1. AMAÇ

Koç Üniversitesi Bilgi Teknolojileri'nin kritik iş fonksiyonlarının kesintiye uğraması durumunda iş faaliyetlerini sürdürmenin ve iş sürekliliği yönetiminin bir parçası olarak bilgi güvenliğinin sürekliliğini sağlamanın önemini vurgulamak, iş faaliyetlerindeki kesintilere karşı stratejiler ve planlar geliştirmek, bilgi sistemlerini felaketlerin etkilerinden korumak ve zamanında yeniden başlatılmasını kolaylaştırmak için yön sağlamak ve gereksinimleri belirlemek amaçlanmaktadır.

2. KAPSAM

Bu prosedür, Koç Üniversitesi (KU) Bilgi Teknolojileri ağında yer alan, kritik varlık niteliğindeki tüm sunucuları, uygulamaları, veritabanlarını, dış kaynak veya Üniversite tarafından geliştirilen tüm uygulamaları kapsamaktadır. KU idari ve akademik çalışanlar, öğrenciler, danışmanlar veya üçüncü taraf kuruluşlar dahil olmak üzere KU bilgi ve bilgi teknolojisi varlıklarına erişimi olan herkes için geçerlidir.

3. REFERANSLAR

3.1 YÖK Öğrenci Disiplin Yönetmeliği

3.2 Koç Üniversitesi İdari Personel Yönetmeliği

3.3 COBIT.2019 kapsamında "Süreç, Organizasyonel Yapılar, Bilgi Akışları ve Varlıkları, İnsanlar, Beceriler ve Etkinlikler, Politikalar ve Prosedürler, Kültür, Etik ve Davranış, Hizmetler, Altyapı ve Uygulamalar" yönetişim bileşenlerinin ilgili yönetişim ve yönetim hedefine uygulanabilecek her biri.

3.4 ISO 27000:2013 Bilgi Güvenliği yönetim standartları ailesi tamamı.

3.5 SANS-CIS kontrolleri (En yaygın ve tehlikeli saldırıları durdurmak için belirli ve uygulanabilir yollar sağlayan, siber güvenlik eylemler dizisidir.)

3.6 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

3.7 6698 sayılı Kişisel Verilerin Korunması Kanunu

3.8 4857 sayılı İş Kanunu

3.9 2547 sayılı Yükseköğretim Kanunu

4. SORUMLULUKLAR

4.1 Bu prosedürün uygulatılmasından Rektör sorumludur.

4.2 Prosedürün yayına hazırlanmasından, onaylanmasından, yayımlanıp devreye alınmasından, iyileştirme takibinin yapılmasından, iş sürekliliği standartlarının uygulandığının kontrol edilmesinden Bilgi Teknolojileri Direktörlüğü sorumludur.

4.3 İş sürekliliği veya felaket durum kurtarma planları içinde bilgi güvenliği gereksinimlerini oluşturmak, uygulamak ve sürdürmekten Bilgi Güvenliği Ekibi sorumludur.

4.4 Olumsuz durumlarda işlerin sürekliliğini sağlamak için bilgi güvenliği olaylarını yönetmek ve bilgi güvenliğini korumaktan Bilgi Güvenliği Ekibi sorumludur.

4.5 Felaket anında iş sürekliliğini sağlamak için kurtarma planlarında yer alan altyapı ile ilgili gerekli teknik aksiyonların alınmasından Yazılım Geliştirme ve Altyapı Operasyonları Ekibi sorumludur.

5. TANIMLAR

5.1 BT Sistemi: Birden fazla kullanıcı için bilgi sağlamak, paylaşmak, depolamak veya işlemek üzere yüklenen, yapılandırılan, veri iletmek veya işlemek için diğer sistemlerle iletişim kuran bir donanım veya sanal bilgi işlem ortamıdır.

5.2 İş Sürekliliği: İş faaliyetlerini önceden tanımlanmış kabul edilebilir düzeyde sürdürmek için Üniversite'nin olayları ve iş aksaklıklarını planlama ve müdahale etme konusundaki stratejik yönetim kabiliyetidir.

5.3 İş sürekliliği planı: Üniversitenin kritik iş süreçlerinin kesintiye uğramasına yanıt vermek için kullanılan plandır. Yüksek kritiklikteki sistemlerin restorasyonu için acil durum planına bağlıdır.

5.4 Felaket kurtarma: Ciddi bir kesintiden sonra Üniversite'nin teknolojik altyapısını ve yeteneklerini geri kazanma ve geri dönüş stratejileridir.

