1. AMAÇ

Bu prosedürün amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında yürütülen kritik süreçlerin, faaliyetlerin ve bilişim hizmetlerinin sürekliliğini etkileyebilecek tehdit ve kesinti durumlarının belirlenmesi, değerlendirilmesi, önleyici ve düzeltici tedbirlerin planlanması, acil durumlara etkin şekilde müdahale edilmesi ve kritik faaliyetlerin belirlenen süreler içerisinde yeniden yürütülebilir hale getirilmesine yönelik yöntem ve sorumlulukların belirlenmesidir.

Bu kapsamda; kritik süreçlerin ve hizmetlerin belirlenmesi, iş etki analizlerinin gerçekleştirilmesi, süreklilik hedeflerinin oluşturulması, acil durum ve iş sürekliliği planlarının hazırlanması, yedekleme ve kurtarma faaliyetlerinin yürütülmesi, tatbikatların gerçekleştirilmesi ve sonuçlarının izlenmesi ile iş sürekliliği sisteminin sürekli iyileştirilmesi amaçlanmaktadır.

2. KAPSAM

Bu prosedür; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi kapsamında yer alan Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde yürütülen kritik süreçleri, hizmetleri, bilişim hizmetlerini, bilgi varlıklarını, teknolojik altyapıyı, tesis ve çalışma alanlarını, insan kaynağını ve iş sürekliliğini etkileyebilecek diğer kaynakları kapsar.

Prosedür; özellikle KYS, BGYS, KVYS, İSYS ve BTHYS kapsamında iş sürekliliği ile ilişkili süreç ve faaliyetlerin bütünleşik olarak yönetilmesini esas alır.

3. SORUMLULUK

3.1. Üst Yönetim;

- İş sürekliliği yönetiminin uygulanması için gerekli kaynakları sağlar.
- Kritik süreç ve hizmetlerin sürekliliğine ilişkin öncelikleri belirler.
- İş sürekliliği ile ilgili plan, hedef ve iyileştirme faaliyetlerini değerlendirir.
- Gerektiğinde acil durum ve iş sürekliliği faaliyetlerinin başlatılmasını sağlar.

3.2. İlgili Birim Yöneticileri

- Sorumlu oldukları süreç ve hizmetlerin kritikliği konusunda değerlendirme yapar.
- Kritik faaliyetleri ve bunların bağımlılıklarını belirler.
- İş etki analizi çalışmalarına katılır.
- İş sürekliliği ve acil durum planlarının uygulanmasını sağlar.
- Acil durumlarda kendilerine verilen görevleri yerine getirir.

3.3. EYS Sorumluları / Süreç Sorumluları

- Kritik süreçlerin belirlenmesi ve değerlendirilmesine katkı sağlar.

- İş etki analizi çalışmalarını koordine eder.
- Süreklilik hedeflerinin belirlenmesini ve güncel tutulmasını takip eder.
- İş sürekliliği planlarının ilgili süreçlerle uyumlu olmasını sağlar.
- Tatbikat ve test sonuçlarının izlenmesini ve gerekli iyileştirmelerin yapılmasını takip eder.

3.4. Bilgi İşlem ve Teknik Birimler

- Bilişim altyapısının sürekliliğini sağlayacak teknik tedbirleri uygular.
- Kritik sistem, uygulama, ağ ve altyapı bileşenlerini belirler.
- Yedekleme ve geri dönüş faaliyetlerini yürütür.
- Teknik arıza ve kesintilere müdahale eder.
- Teknik kurtarma ve yeniden devreye alma faaliyetlerini gerçekleştirir.
- Yapılan yedekleme ve geri dönüş testlerine ilişkin kayıtları muhafaza eder.

3.5. Tüm Çalışanlar

- Kendilerine bildirilen acil durum ve iş sürekliliği kurallarına uyar.
- Karşılaştıkları kesinti, olay veya acil durumları ilgili sorumlulara bildirir.
- Kendilerine verilen acil durum görevlerini yerine getirir.
- İş sürekliliği planları ve acil durum prosedürleri kapsamında gerçekleştirilen eğitim ve tatbikatlara katılır.

