ZBEÜ BİLGİ İŞLEM DAİRE BAŞKANLIĞI
İŞ SÜREKLİLİĞİ YÖNETİM PROSEDÜRÜ

Revizyon Takibi:

Sıra No	Rev. No	Tarih	Hazırlayan	Revizyon Nedeni	Onaylayan	İmza
1						
2						
3						
4						

1. AMAÇ:

ZBEÜ Bilgi İşlem Daire Başkanlığı, kritik süreçlerinde yaşanabilecek kesintileri mininize etmek ve müdahale yöntemlerini belirlemeyi amaçlamaktadır.

2. KAPSAM:

Bilgi Güvenliği Yönetim Sisteminde belirlenen kurum için önem teşkil eden süreçleri kapsamaktadır.

3. SORUMLULUK:

Bu prosedürün uygulanmasından Bilgi Güvenliği Kurulu ve Daire Başkanı sorumludur.

4. TANIMLAR:

YGG: Yönetim Gözden Geçirme Toplantısı

KEVK: Kabul Edilebilir Veri Kaybı

KEKS: Kabul Edilebilir Kesinti Süresi

DF: Düzeltici Faaliyet Formu

5. UYGULAMA:

5.1 İş Sürekliliği Yönetimi

Bilgi Güvenliği Kurulu ve birim sorumluları bir araya gelerek, süreçleri ve kesintiye uğramaları durumunda etkilerinin ne olacağını ZBEÜ_FR.17.01 - İş Sürekliliği Planı ve Kritik Süreçler Listesi dokümanını inceleyerek, kritik ve kontrol altında tutulması gereken varlık ve süreçler belirlenir. Bulunan kritik varlık ve süreçler listelenir. Bilgi Güvenliği Kurulu kritik varlık ve süreçleri belirledikten sonra bu varlık ve süreçlere destek olan ilgili birim sorumluları ve tedarikçileri listeye eklenir.

Kritik varlık ve süreçler belirlendikten sonra süreklilik için önemli sistem gereksinimleri yedeklenmelidir. ZBEÜ_FR_17-01-İş Sürekliliği Planı ve Kritik Süreçler Listesi yılda en az bir kez olacak şekilde Yönetim Temsilcisi tarafından talep edilir ve güncelleme var ise gözden geçirilerek ilgili birim tarafından revize edilir. Yapılan revizyon işlemleri yıllık olarak YGG 'de değerlendirilir.

Her kritik varlık ve süreç için KEKS ve KEVK değerleri ilgili birimlerden görüş alınarak ZBEÜ_FR_10-01-İş Sürekliliği Planı ve Kritik Süreçler Listesi 'nde belirtilir.

Kritik İş Süreçleri kesintiye uğradığı zaman ulaşılacak kişi ve yapılacak ilk aksiyonlar, KEKS ve KEVK ile birlikte ZBEÜ_FR_17-01-İş Sürekliliği Planı ve Kritik Süreçler Listesi 'ne işlenir. Kesinti gerçekleştiğinde neler yapılacağı ayrıntılı olarak ZBEÜ_FR_17-01-İş Sürekliliği Planı ve Kritik Süreçler Listesi 'ndeki tanımlara uygun olarak hareket edilir.

ZBEÜ_FR_17-01-İş Sürekliliği Planı ve Kritik Süreçler Listesi 'nde süreç ve aksiyonlarda yapılması gereken değişiklikler, aksaklık veya eksiklikler Bilgi Güvenliği Kuruluna bildirilir. Bilgi Güvenliği Kurulu ilgili çalışanlarla birlikte durumu inceler ve uygun görülmesi durumunda listeyi günceller.

5.2 Sabotaj, Elektronik Saldırı, Hırsızlık Gibi Kasıt İçeren Durumların Yönetimi

Herhangi bir kasıt içeren ve bilgi varlıklarına yönelik bir sabotaj durumunun anlaşılması ile birlikte Bilgi İşlem Daire Başkanına veya Bilgi Güvenliği Kuruluna en kısa zamanda haber verilir. Olay hakkında ilgili birim yetkililerine bilgi verilir.

Bilgi İşlem Daire Başkanlığı alt yapısına saldırı olması durumunda; tüm ağlar kullanıma kapatılır ve olası yetkisiz erişimler engellenir. Bilgi Güvenliği Yönetim Temsilcisi tarafından kanıt toplama ve zarar tespit işlemleri başlatılarak Olay İhlal Prosedürü süreçleri başlatılır. Bilgi Güvenliği Yönetim Temsilcisi tüm süreçleri gizlilikle yönetir, delil toplama ve hasar tespiti tamamlandıktan sonra Bilgi İşlem Daire Başkanı'na süreçle ilgili rapor sunulur. Bilgi İşlem Daire Başkanı yasal işlemlerin başlatılıp başlatılmaması ile ilgili kararı verir. Yasal sürecin başlatılması durumunda süreç hizmet aldığımız hukuk bürosu tarafından yönetilir ve takip edilir.

Sabotajı/hırsızlığı gerçekleştiren kişi veya kişiler Bilgi İşlem Daire Başkanlığı personeli ise süreç 657 Sayılı Kanun 'un 124-136 maddelerine göre veya tabi olduğu personel kanununa göre**,** Bilgi İşlem Daire Başkanlığı personeli değil ise süreç Hukuk Müşavirliği tarafından yönetilir.

Bilgi İşlem Daire Başkanlığı bünyesinde kurumun iletişim kurması otoriteler, Destek grupları, dernekler vb. kişi ve kurumlar ile iletişim bilgileri ZBEÜ _FR.17.03 Otoriteler ve Özel İlgi Grupları ile İletişim Listesi dokümanında kayıt altına alınmaktadır. Liste içeriği her yıl en az bir kez gözden geçirilmelidir.

5.3 Tatbikatlar

İş sürekliliğinin sağlanması için kullanılan sistemlerde tatbikatlar planlanmalıdır. Bilgi Güvenliği Kurulu tarafından ZBEÜ_FR_17-04-Yıllık Tatbikat Planı hazırlanır. Hazırlanan planda yazılım ve donanım cihazlarının sürekliliğinin sağlanması göz önünde bulundurulur. Tatbikatı gerçekleştiren veya gözlemleyen kurum personeli tarafından ZBEÜ_FR_17-02-Tatbikat Raporu düzenlenir ve Bilgi İşlem Daire Başkanı tarafından kontrol edilir. Tatbikat raporlarının içeriği ve plana uygun hareket edilip edilmediği yıllık periyodlarda kontrol edilmek üzere Bilgi İşlem Daire Başkanı tarafından talep edilir, raporların içeriğinde veya yıllık planda uygunsuzluk var ise DF açılarak sorun takip edilir. Gerçekleştirilen tatbikatlar yıllık olarak YGG 'de değerlendirilir.

5.4 Sistem Sürekliliği

Bilgi İşlem personeli kritik varlık ve süreçlerinin sürekliliğin sağlanmasında yedeklilik durumları ve acil durumda nasıl hareket edileceği ZBEÜ_FR.17.01 İş Sürekliliği Planı ve Kritik Süreçler Listesi'nde belirtilir.

6. İLGİLİ DOKÜMANLAR:

ZBEÜ_FR_17-01-İş Sürekliliği Planı ve Kritik Süreçler Listesi

ZBEÜ_FR_17-02-Tatbikat Raporu

ZBEÜ_FR_17-03-Otoriteler ve Özel İlgi Grupları ile İletişim Listesi

ZBEÜ_FR_17-04-Yıllık Tatbikat Planı