

	<b>SÜLEYMAN DEMİREL ÜNİVERSİTESİ</b> <b>Bilgi İşlem Daire Başkanlığı</b> <b>İş Sürekliliği ve Acil Durum Yönetimi Prosedürü</b>	Doküman No	PR-001
		İlk Yayın Tarihi	22.1.2020
		Revizyon Tarihi	22.1.2020
		Revizyon No	000
		Sayfa No	1 / 6

## 1.AMAÇ

Bu prosedürün amacı, Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığının Bilgi Teknolojileri kapsamındaki sağladığı hizmetlerin, süreçlerin, faaliyetlerin durumunu, hizmetlerinden faydalanan paydaşların kritiklik durumunu, hizmetleri sağlarken yararlanılan alt yapı ve kaynakların durumunu değerlendirmek ve iş sürekliliğinde kesintiye sebep olabilecek durumların belirlenmesi ve yürütülen faaliyetlerin sürekliliğini sağlamak amacıyla acil durumlar için alınması gereken önlemler ve acil durumlara müdahale durumunda alınabilecek önlemlerin saptanarak kesintiye uğramaksızın iş sürekliliğinin sağlanmasının yöntemlerini saptamaktır.

## 2.KAPSAM

Bu prosedür, Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı'nın hizmetleri, faaliyetleri, varlıkları ve süreçlerinin sürekliliğini sağlamak amacıyla alınması gereken önlemler ve acil durumlara müdahale şekillerini kapsar.

## 3.SORUMLULUK

„Bilgi İşlem Daire Başkanlığı çalışanları, yönettikleri veya bir parçası oldukları operasyonel süreçlerle ilgili iş kesintilerinin nedenlerinin belirlenmesinde, önlem alınmasında ve gerektiğinde kendilerinin de katkısıyla önceden oluşturulmuş iş sürekliliği planının doğru zamanda ve hatasız bir şekilde yürürlüğe koyulmasında ana sorumluluk sahibidir.

## 4. TANIMLAR

- **MEKS:** (MTPoD: Maximum Tolerable Period of Distruption). Bir iş süreci veya BT bileşeni için kurumun kabul edebileceği maksimum kesinti süresini ifade etmektedir.
- **KEKS:** (RTO : Recovery Time Objective). Kesintiye uğrayan iş sürecinin veya BT bileşeninin ne kadar süre sonra çalışır hale getirileceğine dair hedef süredir.
- **KEVK:** (RPO : Recovery Point Objective). Bir iş süreci veya BT bileşeni için kurumun kabul edebileceği maksimum veri kaybını süre olarak ifade eder.

## 5.UYGULAMA

### 5.1. İş Sürekliliği Yönetimi

	<b>SÜLEYMAN DEMİREL ÜNİVERSİTESİ</b> <b>Bilgi İşlem Daire Başkanlığı</b> <b>İş Sürekliliği ve Acil Durum Yönetimi Prosedürü</b>	Doküman No	PR-001
		İlk Yayın Tarihi	22.1.2020
		Revizyon Tarihi	22.1.2020
		Revizyon No	000
		Sayfa No	2 / 6

