MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

BİLGİ GÜVENLİĞİ SÜREKLİLİĞİ PROSEDÜRÜ

İçindekiler

1 Amaç

Bu doküman, ISO 27001 Bilgi Güvenliği Yönetim Sistemi(BGYS) kapsamında iş sürekliliğini sağlamayı amaçlamaktadır.

2 Kapsam

Bu doküman ISO 27001 BGYS Kapsam Analizi dokümanında belirtilen tüm bilgi varlıklarını kapsar.

3 Sorumluluk

Görev / Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
BGYS Birim Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
Incremental Yedek	Yedekleme sistemlerinde, o an yedeklenecek verinin bir önceki yedekten devam edilmesi, sonraki yedeklemelerde sadece değişikliklerin ve yeni verinin kaydedilmesi işlemidir.
Full Yedek	Yedekleme sistemlerinde, her yedekleme sürecinde yedeklenecek sistemin ve verinin tam olarak kaydedilmesi işlemidir.
Replikasyon	Verinin bulunduğu sistemden başka bir sisteme tam olarak kopyalanması

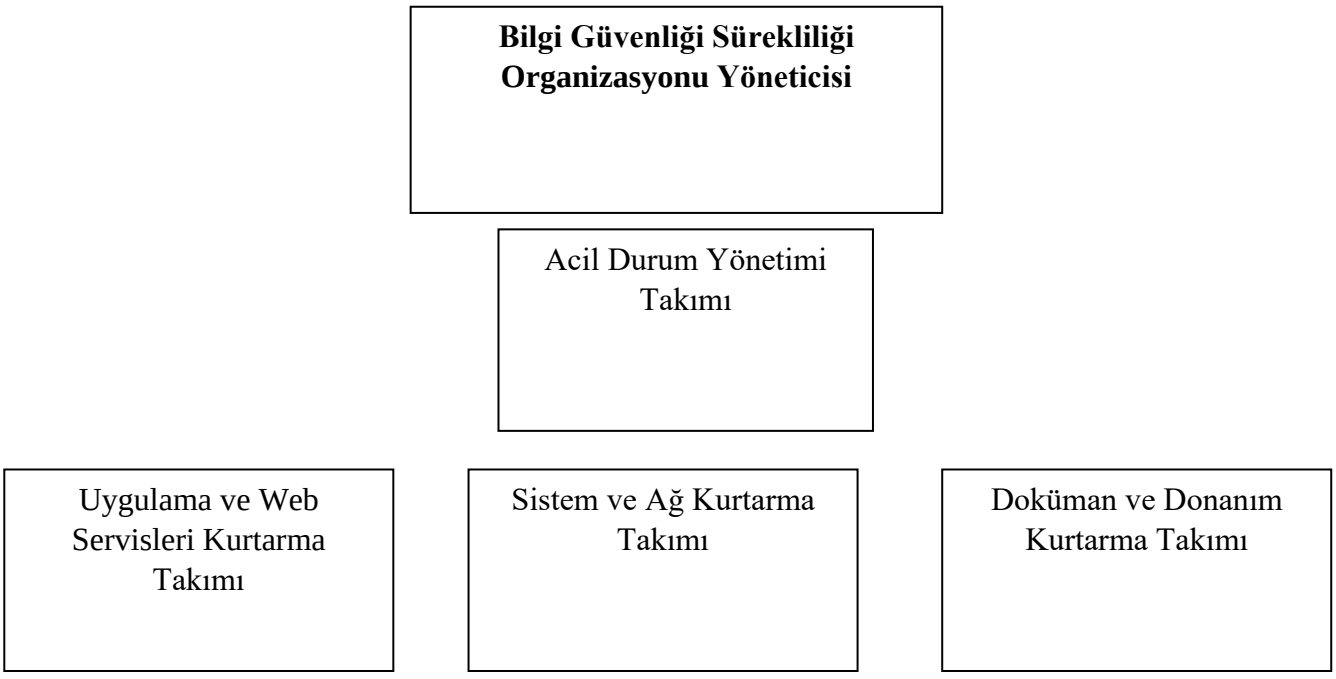
5 İşlem Detayı

5.1 Bilgi Güvenliği Sürekliliği

Deprem, yangın, fırtına, sel, bombalama, sabotaj, donanım veya yazılım hatası, elektrik ve telekomünikasyon kesintisi gibi önceden tahmin edilebilen veya edilemeyen olaylar sonucunda ortaya çıkabilecek acil durumlarda nasıl hareket edileceğinin ve neler yapılacağının planlanmasını ve acil durumlara neden olabilecek olaylar oluştuğunda bile kritik kurum fonksiyonlarının devam edebilmesini hedefler. Yönetim, acil durumlar için yeterli ve yetkin personeli hazır hale getirecek ve gerekli araçları sağlayacaktır. Bu doküman organizasyon değişiklikleri hizmet değişiklikleri durumunda gözden geçirilecektir.

5.2 Bilgi Güvenliği Sürekliliği Organizasyonu

Kurumdaki iş süreçlerini takip eden, süreci engelleyen ve durduran sorun ve olaylara karşı süreklilik planlarını uygulayan, zaman içinde bu planları değiştiren ve geliştiren personellerin oluşturduğu yapının adı Bilgi Güvenliği Sürekliliği Organizasyonudur. Bilgi güvenliği sürekliliği organizasyonu aşağıdaki gibidir. Bilgi güvenliği sürekliliği ile ilgili tüm raporlar BGYS yöneticisi tarafından saklanır.