5.5 Felaket kurtarma planı: Bir acil durum veya felaket tarafından kesintiye uğrayan bir aktiviteyi, tanımlanmış bir zaman ve maliyet içinde kurtarmak için insan, fiziksel, teknik ve prosedürel kaynaklar kümesinin yer aldığı planlardır.

5.6 Failover Testi: Sistemin ek kaynak ayırabilme ve işlemleri yedekleme sistemlerine taşıyabilme yeteneğinin doğrulanmasıdır.

6. TEMEL PRENSİPLER

6.1 Bu prosedür ve bağlantılı diğer yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde KU idari personeli için 4857 sayılı İş Kanunu ve Koç Üniversitesi İdari Personel Yönetmeliği, KU akademik personel için 2547 sayılı YÖK Kanunu, öğrenciler için YÖK Öğrenci Disiplin Yönetmeliği işletilmektedir.

6.2 İş Sürekliliği Sınıflandırması

6.2.1 İş Sürekliliği Sınıflandırması, bir BT sisteminin kritiklik düzeyini değerlendirmek için kullanılmaktadır. Bir BT sisteminin kritikliği, Üniversite'ye sağladığı iş süreçleri ve hizmetlerle ilişkilendirilmektedir.

6.2.2 Süreç sahiplerine, BT sistemleri ve uygulamalarında hangi iş sürekliliği önlemlerinin uygulanması gerektiğini belirlemek için ilgili tanımlar sağlanmaktadır.

6.3 İş Sürekliliği Prosedürleri

6.3.1 Süreklilik planlaması, Üniversite'nin iş süreçlerini ve kritik sistemlerini sürdürmek ve kurtarmak için tasarlanmış geniş bir faaliyet kapsamını temsil etmektedir. Bir BT sistemi için gerekli olan iş sürekliliği prosedürlerinin kapsamı, atanan kritiklik seviyesine bağlı olarak değişmektedir.

6.3.2 Süreklilik planlaması için prosedür yelpazesi aşağıdakileri içermektedir: İş etki analizi, sistem kurtarma prosedürleri/planları, felaket kurtarma planları ve RTO/RPO Analizleri.

6.3.2.1 İş Etki Analizi: İş Etki Analizi (BIA), bir sistemin kritik iş süreçlerini tanımlar, maksimum kabul edilebilir kesinti süresi için tahminler atar ve bir felaket durumunda sistemin yeniden oluşturulması veya restorasyonu için öncelikleri belirler.

6.3.2.2 Sistem Kurtarma Prosedürleri/Planları: Sistem kurtarma prosedürleri/planları (SRP), bir sistemin yedekleme ortamından veya diğer kaynaklardan kurtarılmasına yönelik genel prosedürleri/planları sağlar.

6.3.2.3 Felaket Kurtarma Planları: Felaket kurtarma planı (DRP), beklenmedik bir olaydan sonra Üniversite'nin faaliyetine hızlı bir şekilde devam etmesine yardımcı olan bir stratejidir. Bir felaket kurtarma planı iyi bir şekilde belgelendirilir, yapılandırılır ve uygulanabilirliğini sürdürmek için düzenli olarak gözden geçirilir.

6.3.2.4 RPO/RTO Analizi: Kurtarma Noktası Hedefi (RPO) ve Kurtarma Süresi Hedefi (RTO), bir felaket kurtarma veya veri koruma planının en önemli iki parametresidir. Bu analizler,

Üniversite'ye felaket kurtarma planı oluşturmak için rehberlik edebilecek hedeflerdir. RPO / RTO, iş etki analiziyle birlikte, iş sürekliliği planına dahil edilmek üzere uygulanabilir stratejilerin belirlenmesi ve analiz edilmesi için temel sağlar.

RPO, ağ kesintisi sırasında kaybolacak veya yeniden girilmesi gerekecek değişken veri miktarını belirler. RTO, kesinti normal iş operasyonlarının akışını ciddi ve kabul edilemez şekilde engellemeye başlamadan önce geçebilecek "gerçek zaman" miktarını belirler.

6.4 İş Sürekliliği Yöntemleri

6.4.1 İş Sürekliliği Yöntemleri, sistem kullanılabilirliğini ve veri kurtarma stratejilerini tanımlamaktadır. Bir sistemin nasıl tasarlandığı, özellikle arıza süresiyle ilgili olarak, sisteme atanan kritiklik seviyesine bağlı olarak değişmektedir. Çeşitli kullanılabilirlik seçenekleri şunları içermektedir: Yüksek kullanılabilirlik, kurtarılabilir ve güvenli. Veri kurtarma ve yedekleme stratejileri de sistemin kritikliğine ve sağladığı iş süreçlerine bağlı olarak farklılık göstermektedir. Kurtarma ve yedekleme stratejisi seçenekleri şunları içermektedir: tam yedekleme, artırımlı yedekleme.