- İş Sürekliliği Yönetimi için ekip liderliği ve gerekli görevlendirmeleri Daire Başkanı yapar. Hasar Tespiti, Acil Durum Yönetimi, Kurtarma Yönetimi gibi konularda sorumlular atar ve bunu duyurur.
- Bilgi Güvenliği Ekibi ve birim sorumluları bir araya gelerek, süreçleri ve kesintiye uğramaları durumunda etkilerinin ne olacağını inceleyerek, birim için kritik ve kontrol altında tutulması gereken süreçleri belirlerler.
- Her kritik süreç için Maksimum Kabul Edilebilir Kesinti Süresi , Kabul Edilebilir Kesinti Süresi ve Kabul Edilebilir Veri Kaybı değerleri yine ekip tarafından belirlenir.
- Kritik İş Süreçleri kesintiye uğradığı zaman ulaşılabilecek kişi ve yapılacak ilk aksiyonlar, MKEKS, KEKS ve KEVK ile birlikte Acil Durum Eylem Planına işlenir. Kesinti süreçlerinde neler yapılacağı ayrıntılı olarak Acil Durum Genel Koruma Planına uygun olarak gerçekleştirilir.
- İş Sürekliliği Yönetim Sistemi'nin geçerliliği yapılan iç tetkikler ile İç Tetkik Prosedürüne uygun olarak denetlenir ve geçerliliği kontrol altında tutulur.
- Bilgi Güvenliği Ekibi toplantılarında Kritik Süreçleri tekrar gözden geçirir ve eklenen, kaldırılan veya değişen kritik süreçler kontrol altında tutulur.
- Kritik süreçlerde, yapılması gereken değişiklikler, aksaklık veya eksiklikler iç haberleşme ile Bilgi Güvenliği Ekip Liderine bildirilir. Bilgi Güvenliği Ekip Lideri ilgili çalışanlarla birlikte durumu inceler ve uygun görüldüğünde gerekli değişiklik yapılır

İş sürekliliğinde kesintiye sebep olabilecek durumlar ve alınacak önlemler aşağıda belirtilmiştir:

İş Kesintileri	Sürekliliği	Olasılık	Alınabilecek Önlemler	Sonuç	Çözümler
Verilerin silinmesi, bozulması, kaybedilmesi ya da hasar görmesi		UZAK-KRİTİK	Otomatik yedekleme sistemleri ile belirli periyotlarda (günlük, haftalık, aylık vb.) düzenli olarak verinin korunması sağlanır.	Verilerin zarar görmesi sistemin işleyişine direk olumsuz etki eder. Geçici ya da sürekli sisteme zarar verir.	Sistemde en kritik kesintilerdendir. Güncel yedek, veri kaybı işleminden sonra en kısa sürede, ilgili sistem ya da ana bilgisayara indirilip, veri güvenliği kontrol edilmelidir.
		MUHTEME	Yazılımın yedeği	Sistemin	Yazılımın yedeği elimizde



**SÜLEYMAN DEMİREL ÜNİVERSİTESİ**  
**Bilgi İşlem Daire Başkanlığı**  
**İş Sürekliliği ve Acil Durum Yönetimi Prosedürü**

Doküman No

PR-001

İlk Yayın Tarihi

22.1.2020

Revizyon Tarihi

22.1.2020

Revizyon No

000

Sayfa No

3 / 6

Paydaşlarımızdaki yazılımımızın bozulması	L-ZARAR	paydaşlar adına tutulmaktadır.	işleyişini geçici olarak durdurur.	olduğundan kolayca tekrar kurulumu sağlanarak sorun ortadan kaldırılmış olacaktır.
Server (Ana Bilgisayar) Arızası	UZAK-KRİTİK	Harici disk üzerinden yedekleme ile tüm yapılanlar burada kayıt altındadır.	Sistemin tamamen devre dışı kalması durumudur. En kritik seviyedeki iş sürekliliği kesintisidir.	Harici bulunan bu disk sayesinde veri kaybı yaşanmayacaktır.
Elektrik kesintisi	MUHTEME L-ZARAR	UPS ve güç kaynağıyla sistemin hiç kapanmaması.	Kısa süreli kesintilerde problem teşkil etmez.	UPS ve jeneratörler sistemin kapanmasına ve her türlü elektrik akımına karşı koruma sağlayacaktır.
İnternetin kesilmesi	MUHTEME L-ZARAR	Yedekleme amacı ile başka bir internet hattı bulundurmak.	İnternetin kesilmesi sonucunda dış network tamamen devre dışı kalır.	Ana hattın kesilmesi halinde yedek hat otomatik devreye girecektir. Bu sayede internet kesintisinden etkilenme minimum seviyede olacaktır.
İç networkün kesilmesi	MUHTEME L-ZARAR	Yedek donanım cihazları ve kabloların bulundurulması.	Kurum içinde veri alışverişi sağlanamaz. Erişim kopar.	Bu sayede arıza tespitinden sonra parçaların otomatik olarak değiştirilmesi sağlanacaktır
Kişisel bilgisayarların arızalanması	UZAK-KRİTİK	Yedekte kullanılmayan bir PC bulundurup, her hangi bir arıza durumunda ilgili kullanıcıya devredilmesi	Kullanıcının kısa süreli de olsa işinin aksaması, veri iletişiminin kesilmesi anlamına gelmektedir.	Zarar gören kullanıcı bilgisayarının verileri güvenli bir şekilde serverda bulunduğundan yapılan işler serverdan çekilip çalışmalara devam edilmektedir.
Dışarıdan gelen güvenlik saldırısı (Hacker Attack)	UZAK-KRİTİK	Kurum içinde kullanılan sistemdeki güvenlik duvarı yazılımı ve donanım ile korunmalıdır.	Kurum için de olmaması gereken kritiklerdendir. Güvenlik saldırısı sonucunda verilerin güvenliği ve kurum	Dışarıdan herhangi bir network saldırısı ya da networkü meşgul eden spam saldırısı geldiğinde network cihazları tarafından tespit edilip, zararlı virüs yada dokümanlar silinmelidir.



