EK-E

İÇİNDEKİLER

EK-E 1

EKLER İÇİN VAKA ÇALIŞMASI: "DİRENÇLİ OSB" PROFİLİ 5

1. Genel Kurumsal Bilgiler 6

2. Coğrafi Konum ve Risk Bağlamı 6

3. OSB Yönetimi Tarafından Sunulan Kritik Hizmetler 6

4. Yönetim Sistemleri Durumu 7

5. Mevcut İSYS'nin Durumu 7

EK E.1: OSB'LER İÇİN ÖRNEK OLAY YÖNETİM ORGANİZASYON YAPILARI, ROLLERİ VE SORUMLULUKLARI 9

E.1.1 Giriş 10

E.1.2 Bütünleşik Olay Yönetim Hiyerarşisi ve Raporlama Akışı 10

E.1.3 "Dirençli OSB" İçin Örnek Olay Yönetim Organizasyon Yapısı 10

E.1.4 "Dirençli OSB" Olay Yönetim Ekipleri: Roller, Sorumluluklar ve Yetkinlikler 11

E.1.4 Rollerin Kişilere Atanması ve İletişim Listeleri 11

E.1.5 Diğer OSB'ler İçin Genel Modeller 12

EK E.2.1: "DİRENÇLİ OSB" İÇİN TAMAMLANMIŞ İŞ SÜREKLİLİĞİ PLANI (1) (ÖRNEK: KRİTİK İDARİ VE KOORDİNASYON FAALİYETLERİ) 14

0. YÖNETİCİ ÖZETİ 16

BÖLÜM 1: PLAN YÖNETİŞİMİ 17

BÖLÜM 2: İŞ SÜREKLİLİĞİ ORGANİZASYONU & KOMUTA YAPISI 18

BÖLÜM 3: ANALİTİK TEMEL ÖZETİ 19

BÖLÜM 4: İŞ SÜREKLİLİĞİ STRATEJİLERİ VE ÇÖZÜMLERİ 20

BÖLÜM 5: AKTİVASYON VE OLAY YÖNETİM PROSEDÜRLERİ 23

BÖLÜM 6: İŞ KURTARMA PROSEDÜRLERİ (Kontrol Listesi Formatında) 28

BÖLÜM 7: PLANIN SÜRDÜRÜLEBİLİRLİĞİ (PUKÖ) 33

BÖLÜM 8: EKLER 34

EK E.2.2: "DİRENÇLİ OSB" İÇİN TAMAMLANMIŞ İŞ SÜREKLİLİĞİ PLANI (2) (ÖRNEK: ELEKTRİK DAĞITIMI VE BAKIM HİZMETİ) 46

0. YÖNETİCİ ÖZETİ 48

BÖLÜM 1: PLAN YÖNETİŞİMİ 49

BÖLÜM 2: İŞ SÜREKLİLİĞİ ORGANİZASYONU & KOMUTA YAPISI 50

BÖLÜM 3: ANALİTİK TEMEL ÖZETİ 51

BÖLÜM 4: İŞ SÜREKLİLİĞİ STRATEJİLERİ VE ÇÖZÜMLERİ 53

BÖLÜM 5: AKTİVASYON VE OLAY YÖNETİM PROSEDÜRLERİ 55

BÖLÜM 6: İŞ KURTARMA PROSEDÜRLERİ (KONTROL LİSTELERİ) 60

BÖLÜM 7: PLAN SÜRDÜRÜLEBİLİRLİĞİ (PUKÖ) 64

BÖLÜM 8: EKLER LİSTESİ 66

EK E.3.1: "DİRENÇLİ OSB" İÇİN TAMAMLANMIŞ BT FELAKET KURTARMA (İŞ SÜREKLİLİĞİ) PLANI 73

0. YÖNETİCİ ÖZETİ 74

BÖLÜM 1: GİRİŞ 75

BÖLÜM 2: ORGANİZASYON (BT KURTARMA EKİBİ) 76

BÖLÜM 3: AKTİVASYON VE ÖNCELİKLER 77

BÖLÜM 4: DETAYLI KURTARMA PROSEDÜRLERİ (FAZLARA GÖRE) 80

BÖLÜM 5: NORMALE DÖNÜŞ PROSEDÜRLERİ 84

BÖLÜM 6: PLANIN SÜRDÜRÜLEBİLİRLİĞİ (PUKÖ) 85

PLAN EKLERİ LİSTESİ 87

EK E.3.2: "DİRENÇLİ OSB" İÇİN SİBER OLAYLARA MÜDAHALE PLANI 98

BÖLÜM 1: GİRİŞ VE STRATEJİK ÇERÇEVE 100

BÖLÜM 2: ORGANİZASYON VE ROLLER 101

BÖLÜM 3: OLAY SINIFLANDIRMASI VE AKTİVASYON 102

BÖLÜM 4: OLAY MÜDAHALE SÜRECİ (SANS / PICERL MODELİ) 103

BÖLÜM 5: SENARYO BAZLI EYLEM PLANLARI (PLAYBOOKS) 105

BÖLÜM 6: PLANIN SÜRDÜRÜLEBİLİRLİĞİ (PUKÖ) 107

BÖLÜM 7: EKLER (Siber Odaklı) 107

EKLER İÇİN VAKA ÇALIŞMASI: "DİRENÇLİ OSB" PROFİLİ

ÖNEMLİ NOT: *Bu kılavuzun eklerinde yer alan tüm doldurulmuş şablonlar, dokümanlar ve örnekler, aşağıda özellikleri tanımlanan varsayımsal* ***"Dirençli Organize Sanayi Bölgesi (Dirençli OSB)"*** *senaryosu üzerinden hazırlanmıştır.*

Bu yaklaşımın amacı, İş Sürekliliği Yönetim Sistemi (İSYS) kurulumunun her aşamasında üretilen dokümanların birbirleriyle nasıl ilişkilendirildiğini ve teorik bilgilerin pratik bir OSB ortamına nasıl uyarlandığını somut bir şekilde göstermektir. Kullanıcıların, buradaki örnekleri kendi OSB'lerinin büyüklüğüne, sektörüne ve risk profiline göre uyarlamaları gerekmektedir.

DİRENÇLİ OSB KURUMSAL PROFİLİ

1. Genel Kurumsal Bilgiler

- **OSB Adı:** Dirençli Organize Sanayi Bölgesi (Kısaca "Dirençli OSB")
- **Türü:** Karma Organize Sanayi Bölgesi (Farklı sektörlerden çeşitli büyüklükte firmalara ev sahipliği yapmaktadır).
- **Hukuki Durum:** 4562 Sayılı OSB Kanunu'na göre kurulmuş Özel Hukuk Tüzel Kişiliği.
- **Büyüklük ve Kapasite:**
  - **Toplam Alan:** Yaklaşık 650 Hektar.
  - **Toplam Sanayi Parseli Sayısı:** Yaklaşık 180 adet.
  - **Faal Katılımcı Firma Sayısı:** Yaklaşık 150 adet.
  - **Sektörel Dağılım:** Metal işleme, makine imalatı, otomotiv yan sanayi, kimya, gıda ve ambalaj sektörleri ağırlıklı.
  - **Toplam Çalışan Sayısı (Katılımcılar Dahil):** Yaklaşık 18.000 kişi.
  - **OSB Yönetim Personeli Sayısı:** Yaklaşık 60 kişi (teknik, idari, güvenlik vb.).

2. Coğrafi Konum ve Risk Bağlamı

- **Konum:** Marmara Bölgesi'nde, önemli bir sanayi ve ticaret merkezine yakın konumdadır.
- **Lojistik Bağlantılar:** Ana karayolu ve demiryolu ağlarına erişimi vardır; yakınında uluslararası bir liman bulunmaktadır.
- **Çevresel ve Doğal Riskler:**
  - **Deprem:** 1. Derece Deprem Bölgesi'ne yakın bir lokasyondadır ve aktif fay hatlarından etkilenme potansiyeli bulunmaktadır.
  - **Sel/Taşkın:** OSB'nin bir kısmından geçen küçük bir dere yatağı ve şiddetli yağışlar nedeniyle, özellikle alçak kotlardaki parseller ve altyapı için kısmi sel ve taşkın riski mevcuttur.
  - **Meteorolojik Riskler:** Şiddetli rüzgar ve fırtına, kış aylarında yoğun kar yağışı ve buzlanma potansiyeli vardır.
- **Endüstriyel Riskler:** Karma OSB yapısı nedeniyle yangın, patlama ve kimyasal sızıntı riskleri mevcuttur; bölge içinde BEKRA (Büyük Endüstriyel Kazaların Önlenmesi) kapsamında değerlendirilen tesisler bulunmaktadır.

3. OSB Yönetimi Tarafından Sunulan Kritik Hizmetler

İş Sürekliliği Yönetim Sistemi (İSYS) kapsamına alınan temel hizmetler şunlardır:

- **Elektrik Dağıtımı:** Orta Gerilim (OG) ve Alçak Gerilim (AG) şebeke işletimi.
- **Su Temini:** Kullanma ve Proses suyu temini ve dağıtımı.

- **Atık Su Yönetimi:** Endüstriyel ve evsel atıksu toplama ve Merkezi Atık Su Arıtma Tesisi (AAT) işletimi.
- **Doğalgaz:** Basınç düşürme ve dağıtım hizmetleri.
- **Ulaşım:** OSB içi yol ağı bakımı ve erişim yönetimi.
- **Güvenlik:** 7/24 giriş-çıkış kontrolü, devriye ve CCTV izleme içeren fiziki güvenlik hizmetleri.
- **İdari Hizmetler:** Ruhsatlandırma, katılımcı ilişkileri ve mali işler.
- **BT Altyapısı:** OSB Yönetimi için temel BT ve haberleşme altyapısı desteği.
- **Atık Yönetimi:** Katı atık yönetimi koordinasyonu ve Geçici Depolama Alanı işletimi.
- **Acil Müdahale:** OSB bünyesindeki İtfaiye Teşkilatı ile ilk müdahale hizmetleri.

4. Yönetim Sistemleri Durumu

OSB yönetimi halihazırda aşağıdaki standartları uygulamaktadır:

- **ISO 9001:2015** Kalite Yönetim Sistemi (Sertifikalı).
- **ISO 14001:2015** Çevre Yönetim Sistemi (Sertifikalı).
- **ISO 45001:2018** İş Sağlığı ve Güvenliği Yönetim Sistemi (Uygulama aşamasında, belgelendirme süreci devam ediyor).

5. Mevcut İSYS'nin Durumu

"Dirençli OSB", ISO 22301 standardına uyumlu bir İSYS kurma kararı almıştır. Kılavuzun "Bölüm 0: Temel Oluşturma ve Planlama" aşaması (Politika, Kapsam, Bağlam Analizi) tamamlanmış ve onaylanmıştır. Şu anda "Bölüm 1: İş Etki Analizi" çalışmaları yürütülmektedir.

EK-E: Vaka Çalışması için Planlar

Ek E.1: OSB'ler İçin Örnek Olay Yönetim Organizasyon Yapıları, Rolleri ve Sorumlulukları

OSB'ler İçin Örnek Olay Yönetim Organizasyon Yapıları, Rolleri ve Sorumlulukları

E.1.1 Giriş

*Bir kesinti veya kriz anında etkin bir müdahale ve kurtarma süreci, önceden tanımlanmış, net ve tüm personel tarafından iyi anlaşılmış bir organizasyon yapısına bağlıdır. Bu ek bölümün amacı, OSB'lerin, bir olay anında devreye girecek olan **Bütünleşik Olay Yönetim Yapısı**'nı nasıl kurgulayabileceklerine dair pratik örnekler, detaylı rol tanımları ve görsel şemalar sunmaktır. Bu yapı, ISO 22301 Madde 8.4.2'de istenen "müdahale yapısı"nın temelini oluşturur.*

E.1.2 Bütünleşik Olay Yönetim Hiyerarşisi ve Raporlama Akışı

Etkili bir olay yönetimi, genellikle üç temel seviyede (Stratejik, Taktiksel, Operasyonel) yürütülen faaliyetlerden oluşur. Bu seviyeler arasındaki hiyerarşi ve temel raporlama akışı şu şekildedir:

- **Stratejik Seviye (Kriz Yönetim Ekibi - KYE):** En üst karar alma merciidir. Olayın genel stratejik gidişatını belirler.
- **Taktiksel Seviye (Olay Koordinasyon Ekibi - OKE):** KYE'ye düzenli durum raporları sunar ve KYE'den aldığı stratejik yönlendirmeleri operasyonel seviyeye iletir. Operasyonel ekiplerin faaliyetlerini koordine eder.
- **Operasyonel Seviye (Acil Durum Müdahale Ekipleri - ADME ve İş Sürekliliği Ekipleri - İSE):** Sahada fiili müdahale ve kurtarma faaliyetlerini yürütürler. Kendi faaliyetlerine ilişkin durum güncellemelerini ve kaynak taleplerini OKE'ye raporlarlar.

