BİLGİ SİSTEMLERİ SÜREKLİLİK POLİTİKASI

1. AMAÇ, KAPSAM VE YASAL DAYANAK

1.1 Amaç

Bu politika, Ostim Endüstriyel Yatırımlar ve İşletme A.Ş.'nin ("Şirket") kritik iş süreçlerini ve faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak, olası kesinti veya felaket durumlarında iş faaliyetlerinin minimum etki ile devam ettirilmesini temin etmek amacıyla hazırlanmıştır.

1.2 Kapsam

Bu politika;

- Kritik iş süreçlerini
- Bu süreçleri destekleyen bilgi sistemlerini
- Felaket kurtarma süreçlerini
- Yedekleme ve geri yükleme faaliyetlerini
- Birincil ve ikincil sistem altyapılarını
- Kriz yönetimi ve iletişim süreçlerini
- İş sürekliliği testlerini

kapsar.

1.3 Yasal Dayanak

Bu politika, SPK'nın VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Tebliği ve ilgili mevzuat hükümleri uyarınca hazırlanmıştır.

2. TANIMLAR

İş Sürekliliği: Kesinti durumunda kritik iş süreçlerinin kabul edilebilir önceden tanımlanmış seviyede devam ettirilmesi yeteneği.

İş Etki Analizi (BIA - Business Impact Analysis): Kesinti durumlarının iş üzerindeki etkilerini değerlendiren analiz.

Kritik İş Süreci: Kesintiye uğraması durumunda Şirketin operasyonlarını, mali durumunu veya itibarını önemli ölçüde etkileyen iş süreci.

Kurtarma Süresi Hedefi (RTO - Recovery Time Objective): Bir kesinti sonrasında bir sistem veya sürecin kabul edilebilir maksimum kesinti süresi.

Kurtarma Noktası Hedefi (RPO - Recovery Point Objective): Bir kesinti durumunda kabul edilebilir maksimum veri kaybı süresi.

Felaket: İş operasyonlarını önemli ölçüde etkileyen veya tehdit eden doğal veya insan kaynaklı olay.

Birincil Sistem: Normal operasyonlarda kullanılan ana bilgi sistemleri ve altyapı.

İkincil Sistem (Yedek Alan): Birincil sistemlerin kullanılamadığı durumlarda devreye alınan alternatif sistem ve altyapı.

Warm Site: Temel altyapıya sahip, kısa sürede devreye alınabilecek yedek alan.

Hot Site: Gerçek zamanlı olarak senkronize edilmiş, anında devreye alınabilecek yedek alan.

3. TEMEL PRENSİPLER

3.1 Öncelik Sıralaması

İş süreçleri kritiklik seviyelerine göre sınıflandırılır ve kaynak tahsisi buna göre yapılır.

3.2 Minimal Kesinti

Kesinti sürelerinin minimize edilmesi esastır. RTO ve RPO hedeflerine uyulur.

3.3 Proaktif Yaklaşım

Olası risklere karşı önleyici tedbirler alınır, reaktif olmak yerine proaktif hareket edilir.

3.4 Test Edilebilirlik

Planlar düzenli olarak test edilir, testler dokümante edilir ve iyileştirmeler yapılır.

3.5 Coğrafi Dağılım

Birincil ve ikincil sistemler farklı coğrafi bölgelerde konumlandırılarak aynı risklere maruz kalınması önlenir.

3.6 Sürekli İyileştirme

Test sonuçları, olay değerlendirmeleri ve değişen iş ihtiyaçları doğrultusunda planlar sürekli iyileştirilir.

4. ROL VE SORUMLULUKLAR

4.1 Yönetim Kurulu

- İş Sürekliliği ve Bilgi Sistemleri Süreklilik Politikasını onaylar
- İş sürekliliği için gerekli kaynakları sağlar
- Yıllık iş sürekliliği raporlarını değerlendirir
- Kritik kesintilerde bilgilendirilir

4.2 Üst Yönetim

- İş sürekliliği stratejisini belirler
- İş Sürekliliği Yöneticisini görevlendirir
- Kaynak tahsisini sağlar
- İş Etki Analizi sonuçlarını onaylar
- Kritik kararları alır