5.2.1 Bilgi Güvenliği Sürekliliği Organizasyonu Yöneticisi

Bilgi güvenliği sürekliliği planının geliştirilmesi, uygulaması, test edilmesi ve güncellenmesi faaliyetlerini yürütür ve koordine eder. Bilgi güvenliği sürekliliği organizasyonu yöneticisini karar verme yetkisine sahip bir yöneticilerden seçilmek kaydı ile bir asil bir yedek olarak organizasyonda yer alır. Planın temelini oluşturacak teknik bilgiye sahip kişiler planın geliştirilmesini, test edilmesini ve güncellenmesini yapacaktır. Tüm süreçlerin yönetilmesinden asli sorumlu Bilgi güvenliği sürekliliği organizasyon yöneticisidir.

5.2.2 Acil Durum Yönetimi Takımı (ADYT)

Acil durumlarda karar verici olarak çalışan takımdır. Olası felaket durumunda meydana gelen hasarın boyutlarını ve sistemi yeniden devreye sokmak için gerekli olan tahmini zamanı belirler. Hasar raporunu hazırlar, acil durumlarda sözlü olarak iletişim kurar. Bu rapora göre planın çalıştırılıp çalıştırılmayacağına veya kısmen çalıştırılmasına karar verir. Diğer kurtarma takımları ile koordinasyonu sağlar felaketten etkilenen servisler tekrar devreye alındığında servis sahiplerine bildirimde bulunur. ADYT üyelerinin görevleri aşağıda belirtilmiştir:

5.2.3 ADYT Lideri

Acil durum yönetim takımına başkanlık eder. Görev ve sorumlulukları aşağıdadır.

- Acil durumlarda normal operasyona dönüş konusunda sorumlu kişidir.
- Hasar rapor sonucunda acil bir durum olup olmadığına karar verir ve acil durum oluşmuşsa bilgi güvenliği sürekliliği organizasyonu yöneticisini bilgilendirir.
- Gerekli durumlarda yönetici onayı ile planı aktive eder.
- Bütün takımlardaki elemanlar durumla ilgili kendisine bildirimde bulunur.
- Bilgilendirilen ve harekete geçirilen takımların bilgileri ile kriz durumu bilgileri takım liderinde toplanır.
- Kurtarım operasyonlarının durumu takım liderine bildirilir.

5.2.4 ADYT Lider Vekili ve Yardımcısı

- ADYT liderinin görevini yerine getiremeyeceği durumlarda takıma başkanlık eder. Sorumlulukları şöyledir:

- ADYT liderinin bulunmadığı zamanlarda aynı yetkiye sahiptir. Sorumluluğu ADYT takım lideri ile aynıdır.
- ADYT liderinin bulunduğu ve acil durumun oluştuğu durumlarda ADYT liderinin sorumluluklarına yardımcı olur.

5.2.5 ADYT Üyeleri

ADYT üyelerinin sorumlulukları;

- Acil durumun üyeye bildirilmesi durumunda ADYT liderine durumu haber verir.
- Takım elemanları kendilerini aşan olaylarda durumu ADYT takım liderine görevi devreder.
- Acil durumlarda ADYT lideri ve yardımcısına yardımcı olacaktır.
- Takımlar arası koordinasyon sağlanmasında ve sürecin yönetilmesinde etkin rol alır. ADYT liderini sürekli bilgilendirir.
- Bütün takım elemanları ellerindeki bilgi güvenliği sürekliliği planının güncel olmasından sorumludur.

5.2.6 Uygulama ve Web Servisleri Kurtarma Takımı (UWKT)

UKT üyelerinin görev ve sorumlulukları aşağıdadır:

- Bu takım olası felaket durumlarında SAKT ile birlikte çalışarak uygulamaları ve web servislerini çalışır hale getirir. Uygulamaların kullandığı verilerin yedeklerinden geri dönme adımlarını diğer takımlarla birlikte uygulanması takip eder ve verilerin kullanılabilirliğini test eder.
- Gerektiğinde ilgili tedarikçi firma ile iletişime geçer.
- Yapılan işler ile ilgili ADYT ‘ye bilgi verir.

5.2.7 Sistem Kurtarma Takımı (SAKT)

SAKT üyelerinin görev ve sorumlulukları aşağıdadır:

- Olası felaket durumlarında sistemde var olan sunucuların, veri depolama cihazlarının, ağ cihazlarının ve geniş alan ağ bağlantılarının çalışır hale getirilmesinden sorumludur. UWKT ile veri tabanı, uygulamalar ve web servisleri konusunda iletişimde olmakla da sorumludur.
- Gerektiğinde ilgili tedarikçi firma ile iletişime geçer.
- Yapılan işler ile ilgili ADYT ‘ye bilgi verir.

5.2.8 Doküman ve Donanım Kurtarma Takımı (DDKT)

DDKT üyelerinin görev ve sorumlulukları aşağıdadır:

- Olası felaket durumlarında dokümanların kurtarılması taşınması ve korunmasından sorumludur.
- Gerektiğinde ilgili tedarikçi firma ile iletişime geçer.
- Yapılan işler ile ilgili ADYT 'ye bilgi verir.

5.3 İş Sürekliliği Tehditleri

Acil bir durumda kurum altı temel tehlike ile karşı karşıyadır;

- İletişim ve telekomünikasyon imkânlarının yitirilmesi
- Bilgi işleme kapasitesi ve olanaklarının yitirilmesi
- Altyapıya erişim olanağının yitirilmesi
- Eğitimli insan kaynağının yitirilmesi
- Varlıkların yitirilmesi
- Verinin yitirilmesi

İş sürekliliği tehditleri, kurum içerisindeki iş süreçlerinin gerçekleşmesini engelleyen tehditler olarak tanımlanabilir. Var olan bu riskler sistemde yer alan bilginin bozulmasına ya da varlığın tamamen yok olmasına neden olabilir. Riskler insanlardan ya da dış faktörlerden kaynaklanabilir. İnsanlardan kaynaklanan riskler insanların bilinçli ya da bilinçsiz eylemlerinin bir sonucudur. Var olan bu riskler etkileri ve olma ihtimallerine göre sınıflandırılabilir.