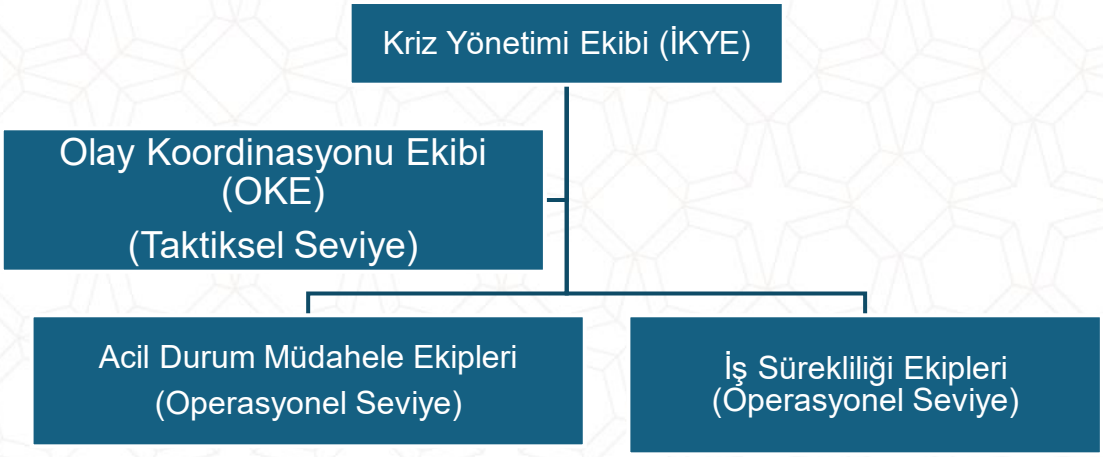
E.1.3 "Dirençli OSB" İçin Örnek Olay Yönetim Organizasyon Yapısı

Aşağıda, "Dirençli OSB" gibi orta-büyük ölçekli bir OSB için uyarlanmış olay yönetim yapısı açıklanmıştır.

- "Dirençli OSB" olay yönetim yapısı üç seviyeden oluşur. **Stratejik Seviye**'de, OSB'nin üst yönetiminden oluşan **Kriz Yönetim Ekibi (KYE)** bulunur. **Taktiksel Seviye**'de, KYE'ye doğrudan bağlı olan ve ondan stratejik yönlendirmeler alan bir **Olay Koordinasyon Ekibi (OKE)** yer alır. **Operasyonel Seviye** ise OKE'nin altında konumlanmış iki ana ekip grubundan oluşur: **Acil Durum Müdahale Ekipleri (ADME) (İtfaiye, Güvenlik, Sağlık)** ve **İş Sürekliliği ve Kurtarma Ekipleri (İSE)**. Hem ADME hem de İSE, kendi faaliyetleri hakkında OKE'ye raporlama yapar ve taktiksel koordinasyon talimatlarını OKE'den alır.

Dirençli OSB – Olay Yönetim Yapısı

(Orta Ölçekli OSB Modeli)



E.1.4 "Dirençli OSB" Olay Yönetim Ekipleri: Roller, Sorumluluklar ve Yetkinlikler

Bu bölümde, yukarıdaki şemada yer alan her bir ekibin ve bu ekipler içindeki anahtar rollerin görev, sorumluluk ve beklenen yetkinlikleri, genel olarak açıklanmaktadır.

E.1.4 Rollerin Kişilere Atanması ve İletişim Listeleri

Yukarıda tanımlanan **roller**, planların ve prosedürlerin ana metninde yer alır. Bu rollere atanacak **kişilerin isimleri, birincil ve yedek olarak görevlendirmeleri ve detaylı iletişim bilgileri (cep telefonu, e-posta vb.)** ise, her bir planın **Ekler** bölümünde yer alan ve kolayca güncellenebilen "İletişim Listeleri"nde tutulmalıdır. Bu yaklaşım, personel değişikliklerinde tüm planı revize etme zorunluluğunu ortadan kaldırarak planların güncel kalmasını kolaylaştırır.

E.1.4.1 Kriz Yönetim Ekibi (KYE) - Stratejik Seviye

- **Genel Sorumluluk:** Olayın OSB üzerindeki genel stratejik etkilerini yönetir, kurumsal itibarı korur ve OSB'nin uzun vadeli hedeflerini güvence altına alacak kararları verir.
- **Örnek Roller ve Detaylı Görevler:**
  - **Kriz Yöneticisi (Lider - Genellikle Bölge Müdürü):**
    - *Sorumlulukları:* Ekibe liderlik eder, nihai stratejik kararları verir, üst yönetim ve yönetim kurulu ile doğrudan iletişimi sağlar.
    - *Gerekli Yetkinlikler:* Liderlik, stres altında karar verme, stratejik düşünme.
  - **Operasyonlar Sorumlusu (Teknikten Sorumlu Bölge Müd. Yrd.):**
    - *Sorumlulukları:* Taktiksel seviyedeki OKE ile ana bağlantıyı kurar, sahadaki operasyonların stratejik hedeflerle uyumunu denetler.
    - *Gerekli Yetkinlikler:* OSB operasyonlarına hakimiyet, teknik bilgi, koordinasyon.
  - **Finans ve İdari İşler Sorumlusu (İdari ve Mali İşler Müdürü):**

- ❑ *Sorumlulukları:* Acil durum harcama yetkilerini yönetir, sigorta süreçlerini başlatır, olayın finansal etkilerini takip eder.
- ❑ *Gerekli Yetkinlikler:* Finansal yönetim, bütçeleme, sigorta süreçleri bilgisi.

▪ **Kurumsal İletişim Sorumlusu / Sözcü:**

- ❑ *Sorumlulukları:* Kriz İletişim Planı'nı yönetir, medya ve diğer dış paydaşlara yönelik tüm açıklamaları koordine eder ve yapar.
- ❑ *Gerekli Yetkinlikler:* Medya ilişkileri, halkla ilişkiler, etkili iletişim becerileri.

E.1.4.2 Olay Koordinasyon Ekibi (OKE) - Taktiksel Seviye

- **Genel Sorumluluk:** Farklı operasyonel ekiplerin faaliyetlerini koordine eder, kaynakları önceliklendirir, bilgi akışını yönetir ve KYE'ye düzenli durum raporları sunar.
- **Örnek Roller ve Detaylı Görevler:**
  - **Olay Koordinatörü (Lider - İSYS Yöneticisi):** ADOM'un işleyişini sağlar, taktiksel toplantılara başkanlık eder, ekipler arası kaynak çakışmalarını çözer.
  - **Altyapı Kurtarma Lideri (Altyapı Müdürü):** Elektrik, su, atıksu gibi altyapı kurtarma ekiplerini koordine eder.
  - **BT Kurtarma Lideri (BT Müdürü):** BT Felaket Kurtarma Ekibi'nin faaliyetlerini koordine eder ve RTO/RPO hedeflerini takip eder. Siber Olaylara Müdahale Planı ve Felaket Kurtarma Merkezi aktivasyonundan sorumludur
  - **İdari Destek Lideri (İdari İşler Şefi):** Personel, lojistik, güvenlik ve satın alma gibi destek faaliyetlerini koordine eder.

E.1.4.3 Operasyonel Ekipler (Müdahale ve Kurtarma)

- **Genel Sorumluluk:** Kendi uzmanlık alanlarındaki planları ve prosedürleri uygulayarak, sahada anlık müdahaleyi gerçekleştirmek ve kritik faaliyetleri/sistemleri kurtarmaktır.
- **Örnek Ekipler ve Sorumlulukları:**
  - **Acil Durum Müdahale Ekipleri (ADME):** Yangın söndürme, yaralılara ilk yardım yapma, personeli tahliye etme, olay yerini güvene alma gibi görevlerden sorumludurlar.
  - **İş Sürekliliği Ekipleri (İSE):** Kendi sorumlu oldukları departmanların kritik faaliyetlerini ilgili İSP'lere göre kurtarmaktan (örn. alternatif tesiste çalışmaya başlama, manuel prosedürleri uygulama) sorumludurlar. Bu ekipler ayrıca BT Felaket Kurtarma Ekibi, Altyapı Kurtarma Ekibi gibi teknik alt ekipleri de içerebilir.

E.1.5 Diğer OSB'ler İçin Genel Modeller

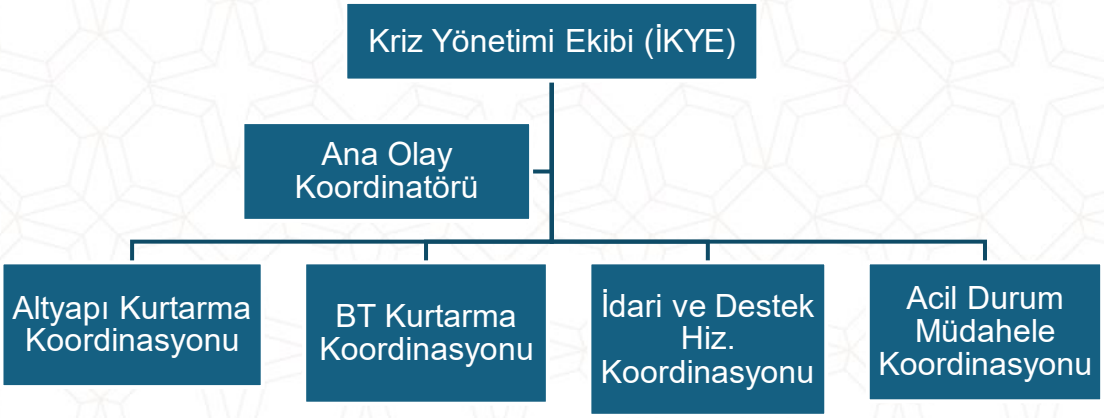
Yukarıdaki "Dirençli OSB" örneği orta-büyük ölçekli bir yapıya karşılık gelmektedir. Diğer OSB'ler, kendi büyüklük ve karmaşıklıklarına göre aşağıdaki genel modelleri uyarlayabilirler.

E.1.5.1 Küçük Ölçekli OSB Modeli

Bu modelde, tüm seviyeler tek bir esnek "Olay Yönetim Ekibi"nde birleşir. Bölge Müdürü stratejik kararları verirken, diğer kilit personel (Teknik ve İdari Sorumlular) hem taktiksel koordinasyonu hem de operasyonel görevleri üstlenir.

E.1.5.2 Büyük veya Çok Kampüslü OSB Modeli

Bu yapıda, Kriz Yönetim Ekibi'ne (KYE) raporlama yapan bir Ana Olay Koordinatörü bulunur. Ana Olay Koordinatörü'nün altında ise Altyapı, BT ve İdari Hizmetler gibi alanlara odaklanmış alt koordinasyon ekipleri yer alır. Her alt koordinasyon ekibi, kendi alanındaki operasyonel ekipleri yönetir.



Ek E.2.1: "Dirençli OSB" İçin Tamamlanmış İş Sürekliliği Planı (1) (Örnek: Kritik İdari ve Koordinasyon Faaliyetleri)

Bilgilendirme Notu: *Bu ek, orta veya büyük ölçekli bir OSB'de, belirli bir fonksiyona yönelik hazırlanmış bir İş Sürekliliği Planı (İSP) örneğidir. Daha küçük ölçekli OSB'ler, bu plandaki unsurları, Ek F.1'de çerçevesi sunulan Bütünleşik Acil Durum Yönetim Planı ile birleştirerek, tüm olayları kapsayan* ***tek ve bütünleşik bir "Olay Yönetim Planı"*** *oluşturmayı değerlendirebilirler.*

"Dirençli OSB" İçin Tamamlanmış İş Sürekliliği Planı (1) (Örnek: Kritik İdari ve Koordinasyon Faaliyetleri)

DOKÜMAN KONTROL

Plan Adı:	Dirençli OSB - Kritik İdari ve Koordinasyon Faaliyetleri İş Sürekliliği Planı
Doküman No:	İSY-İSP-İDARI-001
Versiyon:	1.0
Yürürlülük Tarihi:	01/07/2025
Plan Sahibi:	İdari İşler Müdürü (İFSE Lideri)
Onaylayan:	Mehmet Demirtaş (Bölge Müdürü)

0. YÖNETİCİ ÖZETİ

Kurum: Dirençli Organize Sanayi Bölgesi (OSB); Manisa'da yer alan, 150 katılımcı firmaya altyapı sağlayan, 60 kişilik yönetim kadrosuna ve kendi İtfaiye Teşkilatına sahip bir kamu tüzel kişiliğidir.

Stratejik Süreklilik Hedefi: OSB'nin "beyni" olan Yönetim Binası'nın kaybı durumunda dahi; güvenli operasyonları sürdürmek, yasal yükümlülükleri yerine getirmek, katılımcı firmaların üretim sürekliliğini desteklemek ve kurumsal itibarı korumak amacıyla, belirlenen **5 kritik idari sürecin tamamını**, kendi RTO hedefleri dahilinde, tanımlanmış asgari hizmet seviyelerinde (MBCO) kurtarmak ve sürdürmektir

En Önemli 5 Kritik Süreç ve Hedefler:

#	Kritik Süreç	RTO	MTPD	MBCO (Asgari İş Sürekliliği Hedefi)
1	**Kriz Yönetimi**	**2 sa**	4 sa	KYE'nin güvenli bir alanda toplanıp komutayı alması.
2	**Teknik Koor. (SCADA)**	**2 sa**	4 sa	Altyapı izleme ekranlarına erişim ve telsiz irtibatı.
3	**Kriz İletişimi**	**4 sa**	8 sa	Valilik ve Katılımcılara ilk resmi durum bildirimi.
4	**Acil Finansman**	**8 sa**	24 sa	Kritik ödemelerin (yakıt, iaşe) yapılabilmesi.
5	**Personel Yönetimi**	**12 sa**	24 sa	Personel durum tespiti ve vardiya planlaması.

Öncelikli Tehdit Senaryoları (Risk Kayıt Formu Özeti):

- **N-DRN-001 (Yüksek):** Şiddetli Deprem (Yönetim binasında ağır hasar).
- **YANGIN-YNT-001 (Yüksek):** Bina Yangını (Binanın kullanılamaz hale gelmesi).
- **SIBER-SCD-001 (Yüksek):** Siber Saldırı (Verilere erişimin kaybı).
- **TEK-BT-VM-001 (Orta):** Veri Merkezi Arızası (Dijital erişim kaybı).

Plan Aktivasyon Kriteri: Yönetim binasına güvenli erişimin **4 saatten uzun süre** mümkün olmayacağının teyit edilmesi.