4.3 İş Sürekliliği Yöneticisi

- İş Sürekliliği Planının hazırlanmasını koordine eder
- İş Etki Analizi (BIA) çalışmalarını yönetir
- Test ve tatbikat planlarını hazırlar
- İyileştirme faaliyetlerini yönetir
- Üst yönetime düzenli raporlar sunar

- Kriz yönetim ekibini koordine eder

4.4 Bilgi Sistemleri Yöneticisi

- Bilgi Sistemleri Süreklilik Planını hazırlar
- Teknik kurtarma prosedürlerini oluşturur
- Yedekleme süreçlerini yönetir
- Sistem replikasyonunu sağlar
- Felaket kurtarma testlerini gerçekleştirir
- İkincil sistem altyapısını yönetir

4.5 Süreç Sahipleri

- Sorumlulukları altındaki süreçlerin kritiklik analizini yapar
- RTO ve RPO hedeflerini belirler
- Alternatif çalışma prosedürlerini geliştirir
- İş sürekliliği testlerine katılır
- Kesinti durumlarında süreç kurtarma faaliyetlerini yönetir

4.6 Kriz Yönetim Ekibi

- Kriz durumlarında toplanır
- Durum değerlendirmesi yapar
- Kararlar alır ve uygular
- İletişimi koordine eder
- Normalizasyon sürecini yönetir

5. İŞ ETKİ ANALİZİ (BIA)

5.1 BIA Süreci

5.1.1 İş Süreçlerinin Belirlenmesi

- Tüm iş süreçleri listelenir
- Süreç sahipleri belirlenir
- Süreç bağımlılıkları tanımlanır

5.1.2 Kritiklik Değerlendirmesi

Süreçler aşağıdaki kriterlere göre değerlendirilir:

- Mali etki (gelir kaybı, ceza, ek maliyet)
- Operasyonel etki (üretim durması, hizmet kesintisi)
- Yasal ve düzenleyici etki (uyumsuzluk, ceza)
- İtibar etkisi (marka değeri, müşteri güveni)
- Paydaş etkisi (çalışanlar, müşteriler, tedarikçiler)

5.1.3 Kritiklik Seviyeleri

- Kritik (1): Kesintisi 4 saat içinde ciddi olumsuz etki yaratan süreçler
- Yüksek (2): Kesintisi 24 saat içinde önemli etki yaratan süreçler
- Orta (3): Kesintisi 72 saat içinde etkileri yönetilebilir süreçler
- Düşük (4): Kesintisinin kısa vadede sınırlı etkisi olan süreçler

5.1.4 RTO ve RPO Belirlenmesi

Her kritik süreç için:

- Maksimum Tolere Edilebilir Kesinti Süresi (MTPD)
- Kurtarma Süresi Hedefi (RTO)
- Kurtarma Noktası Hedefi (RPO)
- Minimum İş Sürekliliği Hedefi (MBCO)

belirlenir.

5.1.5 Kaynak İhtiyaçları

- İnsan kaynakları
- Teknoloji kaynakları
- Tesisler ve ekipman
- Bilgi ve veriler
- Üçüncü taraf hizmetler

tanımlanır.

5.2 BIA Güncellemesi

- BIA yılda en az bir kez gözden geçirilir
- Önemli değişikliklerde (yeni süreç, sistem, yapısal değişiklik) güncellenir
- Üst yönetim tarafından onaylanır

6. KRİTİK BİLGİ SİSTEMLERİ

6.1 Kritik Sistemlerin Belirlenmesi

İş Etki Analizi sonuçlarına göre kritik iş süreçlerini destekleyen aşağıdaki sistemler kritik olarak tanımlanmıştır:

Seviye 1 - Kritik Sistemler (RTO < 4 saat)

- [Finansal Raporlama Sistemi]
- [ERP Sistemi - Finans Modülü]
- [KAP Bildirimleri Sistemi]
- [E-posta ve İletişim Sistemleri]
- [Yatırımcı İlişkileri Portalı]

Seviye 2 - Yüksek Öncelikli Sistemler (RTO < 24 saat)

- [İnsan Kaynakları Yönetim Sistemi]
- [Doküman Yönetim Sistemi]
- [Proje Yönetim Sistemi]
- [Müşteri İlişkileri Sistemi]

