

|                                                                                                                                  |                                |                 |            |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------|------------|
| <br>OSTİM TEKNİK<br>ÜNİVERSİTESİ<br>A N K A R A | <b>İŞ SÜREKLİLİĞİ ESASLARI</b> | Doküman No      | BS.TL.003  |
|                                                                                                                                  |                                | Revizyon Tarihi | 07.11.2024 |
|                                                                                                                                  |                                | Revizyon No     | 01         |
|                                                                                                                                  |                                | Sayfa No        | 1 / 6      |

## 1. AMAÇ

Bu doküman OSTİM Teknik Üniversitesi sorumluluğunda yürütülen faaliyetlerin bilgi güvenliği hususlarını, iş sürekliliği ve hizmet erişilebilirliği işleyişinin yapılandırılmasını ve işletilmesini açıklar.

## 2. KAPSAM

İş Sürekliliği Esasları, risklerin ortaya çıkması hallerinde oluşabilecek tam veya kısmi kesintileri yönetecektir.

## 3. TANIMLAR VE KISALTMALAR

- BGYS: Bilgi Güvenliği Yönetim Sistemi. Bilginin gizliliğini, bütünlüğünü ve kesintisiz kullanılabilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümente edilmiş, yönetimce kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünü.
- Bilgi Güvenliği ekibi: Bilgi Güvenliği Yönetim Sistemini kurmak, işletmek, izlemek, gözden geçirmek ve iyileştirmek üzere kurulmuş ekip.
- Kurum: OSTİM Teknik Üniversitesi
- Kapsam: Bilgi Güvenliği Yönetim Sistemi Kapsamı.
- Acil Durum: Kurumun olağan çalışmasını kesintiye uğratacak ve/veya hizmet sunmasını engelleyecek acil ve beklenmedik durumlardır. Afet olarak değerlendirilen olaylar (deprem, yangın, fırtına, sel vb.) ve dikkatsizlik, tedbirsizlik, ihmal, kasıt ve çeşitli nedenlerle meydana gelen olayların (savaş, terörist saldırı, uzun süreli altyapı sorunları vb.) tümünün yol açtığı hallerdir.
- İEA: İş Etki Analizi (Business Impact Analysis).
- Kısmi Kesinti: BT sistemini oluşturan varlıkların sürekliliğinde meydana gelebilecek kısmi kesintilerdir. Kısmi kesintiler aşağıda tanımlanmıştır:
  - Sunucu sistemleri donanım arızaları. Disk, cpu, ram vb. arızaları.
  - Ağ kaynaklı arızalar veya kesintiler. Noktasal cihaz arızaları, konfigürasyon problemleri, switch, kablo kesintileri.
  - Uygulama ve hizmet arızaları veya kesintileri. Uygulama hataları, veri kaybı, konfigürasyon problemleri,
  - DDoS atakları.

|                                                                                                                                  |                                |                 |            |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------|------------|
| <br>OSTİM TEKNİK<br>ÜNİVERSİTESİ<br>A N K A R A | <b>İŞ SÜREKLİLİĞİ ESASLARI</b> | Doküman No      | BS.TL.003  |
|                                                                                                                                  |                                | Revizyon Tarihi | 07.11.2024 |
|                                                                                                                                  |                                | Revizyon No     | 01         |
|                                                                                                                                  |                                | Sayfa No        | 2 / 6      |

- MTPoD: Maksimum Kabul Edilebilir Kesinti Süresi (Maximum Tolerable Period of Distruption). Bir iş süreci veya BT bileşeni için kurumun kabul edebileceği maksimum kesinti süresini ifade etmektedir.
- RPO: Kabul Edilebilir Veri Kaybı (Recovery Point Objective). Bir iş süreci veya BT bileşeni için kurumun kabul edebileceği maksimum veri kaybını süre olarak ifade eder.
- RTO: Kabul Edilebilir Kesinti Süresi (Recovery Time Objective). Kesintiye uğrayan iş sürecinin veya BT bileşeninin ne kadar süre sonra çalışır hale getirileceğine dair hedef süredir.
- DDoS: Dağıtılmış servis durdurma. (Distributed Denial of Services).

#### 4. SORUMLULUKLAR

Bu dokümanın hazırlanması, düzenlenmesi ve yayınlanması Bilgi Güvenliği Ekibi sorumluluğundadır.