- Yangınlar
- Su Baskınları
- Doğal Felaketler
- Fiziksel Etkiler
- Terörist Eylemler
- Elektrik Şebekesinin Bozulması
- Havalandırma Sisteminin İşlevini Yerine Getirememesi
- Bilgi Sistemlerinden Kaynaklanan Hatalar
- Bilgi Sistemleri Üzerinde Hatalı İşlemler
- Siber Saldırılar

- İnsanları Tehdit Eden Unsurlar

İnsan kontrolünde olmayan doğal olaylar bu grup içerisinde tanımlanmaktadır. Çeşitli şekillerde ortaya çıkabilir ve etkisi oldukça değişken olabilir. Tehditlere karşı alınacak önlemlerin geçerliliği, tehditlerin önceden iyi tanımlanmış olmasına bağlıdır.

5.3.1 Tehdit Tanımları

5.3.1.1 Yangın

Yangınlar, tahrip edici yapısı nedeniyle varlıkların tamamen kullanılamaz hale gelmesine neden olmaktadır. Benzin, sigara, aşırı ısı ve oksijen gibi yanıcı gazlar yangınların önemli nedenlerindendir. Yangınlar temel olarak dört sınıfta incelenmektedir. Bu sınıflar A,B,C ve D tipi olarak bölümlenmiştir.

A Tipi: Kâğıt gibi maddelerin yanmasından ortaya çıkar. Söndürülmesi kolaydır.

B Tipi: Sıvı ya da gaz yanıcı maddelerden kaynaklanan yangın tipleridir. Bir takım kontrollere riayet edildiğinde ortaya çıkma ihtimali azdır.

C Tipi: Elektrik bağlantılarından çıkan yangınlardır. İyi planlanmamış elektrik sistemlerinde aniden ortaya çıkabilmektedir.

D Tipi: Yanma kabiliyeti olan metallerden (titanyum, uranyum, fosfor, sodyum, potasyum, alüminyum, magnezyum vs.) kaynaklanan yangınlardır. Söndürülmesi zordur. Özel yangın söndürme sistemleri gerektirir. Yanma riski olan yerlerde kesinlikle bu metaller kullanılmamalıdır.

5.3.1.2 Su Baskınları

Su özellikle elektronik bilgi sistemlerine önemli zararlar verebilmekte ve sistemleri kullanılamaz hale getirmektedir. Çeşitli nedenlerden kaynaklanabilmektedirler.

5.3.1.3 Doğal Felaketler

İnsan kontrolünde olmayan doğal olaylar bu grup içerisinde tanımlanmaktadır. Çeşitli şekillerde ortaya çıkabilir ve etkisi oldukça değişken olabilir. Depremler, fırtınalar bu felaketlerin başta gelenleridir.

5.3.1.4 Fiziksel Etkiler

Bilgi varlıklarının yer aldığı bileşenlerin fiziksel etkiler sonucu kullanılamaz hale gelmesidir. Bu bilerek ya da bilmeyerek gerçekleşebilir. Varlığın üzerinde düşen bir objeden dolayı bozulması, varlığın yanlışlıkla yere düşürülmesi veya kişi/kişiler tarafından fiziksel darbeler ile sistemin kullanılamaz hale gelmesi bu etkilerin başta gelenleridir.

5.3.1.5 Terörist Eylemler

Terörist eylemler, hedef aldığı bölgede yer alan tüm varlıkları tehdit eden ve bu varlıkları yok etmeyi hedefleyen eylemlerdir. Özellikle terörist saldırıların tehdidinde olan ve ülke güvenliği açısından önem taşıyan kurumların bu gibi tehditler ile karşılaşma ihtimali daha yüksektir.

5.3.1.6 Elektrik Şebekesinin Bozulması

Elektrik şebekesinde yaşanan kesintiler, ani voltaj değişiklikleri bu şebekelere bağlı olarak çalışan varlıkların çalışamaz hale gelmesine neden olmaktadır. Özellikle şehirlerdeki yerel elektrik şebekesi üzerinde bu gibi sorunlar yaygın olarak gözlemlenmektedir.

5.3.1.7 Havalandırma Sisteminin İşlevini Yerine Getirememesi

Havalandırma sistemi elektronik bilgi sistemlerinden ya da dış etkilerden dolayı ortamların fazla ısınmasını veya soğumasını engelleyen, ortamdaki havayı temizleyen önemli bir bileşendir. Çalışmaması durumunda, sistem odalarının aşırı ısınarak varlıkların yok olması ya da kullanılamaz hale gelmesine sonucu ortaya çıkabilir.

5.3.1.8 Bilgi Sistemlerinden Kaynaklanan Hatalar

Bilgi sistemlerinde yer alan bileşenlerin üzerinde çalıştığı donanımın ya da uygulamadan kaynaklanan hataların tetiklenmesiyle beraber sistemlerde önemli kesintiler meydana gelebilir. Özellikle bu sistemlere uygulanan yamalar sonucunda bu hatalar oluşabilir. Etkisi ve etkilediği servisin ne olduğuna göre farklı sonuçlar ortaya çıkartabilir.