Seviye 3 - Orta Öncelikli Sistemler (RTO < 72 saat)

- [Destek ve Yardım Masası Sistemi]
- [Toplantı ve Takvim Sistemleri]
- [İç İletişim Platformları]

6.2 Sistem Bağımlılıkları

- Her kritik sistem için bağımlı olduğu altyapı, yazılım ve hizmetler tanımlanır
- Tek hata noktaları (single point of failure) tespit edilir ve elimine edilir
- Bağımlılık haritası oluşturulur ve güncel tutulur

7. BİLGİ SİSTEMLERİ SÜREKLİLİK PLANI

7.1 Planlama Prensipleri

7.1.1 Yedeklilik

- Kritik sistem bileşenleri yedekli olarak tasarlanır
- Birincil ve ikincil sistemler oluşturulur
- Veri replikasyonu sağlanır

7.1.2 Coğrafi Dağılım

- Birincil ve ikincil sistemler yurt içinde farklı coğrafi bölgelerde konumlandırılır
- Doğal ve çevresel felaketlere karşı birincil sistemle aynı risklere maruz kalmayacak lokasyonlar seçilir
- En az 100 km mesafe olması tercih edilir

7.1.3 Veri Senkronizasyonu

- Kritik veriler gerçek zamanlı veya RPO hedeflerine uygun sıklıkta replike edilir
- Veri bütünlüğü sürekli kontrol edilir
- Senkronizasyon hataları otomatik tespit edilir ve uyarı verilir

7.2 Yedekleme Stratejisi

7.2.1 Yedekleme Politikası

Yedekleme Sıklığı:

- Tam Yedekleme: Haftalık
- Artımlı Yedekleme: Günlük
- Kritik Veriler: RPO hedeflerine göre (saatlik veya gerçek zamanlı)
- Veritabanları: Transaction log yedekleme (15-30 dakikada bir)

Yedekleme Lokasyonları:
- Birincil Lokasyon: Aynı veri merkezinde ayrı depolama ünitesi
- İkincil Lokasyon: Farklı coğrafi bölgedeki veri merkezi
- Üçüncül Lokasyon (opsiyonel): Bulut tabanlı yedekleme

Saklama Süreleri:
- Günlük yedekler: 30 gün
- Haftalık yedekler: 3 ay
- Aylık yedekler: 1 yıl
- Yıllık yedekler: Yasal saklama sürelerine uygun

7.2.2 Yedekleme Kapsamı
- Veri tabanları
- Dosya sunucuları
- E-posta sistemleri
- Uygulama yapılandırmaları
- Sistem yapılandırmaları
- Sanal makine imajları
- Kritik dokümanlar

7.2.3 Yedekleme Testleri
- Yedeklerin geri yüklenebilirliği aylık test edilir
- Test sonuçları dokümante edilir
- Başarısız testler derhal araştırılır ve düzeltilir

7.3 İkincil Sistem Mimarisi

7.3.1 Altyapı Gereksinimleri
- İkincil sistem, kritik sistemlerin çalışması için yeterli kapasiteye sahip olmalıdır
- Ağ bağlantıları yedekli ve yüksek bant genişlikli olmalıdır
- Güç kaynakları (UPS, jeneratör) bulunmalıdır
- Soğutma ve çevre kontrol sistemleri uygun olmalıdır

7.3.2 Hot Site Yaklaşımı (Seviye 1 Sistemler)

- Gerçek zamanlı veri replikasyonu
- Sistemler yüklü ve güncel durumda (standby mode)
- Otomatik veya manuel failover mekanizması
- Hedef RTO: < 4 saat

7.3.3 Warm Site Yaklaşımı (Seviye 2-3 Sistemler)

- Günlük veri senkronizasyonu
- Temel altyapı hazır, sistemler kurulu
- Manuel devreye alma
- Hedef RTO: 24-72 saat

7.4 Kurtarma Prosedürleri

7.4.1 Felaket Türlerine Göre Kurtarma

Donanım Arızası:

1. Arızalı bileşeni tespit et
2. Yedek donanımı devreye al
3. Gerekirse yedekten geri yükle
4. Servisi restore et
5. İzleme ve doğrulama yap