BÖLÜM 1: PLAN YÖNETİŞİMİ

1.1 Planın Amacı

Bu İş Sürekliliği Planı'nın (İSP) temel amacı, Dirençli OSB Yönetim Binası'nın erişilemez olduğu bir felaket durumunda, İEA ile belirlenmiş kritik idari ve koordinasyon faaliyetlerinin, önceden tanımlanmış RTO ve MBCO hedefleri doğrultusunda alternatif yöntemlerle (Ilık Alan, Uzaktan Çalışma) yeniden başlatılmasını sağlamaktır.

1.2 Kapsam

Bu plan, Yönetim Binası'ndaki tüm birimler (Bölge Müdürlüğü, İdari, Mali, İmar, Satın Alma, İK) ve bu birimlerin süreçlerini kapsar. Sahadaki teknik müdahaleler (Altyapı İSP) ve yangın söndürme (ADMP) bu planın dışındadır, ancak bu plan o ekiplerin yönetimini kapsar.

Bu plan, Üst Yönetim tarafından onaylanan "İSY-POL-001 İş Sürekliliği Politikası"ndaki "Katılımcı firmalarımızın sürekliliğini desteklemek için kendi yönetim kapasitemizi her koşulda ayakta tutacağız" taahhüdünü hayata geçirir.

1.4 Referans Çerçeve

- **Yasal:** 4562 Sayılı OSB Kanunu, 6331 Sayılı İSG Kanunu, KVKK.
- **Standartlar:** ISO 22301:2019, ISO 31000.
- **İç Düzenlemeler:** Bütünleşik Olay Yönetim Planı, Kriz İletişim Planı (KİP), BT Felaket Kurtarma Planı (BT-FKP).

1.5 Organizasyonun Anlık Görüntüsü

- **Lokasyon:** Tek bir merkezi Yönetim Binası ve ayrı bir İtfaiye/Destek Binası.
- **Personel:** Binada görevli ~40 ofis personeli.
- **Kritik Altyapı:** Tüm sunucular, SCADA merkezi ve fiziksel arşiv Yönetim Binasındadır. (Tek Nokta Hatası).

1.6 Roller & Sorumluluklar (Üst Düzey Özet)

- **Kriz Lideri (Bölge Müdürü):** Aktivasyon yetkilisi ve stratejik karar verici.
- **Olay Yöneticisi (İSYS Yöneticisi):** Saha operasyonlarını koordine eder.
- **İdari Faaliyetler Süreklilik Ekibi (İFSE) Lideri (İdari İşler Müdürü):** Bu planı uygular, Ilık Alanı yönetir.

1.7 Plan Bakımı ve Dağıtımı

Bu plan, İdari İşler Müdürü tarafından yılda en az bir kez gözden geçirilir. Planın güncel kopyası İtfaiye Binası'ndaki (Ilık Alan) "Acil Durum Dolabı"nda basılı olarak saklanır.

BÖLÜM 2: İŞ SÜREKLİLİĞİ ORGANİZASYONU & KOMUTA YAPISI

2.1 Olay Yönetim Hiyerarşisi

Dirençli OSB Olay Yönetimi, üç seviyeli bir hiyerarşiye dayanır:

- **Stratejik Seviye (KYE): Karar:** Yönetim Binası'nın **faaliyet dışı bırakılmasına** ve **İş Sürekliliği Planı'nın (Ilık Alan) aktive edilmesine** onay verir.
- **Taktiksel Seviye (OKE): Koordinasyon:** Ekiplerin alternatif tesise intikalini ve kurulumunu koordine eder.
- **Operasyonel Seviye (İFSE): Uygulama:** Ilık Alanı fiziksel olarak hazırlar ve süreçleri işletir.

2.2 Ekipler, Roller ve Sorumluluklar (Detaylı Matris)

Rol	Sorumlu (Yedek)	Kriz Anındaki Görevi
Kriz Lideri	Bölge Müdürü *(Teknik Md. Yrd.)*	İSP'yi aktive eder. Stratejik kararları (bütçe, iletişim) verir.
Olay Yöneticisi	İSYS Yöneticisi *(Altyapı Müdürü)*	OKE'yi yönetir. İdari ve Teknik ekiplerin eşgüdümünü sağlar.
İFSE Lideri	İdari İşler Müdürü *(İK Müdürü)*	Bu planı uygular. Personelin tahliyesini ve Ilık Alan/Evden çalışma düzenine geçişini yönetir.
Mali İşler Sor.	Muhasebe Şefi *(Finans Uzm.)*	Acil nakit akışını yönetir. Manuel ödeme ve onay süreçlerini (Bölüm 2.3) uygular.
Teknik Koor. Sor.	Altyapı Müdürü *(Elektrik Şefi)*	SCADA terminalini Ilık Alan'da açar. Sahadaki arıza ekiplerini telsizle yönetir.
BT Destek Sor.	Sistem Yöneticisi *(Tekniker)*	Ilık Alan'daki ağ ve bilgisayarları kurar. VPN erişimlerini açar.
Lojistik Sor.	Satın Alma Sor. *(Yön. Asist.)*	İaşe (yemek, su) ve doküman transferini sağlar.

2.3 Olağanüstü Yetki Matrisi

Kriz anında bürokrasiyi azaltmak için aşağıdaki yetkiler tanımlanmıştır:

Fonksiyon	Normal Yetki	Kriz Yetkisi (İSP Aktifken)
Acil Harcama	5.000 TL (Birim Md.)	**50.000 TL** (İFSE Lideri)
Ödeme Onayı	Çift İmza + Sistem	**Tek İmza + Manuel Talimat** (Bölge Md.)
Personel İzni	İK Müdürü	**İFSE Lideri** (Sözlü Onay)
Basın Açıklaması	Yön. Kur. Bşk.	**Kriz Lideri** (Bölge Md.)

2.4 Yetki Devri Sırası

Kriz Lideri'ne 1 saat içinde ulaşılamazsa yetki şu sırayla devredilir:

1. Teknik Md. Yrd. → 2. İdari İşler Müdürü → 3. Altyapı Müdürü.

BÖLÜM 3: ANALİTİK TEMEL ÖZETİ

Bu İş Sürekliliği Planı (İSP), varsayımlara değil, **İEA** ve **RD** kapsamında yürütülen detaylı analizlerin somut sonuçlarına dayanmaktadır.

3.1 Kritik Süreçler ve Kurtarma Hedefleri (İEA Bulguları)

Yönetim Binası'nda yürütülen faaliyetler arasından, OSB'nin varlığını sürdürebilmesi için kritik olan 5 ana süreç belirlenmiştir. Planın operasyonel hedefi, bu süreçleri aşağıdaki **RTO (Hedef Kurtarma Süresi)** ve **MBCO (Asgari Hizmet Seviyesi)** değerlerinde kurtarmaktır.

Tablo 3.1: Kritik İdari Süreçler ve Kurtarma Hedefleri

Öncelik	Kritik Süreç Adı	RTO	MTPD	MBCO (Asgari İş Sürekliliği Hedefi)
1	**Kriz Yönetimi ve Karar Alma**	**2 Saat**	4 Saat	KYE'nin güvenli bir alanda toplanması, yasal otoriteyi (Komuta) devralması ve ilk stratejik kararları (tahliye, durdurma vb.) alması.
2	**Teknik Koordinasyon (SCADA)**	**2 Saat**	4 Saat	Sahadaki altyapı (Elektrik, Su) durumunun izlenebilmesi için SCADA ekranlarına erişim sağlanması ve saha ekipleriyle telsiz irtibatının kurulması.
3	**Kriz İletişimi (Paydaşlar)**	**4 Saat**	8 Saat	Valilik, Bakanlık ve 150 Katılımcı Firmaya ilk "Resmi Durum Bildirimi"nin yapılması (Bilgi kirliliğini önlemek için).
4	**Acil Durum Finansmanı**	**8 Saat**	24 Saat	Krizin yönetimi için gereken acil harcamaların (yakıt, yemek, iş makinesi kiralama) onaylanması ve ödenmesi.
5	**Personel Yönetimi**	**12 Saat**	24 Saat	Tüm personelin sağlık durumunun tespiti, iletişim zincirinin kurulması ve kriz vardiya planının yapılması.

3.2 Kritik BT Sistemleri Kurtarma Hedefleri (RTO/RPO)

İdari ve teknik süreçlerin çalışabilmesi için bağımlı olunan teknolojik altyapının kurtarma hedefleri Tablo 3.2'de sunulmuştur. (Detaylar, Bilişim Teknolojileri Felaket Kurtarma Planı'nda (BT-FKP) yer almaktadır. Örnek BT-FKP, Kılavuz Ek E.3'te sunulmuştur.)

Tablo 3.2: BT Sistemleri Hedefleri

BT Sistemi	Desteklediği Süreç	RTO	RPO	Notlar
SCADA Sunucusu	Teknik Koordinasyon	**1 Saat**	5 Dk	En kritik sistemdir. Kesintisiz izleme şarttır.
VPN / Ağ Erişimi	Tüm Süreçler	**2 Saat**	Veri saklamaz.	Uzaktan çalışma ve Ilık Alan bağlantısı için şarttır.
ERP (Finans Modülü)	Acil Finansman	**8 Saat**	1 Saat	Manuel formlar geçici yedek olarak kullanılır.
E-Posta Sunucusu	Kriz İletişimi	**4 Saat**	1 Saat	Resmi yazışmalar için gereklidir.

3.3 Risk Değerlendirmesi (RD) Özeti

Bu planın aktivasyonunu tetikleyebilecek ve Yönetim Binası'nı tehdit eden öncelikli riskler şunlardır (Ref: Ek C.1 Risk Kaydı):

- **N-DRN-001 (Yüksek): Şiddetli Deprem:** Yönetim binasının yapısal hasar görmesi ve "Girilemez" etiketi alması.
- **YANGIN-YNT-001 (Yüksek): Bina Yangını:** Binanın tahliye edilmesi ve duman/ısı nedeniyle kullanılamaz hale gelmesi.
- **TEK-BT-VM-001 (Orta): Veri Merkezi Arızası:** Binadaki sunucu odasının kaybı nedeniyle tüm dijital erişimin kesilmesi.
- **SIBER-SCD-001 (Yüksek): Siber Saldırı:** Fidye yazılımı nedeniyle sistemlerin kilitlenmesi (Fiziksel bina sağlam olsa bile "dijital bina" kaybı).

3.4 Kritik Bağımlılıklar

Bu süreçlerin kurtarılabilmesi için aşağıdaki kaynaklara mutlak bağımlılık vardır. Planın başarısı bu bağımlılıkların yönetilmesine bağlıdır.

Tablo 3.4: Bağımlılık Matrisi

Kritik Süreç	İç Bağımlılıklar (Olmazsa Çalışamaz)	Dış Bağımlılıklar (Tedarikçi/Kurum)
Kriz Yönetimi	Güvenlik Birimi	AFAD, Valilik (Resmi bilgi ve izinler)
Teknik Koor.	BT Birimi (Ağ ve SCADA bağlantısı)	TEİAŞ, Telekom Operatörü, SCADA
Finans	İSYS Yöneticisi (Onay mekanizması)	Bankalar (Online işlemler ve nakit akışı)
Personel Yön	İK Birimi (İletişim listeleri)	Personel Servis Firması (Acil ulaşım)

BÖLÜM 4: İŞ SÜREKLİLİĞİ STRATEJİLERİ VE ÇÖZÜMLERİ

Bu bölüm, İEA ve RD analizleri sonucunda belirlenen "Yönetim Binası Kaybı" ve "İdari İşlevsizlik" risklerini yönetmek için Dirençli OSB'nin benimsediği temel yaklaşımları tanımlar. Buradaki stratejiler, **Olay Öncesi (Hazırlık)**, **Olay Sırası (Müdahale)** ve **Olay Sonrası (Kurtarma)** olmak üzere üç fazlı bir yapıda kurgulanmıştır.

4.1 Genel Stratejik Yaklaşım

Dirençli OSB Yönetimi, idari faaliyetlerin sürekliliği için "Mekândan Bağımsız Yönetim" ve "Yedekli Veri" felsefesini benimser. Amacımız, fiziksel binamız veya ana sistemlerimiz yok olsa bile, yönetim yeteneğimizi sürdürmektir.

4.2 Olay Öncesi Stratejiler (Önleme ve Hazırlık)

Bu stratejiler, henüz bir kesinti yaşanmadan önce riski azaltmak ve müdahale kapasitesini artırmak için uygulanır.

Tesis Stratejisi (Ilık Alan Hazırlığı):

- **Strateji:** Yönetim binasına alternatif, OSB kontrolünde güvenli bir lokasyonun hazır tutulması.
- **Çözüm:** OSB bünyesindeki İtfaiye Binası Eğitim Salonu, "Yedek Komuta Merkezi" (Ilık Alan) olarak yapılandırılmıştır.
- **Aksiyonlar:** Salonun internet ve enerji altyapısı ana binadan bağımsız hale getirilmiş (yedekli fiber), 5 adet acil durum dizüstü bilgisayarı ve 1 adet SCADA terminali kilitli bir dolapta hazır edilmiştir.

Teknoloji Stratejisi (Uzaktan Erişim ve Kademeli Güvenlik):

- **Strateji:** Personelin ofis dışında güvenli çalışabilmesi ve verinin korunması.
- **Çözüm A (Erişim):** Güvenli VPN (Sanal Özel Ağ) ve Bulut tabanlı dosya paylaşım sistemi.
- **Çözüm B (Kademeli Güvenlik): Katmanlı Veri Güvenliği** yaklaşımıyla; kritik veriler (Mali kayıtlar, İletişim listeleri) **3-2-1 kuralına** uygun olarak yedeklenir ve fidye yazılımı riskine karşı bir kopyası ağdan bağımsız (Çevrimdışı/Offline) ortamda tutulur.