5.3.1.9 Bilgi Sistemleri Üzerinde Hatalı İşlemler

Bilgi kaynaklarını kullanan kullanıcıların veya yöneticilerinin, bilerek ya da bilmeyerek bilgi sistemlerine zarar vermeleridir. İnsanların gereğinden fazla yetkilere sahip olması, sistemler hakkında yeterince bilgi sahibi olmayan kişiler tarafından sistemler üzerinde işlem yapılması veya sistem yöneticisinin yanlışlıkla sistemin çalışmasını bozacak bir işlem yapması bu işlemlere yönelik örneklerden birkaçıdır.

5.3.1.10 Siber Saldırılar

Bilgisayar sistemi varlıklarını etkileyen çalışamaz hale gelmesini ya da varlığın yok olması sonucunu doğurabilen virüs, trojan, arka kapı yazılımlarını kullanan saldırılardır. Etkileri oldukça değişkendir, kolay yayılabilmesi önemli bir tehdit olarak ön plana çıkmasına neden olmaktadır.

5.3.1.11 İnsanları Tehdit Eden Unsurlar

Bilgi varlıklarını yöneten, onları kullanan ve bazı bilgilere sahip olan insanların hastalıklar nedeniyle çalışamaz hale gelmeleri veya bir olay nedeniyle ölmeleri durumunda, hem bu kişilerin sahip oldukları yazılmamış bilgilerin yok olması hem de bu kişilerin yönettiği bilgi varlıklarının yönetilememesi sonucu bu varlıkların da kullanılamaz hale gelmesi durumu ortaya çıkabilmektedir.

5.4 Tehditlerin Sınıflandırılması

Yukarıda ortaya konmuş olan riskler, etkileri ve olma ihtimalleri açısından farklılık göstermektedir. Aşağıdaki tabloda bu riskler olma ihtimalleri ve de etkilerine göre sınıflandırılmıştır. Sınıflandırma amacıyla 0–5 arası değerler alan bir ölçek kullanılmıştır. 5 en yüksek dereceyi 0 ise olma ihtimalinin olmadığını belirtmektedir

Tehdidin Adı	Tehdidin Etkisi	Tehdidin Olma İhtimali
Yangınlar	5	2
Su Baskınları	4	2
Doğal Felaketler	5	3

Tehdidin Adı	Tehdidin Etkisi	Tehdidin Olma İhtimali
Fiziksel Etkiler	3	2
Terörist Eylemler	4	2
Elektrik Şebekesinin Bozulması	2	2
Havalandırma Sisteminin İşlevini Yerine Getirememesi	3	2
Bilgi Sistemlerinden Kaynaklanan Hatalar	2	3
Bilgi Sistemleri Üzerinde Hatalı İşlemler	2	2
Siber Saldırılar	3	4
İnsanları Tehdit Eden Unsurlar	5	2

Sınıflandırılan Tehditlere Karşı Önlemler	
Tehdidin Adı	**Karşı Önlem**
Tüm bilgi altyapısının yok olması	Kritik sistemlerin yedeklerinin sürekli olarak tutulduğu felaket anında devreye alınacak kurtarım merkezi bulunmamaktadır. Yeni dönem bütçesinde araştırması yapılmak üzere planlanmıştır.
Tüm bilgi altyapısının yok olması	Belirlenmiş politika doğrultusunda yedekler düzenli olarak alınmakta ve saklanmaktadır.
Tüm bilgi altyapısının yok olması	Kurumsal ve personelin hazırlamış olduğu kayıtlar düzenli olarak yedeklenmektedir.
Sistem odasında yangın çıkması	Kurumun yangın talimatı bulunmaktadır. Yangın söndürme cihazları ve sistemleri mevcuttur, itfaiye hızla haber verilebilecek iletişim bilgileri ve cihazlar kolay erişilebilir şekilde planlamıştır.
Sistem odasında su baskını	Sistem odasında su baskını tehditi olmayan fiziksel bir konumda bulunmaktadır.
Doğal Felaketler	Kurumun ana binası doğal afetlere dayanacak sağlamlıktadır, tüm bilgi altyapısının yok olması durumunda belirtilmiş olan karşı önlemler gerçekleştirilir.
Fiziksel bir etki sonucu varlık(lar)ın zarar görmesi	İlgili servislere ait bileşenlerin yedeklerinin kurum merkezinde saklanmaması.

