve ayrıcalıklı erişimlerin etkin yönetilmesi	Kurumsal kimlik doğrulama, SSO ve çok faktörlü doğrulama imkânları yaygınlaştırılacak; yetkiler görev ihtiyacına göre verilecek, ayrılan veya görev değiştiren personelin erişimleri zamanında güncellenecek ve ayrıcalıklı hesaplar periyodik olarak gözden geçirilecektir.	Sürekli / 6 aylık yetki gözden geçirme	Yetkisiz erişim riskinin azaltılması, hesap yönetiminin merkezileştirilmesi ve kimlik doğrulama güvenliğinin artırılması hedeflenmektedir.
21. Sistem ve uygulama kayıtlarının (log) merkezi, düzenli ve denetlenebilir şekilde yönetilmesi	Kritik sistem ve uygulama loglarının merkezi olarak toplanması, uygun sürelerle saklanması, zaman senkronizasyonunun sağlanması ve olağandışı durumların incelemeye elverişli hâle getirilmesi için standartlar oluşturulacaktır.	Sürekli / Aylık kontrol	Olayların geriye dönük analiz edilebilmesi, güvenlik incelemelerinin hızlandırılması ve denetim izlerinin güçlendirilmesi hedeflenmektedir.
22. Siber güvenlik zafiyetlerinin tespit ve giderilme sürecinin iyileştirilmesi	Periyodik zafiyet taramaları ve uygun aralıklarla sızma testleri gerçekleştirilecek; tespit edilen bulgular risk seviyesine göre önceliklendirilecek, sorumlu ve hedef tarih atanarak kapanışları kayıt altına alınacaktır.	6 aylık tarama / Yıllık veya ihtiyaç halinde test	Kritik güvenlik açıklarının daha erken tespit edilmesi, giderilme sürelerinin izlenmesi ve tekrar eden bulguların azaltılması hedeflenmektedir.
23. Donanım, yazılım, lisans ve bilişim varlık envanterinin güncelliğinin artırılması	Varlıkların sorumlusu, konumu, teknik özellikleri, garanti/destek süresi, lisans durumu ve yaşam döngüsü bilgileri tekil ve güncel envanterde tutulacak; periyodik sayım ve doğrulama yapılacaktır.	6 aylık kontrol / Sürekli güncelleme	Kaynak planlaması, lisans yönetimi, bakım ve yenileme kararlarının güncel envanter verisine dayandırılması hedeflenmektedir.
24. Kullanıcı destek taleplerinin daha hızlı, ölçülebilir ve izlenebilir şekilde yönetilmesi	Destek talepleri merkezi destek sistemi üzerinden kategori, öncelik ve durum bilgileriyle izlenecek; ilk yanıt ve çözüm süreleri takip edilecek, sık tekrar eden sorunlar için kalıcı çözüm ve bilgi bankası içerikleri oluşturulacaktır.	Sürekli / Aylık performans değerlendirmesi	Destek hizmetlerinde şeffaflığın, cevap hızının ve kullanıcı memnuniyetinin artırılması; tekrar eden arızaların azaltılması hedeflenmektedir.
25. Yazılım geliştirme, test ve canlıya alma süreçlerinin standartlaştırılması	Kurumsal yazılımlarda sürüm kontrolü, kod gözden geçirme, test ortamı, değişiklik kaydı, sürüm notu ve gerektiğinde geri dönüş planı esasları tanımlanacak; kritik değişiklikler kayıtlı ve kontrollü biçimde canlıya alınacaktır.	Her sürüm/değişiklikte	Yazılım değişikliklerinden kaynaklanan hata ve kesintilerin azaltılması, bakım yapılabilirliğin ve geliştirme kalitesinin artırılması hedeflenmektedir.
26. Kurumsal bilgi sistemleri arasındaki entegrasyonların sürekliliğinin ve izlenebilirliğinin artırılması	OBS, AVEBİS, PBS, Portal, Dashboard ve diğer kurumsal sistemler arasındaki entegrasyonlarda hata kayıtları, servis erişilebilirliği, kimlik bilgisi/sertifika süreleri ve veri aktarım sonuçları izlenecek; kritik hatalar için bildirim mekanizması kurulacaktır.	Sürekli	Entegrasyon kaynaklı veri gecikmesi ve hizmet kesintilerinin hızlı tespit edilmesi; sistemler arası veri akışının daha güvenilir hâle getirilmesi hedeflenmektedir.