  (***3-2-1 Kuralı:*** *Verilerin **3** kopyası, **2** farklı ortamda (disk + bulut gibi), **1** kopya tesis dışında (off-site) saklanmalıdır.*)
- **Aksiyonlar:** İdari personel için 35 VPN lisansları alınmış, dizüstü bilgisayarlarına yüklenmiş ve evden erişim testleri 3 ayda bir yapılmaktadır. Çevrimdışı yedekleme ünitesi kurulmuştur.

Süreç Stratejisi (Manuel Yedeklilik):

- **Strateji:** Teknolojiye olan mutlak bağımlılığın azaltılması ("Teknoloji yoksa kalem var").
- **Çözüm:** Kritik süreçler (Satın alma, Ödeme, Evrak Kayıt) için "Manuel Formlar"ın hazırlanması.
- **Aksiyonlar:** Ek-D'de yer alan formların basılı kopyaları (50'şer adet) Ilık Alan'daki "Acil Durum Dolabı"na yerleştirilmiştir.

4.3 Olay Sırası Stratejileri (Müdahale ve Süreklilik)

Kesinti anında hizmetin RTO süreleri içinde (Kriz Yönetimi için 2 saat) yeniden başlatılmasını hedefler.

Hibrit Çalışma Stratejisi (Personel Yönetimi):

- **Kritik Ekip:** Kriz Yönetim Ekibi (KYE) ve Teknik Koordinasyon sorumluları (Toplam ~10-12 kişi) fiziksel olarak **Ilık Alan'a (İtfaiye Binası)** intikal eder.
- **Destek Ekip:** Muhasebe, İK, Satın Alma ve Yazı İşleri gibi destek birimleri (~30 kişi) **evlerine gönderilir** ve VPN üzerinden sisteme bağlanarak süreci yönetir.
- **Tetikleyici:** Yönetim binasına erişimin 4 saatten uzun süre mümkün olmayacağının anlaşılması.

Çok Kanallı İletişim Stratejisi:

- **Kanal 1 (GSM Çalışıyorsa):** "KYE WhatsApp Grubu" ve Personel için "Toplu SMS Sistemi".
- **Kanal 2 (GSM Çöktüyse):** İtfaiye binasındaki "Telsiz Ana İstasyonu" ve "Uydu Telefonu" (2 adet).
- **Hedef:** Katılımcı firmalara ve Valiliğe ilk 4 saat içinde resmi durum bildiriminin yapılması.

Acil Finansman Stratejisi:

- **Nakit:** Banka sistemleri çalışmıyorsa, Mali İşler Müdürü yetkisindeki "Acil Durum Nakit Fonu" (Kasa) kullanılır.
- **Ödeme:** İnternet bankacılığı erişilemezse, banka şubesiyle önceden yapılan protokol gereği manuel talimat (Faks/E-posta) ile işlem yapılır.

Teknoloji Kurtarma Stratejisi (Siber Olay Anı):

- **Çözüm:** Siber saldırı durumunda ağ bağlantılarının fiziksel olarak kesilmesi (İzolasyon) ve temiz çevrimdışı yedeklerden geri yükleme yapılması.
- **Alternatif:** Kurtarma süresi uzarsa Manuel Süreç Stratejisi devreye girer.

4.4 Olay Sonrası Stratejileri (Kurtarma ve İyileştirme)

Bu stratejiler, geçici çözümlerden (Workaround) normal operasyonlara dönüşü sağlar.

- **Normale Dönüş:** Yönetim binasının hasar tespiti ve tadilatı sonrası, personelin kademeli olarak ofise dönüşü.
- **Veri Senkronizasyonu:** Kriz sırasında Manuel (kâğıt) veya yerel PC'lerde tutulan kayıtların (gelen evrak, yapılan ödemeler) ERP sistemine girilmesi.
- **Ders Çıkarma:** Olay sonrası "Kök Neden Analizi" yapılarak planın ve stratejilerin güncellenmesi.

4.5 Senaryo – Strateji – Prosedür Eşleşme Tablosu

Aşağıdaki tablo, hangi risk senaryosunda hangi stratejinin devreye gireceğini özetler:

Prosedür Eşleşme Tablosu

Risk Senaryosu	Birincil Strateji	Uygulama Aracı (Bölüm 6 Referansı)
Bina Kaybı **(Deprem/Yangın)**	Hibrit Çalışma (Ilık Alan + Evden)	**Prosedür İSP-KRİZ-01** (Kriz Yönetimi ve Ilık Alan)
Teknik Altyapı / SCADA Kaybı	Teknoloji Yedekliliği	**Prosedür İSP-TEK-01** (Teknik Koor. ve SCADA)*
Finansal Sistem Erişimsizliği	Acil Nakit ve Manuel Ödeme	**Prosedür İSP-FİN-01** (Acil Finansman)*
Personel Kaybı	Yedekleme Stratejisi	**Prosedür İSP-İK-01** (Personel ve Vardiya)
İletişim Altyapısı Çökmesi	Çok Kanallı İletişim	**Prosedür İSP-İLT-01** (Kriz İletişimi)
Siber Saldırı / BT Kaybı	Manuel İşletim Stratejisi	**Prosedür İSP-MAN-01** (Manuel Çalışma)

BÖLÜM 5: AKTİVASYON VE OLAY YÖNETİM PROSEDÜRLERİ

Bu bölüm, bir olay anında Dirençli OSB'nin müdahale felsefesini, planların hangi kriterlere göre aktive edileceğini, komuta merkezinin nasıl çalışacağını, genel müdahale döngüsünü ve iletişim prosedürlerini tanımlar.

5.1 Aktivasyon Kriterleri ve Yükseltme Akışı (Olay Seviyesi → Plan Aktivasyonu)

Müdahalenin ölçeğini ve hangi planın aktive edileceğini belirlemek için olaylar, ciddiyetlerine göre 4 seviyede sınıflandırılır.

- **Seviye 1: Olay:**
  - **Tanım:** Standart işletme prosedürleri (SOP) veya bakım ekipleri tarafından kısa sürede çözülebilen, kritik hizmetlerin (Elektrik, Su, Arıtma) genel sürekliliğini etkilemeyen teknik veya idari aksaklıklar.
  - **OSB İçin Örnekler:**
    - ❑ Bir dağıtım merkezindeki (DM) tali fiderin açması ve yedek hattan beslemenin otomatik sağlanması.
    - ❑ İdari binadaki bir ofis yazıcısının veya tekil bir iş istasyonunun arızalanması.
    - ❑ AAT (Arıtma) giriş pompa istasyonunda bir pompanın arızalanması ancak yedeğinin (stand-by) devreye girmesi.
    - ❑ İnternet hızında kısa süreli yavaşlama yaşanması.
  - **Aksiyon: İSP AKTİVE EDİLMEZ.** İlgili Birim Yöneticisi (Elektrik İşletme, BT, Bakım) durumu yönetir ve çözer. Kriz Yönetimi'ne raporlanmaz.
- **Seviye 2: Acil Durum (Emergency):**
  - **Tanım:** Can veya mal güvenliğini tehdit eden, sınırlı bir alanda (bina veya tesisin bir bölümü) etkili olan ve OSB'nin kendi acil durum kaynakları (Güvenlik, İtfaiye, İSG) ile yönetilebilen olaylar.
  - **OSB İçin Örnekler:**
    - ❑ Yönetim binası arşiv odasında çıkan küçük çaplı yangın.
    - ❑ Kimyasal depolama alanında sınırlı sızıntı.
    - ❑ Bir personelin iş kazası geçirmesi.
    - ❑ Şüpheli paket ihbarı nedeniyle binanın geçici boşaltılması.
  - **Aktivasyon: Acil Durum Müdahale Planı (ADMP)** derhal aktive edilir. Bina/Bölge tahliye edilir. İSP "Beklemede (Stand-by)" moduna geçer.
- **Seviye 3: İş Kesintisi / Felaket (Disruption / Disaster):**
  - **Tanım:** Acil durum (Seviye 2) kontrol altına alınmış olsa bile, kesintinin;
    - ❑ Yönetim Binası'na **4 saatten fazla** güvenli erişimi engelleyeceği,

- ❑ Kritik altyapı yönetimini (SCADA) veya idari fonksiyonları (ERP) **RTO süreleri (2-8 Saat)** içinde tehdit ettiği, durumlar.

- **OSB İçin Örnekler:**
  - ❑ Yönetim Binası'nın yangın sonrası "ağır hasarlı/girilemez" ilan edilmesi.
  - ❑ Ana Trafo Merkezi'nde patlama ve OSB genelinde uzun süreli enerji kesintisi.
  - ❑ Siber saldırı (Fidye Yazılımı) sonucu tüm sunucuların şifrelenmesi.
- **Aktivasyon:** KYE onayı ile **Bu Plan (İSP)** ve/veya **BT-FKP** aktive edilir. İFSE Lideri koordinasyonunda Ilık Alan (İtfaiye Binası) operasyonu başlar.

- **Seviye 4: Kriz (Crisis):**
  - **Tanım:** Olayın fiziksel boyutunu aşıp, OSB'nin kurumsal itibarını, yasal statüsünü veya finansal yapısını tehdit eder hale gelmesi.
  - **OSB İçin Örnekler:**
    - ❑ OSB kaynaklı bir çevre felaketinin ulusal medyada yer alması.
    - ❑ Büyük bir iş kazası sonrası savcılık tarafından faaliyetin durdurulması.
    - ❑ Katılımcı firmaların OSB yönetimine karşı toplu hukuki işlem başlatması.
  - **Aktivasyon: Kriz Yönetim Planı (KYP)** ve **Kriz İletişim Planı (KİP)** derhal aktive edilir. Komuta Stratejik Seviye'ye (Bölge Müdürü) geçer.

5.2 Komuta Merkezi (ADOM - Acil Durum Operasyon Merkezi)

ADOM, bir Seviye 2 (Acil Durum) veya üzeri olay meydana geldiğinde, Olay Yönetim Ekibi'nin (OYE) toplanarak müdahale ve kurtarma faaliyetlerini koordine edeceği sinir merkezidir.

- **Birincil Acil Durum Merkezi (ADOM):**
  - **Yer:** Yönetim Binası, Zemin Kat Toplantı Odası.
  - **Gerekçe:** Tesise hakim, iletişim altyapısına yakın.
- **İkincil (Yedek) Acil Durum Merkezi (ADOM):**
  - **Yer:** İtfaiye Binası Eğitim Salonu (Ilık Alan).
  - **Gerekçe:** Birincil merkezin kullanılamaması durumunda devreye alınır.
- **ADOM Aktivasyon Kriterleri:** Olay Yöneticisi, Seviye 2 veya üzeri bir olayın teyit edilmesi üzerine ADOM'un aktive edilmesi talimatını verir.
- **Asgari Donanım İhtiyacı:** Telsiz ana istasyonu, yedek piller, sabit hat, beyaz tahta, basılı planlar (ADMP, İSP, KYP), jeneratör hattı.

5.3 Genel Olay Yönetim Döngüsü

Bu plan aktive edildiğinde (Seviye 3), tüm kurtarma faaliyetleri aşağıdaki beş aşamalı yönetim döngüsüne göre yürütülür:

- **Tespit ve Değerlendirme:**

- Olay Yöneticisi, ADMP müdahalesinin bittiğini (alan güvenli) ancak kritik süreçleri etkileyen bir kesinti olduğunu Kriz Lideri'ne raporlar.
- OYE, hızlı bir ilk etki değerlendirmesi yapar.

- **Plan Aktivasyonu ve Kontrol:**
  - Değerlendirme sonucuna göre, Kriz Lideri **İSP'nin resmi olarak aktive edilmesi** kararını verir.
  - OYE, ADOM'da toplanarak komuta ve kontrolü devralır.
- **Kurtarma:**
  - Olay Yöneticisi, İş Kurtarma Ekiplerini (İKE) görevlendirir.
  - İlgili İKE'ler, Bölüm 6'daki prosedürleri uygulamaya başlar. Odak, RTO içinde MBCO seviyesine ulaşmaktır.
- **Normale Dönüş:**
  - Kritik operasyonlar asgari seviyede başlatıldıktan sonra, tam kapasiteye dönüş çalışmaları başlar.
- **Olay Sonrası Değerlendirme:**
  - Operasyon normale döndükten sonra "Öğrenilen Dersler" toplantısı yapılır ve DÖF süreci başlar.

5.4 İletişim Prosedürleri (KİP'e Referans)

İSP aktive edildiğinde iletişim Tablo 5.1'e göre yürütülür. (Detaylar, KİP'te yer alır. Örnek, KİP, Kılavuz Ek G.2'dedir):

Tablo 5.1: İş Sürekliliği İletişim Matrisi (Özet)

Kiminle İletişime Geçilecek	İletişim Sorumlusu	Kullanılacak Yöntem	Zamanlama
İÇ: KYE	Olay Yöneticisi	Yüz yüze / Telsiz	Olayın ilk saatinde ve her 2 saatte bir.
İÇ: Tüm Çalışanlar	Kriz Lideri / İK	Toplu SMS, E-posta	Kesinti netleşince ilk bilgilendirme.
DIŞ: Ana Müşteriler	Satış Sorumlusu	Telefon / E-posta	RTO aşılacağı teyit edildiğinde.
DIŞ: Kritik Tedarikçiler	Satın Alma Sor.	Telefon / E-posta	Akış durdurma kararı alındığında.
DIŞ: Resmi Kurumlar	Kriz Lideri	Resmi Yazı / Telefon	Yasal bildirim gerektiğinde.

5.5 Adaptif Müdahale Senaryoları (Zaman ve Tür Bazlı Akış)

Aşağıdaki tablolar, **Olay Seviyeleri (Bölüm 5.1)** ile pratik saha tepkilerini birleştirir.

