FELAKET KURTARMA PLANI

1. Amaç

Felaket Kurtarma Planı olası tüm kesintileri ve felaketleri öngörmek, bu kesintilerin iş etkilerini belirlemek ve kesinti halinde yapılacakları koordine edecek zemini hazırlamak üzere düzenlenmiştir.

Bu planın hedefi;

- Tüm hizmetler için olası en yüksek servis seviyelerini korumak,
- Felaket anında öngörülen kesinti süreleri içerisinde iş süreçlerini yeniden çalışır hale getirmek,
- Kesintilerin olasılığını ve olumsuz etkisini minimize etmektir.

2. Kapsam

Felaket Kurtarma Planı operasyon verimliliğini ve sürekliliğini sağlayacak şekilde yapılandırılmıştır.

- Hizmetteki aksamaların iş birimleri üzerindeki potansiyel etkileri gözden geçirilip hizmet sürekliliğini sağlayacak şekilde kurtarma planları,
- Şirket çalışanlarının Felaket Kurtarma Planı çerçevesindeki rol ve sorumlulukları,
- Yapılan test ve tatbikatların sonuçları.

3. Tanımlar

- **İş Sürekliliği:** Şirketin operasyonlarına önceden belirlenmiş kabul edilebilir bir seviyede devamını sağlamak üzere, gelişen olaylara ve iş süreçlerindeki aksamalara karşı stratejik ve taktik planlama ve tepki verme yeteneğidir.
- **Felaket Kurtarma Planı:** Gerek olduğu takdirde bir organizasyonun kritik eylemelerine önceden belirlenmiş kabul edilebilir bir seviyede devam edebilmesi için geliştirilmiş, derlenmiş, kullanıma hazır ve dokümante edilmiş bir şekilde tutulan süreçler ve bilgi bütünüdür.
- **İş Etki Analizi (İEA):** İş fonksiyonlarını ve olası bir aksamanın bunlar üzerindeki etkilerinin analiz sürecidir.
- **Tatbikat:** İş sürekliliği planlarının uygun bilgiyi içerdiklerinden ve uygulandıklarında istenen sonucu doğurduklarından emin olmak üzere yapılan kısmi veya tam prova aktiviteleridir.

4. Uygulama

4.1 İş Etki Analizi

İş etki analizi çalışması ile AKFEN'in kritik iş süreçleri, bu süreçleri etkileyebilecek tehditler ve süreçlerin kesintiye uğraması durumunda kurumun göreceği zarar belirlenir. Kurumun iş süreçleri için kabul edilebilir kesinti süreleri (RTO-Recovery Time Objective) süreç sahipleri veya atadıkları temsilciler ile görüşülerek kararlaştırılır. Kurumun iş süreçleri bu değerler doğrultusunda önceliklendirilir. Bir sonraki adım olarak iş süreçlerini

destekleyen BT servisleri belirlenir. BT servisleri için de belirlenmiş kabul edilebilir kesinti süreleri servisin desteklediği iş süreci dikkate alınarak belirlenir.

Bu adım kapsamında yapılacak işlerin özeti aşağıdaki gibidir:

- İş süreçlerinde gerçekleşebilecek kesintinin kuruma olan etkisinin iş etki analizine göre belirlenmesi,
- Her bir süreç için kabul edilebilir kesinti sürelerinin hesaplanması,
- İş etki analizine göre iş süreçlerinin önceliklendirilmesi,
- Süreçleri destekleyen BT servislerinin ve bileşenlerinin belirlenmesi,
- Her bir BT servisi ve bileşeni için kabul edilebilir kesinti sürelerinin belirlenmesi. Sistemlerin felaket anında bir gün, bir hafta ve otuz gün içerisinde çalıştırılması gereken sistemler olarak sınıflandırılması. Aşağıda öncelik durumuna göre sınıflandırılmış AKFEN bünyesindeki sistemlerin öncelik listesi yılda bir kere olmak üzere gözden Bilgi Güvenliği Koordinasyon Kurulu tarafından gözden geçirilmesi ve gerekirse güncellenmesi.