**SÜLEYMAN DEMİREL ÜNİVERSİTESİ**  
**Bilgi İşlem Daire Başkanlığı**  
**İş Sürekliliği ve Acil Durum Yönetimi Prosedürü**

Doküman No

PR-001

İlk Yayın Tarihi

22.1.2020

Revizyon Tarihi

22.1.2020

Revizyon No

000

Sayfa No

4 / 6

			çalışanlarının bilgi güvenliği tehlikeye girer.	
Sistemdeki network cihazlarının fiziksel olarak arızalanması (Router, Gateway, Switch, Adsl Modem vb..)	MUHTEME L-ZARAR	Arızalanan network cihazlarının en kısa sürede yenilenmesi ya da arızanın giderilmesi.	Kurum içi networkü yada Kurum dışı networkünün göçmesi anlamına gelmektedir. Sonuçta erişilebilirlik tehlikeye girer.	Arızalanan network ürününün en kısa zamanda yenisinin temin edilmesi ya da arıza yapan ürünün tamirinin, bakım ve onarımının yaptırılması.
Kurum içinde kullanılan network kablolarının zarar görmesi, kopması ya da takılı olmaması	MUHTEME L-ZARAR	Kullanıcı öncelikle kendi network kablosunun prize takılı olup olmadığını kontrol etmelidir.	Erişim koptuğu anda kurum içinde ya da dışında bilgi kopukluğu yaşanır.	Arızalanan network kablosunun tespit edilmesi, yenilenmesi, test edilmesi, çalışır şekilde kullanıcıya devri.
Laptop (Notebook) cep bilgisayarı, usb memory gibi mobil cihazların arızalanması ya da çalınması.	UZAK-KRİTİK	Bilgisayar Kaydı ile kullanıcılara teslim edilmesi ve önemli verilerin mobil cihazlarda şifrelenerek tutulması	İşin sürekliliğine olumsuz etki eder, kritik seviyedeki sonuçlardandır.	Arızalanan mobil cihazların tamiri, bakımı, ya da yenisini ile değiştirilmesini sağlamak ve mobil cihazlarda verilerin şifrelenerek güvenli bir şekilde taşınmasını temin etmek.
Yangın, deprem, su baskını gibi doğal afetler	OLAĞANÜ STÜ-KRİTİK	Bilgi işlem odasının yangın güvenliği için uygun söndürme sisteminin yer alması, fiziksel olarak bina güvenliği ve sağlamlığı	Yangın, deprem, sel felaketi gibi doğal afetler sonucunda sistem kısmen ya da tamamen devre dışı kalabilir. Olma ihtimali düşüğe olsa kuvvetli zararları olabilir. Gerekli önlemler alındığında olumsuz etkileri azaltmak kısmen mümkündür.	Kurum içinde gerekli söndürme cihazlarının yer alması ve müdahale yöntemleri, yangında öncelikli kurtarılacak olan sistemlerin belirlenmesi her hangi bir felaket senaryosu anında sistemin devamlılığın en kısa sürede sağlanması. Ayrıca ana server doğal felaketslere karşı hiçbir şekilde zarar görmez kabinlerde saklanmaktadır.