Tablo 5.2: Adaptif Müdahale Akışı - Faz 1: Anlık Müdahale (İlk 5-60 Dakika)

OLAY TÜRÜ & ZAMANI	LOKAL OLAY (Yangın vb.) MESAİ SAATLERİ İÇİNDE	BÖLGESEL AFET (Deprem vb.) MESAİ SAATLERİ İÇİNDE	LOKAL OLAY MESAİ DIŞINDA (GECE)	BÖLGESEL AFET MESAİ DIŞINDA (GECE)
PERSONELİN İLK EYLEMİ	**1. Alarm Ver:** Butona bas. **2. Tahliye Et:** Toplanma alanına git. **3. Sayım Ver:** Birim amirine rapor ver.	**1. Çök-Kapan-Tutun:** Sarsıntı bitene kadar bekle. **2. Tahliye:** Güvenli alana çık. **3. Aile İletişimi:** Aileni SMS ile bilgilendir.	**1. Gelme:** Evde kal. **2. Talimat Bekle:** Telefon/SMS bekle.	**1. Önce Aile:** Kendi güvenliğini sağla. **2. Yola Çıkma:** Çağrılmadan tesise gelme. **3. Durum Bildir:** Telefon zinciri ile durumunu ilet.
YÖNETİMİN İLK EYLEMİ	**1. ADMP Aktivasyonu:** Güvenlik/İtfaiye müdahaleyi başlatır. **2. Kriz Lideri Bilgilendirmesi:** Olay Yöneticisi durumu raporlar.	**1. Hasar Tespiti:** Teknik ekip dışarıdan binayı kontrol eder. **2. KYE Toplanma:** Yönetim, açık alanda veya İtfaiye bahçesinde toplanır.	**1. Tespit:** Güvenlik/Nöbetçi Amir olayı tespit eder. **2. Zincirleme Bildirim:** Kriz Lideri aranır.	**1. Uzaktan Toplanma:** KYE güvenli ise WhatsApp/Teams üzerinden durum değerlendirmesi yapar.

Tablo 5.3: Adaptif Müdahale Akışı - Faz 2: Değerlendirme & İletişim (Saat 1-12)

OLAY TÜRÜ & ZAMANI	LOKAL OLAY (Mesai İçi)	BÖLGESEL AFET (Mesai İçi)	LOKAL OLAY (Mesai Dışı)	BÖLGESEL AFET (Mesai Dışı)
KYE AKTİVASYONU	**Fiziksel Toplanma:** ADOM veya İtfaiye Binası'nda toplanır.	**Fiziksel Toplanma:** Güvenli açık alanda veya İtfaiye Binası'nda toplanır.	**Uzaktan Toplanma:** Teams/Telkonferans ile toplanır.	**Uzaktan Toplanma:** İletişim mümkünse Teams/Telkonferans ile toplanır.
HASAR DEĞERLENDİRME	**Detaylı Tespit:** İtfaiye "güvenli" dedikten sonra içeri girilir.	**Dışarıdan Tespit:** Binalara girilmez. Sadece dış hasara bakılır.	**İlk Tespit:** Nöbetçi ekiplerin raporuna dayanır.	**ERTELENİR:** Ulaşım ve güvenlik sağlanana kadar tespit yapılmaz.

OLAY TÜRÜ & ZAMANI	LOKAL OLAY (Mesai İçi)	BÖLGESEL AFET (Mesai İçi)	LOKAL OLAY (Mesai Dışı)	BÖLGESEL AFET (Mesai Dışı)
RESMİ İLETİŞİM	**Durum Bilgisi:** "Olay kontrol altında, bekleyin."	**Önce Aile:** "Tesis kapalıdır, ailenizle ilgilenin."	**Gelme Talimatı:** "Tesise gelmeyin, talimat bekleyin."	**Önce Aile:** "Güvende kalın, yola çıkmayın."

Tablo 5.4: Adaptif Müdahale Akışı - Faz 3: İş Sürekliliği (İSP) Aktivasyonu (Saat 12-72)

OLAY TÜRÜ & ZAMANI	LOKAL OLAY (Mesai İçi)	BÖLGESEL AFET (Mesai İçi)	LOKAL OLAY (Mesai Dışı)	BÖLGESEL AFET (Mesai Dışı)
AKTİVASYON KARARI	**HEMEN AKTİVE EDİLİR:** İFSE ekipleri göreve çağrılır.	**ERTELENİR:** Öncelik insani durumdur. Personel güvenliği teyit edilmeden iş kurtarma başlamaz.	**HEMEN AKTİVE EDİLİR:** İlgili ekipler (BT/Teknik) tesise çağrılır.	**ERTELENİR:** Ulaşım ve güvenlik sağlanana kadar beklenir.
KAYNAK TAHSİSİ	**Operasyonel:** Onarım ve kiralama bütçesi onaylanır.	**İnsani:** Personel desteği (nakit, gıda) önceliklidir.	**Operasyonel:** Uzaktan bütçe onayı verilir.	**İnsani:** Personel desteği önceliklidir.

BÖLÜM 6: İŞ KURTARMA PROSEDÜRLERİ (Kontrol Listesi Formatında)

Bu bölüm, İSP aktive edildikten sonra, ilgili İş Kurtarma Ekipleri (İFSE üyeleri) tarafından uygulanacak olan adım adım kurtarma talimatlarını içerir. Her bir prosedür, ilgili sürecin **RTO** ve **MBCO** hedeflerine ulaşması için tasarlanmıştır.

6.1 Prosedür İSP-KRİZ-01: Kriz Yönetimi ve Karar Alma Sürecinin Kurtarılması

İlgili Süreç:	**Kriz Yönetimi ve Stratejik Karar Alma**
RTO (Hedef Süre):	**2 Saat** (En Yüksek Öncelik)
MBCO (Asgari Hedef):	KYE'nin güvenli bir alanda toplanarak komuta yeteneğini kazanması ve yasal bildirimleri yapabilmesi.
Sorumlu Ekip:	Kriz Yönetim Ekibi (Lider: Bölge Müdürü)

Adım No	**Eylem**	**Tamamlandı mı?**	**Notlar / Kritik Detay**
1	**Durum Teyidi ve Güvenlik:** Yönetim Binası tahliyesinden sonra, tüm KYE üyelerinin ve kritik yöneticilerin (Birim Müdürleri) güvende olduğunu teyit et.	[ ]	Eksik yönetici varsa yetki devri (Bölüm 2.4) uygula.
2	**Alternatif Komuta Merkezi:** İtfaiye Binası Eğitim Salonu'nun (Ilık Alan) "Acil Durum Operasyon Merkezi (ADOM)" olarak aktive edilmesi talimatını ver.	[ ]	İFSE Lideri bu kurulumu yönetir (Ek-C).
3	**Toplanma:** KYE üyeleri ile Ilık Alan'da (veya fiziksel erişim yoksa Teams/Telefon konferansı ile) ilk stratejik toplantıyı başlat.	[ ]	İlk toplantı gündemi: Can güvenliği ve yasal durum.
4	**Bağımlılık Kontrolü:** • Sahadan (Güvenlik/İtfaiye) bina hasar durumu bilgisini al. • Valilik/AFAD'dan bölgesel durum bilgisini al.	[ ]	Kararlar bu verilere dayanacaktır.
5	**Stratejik Kararlar:** • Personelin eve gönderilmesi / uzaktan çalışma onayı. • Olağanüstü harcama yetkisinin (50.000 TL) İFSE Liderine verilmesi. • Katılımcılara ve basına yapılacak açıklamanın onayı.	[ ]	Kararlar "Olay Kayıt Formu (Ek-D)"na işlenmelidir.
6	**Resmi Bildirimler:** • Valilik ve Sanayi Teknoloji İl Müdürü'ne "Yönetim Binası devre dışıdır, kriz masamız İtfaiye Binası'ndadır" resmi bildirimini yap. • 150 Katılımcı firmaya resmi durum bildirimini (SMS/E-posta) onayla.	[ ]	Yasal sorumluluk için kritiktir. İletişim Listesi: **Ek-B**.
7	**Raporlama Düzeni:** OKE Lideri'nden her 2 saatte bir "Durum Raporu (SitRep)" alma düzenini başlat.	[ ]	

6.2 Prosedür İSP-TEK-01: Teknik Koordinasyon ve SCADA İzlemenin Kurtarılması

İlgili Süreç:	Teknik Altyapı Yönetimi (Elektrik, Su, Atık Su)
RTO (Hedef Süre):	**2 Saat**
MBCO (Asgari Hedef):	SCADA izleme ekranlarına erişim sağlanması ve sahadaki arıza ekipleriyle telsiz iletişiminin kurulması.
Sorumlu Ekip:	Teknik Koordinasyon Sorumlusu (Altyapı Müdürü)

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
1	**Terminal Erişimi:** İtfaiye Binası'ndaki "Acil Durum Dolabı"ndan yedek SCADA terminalini (dizüstü bilgisayar) ve büyük ekranı çıkart.	[ ]	Anahtar: Güvenlik Amiri / Kutu No: 3
2	**Sistem Bağlantısı:** • Dizüstü Bilgisayarı "Kırmızı Etiketli" (Kriz Ağı) ağ prizine tak. • VPN/Doğrudan bağlantı ile SCADA sunucularına erişimi test et. • Erişim yoksa BT Destek Sorumlusu'nu çağır.	[ ]	BT-FKP planı ile koordine olunmalıdır.
3	**Saha İletişimi:** • Yönetim Binası'ndaki Telsiz Rölesi çalışmıyorsa, saha ekiplerine (Elektrik, Su) "Simplex Kanal"a (Kanal 3) geçmeleri anonsunu yap. • Telsiz çalışmıyorsa ekip liderlerini cep telefonundan ara.	[ ]	İletişim olmadan koordinasyon olmaz.
4	**Operasyonel Kontrol:** • Trafo merkezleri ve pompa istasyonlarının durumunu ekrandan kontrol et. • Kritik alarmları (Su deposu seviyesi, Trafo sıcaklığı) listele.	[ ]	Ekran görüntüsü yoksa, sahadaki ekipten manuel okuma iste.
5	**Koordinasyon:** • İtfaiye Amiri ile görüşerek yangın/arama-kurtarma faaliyetlerinin altyapıya etkisini (elektrik kesme ihtiyacı vb.) öğren. • Durumu Kriz Lideri'ne raporla.	[ ]	

6.3 Prosedür İSP-FİN-01: Acil Durum Finansmanı ve Ödemeler

İlgili Süreç:	Finansal Yönetim ve Satın Alma
RTO (Hedef Süre):	**8 Saat**
MBCO (Asgari Hedef):	Krizin yönetimi için gereken acil harcamaların (yakıt, yemek, iş makinesi kiralama) onaylanması ve ödenmesi.
Sorumlu Ekip:	Mali İşler Sorumlusu (Muhasebe Şefi)

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
1	**Nakit Erişimi:** • Yönetim Binası'ndaki kasaya erişim yoksa, banka şubesine giderek yetkili hesaptan "Acil Durum Nakit Avansı" (10.000 TL) çek. • Nakdi, imza karşılığı İFSE Lideri'ne teslim et.	[ ]	Çift imza yetkisi gerekebilir.
2	**Manuel Talimat Hazırlığı:**	[ ]	Banka Şube Müdürü: [Tel No]

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
	• İnternet bankacılığına (OTP cihazları binada kaldığı için) erişilemiyorsa, "Ek-D Manuel Ödeme Talimatı" formunu kullan. • Formu Bölge Müdürü'ne imzalatarak banka şube müdürüne faksla veya fotoğrafını gönder.		
3	**Acil Satın Alma Onayı:** • Lojistik Sorumlusu'ndan gelen acil ihtiyaçları (Jeneratör yakıtı, kumanya) "Olağanüstü Yetki Limiti" (50.000 TL) dahilinde onayla. • Tedarikçiye "Ödeme Garantisi" vererek malı sevk ettir.	[ ]	Bürokratik süreç (teklif toplama vb.) askıya alınır.
4	**Bordro ve Vergi:** • Kriz maaş gününe denk geldiyse, bankaya "Geçen ayki listeyi tekrarla" talimatı ver. • Vergi ödemeleri için Hukuk Müşaviri ile "Mücbir Sebep" başvurusunu değerlendir.	[ ]	Personel mağduriyeti önlenmelidir.
5	**Kayıt:** Yapılan tüm harcamaları ve verilen sözleri "Manuel Harcama Takip Defteri"ne kaydet.	[ ]	Kriz sonrası mutabakat için şarttır.

6.4 Prosedür İSP-İK-01: Personel Yönetimi, Vardiya ve Lojistik Destek

Bu prosedür, kriz anında insan kaynağının güvenliğini, sürdürülebilirliğini (yorgunluk yönetimi) ve fiziksel ihtiyaçlarını (yemek, barınma) yönetmek için uygulanır.