Veri Merkezi Kesintisi:

1. Kesinti seviyesini değerlendir
2. Kriz yönetim ekibini topla
3. İkincil sisteme geçiş kararı al
4. Failover prosedürünü uygula
5. Servisleri ikincil sistemde başlat
6. Kullanıcılara duyuru yap
7. İzleme ve stabilizasyon sağla

Siber Saldırı (Ransomware vb.):

1. Etkilenen sistemleri izole et
2. Saldırıyı analiz et ve durdur
3. Temiz yedeklerden geri yükle
4. Güvenlik yamalarını uygula
5. Sistemleri tekrar devreye al
6. İlgili mercileri bilgilendir

Doğal Afet:

1. Personel güvenliğini sağla
2. Hasar değerlendirmesi yap
3. İkincil sisteme geçiş yap
4. Alternatif çalışma lokasyonlarını aktive et
5. Uzaktan çalışmayı aktive et

7.4.2 Kurtarma Adımları Dokümantasyonu

Her kritik sistem için:

- Adım adım kurtarma prosedürü
- Sorumlu kişiler ve iletişim bilgileri
- Gerekli araç ve gereçler
- Beklenen süreler
- Kontrol noktaları
- Geri dönüş (failback) prosedürü

oluşturulur ve güncel tutulur.

8. KRİZ YÖNETİMİ

8.1 Kriz Yönetim Ekibi

Ekip Yapısı:

- Kriz Yöneticisi: Genel Müdür
- Teknik Koordinatör: Bilgi Sistemleri Sorumlusu
- İletişim Sorumlusu: Bilgi Sistemleri Yöneticisi
- Yasal Danışman: Hukuk Müşaviri / Avukat
- Bilgi Güvenliği Sorumlusu

8.2 Kriz İletişim Planı

8.2.1 İç İletişim

- Çalışanlara durum güncellenmesi
- Alternatif iletişim kanalları (SMS, kişisel e-posta)
- Bilgilendirme sıklığı

8.2.2 Dış İletişim

- Yönetim kurulu bilgilendirmesi
- SPK bildirimleri (gerektiğinde)
- KAP duyuruları (gerektiğinde)
- Müşteri ve paydaş bilgilendirmesi

- Medya iletişimi (kritik durumlarda)

8.2.3 İletişim Şablonları

- Olağanüstü durum bildirimi
- Durum güncelleme e-postası
- Normalleşme bildirimi
- KAP bildirimi şablonu (gerektiğinde)

8.3 Karar Verme Mekanizması

Devreye Alma Kriterleri:

- Kesinti süresi tahminleri
- Etkilenen sistem kritikliği
- İş etkisi büyüklüğü
- Alternatif çözüm olasılıkları

Devreye Alma Yetkileri:

- Seviye 1 sistemler: Genel Müdür onayı
- Seviye 2-3 sistemler: Bilgi Sistemleri Sorumlusu onayı
- Acil durumlar: Bilgi Sistemleri Yöneticisi inisiyatifi, sonrasında bilgilendirme

9. TEST VE TATBİKATLAR

9.1 Test Programı

9.1.1 Test Türleri

Masa başı Testler:

- Sıklık: Yılda bir
- Amaç: Planları gözden geçirme, rol netleştirme
- Katılımcılar: Kriz yönetim ekibi, süreç sahipleri
- Süre: 2-4 saat

Teknik Testler:

- Yedekleme-geri yükleme testi: Aylık
- Failover testi: 6 ayda bir
- Tam felaket kurtarma testi: Yılda bir
- Sistem replikasyon testi: 3 ayda bir

Fonksiyonel Testler:

- Alternatif çalışma lokasyonu testi: Yılda bir

- İletişim planı testi: 6 ayda bir
- Personel hazırlık testi: Yılda bir

Tam Kapsamlı Tatbikat:
- Sıklık: Yılda bir kez
- Tüm planların entegre testi
- Gerçek senaryoya yakın simülasyon
- Tüm ekiplerin katılımı

9.1.2 Test Senaryoları
- Veri merkezi yangını
- Uzun süreli elektrik kesintisi
- Siber saldırı (ransomware)
- Donanım arızası
- Deprem
- Anahtar personel kaybı
- Tedarikçi kesintisi