Sınıflandırılan Tehditlere Karşı Önlemler	
Tehdidin Adı	**Karşı Önlem**
Terörist Eylemler	Kuruma girişlerin kontrollü yapılacağı fiziksel güvenlik koşullarının sağlanması, kritik bölgelerin sürekli olarak izlenmektedir
Elektrik kesintisi sonucunda servislerin kullanılamaz hale gelmesi	Servislerin elektrik enerjisinin sağlandığı sistemde elektrik kesintisi anında merkezi jeneratör devreye girmektedir ayrıca UPS kullanılmaktadır. UPS 'lerde bir problem olması durumunda ön müdahaleyi yapacak yetkin personel kurum içeresinde yer almaktadır. Büyük problemlerde ilgili firma ile iletişime geçilecektir.
Elektrik şebekesindeki ani voltaj değişiklikleri	Servislerin elektrik enerjisinin sağlandığı sistemde UPS kullanılmaktadır.
Servislerin üzerinde çalıştığı elektronik varlıkların bulunduğu ortamın sıcaklığının aşırı düşmesi ya da yükselmesi	Bu ortamlarda sıcaklığı düzenleyen klima sistemleri kullanılmaktadır, ortamların sıcaklıklarının ölçülmekte ve sürekli takibini yapılmaktadır.
Servislerin üzerinde çalıştığı ortamda toz bulunması ve varlıkların zarar görmesi	Sistem odasının toza karşı yalıtımı iyi seviyededir.
Yeni yamaların bilgi sistemlerinin işleyişine zarar vermesi	Yamaların merkezi olarak dağıtılmasını sağlayacak yazılımlar sistemde kuruludur. Sadece güvenlik yamaları son kullanıcılara merkezi dağıtılmaktadır. Sunucularda güvenlik yamaları test edilerek uygulanmaktadır.
Yetkisiz personel tarafından sistemler üzerinde değişiklik yapılması	Sisteme sadece yetki verilen personelin giriş yapabilmesi için güvenlik ayarları yapılmıştır, Sistem odasına girişler şifrelenmiş ve fiziksel erişimler kayıt altına alınmaktadır.
Yedeklerden geri dönüş sırasında ortaya çıkabilecek veri kayıpları ve prosedürlerin eksik olması	Kurumda, verilerin yedeklerden geri dönülmesi konusunda prosedürler mevcuttur ayrıca dönemsel testlerin yapıldığı test ortamı yer almaktadır.
Personel tarafından yapılan hatalı bir işlem sonucunda sistemin işleyişinin bozulması	Sistem yedeklerinin sağlıklı olarak alınmaktadır. Bilgi İşlem Müdürlüğü personeli yetkinlikleri çerçevesinde erişim hakları düzenlenmiştir.
Antivirüs, trojan ve arka kapı yazılımlarını sistemlere bulaşması	Merkezi antivirüs yazılımı çalışmaktadır ve düzenli güncellenmesi yapılmaktadır, güvenlik duvarları gereksiz trafiği filtreleyecek şekilde ayarlıdır, saldırı tespit sistemi (IDS,IPS) uygun şekilde konfigüre

Sınıflandırılan Tehditlere Karşı Önlemler	
Tehdidin Adı	**Karşı Önlem**
sonucunda sistemlerin kullanılamaz hale gelmesi	edilmiştir. Ağ ortamında ki donanımlar ve hareketleri online takip edilmektedir.
Sisteme yapılan kontrolsüz erişimler sonucu sistemin dış müdahalelere açık hale gelmesi ve sistemin dış unsurlarca devre dışı bırakılması	Ağ dışı erişimler IP adres sınırlamalı ve sadece ilgili sunucu ile sınırlandırılmıştır.
Yedekleme yazılımları ile yedeği alınamayan konfigürasyon bilgilerinin kayıp olması.	Yedekleme sunucusu günlük olarak kendi yedeğini de almaktadır
Kurum açısından önem taşıyan bilginin bütünlüğünün bozulması	Kritik varlıklara yapılan erişimler denetlenmekte ve hareket kayıtları tutulmaktadır.
İş süreçlerinin sahibi olan, kurum servislerinden sorumlu kişilerin toplu olarak işten ayrılması, vefat etmesi vb.	Operatör seviyesindeki personel birbirlerinin yedeği kapsamındadır. Ayrıca görev ve sorumluluklar belirlenmiş prosedürlere bağlanmıştır.
Donanım arızaları	Kritik donanımların güç kaynaklarının ve disk sistemlerinin yedekli durumdadır.
İletişim olanaklarının yitirilmesi	Kritik servislerin bulunduğu ortamlarda alternatif iletişim olanağı bulunmaktadır. Lokal telefon ve GSM olarak erişimler bulunmaktadır. Ayrıca kurumsal olarak IP telefon kullanımı bulunmaktadır.

5.5 İş Sürekliliği Kapsamı

İş sürekliliğini sağlamak için yürütülen süreçlerin ve bu süreçlerden sorumlu takımların kontrol ettiği ve yürüttüğü sistem ve süreçlerdir. Bu sistem ve servisler sürekli tehdit altındadır. Felaket durumunda ve öncesinde alınacak önlemlerin ve yapılacak çalışmaların yürütülmesi için, sistem ve servislerin erişilebilirlik açısından önem dereceleri belirlenmiştir.

5.5.1 Kritik Servisler

Servis Adı	Servis Sahibi	Kabul Edilebilir Kesinti Süresi
Uygulama ve Veritabanı Hizmeti İşletim Hizmeti	Bilgi İşlem	3 Saat

Fiziksel Güvenlik Hizmeti	Bilgi İşlem	3 Saat
Ağ İletişimi Hizmeti	Bilgi İşlem	3 Saat
Ağ ve Sunucu Güvenliği Hizmeti	Bilgi İşlem	3 Saat

Uygulama ve Veritabanı Hizmeti İşletim Hizmeti: Bu hizmet, var olan uygulamaların ve veritabanlarının işletilmesini kapsar.

Fiziksel Güvenlik Hizmeti: Bu hizmet, Bilgi varlıklarının korunması için gerekli kamera kayıtları, giriş kontrollerini kapsar.

Ağ İletişimi Hizmeti: Bu hizmet, Kurum ihtiyaçlarına uygun olarak kablolu, kablosuz ağ ve IP Telefon Sistemleri mimarisinin düzenlenmesi ve ağ cihazlarının yapılandırılması kapsar.

Ağ ve Sunucu Hizmeti: Bu hizmet, Ağ ve sunucu sistemlerinin güvenliği için mimarinin belirlenmesi, firewall, NAC, SIEM, Anti Spam ve cihazların yapılandırma ayarlarını kapsar.