İlgili Süreç:	İnsan Kaynakları ve İdari Destek
RTO (Hedef Süre):	**12 Saat**
MBCO (Asgari Hedef):	Tüm personelin sağlık/güvenlik durumunun teyidi, Kriz Ekibi için vardiya/dinlenme planı ve iaşe organizasyonu.
Sorumlu Ekip:	İFSE Lideri (Destek: İK Sorumlusu ve Lojistik Sorumlusu)

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
1	**Personel Durum Tespiti (Headcount):** Toplanma alanındaki sayım listelerini al. Sahada olmayan personel için "Telefon Zinciri"ni (Ek B) başlat. Ulaşılamayan personeli Güvenlik ve İtfaiye'ye (Arama-Kurtarma) bildir.	[ ]	*Önce can güvenliği. Kayıp personel varsa operasyon başlamaz.*
2	**Tıbbi ve Psikolojik Destek:** Yaralı personel varsa revire/hastaneye sevkini koordine et. Şoktaki personel için güvenli bir dinlenme alanı oluştur.	[ ]	*Travma yönetimi.*
3	**Personel Ayrıştırma (Demobilizasyon):** Kriz anında sahada aktif görevi olmayan personeli (Arşiv, Stajyer, Bordro vb.) belirle. Onlara "Güvenli şekilde evlerinize dönün ve VPN talimatını bekleyin" emrini ver.	[ ]	*Kriz alanındaki kalabalık, kaosa neden olur.*
4	**Kriz Ekibi Lojistiği (Ilık Alan):** İtfaiye Binası'ndaki mutfak sorumlusuyla görüş. Kriz ekibi (yaklaşık 15 kişi) için 24 saatlik su, çay/kahve ve kuru gıda stoğunu toplantı salonuna taşıt.	[ ]	
5	**Vardiya Planlaması:** Krizin 24 saatten uzun süreceği kesinleşirse, KYE ve SCADA operatörleri için **"12**	[ ]	*Yorgunluk = Hata. 18 saatten fazla çalışma yasaktır.*

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
	Saatlik Vardiya Çizelgesini" (A Takımı: 08:00-20:00, B Takımı: 20:00-08:00) hazırla ve personele tebliğ et.		
6	**Yedek Personel (Deputy) Çağrısı:** Vardiya listesindeki boşluklar için "Yedek Personel Listesi"ndeki (Ek-B) çalışanları ara ve göreve (İtfaiye Binası'na) gelmeleri talimatını ver.	[ ]	*Yedeklerin ulaşımı için araç gönder.*
7	**Konaklama Düzeni:** Eve gidemeyecek durumda olan veya gece vardiyasında kalacak personel için İtfaiye Binası yatakhanesinde veya anlaşmalı otelde yer ayır.	[ ]	*Dinlenme kalitesi kritiktir.*

6.5 Prosedür İSP-İLT-01: Kriz İletişimi ve Paydaş Bilgilendirme

Bu prosedür, kriz anında bilgi kirliliğini önlemek, OSB'nin itibarını korumak ve paydaşları (Katılımcılar, Kamu) doğru yönlendirmek için uygulanır.

İlgili Süreç:	Kriz İletişimi (İç ve Dış Paydaşlar)
RTO (Hedef Süre):	**4 Saat**
MBCO (Asgari Hedef):	Valilik, Bakanlık ve 150 Katılımcı Firmaya ilk resmi durum bildiriminin yapılması.
Sorumlu Ekip:	İletişim Sorumlusu (Kurumsal İletişim Müdürü)

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
1	**İletişim Altyapı Kontrolü:** GSM şebekeleri çalışıyor mu? İnternet var mı? Eğer yoksa, İtfaiye Binası'ndaki **Uydu Telefonu**nu ve **Telsiz** sistemini devreye al.	[ ]	*Kanal 1: Yönetim, Kanal 2: Operasyon.*
2	**Mesaj Hazırlığı (Taslak Kullanımı):** "Kriz İletişim Planı" içindeki **"Taslak A: Bina Erişimi Yok"** şablonunu mevcut duruma (Yangın/Deprem) göre doldur. (Ne oldu? Ne yapıyoruz? Ne zaman döneceğiz?)	[ ]	*Sıfırdan metin yazma, şablonu kullan.*
3	**Onay Alma:** Hazırlanan basın bülteni ve katılımcı duyurusunu Kriz Yöneticisi'ne (Bölge Müdürü) okut ve **yazılı/sözlü onay** al.	[ ]	*Onaysız bilgi felakettir.*
4	**Resmi Bildirim (Kamu):** Valilik Özel Kalemi ve Sanayi Teknoloji İl Müdürlüğü'nü öncelikli hattan ara. Durumu sözlü bildir, ardından resmi yazıyı faks/KEP ile geç.	[ ]	*Yasal zorunluluk.*
5	**Katılımcı Duyurusu:** 150 katılımcı firmanın yetkilisine **Toplu SMS** ve **E-posta** yoluyla bildir: *"Yönetim Binası geçici olarak hizmet dışıdır. Acil durumlar için Kriz Masası'na [Yedek Tel No] üzerinden ulaşabilirsiniz."*	[ ]	*SMS sistemi çalışmıyorsa, sektör temsilcilerini (10 kişi) ara.*
6	**Medya ve Sosyal Medya Takibi:** Bir personeli "Medya İzleme" ile görevlendir. OSB hakkında çıkan asılsız haberleri (örn. "OSB tamamen yandı") tespit et ve düzeltici açıklama yayınla.	[ ]	*Dedikodu hızla yayılır.*
7	**Web Sitesi Güncellemesi:** OSB web sitesine "Acil Durum Bilgilendirme Banner"ı ekle. Güncel durum raporlarını buradan yayınla.	[ ]	*Şeffaflık güven verir.*

6.6 Prosedür İSP-MAN-01: Manuel (Kağıt Tabanlı) Çalışma Operasyonu

Bu prosedür, siber saldırı veya altyapı çökmesi nedeniyle BT sistemlerinin (ERP, EBYS, E-posta) RTO süreleri içinde kurtarılamadığı durumlarda uygulanır.

Tetikleyici:	**BT Sistemlerinin RTO süresinde (8-24 Saat) kurtarılamaması veya devam eden Siber Saldırı.**
Amaç:	Teknoloji olmadan iş süreçlerinin yasal ve izlenebilir şekilde yürütülmesi.
Sorumlu Ekip:	Tüm İdari Personel (Koordinatör: İFSE Lideri)

Adım No	**Eylem**	**Tamamlandı mı?**	**Notlar / Kritik Detay**
1	**Manuel Kiti Dağıt:** İtfaiye Binası'ndaki "Acil Durum Dolabı"ndan "Manuel İşlem Klasörleri"ni (Ek-D) çıkar. Satın Alma, Evrak Kayıt ve Muhasebe birimlerine ilgili formları ve defterleri dağıt.	[ ]	*Her birim kendi formunu almalıdır.*
2	**Evrak Kayıt Sistemi:** Gelen resmi evrakları "Gelen Evrak Defteri"ne elle işle, üzerine tarih/saat at ve "Sistem Dışı Kayıt" kaşesi bas. Giden evrakları zimmet defteriyle teslim et.	[ ]	*Evrak kaybı yasal risk doğurur.*
3	**Satın Alma ve Stok:** Acil ihtiyaçlar için "Manuel Satın Alma Talep Formu" kullan. Depodan çıkan malzemeyi "Stok Düşüm Fişi" ile kaydet.	[ ]	*ERP yoksa stok takibi kağıtla yapılır.*
4	**Ödeme ve Finans:** Banka talimatlarını daktilo veya el yazısı ile "Manuel Talimat Formu"na yaz. Bölge Müdürü ve Mali İşler Müdürü'ne (Çift İmza) imzalat. Şubeye kurye veya faks ile ilet.	[ ]	*Telefonda şube müdürüyle teyitleş.*
5	**İş Takibi ve Arşiv:** Doldurulan tüm formların bir kopyasını al ve "İşlenmedi" klasöründe biriktir. Orijinallerini işlem yapana ver.	[ ]	*Sistem gelince veri girişi için.*
6	**Veri Girişi (Normale Dönüş):** Sistemler açıldığında, "Veri Giriş Ekibi" kur. Klasördeki tüm manuel kayıtları ERP sistemine geriye dönük tarihle işle.	[ ]	*Veri bütünlüğü sağlanmalıdır.*

BÖLÜM 7: PLANIN SÜRDÜRÜLEBİLİRLİĞİ (PUKÖ)

Bu bölüm, İSP'nin güncel, personelin hazır ve sistemlerin çalışır durumda kalmasını sağlamak için uygulanacak **Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ)** döngüsünü tanımlar. Bu sürecin yönetiminden **İSYS Yöneticisi** sorumludur.

7.1 Eğitim ve Farkındalık Programı

Amaç: Personelin kriz anında "ne yapacağını" refleks haline getirmesi.

Hedef Kitle	Eğitim Konusu	Sıklık	Sorumlu
Tüm Personel	**Genel Farkındalık:** Acil durum alarmları, tahliye yolları, toplanma alanları ve "Önce Can Güvenliği" ilkesi.	İşe Girişte & Yılda 1	İK / İSG
Kriz Yönetim Ekibi (KYE)	**Stratejik Karar Alma:** Kriz senaryolarında yetki kullanımı, medya iletişimi ve liderlik simülasyonları.	Yılda 1	Bölge Müdürü
İFSE Ekibi	**Plan Uygulama:** Ilık Alan aktivasyonu, manuel formların kullanımı, telsiz iletişimi ve SCADA yedek terminal eğitimi.	6 Ayda 1	İSYS Yöneticisi
Yedekler (Deputies)	**Gölge (Shadowing):** Asıl sorumlunun görevlerini devralma pratiği.	Yılda 1	İlgili Birim Md.

7.2 Test ve Tatbikat Programı

Amaç: Planın kağıt üzerinde kalmayıp sahada çalıştığını doğrulamak.

Dönem	Tatbikat Türü	Senaryo / Kapsam	Katılımcılar
Ç1 (Mart)	**Haberli İletişim Testi**	Mesai saati dışında "Telefon Zinciri" ve "Toplu SMS" sisteminin test edilmesi.	Tüm Personel
Ç2 (Haziran)	**Masa Başı Tatbikatı**	**Senaryo:** Yönetim Binası Yangını. **Odak:** Karar alma, Ilık Alan'a geçiş kararı ve İletişim Planı.	KYE & İFSE Liderleri
Ç3 (Eylül)	**Teknik Test**	**Senaryo:** SCADA Sunucu Arızası. **Odak:** Yedek terminalden sisteme erişim ve verilerin kontrolü.	Teknik Koor. & BT
Ç4 (Aralık)	**Fonksiyonel Tatbikat**	**Senaryo:** Şiddetli Deprem. **Odak:** Ilık Alan'ın fiilen açılması, jeneratör ve ağın çalıştırılması, personelin intikali.	İFSE Ekibi

7.3 Planın Gözden Geçirilmesi ve Güncellenmesi

Bu plan statik değildir. Aşağıdaki tetikleyiciler oluştuğunda Plan Sahibi tarafından revize edilir:

- **Periyodik:** Yılda bir kez (Ocak ayı) tam gözden geçirme.
- **Değişiklik Bazlı:**
  - Kritik personel (Bölge Müdürü, İdari İşler Md.) değiştiğinde **(Derhal)**.
  - Yönetim binasında tadilat veya yerleşim değişikliği olduğunda.

  - Yeni bir kritik yazılım (ERP, SCADA sürümü) devreye alındığında.
- **Olay Sonrası:** Her tatbikat veya gerçek olay sonrasında yapılan "Alınan Dersler Toplantısı" çıktısına göre.

Dağıtım Kontrolü: Güncel planın basılı kopyası, "Eski kopyaların imha edildiği" teyit edilerek **İtfaiye Binası Kriz Dolabı**'na ve **Bölge Müdürü**'ne teslim edilir.

BÖLÜM 8: EKLER

Bu planın operasyonel olarak uygulanabilmesi için gerekli olan ve planla birlikte saklanan destekleyici dokümanlardır.

- **Ek-A: Eylem Kartları (Action Cards)** (Bölge Müdürü, İFSE Lideri, Mali İşler vb. için cep kartları).
- **Ek-B: İletişim Listeleri** (KYE, İFSE, Kritik Paydaşlar, Acil Durum Servisleri). *Gizli tutulmalıdır.*
- **Ek-C: Ilık Alan (İtfaiye Binası) Erişim ve Kurulum Talimatı** (Anahtar kimde, şalter nerede, ağ şifresi vb.).
- **Ek-D: Manuel Çalışma Formları Seti** (Satın Alma, Ödeme Talimatı, Olay Kayıt Formu, Gelen Evrak Defteri).
- **Ek-E: Vaziyet Planı ve Kritik Noktalar** (Toplanma alanları, tahliye yolları, enerji kesme noktaları).

ONAY

Bu İş Sürekliliği Planı, Dirençli OSB'nin kurumsal direncini artırmak, afet durumlarında yönetim zafiyetini önlemek ve paydaşlarına karşı sorumluluklarını yerine getirmek amacıyla hazırlanmıştır.

Hazırlayan:	**Onaylayan:**
(İmza)	*(İmza)*
İdari İşler Müdürü	**Mehmet Demirtaş**
Plan Sahibi / İFSE Lideri	Bölge Müdürü
Tarih: 01/07/2025	Tarih: 01/07/2025

EK-A: EYLEM KARTLARI (GÖREV KARTLARI)

Bu kartlar, krizin ilk anlarındaki stresi yönetmek ve kilit personelin kritik adımları atlamasını önlemek için hazırlanmış, lamine edilerek personele dağıtılacak "Hızlı Başvuru" araçlarıdır.