9.2 Test Dokümantasyonu
Test Planı:
- Test tarihi ve saati
- Test türü ve senaryosu
- Katılımcılar
- Test kapsamı
- Başarı kriterleri
- Risk değerlendirmesi

Test Raporu:
- Test özeti
- Gözlemler
- Başarılı/başarısız kontrol noktaları
- Tespit edilen sorunlar
- İyileştirme önerileri
- Aksiyon planı

9.3 İyileştirme Süreci

- Test sonuçları analiz edilir
- Aksiyon maddeleri belirlenir
- Sorumlular atanır
- Takip edilir ve kapatılır
- Planlar güncellenir

10. SÜRDÜRME VE GÜNCELLEME

10.1 Plan Bakımı

Düzenli Gözden Geçirme:

- Yılda en az bir kez komple gözden geçirme
- Test sonrası güncelleme
- Değişiklik sonrası güncelleme

Güncellemeyi Tetikleyen Durumlar:

- Yeni kritik sistem devreye alınması
- Organizasyon yapısı değişikliği
- Anahtar personel değişikliği
- Lokasyon değişikliği
- Altyapı değişikliği
- Tedarikçi değişikliği
- Yaşanan olay sonrası dersler

10.2 Versiyon Kontrolü

- Tüm değişiklikler kayıt altına alınır
- Versiyon numaraları güncellenir
- Değişiklik geçmişi tutulur
- Güncel versiyonlar dağıtılır
- Eski versiyonlar arşivlenir

10.3 Dağıtım ve Erişim

- Güncel planlar güvenli bir şekilde saklanır
- Yetkili kişiler erişebilir
- Fiziksel ve elektronik kopyalar mevcuttur
- Uzaktan erişim sağlanır
- Yedek kopyalar farklı lokasyonlarda bulunur

11. EĞİTİM VE FARKINDALIK

11.1 Eğitim Programı

Genel Farkındalık Eğitimi:

- Hedef: Tüm çalışanlar
- Sıklık: Yılda bir, yeni işe başlayanlara hemen
- İçerik: İş sürekliliği temelleri, roller, acil durum prosedürleri

Kritik Personel Eğitimi:

- Hedef: Kriz yönetim ekibi, süreç sahipleri, teknik ekip
- Sıklık: 6 ayda bir
- İçerik: Detaylı planlar, sorumluluklar, teknik prosedürler

Senaryo Bazlı Eğitim:

- Simülasyonlarla uygulamalı öğrenme
- Karar verme egzersizleri
- Stres yönetimi

11.2 Dokümantasyon

- Eğitim materyalleri hazırlanır
- Eğitim kayıtları tutulur
- Katılım takip edilir
- Etkinlik değerlendirmesi yapılır

12. RAPORLAMA VE GÖZETİM

12.1 Periyodik Raporlama

Yönetim Kuruluna Yıllık Rapor:

- İş sürekliliği hazırlık durumu
- Test sonuçları özeti
- Yaşanan olaylar ve müdahaleler
- İyileştirme faaliyetleri
- Yatırım ihtiyaçları

Üst Yönetime Altı Aylık Rapor:

- Test ve tatbikat sonuçları
- Aksiyon maddelerinin durumu
- Risk değişiklikleri

- Plan güncellemeleri

12.2 Olay Sonrası Değerlendirme

- Her gerçek kesinti sonrası değerlendirme yapılır
- Edinilen Tecrübe (Lessons Learned) dokümanı hazırlanır
- İyileştirmeler planlanır ve uygulanır

13. İLGİLİ DOKÜMANLAR

- Bilgi Güvenliği Politikası
- Olay Yönetimi Politikası
- Yedekleme ve Geri Yükleme Prosedürü
- Felaket Kurtarma Prosedürü
- Kriz İletişim Planı
- Teknik Kurtarma Prosedürleri (sistem bazında)
- İş Etki Analizi Raporu
- Test Planları ve Raporları

Bu politika, SPK'nın VII128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Tebliği uyarınca hazırlanmış Yönetim Kurulu'nun 16.12.2025 tarihli toplantısında kabul edilmiştir.