27. Yönetim ve raporlama sistemlerinde veri kalitesi ve güvenilirliğinin artırılması	Dashboard ve kurumsal raporlarda kullanılan veriler için eksiklik, tutarsızlık, mükerrer kayıt ve beklenmeyen değişim kontrolleri geliştirilecek; mümkün olan alanlarda otomatik doğrulama ve birim bazlı kontrol mekanizmaları uygulanacaktır.	Sürekli / Aylık veri kalite kontrolü	Yönetim kararlarında kullanılan verilerin doğruluk, bütünlük ve güncellik düzeyinin artırılması; hatalı verinin erken tespit edilmesi hedeflenmektedir.
28. Kurumsal web uygulamalarının erişilebilirlik, mobil uyumluluk ve kullanılabilirlik açısından geliştirilmesi	Yeni ve mevcut uygulamalarda klavye ile kullanım, renk/kontrast, form etiketleri, okunabilirlik, mobil ekran uyumu ve temel erişilebilirlik kontrolleri geliştirme ve güncelleme süreçlerine dâhil edilecektir.	Her büyük sürümde / Yıllık genel kontrol	Farklı cihaz ve kullanıcı ihtiyaçlarında daha erişilebilir, anlaşılır ve tutarlı dijital hizmet sunulması hedeflenmektedir.

İyileştirilecek Durum*	Planlanan Eylemler	Eylem Uygulama Tarih Aralığı	Sonuç ve Açıklamalar
29. Kurumsal e-posta güvenliğinin ve oltalama saldırılarına karşı dayanıklılığın artırılması	Spam/oltalama filtreleri, güvenli e-posta yapılandırmaları ve şüpheli e-posta bildirim süreçleri gözden geçirilecek; kullanıcı farkındalığını ölçmek ve geliştirmek üzere örnek senaryo ve bilgilendirme çalışmaları yapılacaktır.	Sürekli / Yıllık farkındalık çalışması	Zararlı bağlantı, sahte e-posta ve kimlik bilgisi ele geçirme kaynaklı olayların azaltılması; şüpheli durumların daha hızlı raporlanması hedeflenmektedir.
30. Teknik dokümantasyonun güncelliğinin ve kurumsal bilgi sürekliliğinin artırılması	Ağ topolojileri, sistem mimarileri, servis listeleri, kritik konfigürasyon bilgileri, bakım prosedürleri, tedarikçi/destek bilgileri ve acil müdahale adımları kontrollü bir dokümantasyon yapısında güncel tutulacaktır.	Sürekli / 6 aylık gözden geçirme	Kişiye bağımlılığın azaltılması, arıza ve görev devri süreçlerinde müdahale hızının artırılması ve kurumsal hafızanın korunması hedeflenmektedir.
31. Altyapı kapasite planlamasının veriye dayalı hâle getirilmesi	Sunucu işlemci/bellek/disk kullanımı, depolama büyümesi, ağ bant genişliği, istemci ve servis yükleri dönemsel olarak analiz edilerek kapasite eşikleri ve yatırım ihtiyaçları önceden belirlenecektir.	3 aylık analiz / Yıllık planlama	Kaynak yetersizliğine bağlı performans sorunlarının oluşmadan önce öngörülmesi ve yatırım planlarının gerçek kullanım verilerine dayandırılması hedeflenmektedir.
32. Kullanıcı memnuniyeti ve geri bildirimlerin sistematik olarak iyileştirme faaliyetlerine dönüştürülmesi	Memnuniyet anketleri, destek sistemi geri bildirimleri, birim talepleri ve kullanıcı önerileri periyodik olarak analiz edilecek; tekrar eden veya yüksek etkili konular için iyileştirme eylemleri oluşturularak sonuçları izlenecektir.	Yıllık anket / 3 aylık geri bildirim değerlendirmesi	Kullanıcı beklentilerinin ölçülebilir biçimde takip edilmesi, hizmet önceliklerinin gerçek ihtiyaçlara göre belirlenmesi ve sürekli iyileştirme kültürünün güçlendirilmesi hedeflenmektedir.

**İyileştirme konuları; memnuniyet anketleri, iç tetkik sonuçları, risk değerlendirmeleri, öğrenci/personel geri bildirimleri, destek kayıtları, sistem izleme verileri, dış değerlendirici görüşleri ile mevzuat ve teknoloji değişiklikleri dikkate alınarak belirlenir.*