  Felaket Anında Bir Gün İçinde Çalıştırılması Gereken Sistemler

  - Active Directory
  - Veri Tabanı Sunucu
  - Uygulama Sunucu
  - Muhasebe Yazılımı
  - İnternet Erişimi Mail Sunucu
  - İnsan Kaynakları Sistemi

  Felaket Anında Bir Hafta İçinde Çalıştırılması Gereken Sistemler

  - Antivirüs ve Windows Güncelleme Sunucu
  - Doküman Yönetim Sistemi
  - SSL-VPN sistemi

  Felaket Anında Otuz Gün İçinde Çalıştırılması Gereken Sistemler

  - Ağ izleme sistemi
  - Arşiv sistemi
- Mevcut teknolojik altyapının belirlenen kabul edilebilir kesinti süresi değerlerini sağlamada eksik kalan yanlarının tespit edilmesi ve teknolojik yatırım gereken alanların belirlenmesi,

İş etki analizinin yapılması Bilgi Güvenliği Koordinasyon Kurulu'nun görevidir.

4.2 Felaket Senaryoları Müdahale Planı

Risk	Sistem Odasına Girilemiyor Olması	Enerji Kesintisi
Olası Senaryo	Yangın, Deprem	Kesintisiz güç kaynağı arızası, Jeneratör arızası
Olasılık	Düşük	Düşük
Etki Düzeyi	Yüksek	Yüksek
Etkilenen İşlevler	Sunuculardan hizmet alan tüm BT altyapısı	Tüm BT servisleri
Aksiyon Planı	• Tüm canlılar güvenlik amacıyla sistem odasından uzaklaştırılır. • Yangın sebebiyle giriş yapılamıyorsa itfaiye aranır. • Deprem sebebiyle giriş yapılamıyorsa itfaiye veya kurtarma ekipleri aranır. Sistem odasına giriş mümkün olduğunda zarar araştırması Hasar Tespit Takımı tarafından yapılır.	• Sorun AKFEN merkez bina bakım biriminin ilgili personeline bildirilir ve çözüm süreci takip edilir. • Mekanik İşler tarafından arızanın giderilmesi sağlanır. • Arızanın giderilmesi müteakip tüm sistemlerin çalışabilirliği sistemle ilgili Birimler/Gruplar tarafından kontrol edilir.
Sorumluluklar	AKFEN Güvenlik Ekibi	Bina Bakım/Mekanik Ekibi, Bilgi İşlem Müdürü
Önleyici Faaliyet	Yangın Söndürme sistemleri	Yedek UPS, Jeneratör bakımları
Kaynaklar	Personel, mobil telefon	Jeneratör, UPS uniteleri, İnsan kaynağı

Risk	Doğal Afetler ve Sabotaj	Ağ Hizmetleri Kesintisi
Olası Senaryo	Yangın, Deprem	LAN, WAN arızaları
Olasılık	Düşük	Düşük
Etki Düzeyi	Çok Yüksek	Yüksek
Etkilenen İşlevler	Tüm İşlevler	Ağla ilişkili tüm sistem ve süreçler
Aksiyon Planı	• İlgili kurumlarla (İtfaiye, emniyet vb.) ile iletişime geçilir. • Doğal afet veya sabotajla ilgili hasar tespiti yapılır. • Sistemlerin çalışabilirliği test edilir. • Çalışmayan sistem varsa yedek sistem üzerinde çalışması sağlanır. Bilgilerin tamlık ve doğruluk kontrolü yapılır.	• Ağ sistemlerine arıza bildirimi yapılır. • Arızanın tipine göre arıza network personeli tarafından veya servis sağlayıcı tarafından giderilir. • Sorunun giderilmesine müteakip ilgili tüm birimlere arızanın giderildiği bilgisi verilir. • Arızanın kök sebebinin bulunup düzeltici faaliyetin gerçekleştirilmesi sağlanır.
Sorumluluklar	AKFEN Güvenlik Ekibi	Bilgi İşlem Müdürü arızanın giderilmesinden sorumludur
Önleyici Faaliyet	Yangın Söndürme sistemleri, Fiziksel güvenlik önlemleri	İzleme, yedekli çalışma
Kaynaklar	Personel, telefon, yedek medyalar, donanım	Ağ cihazları, elektronik posta iletişimi