4. TANIMLAR

- **İş Sürekliliği:** Bir kesinti veya acil durum sonrasında kritik ürün ve hizmetlerin kabul edilebilir önceden belirlenmiş seviyelerde sürdürülebilmesi ve faaliyetlerin yeniden başlatılabilmesi için gerçekleştirilen planlama ve uygulama faaliyetlerinin bütünüdür.
- **İş Etki Analizi (İEA):** Bir kesinti veya bozulmanın süreçler, hizmetler ve kurum üzerindeki etkilerini belirlemek ve süreklilik önceliklerini ortaya koymak amacıyla gerçekleştirilen analizdir.
- **MAO / MTPD (Maksimum Tolere Edilebilir Kesinti Süresi):** Bir faaliyet, süreç veya hizmetin kesintiye uğraması halinde kurumun tolere edebileceği en uzun kesinti süresidir.
- **RTO (Kurtarma Süresi Hedefi):** Kesintiye uğrayan bir süreç, hizmet veya sistemin kabul edilebilir seviyede yeniden çalışır hale getirilmesi için hedeflenen süredir.
- **RPO (Kurtarma Noktası Hedefi):** Bir kesinti durumunda kabul edilebilir maksimum veri kaybını ifade eder ve zaman cinsinden belirlenir.
- **Kritik Süreç:** Kesintiye uğraması halinde kurumun faaliyetlerini, hizmet sunumunu, yasal yükümlülüklerini veya paydaşlara karşı sorumluluklarını önemli ölçüde etkileyebilecek süreçtir.
- **Acil Durum:** İnsan, tesis, bilgi, teknoloji, hizmet veya kurum faaliyetleri üzerinde olumsuz etki oluşturan ve normal faaliyetlerin devamını engelleyen veya önemli ölçüde aksatan olaydır.

- **İş Sürekliliği Planı:** Bir kesinti veya acil durum sonrasında kritik faaliyetlerin sürdürülebilmesi ve yeniden başlatılabilmesi için uygulanacak görev, sorumluluk, kaynak ve faaliyetleri belirleyen dokümandır.
- **Tatbikat:** İş sürekliliği ve acil durum planlarının uygulanabilirliğini değerlendirmek amacıyla kontrollü olarak gerçekleştirilen test veya uygulamadır.
- **Kurtarma:** Kesinti sonrasında süreç, hizmet, sistem veya bilgi varlıklarının belirlenen hedefler doğrultusunda yeniden kullanılabilir hale getirilmesi faaliyetidir.

5. UYGULAMA

5.1. İş Sürekliliği Yönetimi

İş sürekliliği yönetimi aşağıdaki temel faaliyetler kapsamında yürütülür:

- Kritik süreçler, hizmetler ve bunların iş sürekliliği açısından önem taşıyan bağımlılıkları belirlenir.
- Kritik süreçlerin ihtiyaç duyduğu insan kaynağı, bilgi, teknoloji, tesis, altyapı, tedarikçi ve diğer kaynaklar belirlenir.
- Süreçlerin kesintiye uğraması halinde ortaya çıkabilecek etkiler İş Etki Analizi ile değerlendirilir.
- Her kritik süreç ve hizmet için uygun **MAO/MTPD, RTO ve RPO** değerleri belirlenir.
- Kritik süreçlerin sürdürülebilmesi için gerekli önleyici ve azaltıcı tedbirler belirlenir.
- Kesinti veya acil durum halinde uygulanacak faaliyetler ilgili İş Sürekliliği Planı ve Acil Durum Eylem Planlarında tanımlanır.
- İş sürekliliği planlarında görevli kişiler, iletişim bilgileri, ilk müdahale adımları, kurtarma faaliyetleri ve yeniden devreye alma yöntemleri belirlenir.
- Kritik süreçlerde meydana gelen organizasyonel, teknolojik, mevzuatsal veya operasyonel değişiklikler iş sürekliliği açısından değerlendirilir.
- İş sürekliliği planları belirlenen periyotlarda ve önemli değişiklikler sonrasında gözden geçirilir.
- İş sürekliliği yönetiminin etkinliği tatbikat, test, iç tetkik, olay sonrası değerlendirme ve yönetim değerlendirmeleri ile izlenir.
- Tespit edilen uygunsuzluklar ve iyileştirme ihtiyaçları ilgili süreçler üzerinden takip edilir.

