

BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ YÖNETİMİ AKIŞ SÜREÇ KARTI

Doküman No	BÜ. SRÇ.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	1/10

Sürecin Tipi	<input type="checkbox"/> Ana Süreç <input checked="" type="checkbox"/> Süreç <input type="checkbox"/> Alt Süreç
Bağlı Olduğu Üst Sürecin Adı	Yönetimsel Süreçler Ana Süreci
Sürecin Sahibi	• Bilgi İşlem Daire Başkanlığı
Sürecin Uygulayıcıları	• Sürecin çeşitli alt faaliyetlerini yürüten ekipler (Yazılım, Sistem, Ağ ve Donanım, Çağrı Merkezi) • Tüm Birimler
Sürecin Kapsamı ve Amacı	<p>Bilgi teknolojileri ve bilgi kaynaklarının etkin ve güvenli bir şekilde yönetilmesi, üniversitenin dijital altyapısını güçlendirerek eğitim, araştırma ve yönetim faaliyetlerinin sürdürülebilirliğini ve verimliliğini sağlamak. Bu sürecin temel amacı, bilgi güvenliği, erişim kolaylığı ve teknolojik altyapının sürekli iyileştirilmesi yoluyla tüm paydaşlara en yüksek düzeyde destek sunmaktır.</p> <p>Bu süreç; bilgi teknolojileri altyapısının yönetimi, bilgi güvenliği politikalarının oluşturulması ve uygulanması, yazılım ve donanım envanterinin güncellenmesi, veri tabanları ve bilgi kaynaklarının erişilebilir kılınması, kullanıcı destek hizmetlerinin sağlanması gibi faaliyetleri kapsar. Ayrıca, teknolojik yeniliklerin entegrasyonu, dijital dönüşüm projeleri, lisanslama ve veri güvenliği konularını da içerir.</p>
Etkilediği Süreçler	Tüm Ana Süreçler
Etkilendiği Süreçler	Tüm Ana Süreçler
Alt Süreçleri	<ol style="list-style-type: none">Bilgi Teknolojileri Yönetimi ve Güvenliği SüreciYazılım ve Donanım Destek Operasyonları Yönetimi Süreci