## 5.2. Afet Yönetimi

	<b>SÜLEYMAN DEMİREL ÜNİVERSİTESİ</b> <b>Bilgi İşlem Daire Başkanlığı</b> <b>İş Sürekliliği ve Acil Durum Yönetimi Prosedürü</b>	Doküman No	PR-001
		İlk Yayın Tarihi	22.1.2020
		Revizyon Tarihi	22.1.2020
		Revizyon No	000
		Sayfa No	5 / 6

a) Yangın, Deprem, Sel gibi acil durumlarda yapılması gereken faaliyetler ve ilk müdahale şekilleri Acil Eylem Planı içerisinde yer aldığı şekilde gerçekleştirilir.

b) Afet yönetimi ile ilgili şartlar çalışanlara oryantasyon eğitimi ile birlikte verilir ve ilgili konularda sorumluların kimler olduğu bildirilir. Her acil durum için sorumlu daire başkanıdır.

### 5.3. İş Etki Analizi

İş etki analizi yapma aşamaları aşağıda verilmiştir.

- Yönetim Temsilcisi tarafından, kurumun Bilgi Teknolojileri hizmetlerinin neler olduğu, sorumlularının kimler olduğu belirlenir.

Aynı zamanda;

- İş sürekliliğini etkileyecek varlıklar/süreçler belirler. Belirlenen varlıklarda oluşabilecek iş olaylarını araştırır.
- RTO(zaman kaybı)-RPO(veri kaybı) -MAO (max.tolerans) zamanlarını tespit eder.
- Aksiyon planını oluşturur ve bunun için sorumlular atar.
- Test planına karar verilir.
- İş Etki Analizi Yönetim Temsilcisi tarafından periyodik olarak gözden geçirilir. Değişiklik olması durumunda İş Etki Analizi güncellenir.

### 5.4. Tatbikat Yapılması

İş etki analizi sonucunda ortaya çıkan ve iş sürekliliğini etkileyen proses adımları ile ilgili tatbikat sıklığı belirlenir. İş Etki Analizinde belirtildiği şekilde belirlenen sıklıkta tatbikatlar yapılarak tatbikat değerlendirme formuna işlenir.

### 5.5. Yedekleme İşlemleri

Sunucu, ağ cihazları ve özel kritik yazılımlar da dahil olmak üzere iş sürekliliğini etkileyen tüm kritik cihazların yedekleri alınır. Yedeklerin alınma sıklığına, kullanılan uygulamanın özelliğine göre karar verilir. Ağ ve Sistem Birim Sorumlusu tarafından yedekleme yapılacak olan cihazlar, periyotları ve sorumlu kişisi belirlenir. Yedekleme işlemi sistemin gizliliğini- bütünlüğünü ihlal etmeden yapılır. Ağ ve Sistem Birim Sorumlusu tarafından yedekleme kanıtları saklanır. Yedeklerden geri dönüşüm yapıp yapılmadığı en az yılda bir defa test edilir.

## 6.İLGİLİ DOKÜMANLAR

	<b>SÜLEYMAN DEMİREL ÜNİVERSİTESİ</b> <b>Bilgi İşlem Daire Başkanlığı</b> <b>İş Sürekliliği ve Acil Durum Yönetimi Prosedürü</b>	Doküman No	PR-001
		İlk Yayın Tarihi	22.1.2020
		Revizyon Tarihi	22.1.2020
		Revizyon No	000
		Sayfa No	6 / 6

- FR-001 Tatbikat Değerlendirme Formu
- PL-001 Acil Durum Eylem Planı
- PL-002 Acil Durum Genel Korunma Planı
- PL-011 İş Sürekliliği Planı
- RPR-007 İş Sürekliliği Kesinti Raporu
- FR-006 Olay İhlal Formu

## 7.REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.01.2020	İlk yayın.