5.2. Kritik Süreçlerin ve Hizmetlerin Belirlenmesi

Kritik süreç ve hizmetlerin belirlenmesinde aşağıdaki hususlar dikkate alınır:

- Sürecin kurum faaliyetleri açısından önemi,
- Yasal ve mevzuat şartları,
- Paydaş ve hizmet alanların ihtiyaçları,
- Bilgi güvenliği gereksinimleri,
- Kişisel veri ve gizlilik gereksinimleri,
- Bilişim hizmetlerine bağımlılık,

- İnsan kaynağı bağımlılığı,
- Fiziksel alan ve altyapı bağımlılığı,
- Tedarikçi ve dış hizmet bağımlılıkları,
- Veri ve bilgi varlıklarına bağımlılık,
- Kesintinin finansal, operasyonel, hukuki ve itibari etkileri,
- Kesintinin kabul edilebilir süresi.

Belirlenen kritik süreçler İş Etki Analizi kapsamında değerlendirilir ve gerekli süreklilik hedefleri belirlenir.

5.3. İş Etki Analizi

İş Etki Analizi aşağıdaki aşamalar izlenerek gerçekleştirilir:

1. Süreç ve hizmetlerin belirlenmesi,
2. Süreç ve hizmetlerin kritikliği açısından değerlendirilmesi,
3. Süreçlerin bağımlı olduğu bilgi, insan, teknoloji, tesis, altyapı ve tedarikçilerin belirlenmesi,
4. Kesinti senaryolarının ve olası etkilerin değerlendirilmesi,
5. MAO/MTPD değerlerinin belirlenmesi,
6. RTO değerlerinin belirlenmesi,
7. RPO değerlerinin belirlenmesi,
8. Mevcut süreklilik tedbirlerinin değerlendirilmesi,
9. İlave tedbir ve aksiyonların belirlenmesi,
10. Sorumluların ve gerekli kaynakların belirlenmesi,
11. Test ve tatbikat ihtiyaçlarının belirlenmesi.

İş Etki Analizi belirlenen periyotlarda ve aşağıdaki durumlarda yeniden değerlendirilir:

- Kritik süreç veya hizmetlerde değişiklik olması,
- Yeni hizmet veya sistem devreye alınması,
- Önemli organizasyon değişikliği yapılması,
- Kritik tedarikçi veya bağımlılıkların değişmesi,
- Önemli bir kesinti veya acil durum yaşanması,
- Tatbikat sonucunda önemli bir eksiklik tespit edilmesi,
- Risk değerlendirmesi sonucunda ihtiyaç ortaya çıkması.

5.4. Acil Durum Yönetimi

Yangın, deprem, su baskını, elektrik kesintisi, iletişim veya ağ kesintisi, kritik sistem arızası, siber güvenlik olayı, veri kaybı, donanım arızası ve benzeri acil durumlarda ilgili Acil Durum Eylem Planı ve İş Sürekliliği Planında belirlenen faaliyetler uygulanır.

Acil durumlarda öncelik sırası;

1. İnsan hayatı ve çalışan güvenliğinin korunması,
2. Acil durumun kontrol altına alınması,
3. Kritik bilgi ve varlıkların korunması,
4. Kritik süreç ve hizmetlerin devamlılığının sağlanması,
5. Sistem ve hizmetlerin kurtarılması,
6. Normal faaliyetlere kontrollü dönüşün sağlanması şeklinde uygulanır.

Acil durumun niteliğine göre ilgili birim yöneticisi, EYS sorumluları, Bilgi İşlem ve teknik ekipler ile diğer yetkililer koordineli olarak hareket eder.

