1. Amaç

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

3. Sınırları

Olağan dışı durumun tespiti ile başlar gerekli işlemlerin / düzenlemelerin yapılması ile son bulur.

4. Tanımlar

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

- 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 ulaşılacak 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 Sürekliliği kesintileri	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.
Paydaşlarımızdaki yazılımımızın bozulması	MUHTEMEL-ZARAR	Yazılımın yedeği Paydaşlar adına tutulmaktadır.	Sistemin işleyişini geçici olarak durdurur.	Yazılımın yedeği elimizde 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 yaşanmayacaktır.
Elektrik kesintisi	MUHTEMEL-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	MUHTEMEL-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	MUHTEMEL-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, herhangi bir arıza durumunda ilgili kullanıcıya devredilmesi	Kullanıcının kısa sürelide olsa işinin aksaması, veri iletişiminin kesilmesi anlamına gelmektedir.	Zarar gören kullanıcı bilgisayarının verileri güvenli bir şekilde server da bulunduğundan yapılan işler server dan çekilip çalışmalara devam edilmektedir.

İş Sürekliliği kesintileri	Olasılık	Alınabilecek Önlemler	Sonuç	Çözümler
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 çalışanlarının bilgi güvenliği tehlikeye girer.	Dışarıdan herhangi bir network saldırısı ya da networkü meşgul eden spam saldırısı geldiğinde network cihazları tarafından tespit edilip, zararlı virüs ya da dokümanlar silinmelidir.
Sistemdeki network cihazlarının fiziksel olarak arızalanması (Router, Gateway, Switch, Adsl Modem vb..)	MUHTE MEL-ZARAR	Arızalanan network cihazlarının en kısa sürede yenilenmesi ya da arızanın giderilmesi.	Kurum içi networkü ya da 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	MUHTE MEL-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 yenisi ile değiştirilmesini sağlamak ve mobil cihazlarda verilerin şifrelenerek güvenli bir şekilde taşınmasını temin etmek.
Yangın, deprem, su baskını gibi doğal afetler	OLAĞAN ÜSTÜ-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 düşükte 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 herhangi bir felaket senaryosu anında sistemin devamlılığın en kısa sürede sağlanması. Ayrıca

5.2. Afet Yönetimi

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 yapılıp yapılamadığı en az yılda bir defa test edilir.