KART 0: KRİZ YÖNETİCİSİ (BÖLGE MÜDÜRÜ)

ROL: KRİZ YÖNETİCİSİ (KYE LİDERİ)	SORUMLULUK: STRATEJİK KARAR VE KAMU İLETİŞİMİ
FAZ 1: İLK 30 DAKİKA (KARAR VE AKTİVASYON)	**DURUM**
[ ] 1. Güvenlik Teyidi: **Kendi güvenliğini sağla. KYE üyelerinin ve Birim Müdürlerinin durumunu (Sayım Sonucu) İFSE Lideri'nden öğren.**	☐
[ ] 2. Durum Analizi: **Olay Yöneticisi'nden ilk brifingi al. (Bina ne durumda? Ne kadar süre giremeyeceğiz?)**	☐
[ ] 3. KARAR: **Yönetim Binası'nın** "Kullanılamaz" **olduğunu ilan et ve** "İş Sürekliliği Planı (İSP) Aktive Edilmiştir" **emrini ver.**	☐
[ ] 4. Lokasyon: **Kriz Yönetim Ekibi'ni (KYE)** İtfaiye Binası'na (Ilık Alan) **çağır.**	☐
FAZ 2: İLK 4 SAAT (STRATEJİ VE İLETİŞİM)	
[ ] 5. Resmi Bildirim: **Valilik ve Sanayi Teknoloji İl Müdürü'nü bizzat ara: *"Yönetim Binamız devre dışıdır, operasyonu İtfaiye Binası'ndan yönetiyoruz."***	☐
[ ] 6. Personel Kararı: **İdari personelin eve gönderilmesi (Uzaktan Çalışma) kararını onayla.**	☐
[ ] 7. Bütçe Onayı: **İFSE Lideri'ne acil durumlar için** 50.000 TL **olağanüstü harcama yetkisini sözlü/yazılı ver.**	☐
[ ] 8. Medya: **İletişim Sorumlusu'nun hazırladığı basın duyurusunu ve katılımcı mesajını onayla.**	☐
SÜREKLİ GÖREVLER	
[ ] 9. Liderlik: **Her 2 saatte bir KYE toplantısına başkanlık et. Stratejik yönü belirle.**	☐

KART 1: İFSE LİDERİ (İDARİ İŞLER MÜDÜRÜ)

ROL: İFSE LİDERİ	SORUMLULUK: EKİP LİDERLİĞİ VE KOORDİNASYON
İLK 15 DAKİKA (GÜVENLİK VE DURUM)	**DURUM**
[ ] 1. Tahliye Teyidi: **Kendi ekibinin (İdari, Mali, Satın Alma) tam ve güvende olduğunu "Toplanma Alanı"nda teyit et.**	☐
[ ] 2. İlk Brifing: **Olay Yöneticisi'nden (İSYS Yöneticisi) binanın durumu hakkında ilk bilgiyi al. (Ne kadar süre kapalı kalacağız?)**	☐
[ ] 3. Aktivasyon: **Kriz Yöneticisi'ne (Bölge Müdürü) "İdari İSP'nin aktive edilmesini" öner ve onay al.**	☐
[ ] 4. Ekip Toplanması: **İFSE üyelerini (Mali, Teknik, BT, Lojistik) topla ve "Ilık Alan'a (İtfaiye Binası) geçiyoruz" talimatını ver.**	☐
İLK 1 SAAT (HAZIRLIK)	
[ ] 5. Personel İletişimi: **Tüm idari personele şu mesajı geç: *"Yönetim Binası kapalıdır. Kriz Masası İtfaiye Binası'na geçmiştir. Destek ekipler evlerine dönsün ve 2. talimatı beklesin."***	☐
[ ] 6. Ilık Alan Kurulumu: **BT ve Lojistik sorumlusunun İtfaiye Binası'ndaki kurulumu başlatmasını denetle.**	☐

ROL: İFSE LİDERİ	SORUMLULUK: EKİP LİDERLİĞİ VE KOORDİNASYON
[ ] 7. Raporlama: **OKE Lideri'ne "İdari Operasyonlar İtfaiye Binası'na taşınıyor" raporunu ver.**	☐
SÜREKLİ GÖREVLER	
[ ] 8. Koordinasyon: **Her 2 saatte bir ekibinle kısa durum toplantısı yap.**	☐
[ ] 9. Kaynak Yönetimi: **Olağanüstü harcama taleplerini onayla.**	☐

KART 2: MALİ İŞLER SORUMLUSU (MUHASEBE ŞEFİ)

ROL: MALİ İŞLER SORUMLUSU	SORUMLULUK: ACİL DURUM FİNANSMANI
İLK 60 DAKİKA (NAKİT AKIŞI)	DURUM
[ ] 1. Kasa Kontrolü: **Yönetim binasındaki kasaya erişim yoksa, "Banka Acil Durum Protokolü"nü başlat.**	☐
[ ] 2. Nakit Temini: **Şubeden veya ATM'den acil harcamalar için (Yakıt, Yemek)** 10.000 TL **nakit avans çekimini organize et.**	☐
[ ] 3. Kayıt: **"Kriz Harcama Defteri"ni (Ek-D) aç ve ilk bakiyeyi kaydet.**	☐
SÜREKLİLİK (ÖDEME YÖNETİMİ)	
[ ] 4. Manuel Talimat: **İnternet bankacılığına erişilemiyorsa, **"Manuel Ödeme Talimatı Formu"**nu (Ek-D) hazırla.**	☐
[ ] 5. İmza: **Talimatı Bölge Müdürü'ne (veya vekiline) imzalat.**	☐
[ ] 6. İletim: **Talimatı banka şube müdürüne WhatsApp/Faks yoluyla ilet ve telefonla teyit al.**	☐
[ ] 7. Satın Alma Onayı: **Olağanüstü Harcama Limiti** (50.000 TL) **dahilindeki acil talepleri kontrol et ve tedarikçiye ödeme garantisi ver.**	☐

KART 3: TEKNİK KOORDİNASYON SORUMLUSU (ALTYAPI MÜDÜRÜ)

ROL: TEKNİK KOOR. SORUMLUSU	SORUMLULUK: SCADA VE SAHA İLETİŞİMİ
İLK 60 DAKİKA (BAĞLANTI)	DURUM
[ ] 1. Terminal: **Ilık Alan'daki "Acil Durum Dolabı"ndan yedek SCADA dizüstü bilgisayarını al.**	☐
[ ] 2. Bağlantı: **Dizüstü bilgisayarını "Kırmızı Etiketli" (Kriz Ağı) prize tak ve SCADA'ya giriş yap.**	☐
[ ] 3. Sorun Giderme: **Bağlantı yoksa, BT Destek Sorumlusu'nu yanına çağır.**	☐
SÜREKLİLİK (SAHA YÖNETİMİ)	
[ ] 4. Telsiz Kanalı: **Saha ekiplerine (Elektrik/Su) "Kanal 3"e geçmeleri talimatını ver (Yönetim Binası rölesi devre dışı olabilir).**	☐
[ ] 5. İzleme: **Kritik alarmları (Depo seviyesi, Trafo sıcaklığı) izle ve saat başı KYE'ye raporla.**	☐
[ ] 6. Ekip Yönetimi: **Sahadaki arıza ekiplerinin yemek ve dinlenme ihtiyaçlarını İFSE Lideri'ne bildir.**	☐

KART 4: BT DESTEK SORUMLUSU (SİSTEM YÖNETİCİSİ)

ROL: BT DESTEK SORUMLUSU	SORUMLULUK: ILIK ALAN VE VPN AKTİVASYONU
İLK 60 DAKİKA (KURULUM)	**DURUM**
[ ] 1. Erişim: **İtfaiye Binası'ndaki BT dolabını aç (Anahtar Güvenlikte).**	☐
[ ] 2. Ağ: **Odadaki "Acil Durum Switch"ini aç ve internet bağlantısını test et.**	☐
[ ] 3. Donanım: **5 adet yedek dizüstü bilgisayarı ve yazıcıyı masalara kur, fişlerini tak.**	☐
SÜREKLİLİK (UZAKTAN ERİŞİM)	
[ ] 4. VPN: **Firewall üzerinden "Kriz VPN Grubu"nu aktif et (35 Lisans).**	☐
[ ] 5. Destek: **Evden çalışan personelin bağlantı sorunları için "Uzaktan Destek Hattı"nı (Cep Tel) açık tut.**	☐
[ ] 6. Güvenlik: **Şüpheli bir siber aktivite (Fidye yazılımı vb.) görürsen derhal İFSE Lideri'ni uyar.**	☐

EK-B: KRİTİK İLETİŞİM LİSTELERİ

(Uyarı: Bu liste Kişisel Veriler (KVKK) içerir. Sadece yetkili personelin erişimine açıktır ve şifreli saklanmalıdır.)

Tablo B.1: İÇ PAYDAŞLAR - KRİZ YÖNETİM VE OPERASYON EKİPLERİ

ROL / GÖREV	İSİM SOYİSİM	CEP TELEFONU (Birincil)	YEDEK İLETİŞİM (Ev/Yakın)	TELSİZ KANALI
Kriz Yöneticisi (KYE Lideri)	Mehmet Demirtaş	0532 XXX XX 01	0236 XXX XX 01	CH-1
Olay Koordinatörü (OKE Lideri)	Elif Kaya	0533 XXX XX 02	0505 XXX XX 02	CH-1
İFSE Lideri (İdari İşler Md.)	Ahmet Yılmaz	0542 XXX XX 03	0236 XXX XX 03	CH-2
Mali İşler Sorumlusu	Ayşe Çelik	0535 XXX XX 04	0555 XXX XX 04	CH-2
Teknik Koor. Sorumlusu	Hasan Demir	0530 XXX XX 05	0544 XXX XX 05	CH-3
BT Destek Sorumlusu	Can Öztürk	0536 XXX XX 06	0532 XXX XX 06	CH-2
Lojistik Sorumlusu	Zeynep Aksoy	0537 XXX XX 07	0543 XXX XX 07	CH-2
Güvenlik Amiri	Murat Şahin	0538 XXX XX 08	Dahili: 111	CH-1

Bu liste, asil sorumluların ulaşılamaz olduğu durumlarda veya 12 saatlik vardiya sistemine (A/B Takımı) geçildiğinde göreve çağrılacak personeli tanımlar.

Tablo B.2 YEDEK PERSONEL VE VARDİYA LİSTESİ

KRİTİK ROL	ASİL SORUMLU (A Takımı)	1. YEDEK (B Takımı)	YEDEK İLETİŞİM	2. YEDEK (Acil)
Kriz Yöneticisi (KYE Lideri)	Mehmet Demirtaş	**Ali Yıldız** (Teknik Md. Yrd.)	0532 XXX XX 20	Yön. Kur. Bşk.
Olay Koordinatörü (OKE Lideri)	Elif Kaya	**Hasan Demir** (Teknik Koor. Sorumlusu)	0533 XXX XX 21	Satın Alma Md.
İFSE Lideri (İdari İşler Md.)	Ahmet Yılmaz	**Selin Can** (İK Müdürü)	0542 XXX XX 22	Muhasebe Yrd.
Mali İşler Sorumlusu	Ayşe Çelik	**Burak Tan** (Finans Uzmanı)	0535 XXX XX 23	Operatör 3
Teknik Koor. Sorumlusu	Hasan Demir	**Müh. Cemil** (Bakım Şefi)	0536 XXX XX 24	Dış Firma (SLA)
BT Destek Sorumlusu	Can Öztürk	**Emre Su** (Tekniker)	0537 XXX XX 25	İdari İşler
Lojistik Sorumlusu	Zeynep Aksoy	**xxx**		

Tablo B.3: DIŞ PAYDAŞLAR - ACİL DURUM HİZMETLERİ VE KAMU KURUMLARI

KURUM	İLGİLİ BİRİM / KİŞİ	ACİL DURUM HATTI	ALTERNATİF / NOTLAR
Genel Acil Çağrı	Operasyon Merkezi	**112**	Yangın, Polis, Ambulans
AFAD İl Müdürlüğü	Nöbetçi Amirliği	0236 231 XX XX	Faks: 0236 231 XX XX
Sanayi ve Teknoloji İl Md.	İl Müdürü	0236 233 XX XX	Resmi bildirim için
TEİAŞ (Elektrik)	Yük Tevzi Merkezi	0312 XXX XX XX	Enerji kesintisi bilgisi
MASKİ (Su/Kanal)	Arıza İhbar	185	Su kesintisi/patlak
Doğalgaz Dağıtım	Acil Müdahale	187	Gaz kaçağı durumunda
OSBÜK	Kriz Masası	0312 419 XX XX	Sektörel koordinasyon

Tablo B.4: KRİTİK TEDARİKÇİ VE HİZMET SAĞLAYICILAR

(İdari ve Teknik operasyonların sürdürülmesi için öncelikli firmalar)

HİZMET TÜRÜ	FİRMA ADI	YETKİLİ KİŞİ	7/24 TELEFON	SÖZLEŞME TİPİ
Mobil Jeneratör	Güçsan Enerji A.Ş.	Ali Güçlü	0532 XXX XX 10	4 Saatte Teslim (SLA)
BT / Sunucu Desteği	TeknoNet Bilişim	Burak Tekin	0850 XXX XX XX	2 Saatte Müdahale
Personel Yemeği	Lezzet Catering	Fatma Usta	0533 XXX XX 12	Günlük 100 Kişilik Kapasite
Personel Servisi	Turizm Taşımacılık	Mehmet Şoför	0542 XXX XX 13	Acil Tahliye Aracı
SCADA Bakım	Otomasyon Ltd.	Mühendis Veli	0535 XXX XX 14	Uzaktan Erişim Yetkili
Banka (Nakit)	X Bankası Şb. Md.	[İsim Soyisim]	05XX XXX XX 15	Manuel Talimat Protokolü

EK-C: ILIK ALAN (İTFAİYE BİNASI) ERİŞİM VE KURULUM TALİMATI

Doküman No: ISY-PLAN-ISP-001 (Ek-C)

Lokasyon: OSB İtfaiye Binası - 1. Kat Eğitim Salonu

Kapasite: 12 Kişilik Çalışma Alanı + Kriz Masası

1. AMAÇ VE KAPSAM

Bu talimat, Yönetim Binası'nın kullanılamaz hale gelmesi durumunda, Kriz Yönetim Ekibi (KYE) ve İdari Faaliyetler Süreklilik Ekibi'nin (İFSE), **İtfaiye Binası'ndaki Alternatif Çalışma Alanı'na (Ilık Alan)** nasıl gireceğini, sistemleri nasıl kuracağını ve operasyonu nasıl başlatacağını tanımlar.