5.5. İş Sürekliliğini Etkileyebilecek Kesintiler ve Alınacak Önlemler

İş Sürekliliği kesintileri	**Olası Etki**	**Alınabilecek Önlemler**	**Müdahale / kurtarma Faaliyeti**
Verilerin silinmesi, bozulması, kaybedilmesi ya da hasar görmesi	Veri bütünlüğünün ve erişilebilirliğinin etkilenmesi	Düzenli yedekleme, erişim kontrolleri, veri bütünlüğü kontrolleri	Uygun yedekten geri dönüş yapılması ve veri bütünlüğünün doğrulanması
Kritik sunucu / sistem arızası	Kritik hizmetlerin kullanılamaması	Yedekleme, donanım bakım ve izleme, gerekli yedek donanım	Arızanın giderilmesi, gerekli olması halinde yedekten veya alternatif sistemden hizmetin yeniden başlatılması
Elektrik kesintisi	Sistem ve hizmetlerin kesintiye uğramas	UPS, jeneratör ve uygun enerji altyapısı	Alternatif enerji kaynaklarının devreye alınması ve sistemlerin kontrollü çalıştırılması
İnternetin kesilmesi	Dış sistemlere ve internet tabanlı hizmetlere erişimin kesilmesi	Yedek bağlantı, ağ izleme ve alternatif iletişim yöntemleri	Yedek bağlantının devreye alınması ve ana bağlantının yeniden tesis edilmesi
Kurum içi ağ kesintisi	İç sistemlere ve hizmetlere erişimin kesilmesi	Yedek ağ cihazları, altyapı bakımı ve izleme	Arıza kaynağının belirlenmesi, cihaz veya bağlantının değiştirilmesi ve hizmetin yeniden sağlanması
Kullanıcı bilgisayarların arızalanması	Kullanıcının görevini yerine getirmesinde geçici kesinti	Yedek cihaz, veri yedekleme ve standart donanım yönetimi	Kullanıcıya uygun yedek cihaz sağlanması ve gerekli verilerin geri yüklenmesi
Dışarıdan gelen güvenlik saldırısı (Hacker Attack)	Bilgi varlıklarının gizlilik, bütünlük veya erişilebilirliğinin	Güvenlik duvarı, güvenlik yazılımları, erişim kontrolleri, yedekleme, izleme ve olay yönetimi	Olay müdahale süreçlerinin uygulanması, etkilenen sistemlerin izole edilmesi, kurtarma ve güvenlik

	etkilenmesi		kontrollerinin gerçekleştirilmesi
Sistemdeki network cihazlarının fiziksel olarak arızalanması (Router, Gateway, Switch, Adsl Modem vb..)	Kurum içi veya dışı ağ erişiminin kesilmesi	Yedek cihaz, bakım ve izleme	Arızalı cihazın değiştirilmesi veya onarılması
Kurum içinde kullanılan network kablolarının zarar görmesi, kopması ya da takılı olmaması	Kullanıcı veya sistem bağlantısının kesilmesi	Fiziksel altyapının kontrolü ve yedek malzeme	Arızalı bağlantının tespiti, değiştirilmesi ve test edilmesi
Taşınabilir cihazın arızalanması veya kaybolması	Cihazdaki bilgiye erişimin kaybedilmesi veya bilgi güvenliği riski	Zimmet, şifreleme, erişim kontrolü ve yedekleme	Cihazın erişimlerinin kapatılması, gerekli bildirimlerin yapılması ve yedeklerden çalışmanın sürdürülmesi
Yangın, deprem, su baskını gibi doğal afetler	Tesis, insan, bilgi varlıkları ve hizmetlerde geniş kapsamlı kesinti	Fiziksel güvenlik, yangın söndürme sistemleri, yedekleme, alternatif çalışma alanları ve acil durum planları	Acil durum planlarının uygulanması, kritik kaynakların korunması ve hizmetlerin önceliklendirilerek yeniden başlatılması
Kritik tedarikçi / dış hizmet kesintisi	Bağımlı hizmetlerin kullanılamaması	Tedarikçi değerlendirmesi, alternatif kaynak ve süreklilik şartları	Alternatif hizmet veya tedarikçinin devreye alınması ve hizmetin yeniden sağlanması

Süreçlerin özelliklerine göre ilave kesinti senaryoları belirlenebilir.

5.6. İş Sürekliliği Planlarının Hazırlanması

Kritik olarak belirlenen süreç ve hizmetler için gerekli görülen durumlarda İş Sürekliliği Planları hazırlanır.

İş Sürekliliği Planlarında asgari olarak aşağıdaki bilgiler bulunur:

- Planın amacı ve kapsamı,
- Kritik süreç / hizmet,
- Kritik kaynaklar,
- Görev ve sorumluluklar,
- İletişim bilgileri,
- Olası kesinti senaryoları,
- İlk müdahale faaliyetleri,
- Kurtarma faaliyetleri,

- RTO ve RPO değerleri,
- Gerekli teknik ve operasyonel kaynaklar,
- Alternatif çalışma yöntemleri,
- Yeniden devreye alma adımları,
- Normal faaliyetlere dönüş yöntemi.

Planlar kontrollü şekilde yayımlanır ve güncel tutulur.

5.7. Afet Yönetimi

Yangın, deprem, sel, su baskını, büyük ölçekli enerji kesintisi ve benzeri afet durumlarında yapılacak faaliyetler ilgili Acil Durum Eylem Planı ve diğer ilgili planlarda belirtilen şekilde gerçekleştirilir.

Acil durumlara ilişkin görev ve sorumluluklar çalışanlara uygun eğitim, bilgilendirme ve tatbikatlar aracılığıyla duyurulur.