##### İş Sürekliliği Yöneticisi

- Bölümlerine ait iş etki analiz çalışmasını hazırlar ve onaylar.
- Kısmi kesinti durumlarının başlatılmasına ve sonlandırılmasına karar verir.
- Sistem bazında hazırlanan iş süreklilik ve test planlarının hedeflenen amaçlara uygunluğunu kontrol eder. Planların yıllık periyotlarda güncellenmesini koordine eder.
- İş sürekliliği test sonuçlarını değerlendirir. Eksikliklerin ve iyileştirmelerin yapılması için iş planlarını hazırlar ve onaylar.
- İş etki analizi içerisinde tanımlanan varlıkların sürekliliğinin kesintiye uğraması durumunda iş sürekliliği organizasyon şemasında belirtilen takımları oluşturur, koordine eder ve yönetir.
- İş etki analizi içerisinde tanımlanan varlıkların kesintiye uğraması durumunda, ilgili varlıkları kullanan kullanıcıların bilgilendirilmesini (kesintinin süresi, kapsamı, etkileri vb.), sorun ile ilgili gelen taleplere (telefon, e-posta veya çağrı sistemi aracılığıyla) cevap verilmesini sağlar.
- Kesinti sorunu ile ilgili Kurum içi ve dışı iletişim koordinasyonunu sağlar.
- İş etki analizi içerisinde tanımlanan varlıkların sürekliliğinin kesintiye uğraması durumunda acil durum yönetim çalışmalarına katılarak koordine eder.

|                                                                                                                                  |                                |                 |            |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------|------------|
| <br>OSTİM TEKNİK<br>ÜNİVERSİTESİ<br>A N K A R A | <b>İŞ SÜREKLİLİĞİ ESASLARI</b> | Doküman No      | BS.TL.003  |
|                                                                                                                                  |                                | Revizyon Tarihi | 07.11.2024 |
|                                                                                                                                  |                                | Revizyon No     | 01         |
|                                                                                                                                  |                                | Sayfa No        | 3 / 6      |

### Acil Durum Ekiplerinin Sorumlulukları:

- İş etki analizi içerisinde tanımlanan varlıkların “acil durum” tanımı kapsamında kesintiye uğraması durumunda, kurtarma çalışmaları süresince uygulanacak faaliyetleri gerçekleştirir (geçici sistem kurulması, geçici süreç / sistem / uygulama değişikliği vb.) ve üst yönetimi konu hakkında bilgilendirir.
- Donanım, kesintisiz güç kaynakları, elektrik panoları (UPS) gibi ortamları korumak üzere gerekli tedbirleri almak.

### Tüm Çalışanlar / Ziyaretçiler / 3. Taraf Kullanıcılar

- Acil durum ortaya çıktığında kendilerine gösterilen yönlendirme komutlarına uygun davranmak.
- Acil durumu fark ettiklerinde en kısa sürede ilgili tarafları uyarmak.

### Kısmi Kesinti Durum Yönetimi

Kısmi kesintiler halinde yapılması gereken işlemler bu bölümde anlatılmıştır.

- İş sürekliliği faaliyetleri kapsamında, bir varlığın kesintiye uğraması ile başlatılacak olan çalışmalar ile ilgili esaslar aşağıdaki gibidir:
- Kısmi kesinti durum yönetimi iş etki analizi içerisinde tanımlanmış bir varlığa ait kesinti bildiriminin çağrı sistemi, yardım masası telefonu, e-posta ve/veya sözlü olarak alınması ile başlar.
- İş Sürekliliği Yöneticisi tarafından kesinti ile ilgili acil durum veya kısmi kesinti durum çalışmalarına başlanılıp başlanılmayacağına karar verilir.
- İş Sürekliliği Yöneticisi tarafından kısmi kesinti durum başlangıç kararından sonra ekiplerin yönlendirilmesini sağlar.
- Ekiplerin sorumluluklarına uygun olarak çalışmalar başlatılır.
- Kesinti ile ilgili sorunlar giderildikten sonra İş Sürekliliği Yöneticisi tarafından kısmi kesinti durumu sonlandırılır.