Hazırlayan	Onaylayan

KONTROLLÜ

BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ YÖNETİMİ AKIŞ SÜREÇ KARTI

Doküman No	BÜ. SRÇ.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	2/10

SÜRECİN İZLEME YÖNTEMİ	SÜRECİN GÖZDEN GEÇİRME PERİYODU	SÜRECİN PERFORMANS GÖSTERGELERİ
<ol style="list-style-type: none">KPI (Anahtar Performans Göstergeleri) Takibi: Sistem kullanılabilirliği, erişim hızı, teknik destek çözüm süresi, veri güvenliği ihlalleri gibi KPI'ların belirlenmesi ve periyodik olarak ölçülmesi.Kullanıcı Memnuniyet Anketleri: Öğrenci, akademik ve idari personel gibi kullanıcı gruplarının sistem ve destek hizmetlerinden ne kadar memnun olduklarını anlamak için yılda en az bir kez memnuniyet anketleri yapılması.Olay Yönetimi ve Güvenlik İhlali Raporları: Siber güvenlik olayları, veri ihlalleri, sistem arızaları gibi durumların kayıt altına alınması ve analiz edilmesi.Düzenli Güvenlik ve Sistem Güncellemeleri: Sistem ve güvenlik güncellemelerinin düzenli olarak uygulanması ve sonuçlarının izlenmesi.Sistem Yedekleme ve Kurtarma Testleri: Veri yedekleme süreçlerinin düzenli olarak test edilmesi ve kurtarma işlemlerinin başarı oranlarının izlenmesi.Erişim ve Hata Loglarının Takibi: Sistem erişim loglarının ve hata raporlarının incelenmesi, güvenlik ve sistem kesintilerinin hızlıca tespit edilmesi için önemlidir.	<ol style="list-style-type: none">Güvenlik İhlalleri ve Olaylar Sonrası: Güvenlik ihlalleri, veri kayıpları veya kritik sistem arızaları sonrası, sürecin gözden geçirilmesi ve yeni önlemlerin alınması.Yeni Teknolojik Gelişmeler: Yeni yazılım, donanım veya dijital kaynaklar kullanıma girdiğinde, mevcut süreçlerin bu yeniliklerle uyumlu hale getirilmesi için gözden geçirme yapılması.Kullanıcı Geribildirimleri: Kullanıcı memnuniyeti ve destek hizmetlerine yönelik yapılan anket sonuçları doğrultusunda, süreçlerin gözden geçirilmesi ve iyileştirilmesi.	<ol style="list-style-type: none">Sistem Kullanılabilirlik Oranı: Bilgi teknolojileri altyapısının (sunucular, ağ, veri tabanları vb.) erişilebilirlik oranı.Ortalama Arıza Giderme Süresi: Bir arıza veya sistem kesintisinin giderilme süresi.Kullanıcı Memnuniyeti Oranı: Kullanıcılardan (öğrenci, akademik ve idari personel) alınan geri bildirimler doğrultusunda bilgi teknolojileri hizmetlerine yönelik memnuniyet oranı.Destek Talebi Çözüm Süresi: Teknik destek ekiplerine iletilen taleplerin ortalama çözüm süresi.Güvenlik İhlal Sayısı: Yıl içinde meydana gelen güvenlik ihlali, veri sızıntısı veya saldırı sayısı.Kaynak Kullanımı (Veri Tabanı ve Dijital Kaynaklar): Veri tabanı ve dijital kaynakların kullanım oranları.Sistem Güncellemeleri ve Bakım Oranı: Sistem ve güvenlik güncellemelerinin düzenli ve eksiksiz yapılma oranı.Eğitim Katılım Oranı: Kullanıcılara verilen bilgi teknolojileri eğitimlerine katılım oranı.Donanım ve Yazılım Envanter Güncellemeleri: Yıl içinde güncellenen donanım ve yazılım envanter sayısı.
Hazırlayan	Onaylayan	