5.5.2 Temel Servisler

Servis Adı	Servis Sahibi	Kabul Edilebilir Kesinti Süresi
Aktif Dizin Servisi	Bilgi İşlem	3 Saat
E- Posta Servisi	Bilgi İşlem	4 Saat
Yedekleme Servisi	Bilgi İşlem	4 Saat
Alt Yapı Destek Hizmeti	Bilgi İşlem	5 Saat
Sunucu Destek Hizmetleri	Bilgi İşlem	5 Saat
Ağ İletişimi Altyapı Hizmeti	Bilgi İşlem	5 Saat
Web Sayfası İşletimi Hizmeti	Bilgi İşlem	5 Saat
Uygulama Geliştirme Hizmeti	Bilgi İşlem	5 Saat
Personel ve Özlük İşlemleri Hizmeti	İnsan Kaynakları	6 Saat
Dosya Paylaşım Servisi	Bilgi İşlem	6 Saat
BGYS Servisi	Bilgi İşlem	6 Saat

Aktif Dizin Servisi: Bu hizmet, Kurum aktif dizin kullanıcı hesaplarının oluşturulması, güvenlik ayarlarının ve parola politikalarının belirlenmesi ve işletilmesi sürecini kapsar.

E-Posta Servisi: Bu hizmet, Kurum içi elektronik posta hesaplarının ve sunucularının işletilmesi sürecidir. Bu süreç personelin elektronik posta hesaplarının açılması, posta hesaplarının yönetimi ve işletimini kapsar.

Yedekleme Servisi: Bu hizmet, kurum sunucularının yedekleme, yedekten geri dönüş işlemlerinin yürütülmesini kapsar.

Alt Yapı Destek Hizmeti: Bu hizmet, Kuruma hizmet veren bilişim sistemlerinin işlevlerini yerine getirmesi için gerekli, elektrik, iklimlendirme, uyarı sistemleri gibi sistemlerin işletilmesini kapsar.

Sunucu Destek Hizmetleri: Bu hizmet, Kurum için ihtiyaç duyulan uygulamaların çalışması için gerekli sunucu kurulumu, bakım ve destek işlemlerini kapsar.

Ağ İletişimi Altyapı Hizmeti: Bu hizmet, Kurum içinde yeni yapılan binalarda ya da kurum içinde ağ bağlantısı için kablo uçların toplanması ve kabin içinde sonlandırılması ve oluşan arızaların giderilmesi ve gerekli malzemelerin temini işlemlerini kapsar.

Web Sayfası İşletimi Hizmeti: Bu hizmet, Kurum birimlerinin web sayfalarının oluşturulması, güncellenmesi, yayınlanması ve işletilmesini kapsar.

Uygulama Geliştirme Hizmeti: Bu hizmet, yeni bir yazılım oluşturma süreçlerini kapsar.

Personel ve Özlük İşlemleri Hizmeti: Bu hizmet, Personel ve Eğitim İşlemleri, Hastalık, mazeret ve yıllık izinlerin düzenlenmesi, izin kayıt sistemi, atama görevlendirme, pasaport işleri vb. İşlemleri kapsar.

Dosya Paylaşım Servisi: Bu hizmet, kurum içi elektronik dosya paylaşım hizmetlerinin işletilmesini kapsar.

BGYS Servisi: Bu hizmet, kapsam dahilinde bilgi güvenliği yönetim sisteminin tüm süreçlerini kapsar.

5.5.3 Az Kritik Servisler

Servis Adı	Servis Sahibi	Kabul Edilebilir Kesinti Süresi
Sistem ve Ağ Tabanlı Tedarik Hizmeti	Bilgi İşlem	1 Gün ve Üzeri
Uygulama Tabanlı Tedarik Hizmeti	Bilgi İşlem	1 Gün ve Üzeri
İdari Tabanlı Tedarik Hizmeti	İdari İşler	1 Gün ve Üzeri
Son Kullanıcı Destek Servisleri	Bilgi İşlem	12 - 24 Saat
Misafir İnternet Erişim Hizmeti	Bilgi İşlem	1 Gün ve Üzeri
İdari ve Mali İşlemler Hizmeti	İdari İşler	1 Gün ve Üzeri

Sistem ve Ağ Tabanlı Tedarik Hizmeti: Bilişim tabanlı satın alma ihale işlemlerini kapsar.

Uygulama Tabanlı Tedarik Hizmeti: Uygulama tabanlı satın alma ihale işlemlerini kapsar.

İdari Tabanlı Tedarik Hizmeti: İdari tabanlı satın alma ihale işlemlerini kapsar.

Son Kullanıcı Destek Servisleri: Bu hizmet, bilgisayar ve çevre birimlerinin kurulum, bakım ve onarımı (İşletim sistemi kurulumu, Anti virüs programı kurulumu, yazıcı kurulumu, veri aktarımı, onarım vb.) ve bilgisayar çevre birimleri teknik şartnamelerinin hazırlanma işlemlerini kapsar.

Misafir İnternet Erişim Hizmeti: Bu hizmet, kurum personeli olmayan kullanıcılara internet erişim hizmeti verilmesi sürecini kapsar.

İdari ve Mali İşlemler Hizmeti: Bu hizmet, Başkanlık bütçesinin hazırlanması, birim faaliyet raporunun düzenlenmesi , Yıllara sair Mali Durum Beklentiler Raporu, İletişim Rehberi, İş Tanımı Görev yetki ve sorumluluklar, Dosyalama Sistemi Düzenlemesi, Başkanlığın araç gereç ihtiyaçlarının sağlanması, Mal ve Hizmetlerin ihale işlemleri tamamlandıktan sonra ödemeler için komisyonlardan gelen evrakların incelenerek ilgili birime gönderilmesi, Personel maaşlarının düzenlenmesi, terfi kadro dereceleri vb. personel maaşın a yansıtmak vb., Taşınır Mal Kayıt İşlemleri.