### Bilgi güvenliği sürekliliğinin planlanması

Olumsuz durumlarda, örneğin bir kriz ve felaket boyunca, bilgi güvenliği ve bilgi güvenliği yönetimi sürekliliğinin gereksinimlerini belirlemek amacı ile aşağıdaki çalışmaları gerçekleştirir.

- Bilgi güvenliği gereksinimlerinin karşılanması amacı ile Bilgi İşlem sorumlusu İş – Etki Analizi hazırlar.
- BİM bağlamında İş sürekliliği planlarını dokümante eder.
- Kurumun iş sürekliliği planları çerçevesinde personel / altyapı / bilgi desteği sağlar.

|                                                                                                                                  |                                |                 |            |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------|------------|
| <br>OSTİM TEKNİK<br>ÜNİVERSİTESİ<br>A N K A R A | <b>İŞ SÜREKLİLİĞİ ESASLARI</b> | Doküman No      | BS.TL.003  |
|                                                                                                                                  |                                | Revizyon Tarihi | 07.11.2024 |
|                                                                                                                                  |                                | Revizyon No     | 01         |
|                                                                                                                                  |                                | Sayfa No        | 4 / 6      |

İş Sürekliliği / acil durum planları, Bilgi İşlem Daire Başkanlığı kapsamında yer alan bilgi varlıkları envanter dokümanına bağlı olarak yapılan risk değerlendirme çalışmaları kapsamında gözden geçirilir. İş etki analizini etkileyecek bir değişiklik yapıldığında iş sürekliliği / acil durum planları derhal güncellenir.

Herhangi bir durum ortaya çıkmaması halinde iş sürekliliği planları yılda en az bir kez Bilgi Yönetim Daire Başkanlığı koordinasyonunda ilgili birimlerle gözden geçirilir.

Kurum dahilinde ortaya çıkabilecek yangın, sel, su basması gibi fiziksel durumlarda etkilenen BİM?? alanlarında “Acil Durum Müdahale ve İş Planı” uygulanır.

Referans Doküman: İş Etki Analizi

### Bilgi güvenliği sürekliliğinin uygulanması

OSTİM Teknik Üniversitesi, olumsuz bir olay süresince bilgi güvenliği için istenen düzeyde sürekliliğin sağlanması için aşağıdaki planlama ve dokümantasyonu hazırlar:

İlgili tüm birimler için kritik bilgi varlıkları (sunucular, sistemler, uygulamalar, teçhizatlar, belgeler vb.) ile bu bilgi varlıklarının taşıdığı riskler ve bu riskleri kullanabilecek olası tehditler Varlık Envanteri dokümanında tanımlanır. Risk değerlendirme toplantılarında iş sürekliliği gereksinimleri ve hedefleri gözden geçirilir.

Referans Doküman:  
Envanter Risk Tablosu  
İş Etki Analizi

İlgili tüm birimlerin sorumluluklarındaki varlıklar için (sunucular, sistemler, uygulamalar, teçhizatlar, basılı malzemeler vb.) iş etki analizi gerçekleştirilirken, ilgili varlıkların sürekliliğin kesintiye uğraması durumunda kurumun karşı karşıya kalacağı operasyonel problemler değerlendirilir.

İş etki analizi sırasında aşağıdaki metrikler göz önüne alınmıştır:

- Tanımlanmış kritik varlığı kullanan (erişen, kullanan, değiştiren) yaklaşık kullanıcı sayısı.
- İlgili varlığın bağımlılıkları (bağlı olduğu altyapılar, 3. Taraf bağımlılıkları)

Bu kapsamda hazırlanan iş etki analiz çalışması MTPoD, RTO ve RPO değerleri ile birlikte Başkanlık İş Etki Analizi Dokümanı hazırlanır.