KONTROLLÜ



**BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ
YÖNETİMİ AKIŞ SÜREÇ KARTI**

Doküman No	BÜ. SRC.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	3/10

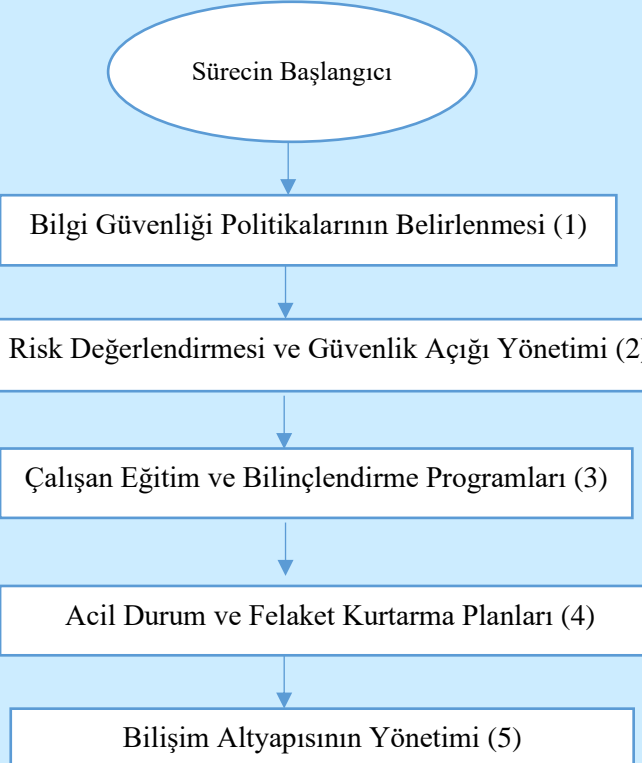
Hazırlayan

Onaylayan

KONTROLLÜ

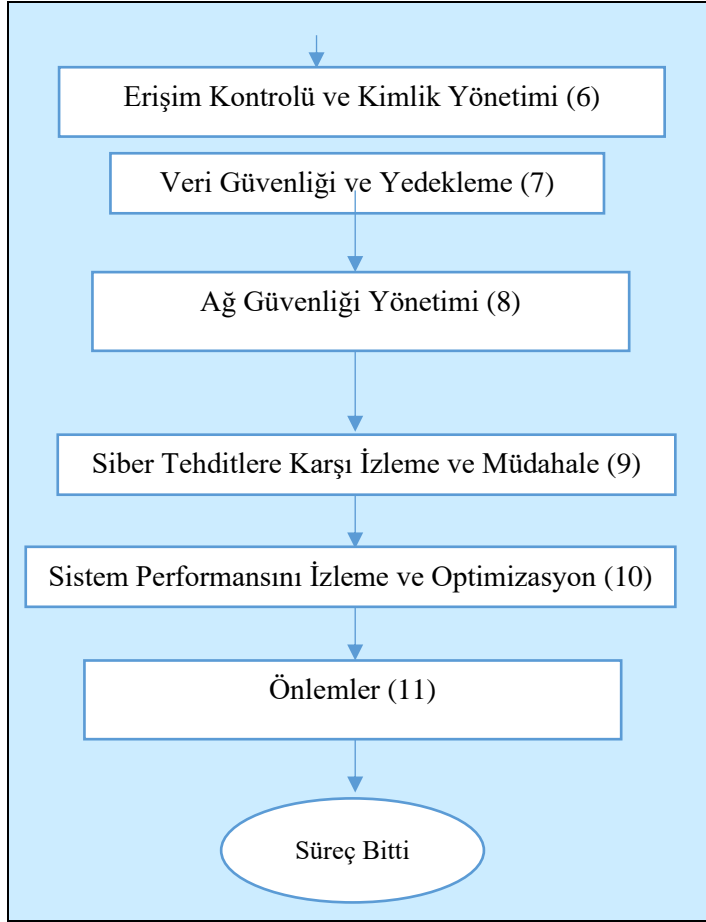
BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ YÖNETİMİ AKIŞ SÜREÇ KARTI

Doküman No	BÜ. SRC.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	4/10

(I) Bilgi Teknolojileri Yönetimi ve Güvenliği Süreci Akış Planı	No	Faaliyet	PUKÖ Döngüsü
	1	Bilgi Güvenliği Politikalarının Belirlenmesi - Güvenlik politikalarının oluşturulması ve güncellenmesi. - Güvenlik standartlarının ve prosedürlerinin belirlenmesi. - Kurumsal bilgi güvenliği farkındalık programlarının oluşturulması.	Planlama
	2	Risk Değerlendirmesi ve Güvenlik Açığı Yönetimi - Bilişim sistemlerinde güvenlik açığı taramaları yapılması. - Risk değerlendirme raporlarının hazırlanması ve güvenlik açığı giderme süreçlerinin izlenmesi. - Güvenlik zafiyetlerinin çözülmesi için eylem planları oluşturulması.	Planlama
	3	Çalışan Eğitim ve Bilinçlendirme Programları - Çalışanlara yönelik bilgi güvenliği eğitimlerinin düzenlenmesi. - Kullanıcıların siber tehditlere karşı bilinçlendirilmesi. - İç denetim ve güvenlik tatbikatları ile farkındalık artırılması.	Planlama
	4	Acil Durum ve Felaket Kurtarma Planları - Felaket kurtarma stratejilerinin oluşturulması ve test edilmesi. - Acil durum planlarının hazırlanması ve sürekli olarak güncellenmesi. - Felaket senaryolarına karşı hazırlıklı olmak için tatbikatlar düzenlenmesi.	Planlama
	5	Bilişim Altyapısının Yönetimi - Bilişim altyapısının kurulumu ve bakımı. - Donanım, yazılım ve ağ altyapısının güncellenmesi. - Bulut bilişim ve veri merkezleri ile ilgili yönetim faaliyetleri.	Uygulama