5.6 Bilgi Güvenliği Sürekliliği Planı Yapısı

5.6.1 Felaket Kurtarma Stratejisi

Felaket durumlarında atılacak adımlar ve felaket kurtarım stratejisi aşağıda anlatılmıştır. Felaket kurtarımı servis bazlı olarak yapılmaktadır.

Acil bir durumda izlenecek prosedürler aşağıdadır:

- Kurum içinde acil bir durum oluştuğunda, durumu fark eden çalışan ADYT üyesine durumu bildirir.
- ADYT üyesi, zarar boyutlarını değerlendirir.
- ADYT Üyesi, ADYT Liderini bilgilendirir.
- ADYT Lideri planın aktive edilip edilmeyeceğine organizasyon yöneticisine danışarak karar verir.
- Danışma acil durumlarda sözlü normal şartlarda mail yolu ile yapılır.
- Plan aktive edilirse ilgili takımlar ADYT Lideri tarafından bilgilendirilir.
- ADYT Lideri koordinesinde ilgili kurtarma faaliyeti başlatılır.

- Servisin kurtarımı sonrasında servis sahibine ve durumu bildiren çalışana ADYT lideri tarafından sözlü ya da mail yolu ile bilgi verilir.
- Yapılan işlemler ve eğer karşılaşılırsa çıkan problemler kayıt altına alınır.

5.6.2 Acil Durumun Aktive Edilmesi

ADYT Lideri servislerin kabul edilebilir kullanım süreleri baz alınarak bir durumun acil durum olup olmadığına karar verir. Acil durum olması halinde Bilgi Güvenliği Sürekliliği planını aktive eder.

5.6.3 Yedekleme Faaliyetleri

Yedekleme faaliyetleri ve planlaması sunucuların varlık değerleri dikkate alınarak yapılır. Yedekleme faaliyetleri Bilişim Sistemleri Şube Müdürlüğü tarafından planlanıp alınmaktadır.

5.6.4 Kurtarma Planları

Kurum bünyesinde kullanılan servisler aşağıda sayılan servislerin çalışmasına bağlıdır.

Kurtarma aksiyonları yukarıda bahsedilen Bilgi Güvenliği tehditlerinin gerçekleşmesi durumunda planlanmıştır.

Servis Adı	Kurtarma Planı
Uygulama ve Veritabanı Hizmeti İşletim Hizmeti	Veritabanı ve uygulama yedekleri alınmaktadır. En son yedekten geri dönülür.
Fiziksel Güvenlik Hizmeti	Personel ile süreklilik sağlanır. Erişim için yedeklilik mevcuttur. Yedek cihazlar devreye alınır.
Ağ İletişimi Hizmeti	Konfigürasyon yedekleri alınmaktadır. Standby olarak çalışan Ağ cihazları aktif edilir.
Ağ ve Sunucu Güvenliği Hizmeti	Konfigürasyon yedekleri alınmaktadır. Standby olarak çalışan Ağ cihazları aktif edilir.
Aktif Dizin Servisi	Konfigürasyon yedekleri ve sanal imajlar alınmaktadır. Yedeklerden geri dönüş sağlanır.

Servis Adı	Kurtarma Planı
E- Posta Servisi	Mailbox yedekleri ve sunucu imajları alınmaktadır. Yedeklerden geri dönüş sağlanır.
Yedekleme Servisi	Konfigürasyon yedekleri alınır. Yedeklerden geri dönüş sağlanır.
Alt Yapı Destek Hizmeti	Sistemler aktif aktif olarak yedeklidir. Diğer sistem üzerinden çalıştırıştır.
Sunucu Destek Hizmetleri	Sunucular kontrol edilir. İmaj yedekleri bulunaktadır. En son yedekten geri dönülür.
Ağ İletişimi Altyapı Hizmeti	Yedek sarf malzemeler bulundurulur. Gerekli malzeme değişimi yapılır.
Web Sayfası İşletimi Hizmeti	Konfigürasyon yedekleri alınmaktadır. Yedeklerden dönüş sağlanır.
Uygulama Geliştirme Hizmeti	Kaynak kodlar yedeklenmektedir.
Personel ve Özlük İşlemleri Hizmeti	Yedek görevliler tanımlanır.
Dosya Paylaşım Servisi	Dosya yedekleri alınmaktadır. En son yedekten geri dönülür.

5.7 Bilgi Güvenliği Sürekliliği Planı Yönetimi

Bilgi güvenliği sürekliliği planı işlevini yerine getirebilmesi için planın periyodik ve belirli durumlarda güncellenmesi gereklidir. Ayrıca aşağıda belirtilen durumlarda plan güncellenecek veya gözden geçirilir:

- Sistem veya uygulama yazılımlarının değişmesi sonrasında
- Yeni bir cihazın sisteme katılması veya var olan bir cihazın değiştirilmesi sonrasında
- Ağ alt yapısının topolojisinin veya bileşenlerinin değişmesi sonrasında
- Organizasyon veya iş süreçlerinin değişmesi sonrasında
- Personel değişimleri (işe alım veya işten ayrılma) sonrasında

- Tedarikçi değişimleri (Bakım anlaşmaları) sonrasında
- Testler sonucunda öğrenilen kritik derslerden sonra
- Planın acil durumlarda işletimi sonucunda ortaya çıkan problemlerden sonra
- Değişen dış etkenler sonucunda planda güncellenme gerektiğinde
- Risk analizinde belirlenen eksiklikler sonrasında
- Plan gözden geçirmelerinde ortaya çıkan eksiklerden sonra