Afet durumlarında öncelikle insan güvenliği sağlanır; daha sonra kritik bilgi varlıklarının, altyapının ve hizmetlerin korunması ve yeniden devreye alınmasına yönelik faaliyetler yürütülür.

5.8. Tatbikat ve Testlerin Yapılması

İş Etki Analizi ve İş Sürekliliği Planları doğrultusunda gerekli görülen iş sürekliliği ve acil durum senaryoları için tatbikat veya teknik testler gerçekleştirilir.

Tatbikat ve testlerde;

- Planların uygulanabilirliği,
- Görev ve sorumlulukların uygunluğu,
- İletişim yöntemlerinin etkinliği,
- Kurtarma sürelerinin hedeflerle uyumu,
- Yedeklerden geri dönüş kabiliyeti,
- Alternatif çalışma yöntemleri,
- Teknik altyapının yeterliliği değerlendirilir.

Tatbikat ve test sonuçları “Tatbikat Değerlendirme Formuna” kaydedilir. Tespit edilen eksiklikler için gerekli düzeltici ve iyileştirici faaliyetler başlatılır.

5.9. Yedekleme ve Geri Dönüş İşlemleri

İş sürekliliği açısından kritik olan bilgi, sistem, uygulama, sunucu ve diğer bilişim varlıklarının yedeklenmesi ilgili yedekleme süreçlerine uygun olarak gerçekleştirilir.

Yedekleme;

- Belirlenen periyotlarda,
- Bilginin gizlilik, bütünlük ve erişilebilirliği korunarak,
- Yetkilendirilmiş personel tarafından,
- Belirlenen saklama sürelerine uygun şekilde gerçekleştirilir.

Yedekleme yapılacak sistemler, yedekleme periyotları, sorumlular ve gerekli saklama koşulları ilgili plan veya kayıtlar üzerinden belirlenir.

Yedekleme işlemlerine ilişkin kanıt ve kayıtlar muhafaza edilir.

Yedeklerden geri dönüş yapılabilirliği **en az yılda bir kez** veya ihtiyaç duyulan durumlarda test edilir. Test sonuçları kayıt altına alınır ve başarısız sonuçlar için gerekli iyileştirme faaliyetleri gerçekleştirilir.

5.10. Kesinti Sonrası Değerlendirme

Gerçekleşen önemli kesinti veya acil durum sonrasında;

- Olayın nedeni,
- Etkilenen süreç ve hizmetler,
- Kesinti süresi,
- Veri kaybı,
- Uygulanan müdahale ve kurtarma faaliyetleri,
- Planlanan RTO/RPO değerlerine uyum,
- Alınan önlemlerin etkinliği,
- Yaşanan aksaklıklar,
- Tekrarını önlemek için yapılması gereken faaliyetler değerlendirilir.

Gerekli olması halinde İş Etki Analizi, Risk Değerlendirmesi, İş Sürekliliği Planları ve ilgili diğer EYS dokümanları güncellenir.

5.11. İş Sürekliliği Yönetiminin İzlenmesi ve İyileştirilmesi

İş sürekliliği faaliyetlerinin etkinliği;

- İş Etki Analizleri,
- Tatbikat ve test sonuçları,
- Gerçekleşen kesinti ve olaylar,
- İç tetkikler,
- Düzeltici ve İyileştirici Faaliyetler,
- Risk değerlendirmeleri,
- Yönetimin gözden geçirmesi aracılığıyla izlenir.

Tespit edilen uygunsuzluk, eksiklik ve iyileştirme ihtiyaçları ilgili EYS süreçleri üzerinden takip edilir.

İş sürekliliği yönetiminde gerçekleştirilen değişiklikler Değişiklik Yönetimi süreçlerine uygun şekilde kontrol edilir.

6.İLGİLİ DOKÜMANLAR

- Tatbikat Değerlendirme Formu
- Acil Durum Eylem Planı
- Acil Durum Genel Korunma Planı
- İş Sürekliliği Planı
- İş Sürekliliği Kesinti Raporu

7.REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.01.2020	İlk yayın.
001	22.01.2024	Kontrol kısmı güncellenmiştir.
002	16.09.2026	SDÜ Entegre Yönetim Sistemi yapısına uygun olarak kapsam, sorumluluklar, iş etki analizi, acil durum yönetimi, tatbikat, yedekleme, kurtarma ve iş sürekliliği yönetimi açısından yeniden düzenlenmiştir.