Hazırlayan	Onaylayan

KONTROLLÜ

	6	Erişim Kontrolü ve Kimlik Yönetimi – Kullanıcı erişim haklarının belirlenmesi ve yönetilmesi. – Kimlik doğrulama yöntemlerinin uygulanması.	Uygulama
	7	Veri Güvenliği ve Yedekleme – Verilerin şifrelenmesi ve güvenli depolanması. – Veri yedekleme süreçlerinin düzenlenmesi. – Yedekleme stratejilerinin test edilmesi ve iyileştirilmesi.	Uygulama
	8	Ağ Güvenliği Yönetimi – Güvenlik duvarları, antivirüs ve antispam sistemlerinin kurulması ve yönetilmesi. – Ağa erişim kontrolü, izleme ve analiz süreçlerinin yönetilmesi.	Uygulama
	9	Siber Tehditlere Karşı İzleme ve Müdahale – Güvenlik izleme araçlarının kurulması. – Siber saldırılara karşı aktif izleme ve raporlama. – Olay müdahale ve analiz süreçlerinin oluşturulması.	Uygulama
	10	Sistem Performans İzleme ve Optimizasyonu: KONTROL – Bilişim sistemlerinin performans izleme ve raporlama. – Sistem kaynaklarının verimli kullanımını sağlamak için optimizasyon yapılması. Kapasite planlaması ve sistem genişletme stratejilerinin belirlenmesi.	Kontrol

Hazırlayan	Onaylayan

KONTROLLÜ

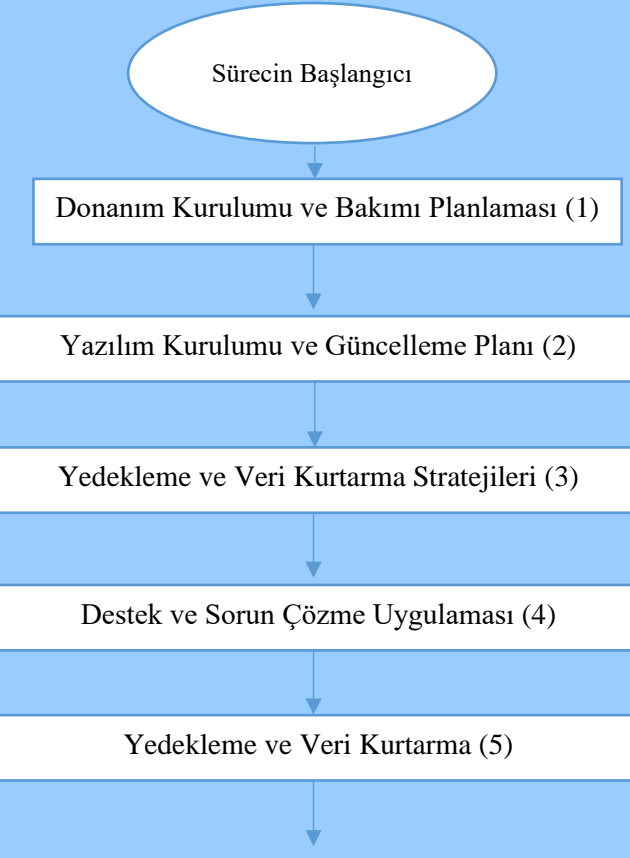
BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ YÖNETİMİ AKIŞ SÜREÇ KARTI

Doküman No	BÜ. SRC.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	6/10

	11	<ul style="list-style-type: none">- Güvenlik açıklarının çözülmesi ve iyileştirme süreçlerinin başlatılması.- Sistemdeki zafiyetlere karşı önleyici tedbirlerin alınması.- Eğitim ve farkındalık programlarının güncellenmesi ve yeni tehditlere karşı uyarlanması.	Önlem Al
--	----	---	----------