6.4.2 Sistem Kullanılabilirliği

6.4.2.1 Yüksek Kullanılabilirlik: Bir sistemi otomasyon vasıtasıyla bir arızadan hızlı bir şekilde kurtulabilen sistemlerdir. Bir sistemden diğerine geçerken az miktarda kapalı kalma süresi olabilmektedir, ancak işleme devam edilmektedir. Planlanmamış kesintiler veya kesintilerin olmaması hedeflenmektedir. Fiziksel olarak aynı etki alanında yer almayan tesisler, yerel kesintilerin sistemin yüksek kullanılabilirliğine engel olmamasını sağlamak için kullanılmaktadır. Yüksek kullanılabilirliği sağlayan kaynakların gerekli donanım ve sistem kaynağı bileşenlerini karşıladığından ve aralarında gerçek zamanlı eşitlemenin sağlanması gerekmektedir.

6.4.2.2 Kurtarılabilir: Verinin yeniden oluşturulması için gerekli olan bileşenlerin mevcut olduğu web, dosya sunucuları vb. sistemler için uygulanabilecek yedek altyapı

sistemleridir. Verinin yeniden oluşturulması manuel müdahale ile gerçekleştirildiği için tolere edilebilir bazı kesintiler yaşanabilmektedir.

6.4.2.3 Güvenli: Verinin yeniden oluşturulması için gerekli olan bileşenlerin mevcut olmadığı yedek altyapı sistemleridir. Sistemin yedekleri mevcuttur, ancak güncel olmayabilmekte veya eksik olabilmektedir. Bu durumda alternatif bir tesise gerek yoktur.

6.4.3 Veri Kurtarma Stratejileri

6.4.3.1 Tam (Full) Yedek: Seçilen bir veri kaynağının tüm içeriğinin yedeklenmesi durumudur. Artırımlı yedekler alınmadan önce, en az bir kez tam yedek alınmalıdır.

6.4.3.2 Artırımlı (Incremental) Yedek: Bir önceki yedekten sonra yedeklenmemiş olduğu tespit edilen verinin yedeklenmesi durumudur. Yedeklerden geri dönüş sırasında önce tam yedek, sonra sırayla tüm artırımlı yedekler yüklenmelidir.

6.5 Testler

6.5.1 Test etmenin amacı, iş sürekliliği çözümünün Üniversite'nin kurtarma gereksinimlerini karşıladığından emin olmaktır. Planlar, yetersiz veya yanlış kurtarma gereksinimleri, çözüm tasarımı kusurları veya çözüm uygulama hataları nedeniyle beklentiler karşılanamayabilmektedir.

6.5.2 Bir plan testi yürüterek, zayıf yönler belirlenebilmekte ve buna göre ayarlamalar yapılabilmektedir. Gerekli iş sürekliliği testinin türü ve sistem testlerinin gerçekleştirilme sıklığı, sisteme atanan kritiklik düzeyine bağlı olarak değişmektedir.

6.5.2.1 Yedekten Geri Dönüş Testi: Üniversite sistemlerinin etkinliğini ve güvenlik için verileri çoğaltma yöntemlerini ve ihtiyaç duyulması halinde bu verileri güvenilir bir şekilde geri dönüş yeteneklerini değerlendirme sürecidir. Yedekleme ve kurtarma testi, felaket kurtarma planının önemli bir parçasıdır. Kritik bileşenlerde bir değişiklik söz konusu olduğunda yeniden test edilmesi gerekmektedir. Yapılan testler EK-1'de yer alan KU_Yedek Test Takip Envanteri'ne kaydedilmektedir.

6.5.2.2 Failover Testi: Sistemin ek kaynak ayırabilme ve işlemleri yedekleme sistemlerine taşıyabilme yeteneğinin doğrulanması için KU_Yedekleme Envanteri'nde yer alan periyotlarda yedekte bekleyen sistemlerin testleri yapılmaktadır. Yapılan testler EK-1'de yer alan KU_Yedek Test Takip Envanteri'ne kaydedilmektedir.

6.5.3 Test aşamasında tanımlanan küçük sorunlar belgelenmekte ve bir sonraki test döngüsü sırasında yeniden test edilebilmektedir. Maksimum tolere edilebilir duruş süresini veya sistem

kurtarma çabalarını karşılamak için gereken uygun teknolojilerin eksikliği gibi önemli komplikasyonlar derhal giderilmekte ve düzeltilmektedir.