5.7.1 Planın Testi, Güncellenmesi ve Eğitim Faaliyetleri

Kurum bünyesinde yer alan bilgi sistemlerinin zarar gelmesi sonucunda kullanılmaz hale geldiği durumda kurumun işlevine devam edebilmesi mümkün değildir. Böyle bir olayın yaşandığı durumda kurumun görevlerini yerine getirebilmesi için, oluşturulmuş olan felaket kurtarım planlarının düzenli olarak test edilmesi ve ortaya çıkan eksiklikler doğrultunda planın güncellenmesi çok önemlidir. Bilgi güvenliği sürekliliği planı ve diğer tüm planlar yaşayan dokümanlardır ve düzenli aralıklarla (kurum içinde en geç yılda bir) kontrol edilmesi, güncellenmesi ve yenilenmesi gereklidir. Bilgi güvenliği sürekliliği ile ilgili tüm adımlardan ve kontrollerinden BGYS Yöneticisi sorumludur. Planın doküman olarak elde bulunmasına ek olarak, yine düzenli aralıklarla plandaki maddelerin test edilmesi kurum veri güvenliği bakımından çok önemlidir. Planın test edilmesinde uygulanabilecek olan yöntemlerden en az bir tanesi seçilen bir servis veya sistem için uygulanır ve bu yöntemler şunlardır:

- **Hipotetik Testler:** Bu test, oluşturulmuş olan prosedürlerin acil durum yönetim takımı tarafından madde madde üzerinden geçilmesi ve tartışılması ile yapılır. Her bir prosedürün üzerinden teker teker geçilmeli ve eksiklikler ortaya çıkartılmalıdır.
- **Bileşen ve Servis Testleri:** Bu testlerde amaç acil durum yönetim takımı tarafından belirlenmiş olan bileşenlerde takım tarafından belirlenmiş olan senaryoların uygulanmasıdır. Veri tabanlarının başka bir makineye dönülerek kontrol edilmesi ve veri tabanı işletim servisinin işlevini yedekten dönülmüş veri tabanı ile yerine getirip getiremediğinin test edilmesi, ana anahtarlama cihazlarından birinin kapatılması durumunda servislerin devamlılığının kontrol edilmesi, bakım anlaşması yapılan firmalardan zamanında destek alıp alınamadığının testi bunlardan bazılarıdır.

- **Tam Kapsamlı Test:** Bu test kurumun merkezindeki bilgi sistemlerinin tamamen devreden çıkartılarak tüm servislerin yedek sistem odasından devreye sokulmasını kapsar. İnsan kaynağının planlamada yer almasına dikkat edilmelidir. Testin sonucunda sistemlerin devreye alınma süreleri ve planının beklenen sonucu verip vermediği ayrıntılı olarak incelenmelidir.

"**Bilgi Güvenliği Sürekliliği Tatbikat Planı**" iş sürekliliği testlerinin kayıt altına alınması için kullanılır. Testlerin planlanması sürecinde uygulanacak temel adımlar aşağıda ortaya konmaktadır:

5.7.2 Amaçların Belirlenmesi

Oluşturulacak olan test planının amacı ortaya çıkabilecek en olumsuz durumun kontrol edilmesi olmalıdır. Testin uygulanması için gerekli olan tüm çalışanlar belirlenmeli ve ilgili çalışanların teste tam katılımı sağlanmalıdır. Test süresinde uygulanan adımların prosedürlerde tam olarak kapsandığı her adımda kontrol edilmelidir. Testin başarısı prosedürlerin senaryoyu doğru olarak kapsamasına ve teknik bilgi seviyesi daha düşük olan çalışan tarafından uygulanabilir olmasına bağlıdır. Ayrıca testin yapılması sırasında gerçek felaket durumunda faklı olan koşulların dikkate alınması gereklidir. Testin hafta sonu yapılması buna bir örnektir.

5.7.3 Testin Sınırlarının Tanımlanması

Test sırasında uygulanacak olan senaryo ayrıntılı olarak planlanmalıdır. Testlerin karmaşıklığı kademeli olarak arttırılmalıdır. Karmaşık ve kapsamı büyük planlar ile testlere başlanması test amaçlarına ulaşılmasını engelleyecektir.

Test sırasında yapılacak olan kabullenmeler testin başlangıcında belirtilmelidir. Yedekleme teyplerinin felaket merkezinde yer aldığı kabullenmesi buna bir örnektir.

5.7.4 Test Önkoşulları

Teste başlamadan önce test içeriğinin ve konu başlıklarının özetinin dokümanda yer alması gerekmektedir. Bunlar:

- Testin amaçları
- Testin senaryosu

- Testin zamanı
- Tatbikat ekibi
- Takımların karşılaştığı sorunlar
- Testin tamamlanmasının ardından yaşanan sorunların düzeltilmesi için DF açılır.

5.8 Bilgi Güvenliği Sürekliliği Organizasyonu Üyeleri

5.8.1 Bilgi Güvenliği Sürekliliği Ekibi:

Organizasyon Lideri/ Vekili	GSM	E-posta
Tarık KABAK	0553 789 99 98	tkabak@mehmetakif.edu.tr
Ahmet Faruk YILDIRIM	0535 344 96 94	afyildirim@mehmetakif.edu.tr

5.9 Yedek Fazlalıklar

Kurum kritik hizmetleri için farklı lokasyonda yedekliliğini sağlamayı amaçlamaktadır.

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					