Hazırlayan	Onaylayan

KONTROLLÜ

(II) Yazılım ve Donanım Destek Operasyonları Yönetimi Süreci Akış Planı	No	Faaliyet	PUKÖ Döngüsü
	1	Donanım Kurulumu ve Bakımı Planlaması - Yeni donanım ihtiyaçlarının belirlenmesi. - Bakım planlarının oluşturulması (periyodik bakım takvimi ve bakım türleri). - Sistem gereksinimlerinin ve altyapı ihtiyaçlarının belirlenmesi.	Planlama
	2	Yazılım Kurulumu ve Güncelleme Planı - Yazılım kurulum süreçlerinin planlanması. - Yazılım güncelleme ve yamalama takvimi oluşturulması. - Yazılım uyumluluğu için gereksinimlerin belirlenmesi.	Planlama
	3	Yedekleme ve Veri Kurtarma Stratejileri - Yedekleme sıklığı, türü (tam, artımlı, fark birikimli) ve yöntemlerinin belirlenmesi. - Veri kurtarma planlarının tasarlanması.	Planlama
	3	Donanım ve Yazılım Kurulumları - Donanım kurulumlarının yapılması, donanımın test edilmesi ve devreye alınması. - Yazılımın kurulması ve konfigürasyon işlemlerinin gerçekleştirilmesi.	Uygulama
	4	Destek ve Sorun Çözme Uygulaması - Kullanıcı destek taleplerinin alınması ve çözülmesi. - Yazılım ve donanım sorunlarına hızlı müdahale edilmesi. - Performans izleme araçlarının kurulması ve izlenmesi.	Uygulama
	5	Yedekleme ve Veri Kurtarma - Veri yedekleme işlemlerinin yapılması. - Kurtarma senaryolarının tatbik edilmesi ve test edilmesi.	Uygulama
Hazırlayan		Onaylayan	

<p>Donanım ve Yazılım Envanteri Güncellemesi (6)</p> <p>↓</p> <p>Performans İzleme ve Optimizasyon Kontrolü (7)</p> <p>↓</p> <p>Yedekleme ve Veri Kurtarma Kontrolleri (8)</p> <p>↓</p> <p>Destek ve Sorun Çözme Performansının İzlenmesi (9)</p> <p>↓</p> <p>Önlemler (10)</p> <p>↓</p> <p>Süreç Bitti</p>	<p>6</p>	<p>Donanım ve Yazılım Envanteri Güncellemesi</p> <ul style="list-style-type: none">- Donanım ve yazılım envanterinin düzenli olarak güncellenmesi.- Yeni cihazların ve yazılımların envantere dahil edilmesi.	<p>Uygulama</p>
	<p>7</p>	<p>Performans İzleme ve Optimizasyon Kontrolü</p> <ul style="list-style-type: none">- Donanım ve yazılım performanslarının izlenmesi (CPU, bellek, disk kullanımı, ağ hızı, vb.).- Performans düşüşlerinin analiz edilmesi ve gerekirse iyileştirme önerileri geliştirilmesi.	<p>Kontrol</p>
	<p>8</p>	<p>Yedekleme ve Veri Kurtarma Kontrolleri</p> <ul style="list-style-type: none">- Yedekleme işlemlerinin düzenli olarak test edilmesi.- Yedekleme süreçlerinde herhangi bir aksama olup olmadığının kontrol edilmesi.	<p>Kontrol</p>
	<p>9</p>	<p>Destek ve Sorun Çözme Performansının İzlenmesi</p> <ul style="list-style-type: none">- Kullanıcı taleplerinin çözülme süresinin izlenmesi.- Sorunların tekrar etme oranlarının değerlendirilmesi.- Arıza raporlarının zamanında ve doğru şekilde toplanması ve analiz edilmesi.	<p>Kontrol</p>
	<p>10</p>	<ul style="list-style-type: none">- Donanım bakım planının yeniden gözden geçirilmesi ve optimizasyon yapılması.- Kullanıcılara yönelik eğitimlerin düzenlenmesi.- Yazılım ve donanım güvenliği açıklarının giderilmesi.- Donanım arızalarına karşı yedek donanımların tedarik edilmesi.	<p>Önlem Al</p>