6.6 İş Sürekliliği Yardımı

6.6.1 BT Direktörlüğü, BT iş sürekliliği planlama girişimlerinde Üniversite departmanlarına yardımcı olmaktadır. BT Direktörlüğü, BT iş sürekliliği belgelerini geliştirmek ve koordine etmek için gerekli eğitim ve kaynakları Üniversite iş birimlerine etkili ve anlaşılır bir şekilde sağlamaktan sorumludur.

6.7 Tanım dışı durumlar Bilgi Güvenliği Komitesi tarafından değerlendirilmektedir.

7. YÖNTEM

7.1 Kritiklik Düzeyleri

Sistemlerin kritiklik düzeyleri BT Direktörlüğü liderliğinde iş birimleri ile yapılan görüşmeler sonucu belirlenmektedir. BT sisteminin kritikliği bir iş sürecine göre sınıflandırmak için kullanılmaktadır. Seçilen düzey, gerekli iş sürekliliği prosedürlerini, yöntemlerini ve test gereksinimlerini tanımlamaktadır.

7.1.1 **Yüksek:** Üniversite iş operasyonlarını desteklemek için gerekli olan BT sistemleridir. Bu sistemlerin kaybolması veya arızalanması iş operasyonları üzerinde aşırı bir etkiye sahip olacaktır. Sistemlerin maksimum 4 saat veya daha az kapalı kalma süresi olmalıdır.

7.1.2 **Orta:** Üniversite'nin birincil işletme operasyonlarını desteklemek için çok önemli olan BT sistemleridir. Bu sistemlerin kaybolması veya arızalanması iş operasyonları üzerinde önemli bir etkiye sahip olacaktır. Sistemlerin en fazla 12 saat veya daha kısa bir kapalı kalma süresi olmalıdır.

7.1.3 **Düşük:** Üniversite iş operasyonları için önemli olan, operasyonların etkinliğini veya verimliliğini artıran BT sistemleridir. Bu sistemlerin kaybolması veya arızalanması iş operasyonları üzerinde az veya ihmal edilebilir bir etkiye sahip olacaktır. Sistemlerin maksimum arıza süresi 24-72 saat arasında olmalıdır.

	Kritiklik Düzeyleri		
	Yüksek	**Orta**	**Düşük**
İş Sürekliliği Prosedürleri			
İş Etki Analizi (BIA)	Gerekli	Gerekli değil, ancak tamamlanması önerilir	Gerekli değil
Sistem Kurtarma Prosedürleri (SRP)	Gerekli değil, ancak tamamlanması önerilir.	Gerekli değil, ancak tamamlanması önerilir	Gerekli değil
Felaket Kurtarma Planları	Veri Merkezi için gerekli, diğerleri için gerekli değil ama tamamlanması önerilir.	Gerekli değil, ancak tamamlanması önerilir	Gerekli değil
RTO/RPO Analizi	Gerekli	Gerekli değil, ancak tamamlanması önerilir	Gerekli değil
İş Sürekliliği Yöntemleri			
Sistem Kullanılabilirliği	Yüksek Kullanılabilirlik	Kurtarılabilir	Kurtarılabilir
Maksimum Kapalı Kalma Süresi	<4 saat	<12 saat	24 saat - 72 saat
Veri Kurtarma Stratejisi	Sürekli Yedekleme	Artırımlı Yedekleme	Artırımlı Yedekleme veya Yedekleme yok
Uzak lokasyon veri yedekleme	Teknik imkanlar çerçevesinde değerlendirilir.	Gerekli değil	Gerekli değil
Test Etme			
Yedekleme ve Kurtarma Testi	Veri Yedekleme Prosedürü dikkate alınır	Veri Yedekleme Prosedürü dikkate alınır	Veri Yedekleme Prosedürü dikkate alınır
Failover Testi	Gerekli değil, ancak yıllık olarak tamamlanması önerilir	Gerekli değil, ancak yıllık olarak tamamlanması önerilir	Gerekli değil

8. EKLER VE KAYITLAR

EK-1 KU_Yedek Test Takip Envanteri

EK-2 İş Etki Analizi (BIA)

EK-3 Sistem Kurtarma Prosedürleri (SRP)

EK-4 Felaket Kurtarma Planları

EK-5 Acil Durum Planları

EK-6 RTO/RPO Analizi

9. GÖZDEN GEÇİRME

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu Bilgi Teknolojileri Direktörlüğü'ne aittir. Gözden geçirme en az yılda 1 defa yapılır. Gerekli görüldüğü zaman ve durumlarda doküman revize edilir.

10. DEĞİŞİKLİK/DAĞITIM TABLOSU

Değişen sayfa	Tarih	Değişiklik	Değişikliği yapan
Dağıtım (İlgili Bölümler)			
Tüm Koç Üniversitesi			