Referans Doküman:  
İş Etki Analizi

İş etki analizine tabi tutulmuş varlıklar için “İş Sürekliliği Acil Durum Kontrol Planı” hazırlanır. Plan içinde;

- İş Etki Analizi

|                                                                                                                                  |                                |                 |            |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------|------------|
| <br>OSTİM TEKNİK<br>ÜNİVERSİTESİ<br>A N K A R A | <b>İŞ SÜREKLİLİĞİ ESASLARI</b> | Doküman No      | BS.TL.003  |
|                                                                                                                                  |                                | Revizyon Tarihi | 07.11.2024 |
|                                                                                                                                  |                                | Revizyon No     | 01         |
|                                                                                                                                  |                                | Sayfa No        | 5 / 6      |

- Acil Durum Müdahale ve İş Planı
- Sistem Acil Durum Planı
- İş Sürekliliği Planı
- Süreklilik Kontrol Planı
- Acil Durum Ekipleri Listesi
- Kurumun hazırladığı yıllık iş sürekliliği tatbikat planı yer alır. İş sürekliliği kapsamında, iş etki analizi içerisinde bulunan varlıklar için kontrol planları ilgili eylemler, varlık sahipleri veya sorumlu işletmenler tarafından hazırlanır.

Süreklilik kontrol planı içerisinde aşağıdaki bilgilerin bulunması zorunludur:

- Kontrolün hangi aralıklar ile gerçekleştirileceği,
- İlgili varlık ve/veya işletmen sorumlusu (koordinasyon sorumlusu),
- Kontrol sırasında kullanılacak yöntem,
- Kontrol işlemini gerçekleştirecek personel ve sorumlulukları
- Tedarikçi sorumlulukları

Hazırlanan planlar, ilgili üst yönetim kademesi tarafından onaylanır. Kontrollerin sonuçları YGG toplantısında değerlendirilir.

Referans Doküman:

İş Etki Analizi

### **Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi**

Yukarıda tanımlanan çerçeve ve dokümantasyon gereksinimlerinin karşılanıp karşılanmadığını gözden geçirmek için belirlenen düzenli aralıklarla olumsuz olaylar süresince geçerli ve etkili olduğundan emin olmak için belirli aralıklarda doğruluğunu sağlar. İş Sürekliliği kapsamında oluşturulan tüm eylem planları ve diğer planlar (yıllık tatbikat planları) uygunluk ve yeterlilikleri bakımından yılda en az bir kere ilgili üst yönetim kademesi tarafından rutin olarak gözden geçirilir. Gerçekleştirilen tatbikatların ardından tespit edilen eksikliklerin giderilmesi için gözden geçirme ve güncelleme faaliyetleri ilgili yönetim kademesi sorumluluğunda gerçekleştirilir.

### **Bilgi işleme olanaklarının erişilebilirliği. Yedeklilik**

Bilgi işleme olanakları, erişilebilirlik gereksinimlerini karşılamak için yeterli yedeklilik sağlanır. Bilgi işleme olanaklarında yedekli çalışan (aktif – aktif, aktif – pasif, senkron – asenkron, sıralı) cihazlarla, aynı mantıkta çalışan destek cihazları Varlık envanterinde tanımlanmıştır.

Referans Doküman:

Envanter ve Risk Tablosu

|                                                                                                                                  |                                |                 |            |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------|------------|
| <br>OSTİM TEKNİK<br>ÜNİVERSİTESİ<br>A N K A R A | <b>İŞ SÜREKLİLİĞİ ESASLARI</b> | Doküman No      | BS.TL.003  |
|                                                                                                                                  |                                | Revizyon Tarihi | 07.11.2024 |
|                                                                                                                                  |                                | Revizyon No     | 01         |
|                                                                                                                                  |                                | Sayfa No        | 6 / 6      |

#### 5.REVİZYON GEÇMİŞİ

| Revizyon No | Tarih      | Açıklama                                                                                                                                                                                                                                                                                                                     |
|-------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 01          | 07.11.2024 | Entegre Kalite Yönetim Sisteminde kalite yönetiminde zorluklar ile karşılaşılması sebebiyle ISO 9001 Kalite Yönetim Sistemi (KYS) ve ISO 27001 Bilgi Güvenliği Yönetim Sisteminin (BGYS) ve dokümanlarının ayrılması ve ayrı ayrı takip edilmeleri kabul edilmiştir. Bu sebeple doküman kodlamalarında revizyon yapılmıştır. |

| Hazırlayan                      | Kontrol Eden                      | Onaylayan                          |
|---------------------------------|-----------------------------------|------------------------------------|
| İlknur ALŞAHİN<br>Kalite Birimi | Kenan IŞIK<br>Kalite Koordinatörü | Prof.Dr. Murat Ali YÜLEK<br>Rektör |
| E-imzalıdır/paraflıdır          | E-imzalıdır                       | E-imzalıdır                        |