Hazırlayan	Onaylayan

KONTROLLÜ

BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ YÖNETİMİ AKIŞ SÜREÇ KARTI

Doküman No	BÜ. SRC.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	9/10

GİRDİLER	ÇIKTILAR
<ol style="list-style-type: none">İnsan Kaynakları: Bilgi teknolojileri ve bilgi yönetimi alanında uzman personel.Mali Kaynaklar: BT altyapısının sürdürülmesi, güncellemeler, yeni yazılım/donanım alımları ve lisans maliyetleri için ayrılan bütçe.Donanım ve Yazılım Altyapısı: Sunucular, ağ cihazları, yedekleme üniteleri, güvenlik yazılımları ve diğer teknoloji ekipmanları.Dijital Bilgi Kaynakları: Üniversite veya kurum tarafından sağlanan veri tabanları, e-kitaplar, e-dergiler ve diğer dijital kütüphane kaynakları.Politikalar ve Prosedürler: Bilgi güvenliği, veri koruma, kullanıcı erişimi ve BT yönetimi ile ilgili prosedürler, standartlar ve yönergeler.Erişim ve Yetkilendirme Bilgileri: Kullanıcıların BT sistemlerine erişim düzeyleri, kimlik doğrulama bilgileri ve yetkilendirme seviyeleri.Kullanıcı Gereksinimleri ve Geri Bildirimleri: Öğrenci, akademik personel ve idari personelin BT ihtiyaçları ve sistem performansı hakkındaki geri bildirimleri.	<ol style="list-style-type: none">İyileştirilmiş Sistem ve Altyapı Performansı: BT altyapısının yüksek verimle çalışması, sistemlerin sürekliliği ve kesintisiz hizmet sağlanması.Kullanıcı Memnuniyet Raporları: Kullanıcılar (öğrenciler, akademik ve idari personel) tarafından sağlanan geri bildirimler ve anket sonuçlarına dayalı memnuniyet düzeyleri.Güvenlik ve Veri Koruma Raporları: Güvenlik tehditlerinin önlenmesi, güvenlik protokollerinin etkinliği ve veri koruma süreçlerinin başarı durumu.Sistem Güncellemeleri ve Bakım Durumu: Yapılan sistem ve yazılım güncellemelerinin, yedeklemelerin ve bakım işlemlerinin raporlanması.Erişim ve Kullanım Raporları: Bilgi teknolojileri sistemlerine yapılan erişim, kullanım oranları ve dijital kaynakların kullanım raporları.Veri Yedekleme ve Kurtarma Başarı Durumu: Yedekleme süreçlerinin düzgün bir şekilde işlemesi ve gerektiğinde veri kurtarma işlemlerinin başarıyla yapılması.Yeni Teknolojik Entegrasyonlar: Yeni yazılım, donanım ve dijital kaynakların entegre edilmesi, var olan altyapı ile uyumlu hale getirilmesi.

Hazırlayan	Onaylayan

KONTROLLÜ

BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ YÖNETİMİ AKIŞ SÜREÇ KARTI

Doküman No	BÜ. SRÇ.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	10/10

8. **Güncel Teknolojik Bilgiler ve İnovasyonlar:** Yeni teknolojiler, güvenlik önlemleri, yazılım ve donanım güncellemeleri gibi konularda güncel bilgi ve eğilimler.
9. **Güvenlik Protokolleri ve Risk Analizleri:** Bilgi güvenliği için uygulanan protokoller, risk analizleri ve tehdit değerlendirmeleri.

8. **Eğitim ve Destek Hizmetlerinin Etkinliği:** Kullanıcı eğitimi ve teknik destek hizmetlerinin etkinliği, eğitimlerin başarı oranları ve verilen desteklerin çözüm süreleri.
9. **Maliyet ve Bütçe Raporları:** BT altyapı yönetimi ve dijital kaynakların maliyetlerinin raporlanması, bütçeye uygunluk ve kaynakların etkin kullanımı.