Risk	Sunucu Hizmetleri Kesintisi	Virüs Saldırısı / Güvenlik İhlali
Olası Senaryo	Donanım arızası, Veritabanı sorunları, uygulama sunucu sorunları	Virüs saldırısı, Bilgiyi ele geçirmeye çalışma
Olasılık	Orta	Düşük
Etki Düzeyi	Yüksek	Yüksek
Etkilenen İşlevler	J-guar, QlikView, ve diğer ilgili sistemler	Tüm İşlevler
Aksiyon Planı	• Bilgi İşlem Müdürlüğü'ne sorun iletilir. Bilgi İşlem Müdürü tarafından sorun tespiti ve arıza giderimi yapılır. • İlgili birimler tarafından sistemin çalışılırlığı kontrol edilir. • Yaşanan sorunun kök sebebinin bulunup gerekli durumlarda düzeltici faaliyetin gerçekleştirilmesi sağlanır.	• İhlali, saldırıyı fark kişi ya da birimlerin durumu Bilgi İletişim Müdürü'ne bildirir. • Bilgi İşlem Müdürü ekibi ile olayın tespit ve analizinin yapılarak hızlıca gerekli önlemlerin alınmasını temin eder. • Virüs saldırısı var ise mevcut antivirüs programının ilgili virüse karşı korumasının olup olmadığı tespit edilir. Virüs koruması yoksa üretici firmayla iletişime geçilir ve hızlı yama çıkarılması için gerekli çalışmaların yapılması sağlanır. • Gerekli durumlarda güvenlik ihlalini, saldırıyı gerçekleştirenler için adli ve yasal girişimlerde bulunulur. • İhlalin kök sebebinin bulunup düzeltici faaliyetin gerçekleştirilmesi sağlanır.
Sorumluluklar	Etkilenen sistem kullanıcıları, Bilgi İşlem Müdürü	Tüm personel ve Bilgi İşlem Takımı
Önleyici Faaliyet	Sunucu izleme programı, disk ve sunucu donanım yedeklemesi, uygulama sunucu yedeklemesi, ağ cihazları yedeklemesi, enerji yedekliliği	Erişim kontrolü, Endpoint koruma mekanizmaları (antivirüs, host ips, firewall), Ağ ve güvenlik cihazları
Kaynaklar	Donanım ve teçhizat, İnsan Kaynağı	Ağ ve güvenlik cihazları, antivirüs programı

5. Test ve Tatbikatlar

Kurumun iş sürekliliği ve olay yönetimi düzenlemeleri tatbikatlarla denenmedikçe ve güncel tutulmadıkça güvenilir addedilemez. Tatbikatlar olay anında yaşamsal önemde olan ekip çalışması, uyum, güven ve bilginin geliştirilmesi için zorunludur.
Düzenlemeler tatbikatlarla test edilmeli, denetim ve iç değerlendirme süreçleri düzenlemelerin amaca uygun olduğunu teyit etmelidir.
Bu nedenle Bilgi Güvenliği Koordinasyon Kurulu planın yapılmasını koordine eder. Bu kapsamda Bilgi İşlem Müdürü'nün hazırladığı yıllık tatbikat planlarını gözden geçirmek ve onaylamak ile görevlidir.

Felaket Kurtarma Planının test edilmesiyle amaçlananlar aşağıdaki gibidir:

- Planın etkinliğinin belirlenmesi,
- Hazırlık durumunun ve belirlenen ilgili kişilerin kendilerine atanan kurtarma sorumluluklarını yerine getirebilirliklerinin belirlenmesi,

- Kabul edilebilir kesinti süresi zamanları içerisinde kurtarmanın sağlanabildiği ve kullanıcılar tarafından kabul edildiğinden emin olmak için Felaket Kurtarma Planında değişiklik veya güncellemeye ihtiyaç olup olmadığının belirlenmesi.

6. Tatbikat/Test Sonuçlarının Değerlendirilmesi

Bilgi İşlem Müdürü test ve tatbikat sonuçlarının analiz edilerek planın gözden geçirilmesi ve güncellenmesini koordine etmekle görevlidir.

Bilgi İşlem Müdürü tatbikat sonrasında test sonuçlarını dokümante edecek şekilde çalışmalar yapar. Eksikleri ve problemli konuları belirlemek için Bilgi İşlem Müdürü test/tatbikat sonuçlarını Bilgi Güvenliği Koordinasyon Kurulu ile birlikte yapılacak bir toplantı ile gözden geçirir. Toplantı sonucunda oluşacak kanaatlere göre planın eksik kısımlarının düzeltilerek güncellenmesi sağlanır.