Hazırlayan

Onaylayan

KONTROLLÜ

BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ YÖNETİMİ AKIŞ SÜREÇ KARTI

Doküman No	BÜ. SRÇ.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	11/10

RİSKLER

1	Sistem Kesintileri ve Donanım Arızaları: Sunucular, ağ cihazları veya diğer donanımların arızalanması durumunda, hizmetlerin aksaması veya kesilmesi riski.
2	Siber Güvenlik Tehditleri: Virüsler, kötü amaçlı yazılımlar, fidye yazılımları, siber saldırılar veya veri ihlalleri.
3	Veri Kaybı veya Hatalı Veri Yönetimi: Veri kaybı, yanlış veri yönetimi veya hatalı yedekleme işlemleri nedeniyle kritik verilerin kaybolması.
4	Teknolojik Eskiye Altyapı: Eskiye yazılım ve donanımların kullanılması, güncel teknolojiye adapte olamamak.
5	Kullanıcı Hataları ve Eğitim Eksiklikleri: Kullanıcıların yeni sistemleri veya güvenlik protokollerini yanlış kullanması, yeterli eğitim almamaları.
6	Yetersiz Destek ve Teknik Hizmetler: Destek ekibinin yetersiz olması, teknik problemlerin hızlı bir şekilde çözülmemesi.
7	Uyumluluk ve Regülasyon Sorunları: Düzenli uyumluluk denetimleri, ilgili mevzuatın takibi, iç denetim süreçlerinin güçlendirilmesi.
8	Bütçe Aşımı ve Finansal Yetersizlikler: Bilgi teknolojileri altyapısı için ayrılan bütçenin yetersiz kalması veya planlanan projelerin maliyetlerinin aşılması.
9	Kapsam Değişiklikleri ve Proje Yönetimi Sorunları: Projelerde kapsam değişiklikleri veya yöneticilerle olan iletişim eksiklikleri nedeniyle projelerin zamanında tamamlanamaması.
10	Dış Tedarikçi ve Hizmet Sağlayıcı Problemleri: Dış tedarikçilerin veya hizmet sağlayıcıların yükümlülüklerini yerine getirmemesi veya hizmet kalitesinin düşük olması.

Hazırlayan

Onaylayan

KONTROLLÜ

BİLGİ TEKNOLOJİLERİ VE BİLGİ KAYNAKLARININ YÖNETİMİ AKIŞ SÜREÇ KARTI

Doküman No	BÜ. SRC.05
Yayın Tarihi	29.11.2024
Revizyon Tarihi	00.00.0000
Revizyon No	00
Sayfa	12/10

FIRSATLAR

1	Dijital Dönüşüm ve Yenilikçi Teknolojiler: Yeni teknolojilerin (yapay zekâ, bulut bilişim, büyük veri analitiği vb.) entegrasyonu ile süreçlerin daha verimli hale gelmesi.
2	Veri Analitiği ve Karar Destek Sistemleri: Daha hızlı ve bilinçli kararlar alarak organizasyonun stratejik hedeflerine daha hızlı ulaşmak.
3	Bulut Bilişim ile Kaynakların Optimizasyonu: Bulut bilişim altyapılarını kullanarak BT kaynaklarının daha verimli yönetilmesi.
4	İleri Düzey Siber Güvenlik Teknolojileri: Güvenlik duvarları, şifreleme ve diğer ileri düzey güvenlik önlemlerinin kullanılması.
5	Kullanıcı Deneyimi ve Memnuniyetini Artırma: Kullanıcı deneyimini iyileştirerek, hem iç kullanıcıların hem de dış kullanıcıların memnuniyetini artırmak.
6	Veri Paylaşımı ve İşbirliği Fırsatları: Kurumlar arası veri paylaşımı ile daha geniş bir bilgi ağına ulaşmak ve ortak projelerde daha etkili olmak.
7	Çalışanların Eğitim ve Gelişim İmkânlarının Artırılması: Eğitimli personel ile daha verimli sistem kullanımı ve süreçlerin daha hızlı yönetilmesi.
8	Sürdürülebilir Teknoloji Çözümleri: Sürdürülebilirlik hedeflerine katkı sağlamak ve çevresel etkiyi azaltmak.
9	Mobil Teknolojiler ve Uygulamalar: Erişim kolaylığı sağlanarak kullanıcıların esnek bir şekilde hizmetlere ulaşmasını sağlamak.
10	Yapay Zekâ ve Otomasyon ile Verimlilik Artışı: Zaman ve iş gücü tasarrufu sağlayarak, daha verimli bir çalışma ortamı oluşturmak.

Hazırlayan	Onaylayan

KONTROLLÜ