2. ERİŞİM VE GÜVENLİK PROSEDÜRÜ

AŞAMA	TALİMAT / BİLGİ
GİRİŞ YETKİSİ	Bu alana sadece **"Turuncu Yaka Kartlı"** (Kriz Ekibi) personel ve İtfaiye Amiri onayıyla giriş yapılabilir.
ANAHTAR YÖNETİMİ	Eğitim Salonu ve Acil Durum Dolabı'nın yedek anahtarları, İtfaiye Binası girişindeki "Vardiya Amiri Odası"ndaki mühürlü **"Acil Durum Anahtar Kutusu (No: 3)"** içindedir. *Mühür Kodu:* K-001
GÜVENLİK	İFSE Lideri, giriş yaptıktan sonra kapıdaki "Dolu / Operasyon Var" tabelasını asar ve kapı güvenliğini sağlar.

3. SALON YERLEŞİM PLANI VE OTURMA DÜZENİ

Odaya girildiğinde ekipler aşağıdaki düzene göre yerleşmelidir:

BÖLGE	KONUM	KİMLER OTURACAK?	DONANIM
KOMUTA MASASI	Projeksiyon Cihazının önündeki U-Tipi Masa.	• Kriz Lideri (Bölge Md.) • Olay Yöneticisi • İletişim Sorumlusu	• Uydu Telefonu • Telsiz Ana İstasyonu • Ana Bilgi Ekranı
OPERASYON MASASI	Pencere kenarı (Kırmızı Prizlerin olduğu duvar).	• İFSE Lideri • Teknik Koor. (SCADA) • BT Sorumlusu	• SCADA Terminali • Renkli Yazıcı • Ağ Anahtarı (Switch)
DESTEK MASASI	Kapı girişine yakın masa.	• Mali İşler Sorumlusu • Lojistik/Satın Alma	• Manuel Formlar • Kırtasiye Seti • Telefon
LOJİSTİK KÖŞESİ	Odanın sağ arka köşesi.	*Personel Dinlenme Alanı*	• Su, Çay/Kahve • Atıştırmalıklar

4. TEKNİK BAĞLANTI NOKTALARI VE AĞ BİLGİLERİ

Cihazların zarar görmemesi ve bağlantının sağlanması için renk kodlarına uyulmalıdır.

NOKTA TİPİ	RENK / ETİKET	KULLANIM AMACI
UPS HATTI	**KIRMIZI PRİZ**	Kesintisiz güç kaynağına bağlıdır. Sadece **Dizüstü Bilgisayar, Sunucu ve Yazıcı** takınız. (Isıtıcı takmak yasaktır!)
ŞEBEKE HATTI	**MAVİ/BEYAZ PRİZ**	Şehir şebekesidir. Şarj aleti, su ısıtıcı vb. takılabilir.
SCADA AĞI	**PORT D-1**	Sadece **SCADA Terminali** içindir. Özel statik IP tanımlıdır ve üretim ağına (OT) tünellenmiştir.
İDARİ AĞ	**PORT D-2 / D-5**	İdari personel içindir. İnternet ve ERP erişimi açıktır.
WI-FI	**SSID:** OSB_ACIL	**Şifre:** Acil Durum Dolabı'ndaki mühürlü zarfta (Zarf No: WIFI-001)

5. ACİL DURUM DOLABI ENVANTERİ

Odanın köşesindeki çelik dolapta (Anahtar No: 302) aşağıdaki malzemeler hazır tutulmaktadır. **İFSE Lideri** ayda bir kez mühür kontrolü yapar.

RAF 1: TEKNOLOJİ

- [ ] 5 Adet Yedek Dizüstü Bilgisayar (Şarjlı ve VPN Yüklü)
- [ ] 1 Adet SCADA Terminali (Özel Konfigürasyonlu Dizüstü Bilgisayar)
- [ ] 5 Adet El Telsizi ve Yedek Bataryalar

- [ ] 1 Adet 8'li Network Switch ve Kablolar

RAF 2: DOKÜMANTASYON

- [ ] İş Sürekliliği Planı (İSP) - 2 Kopya
- [ ] Kriz İletişim Listeleri (Ek-B)
- [ ] Tesis Vaziyet Planları (A3 Boyutunda)
- [ ] Kırtasiye Seti (Kalem, Zımba, Kâğıt, Bant)

RAF 3: MANUEL FORMLAR (Ek-D Seti)

- [ ] 50 Adet Satın Alma Formu
- [ ] 50 Adet Ödeme Talimatı Şablonu
- [ ] 1 Adet Olay Kayıt Defteri (Log Book)
- [ ] 1 Adet Gelen-Giden Evrak Defteri

6. İLK KURULUM KONTROL LİSTESİ (İLK 15 DAKİKA)

Bu listeyi **BT Destek Sorumlusu** uygular:

- [ ] Elektrik şalterini kaldır ve "Kırmızı Prizlerde" enerji olduğunu kontrol et.
- [ ] Acil Durum Dolabını aç ve dizüstü bilgisayarları masalara yerleştir.
- [ ] Network Switch'i fişe tak ve internet ışığının yandığını teyit et.
- [ ] SCADA terminalini D-1 portuna bağla ve veri akışını test et.
- [ ] Yazıcıyı aç ve test sayfası al.
- [ ] Hazır olduğunda İFSE Lideri'ne **"Sistemler Aktif"** bilgisini ver.

EK-D:MANUEL ÇALIŞMA FORMLARI (ÇEVRİMDIŞI OPERASYON)

(Not: Bu formlardan en az 50'şer adet basılı kopya, İtfaiye Binası'ndaki Acil Durum Dolabı'nda saklanmalıdır.)

D.1 MANUEL SATIN ALMA TALEP FORMU (ACİL DURUM)

Amaç: ERP sistemi çalışmadığında yapılan harcamaların onaylanması ve kayda alınması.

DİRENÇLİ OSB - ACİL DURUM SATIN ALMA FORMU	**FORM NO: .....**
Talep Eden Birim:	.....
Tarih / Saat:	... / ... / 20... - ... : ...
Talep Gerekçesi:	[ ] Yakıt Temini [ ] İaşe/Yemek [ ] Donanım [ ] Diğer
MALZEME / HİZMET TANIMI	**MİKTAR**
1.	.....
2.	.....
3.	.....
TOPLAM TAHMİNİ TUTAR:	
ONAY (İFSE Lideri)	**ONAY (Mali İşler)**
İmza:	İmza: .....
(50.000 TL Limitine Kadar)	*(Bütçe Kontrolü)*

D.2 MANUEL ÖDEME TALİMATI (BANKA İÇİN)

Amaç: İnternet bankacılığına erişilemediğinde faks veya kurye yoluyla para transferi yapmak.

TARİH: ... / ... / 20...

SAAT: ... : ...

KONU: Acil Durum Ödeme Talimatı

..... BANKASI ŞUBE MÜDÜRLÜĞÜNE,

Kurumumuzda yaşanan teknik aksaklık nedeniyle, aşağıda detayları verilen transfer işleminin **ACİLEN** gerçekleştirilmesini ve sonucun tarafımıza telefonla (05XX ... .) bildirilmesini rica ederiz. İşbu talimat, bankanızla imzaladığımız "Acil Durum Protokolü" çerçevesinde iletilmiştir.

GÖNDEREN HESAP NO / IBAN	**TR.....**
ALICI ADI SOYADI / UNVANI	.....
ALICI IBAN	TR.....
TUTAR (Rakamla)	..... TL
TUTAR (Yazıyla)	.....
AÇIKLAMA	Acil Durum Ödemesi - [Malzeme/Hizmet Adı]

YETKİLİ İMZA 1 YETKİLİ İMZA 2

(Bölge Müdürü) (Mali İşler Müdürü)

İmza / Kaşe İmza / Kaşe

D.3 MANUEL GELEN-GİDEN EVRAK KAYIT DEFTERİ

Amaç: EBYS (Elektronik Belge Yönetim Sistemi) çalışmadığında resmi yazışmaların kaybolmasını önlemek.

SIRA NO	**TARİH / SAAT**	**GÖNDEREN / ALICI KURUM**	**KONU / ÖZET**	**TESLİM ALAN / EDEN**	**İMZA**	**ERP'YE GİRİLDİ Mİ?**
001	01.07 / 10:30	Valilik Makamı	Kriz Durum Sorusu	Ali Yılmaz	*(İmza)*	[ ]
002	01.07 / 11:15	EnerjiSA (Giden)	Kesinti Bildirimi	Zeynep Kaya	*(İmza)*	[ ]
003						[ ]

D.4 PERSONEL DURUM TAKİP ÇİZELGESİ

Amaç: Personelin sağlık durumunu ve çalışma yerini (Ev/Ofis) takip etmek.

PERSONEL ADI	BİRİMİ	DURUMU (Güvende/Yaralı)	ÇALIŞMA YERİ (Ilık Alan/Ev)	İLETİŞİM KURULDU MU?
Mehmet Demirtaş	Yönetim	Güvende	Ilık Alan	[X]
Ayşe Çelik	Muhasebe	Güvende	Ev (VPN)	[X]
Ali Veli	Arşiv	Güvende	İdari İzinli	[X]

D.5 OLAY KAYIT FORMU (INCIDENT LOG)

Amaç: Krizin "Kara Kutusu"dur. Alınan kararların hukuki delilidir.

OLAY YÖNETİCİSİ: .....

TARİH: … / ... / 20... (GG.AA.YYYY formatında)

SAAT	OLAY / GELİŞME / KARAR	KİMDEN GELDİ?	KİME İLETİLDİ?	AKSİYON
09:15	Deprem sarsıntısı hissedildi.	-	-	Çök-Kapan uygulandı.
09:18	Bina tahliye emri verildi.	Kriz Lideri	Tüm Personel	Tahliye başladı.
09:30	Toplanma alanında sayım tamam. 2 kişi eksik.	İK Müdürü	Güvenlik Amiri	Arama başlatıldı.
10:00	Yönetim Binası "Kullanılamaz" ilan edildi.	Teknik Birim	Kriz Lideri	İSP Aktivasyon kararı.
10:15	Ilık Alan (İtfaiye) açıldı.	İFSE Lideri	BT / Lojistik	Kurulum başladı.

EK-E: TESİS YERLEŞİM PLANLARI VE KRİTİK NOKTALAR

E.1: GENEL VAZİYET PLANI (TAHLİYE VE TOPLANMA)

- **Amaç:** Yönetim Binası'ndan tahliye edilen personelin güvenli bölgeye ulaşması.
- **Kritik Noktalar:**
  - **Yönetim Binası (BINA-YNT-001):** Krizin merkezi (Kullanılamaz durumda).
  - **Acil Durum Toplanma Alanı (P-1):** Yönetim binası otoparkının kuzey köşesi. (İlk sayım burada yapılır).
  - **İtfaiye Binası (BINA-ITF-001):** Toplanma alanına 200 metre mesafede. **Alternatif Komuta Merkezi (Ilık Alan)** burasıdır.
  - **Güvenlik Kulübesi:** Giriş/Çıkış kontrol noktası.

E.2: ILIK ALAN (İTFAİYE BİNASI EĞİTİM SALONU) YERLEŞİM PLANI

- **Amaç:** İFSE ekibinin İtfaiye Binası'na girdiğinde nereye oturacağını ve sistemi nasıl kuracağını göstermek.
- **Salon Düzeni:**
  - **Masa A (Kriz Yönetimi):** Projeksiyon cihazının karşısı. KYE üyeleri için 4 sandalye.
  - **Masa B (Operasyon):** Duvar kenarı (Prizlere yakın). İFSE Lideri, Teknik Koor., BT Sorumlusu için 3 sandalye.
  - **Masa C (Destek):** Kapıya yakın. Mali İşler ve Lojistik için 2 sandalye.
- **Teknik Noktalar:**
  - **Kırmızı Etiketli Prizler:** Kesintisiz Güç Kaynağına (UPS) bağlıdır. Sadece Server/ Dizüstü Bilgisayar takılır.
  - **Data Portları (D1-D5):** Duvarın sol tarafındadır. "VLAN 10 - Kriz Ağı"na tanımlıdır.
  - **Acil Durum Dolabı:** Odanın sağ arka köşesindedir. (İçinde yedek dizüstü bilgisayarlar, telsizler ve basılı formlar bulunur).
  - **Yazıcı:** Dolabın yanındaki sehpadadır.

E.3: ALTYAPI KESME NOKTALARI (YÖNETİM BİNASI)

- **Amaç:** Binada yangın veya deprem olduğunda enerjiyi keserek güvenliği sağlamak.
- **Elektrik:** Ana pano binanın bodrum kat girişindedir. "Ana Şalter" kırmızı renklidir.
- **Doğalgaz:** Bina dışındaki sarı kutudadır. Vana deprem anında otomatik kapanır, manuel kolu yanındadır.

Ek E.2.2: "Dirençli OSB" İçin Tamamlanmış İş Sürekliliği Planı (2) (Örnek: Elektrik Dağıtımı ve Bakım Hizmeti)

Dirençli OSB" İçin Tamamlanmış İş Sürekliliği Planı (2) (Örnek: Elektrik Dağıtımı ve Bakım Hizmeti)

DOKÜMAN KONTROL

Plan Adı:	Dirençli OSB - Elektrik Dağıtımı ve Bakımı İş Sürekliliği Planı
Doküman No:	İSY-İSP-ELK-001
Versiyon:	1.0
Yürürlülük Tarihi:	01/07/2025
Plan Sahibi:	Elektrik İşletme Müdürü (ESE Lideri)
Onaylayan:	Mehmet Demirtaş (Bölge Müdürü)

0. YÖNETİCİ ÖZETİ

- **Kurum:** Dirençli Organize Sanayi Bölgesi (OSB); 150 katılımcı firmanın üretim sürekliliği için hayati öneme sahip olan elektrik dağıtım şebekesini işleten lisanslı dağıtım kuruluşudur.
- **Stratejik Süreklilik Hedefi:** Ana Trafo Merkezi arızası, ulusal şebeke kesintisi veya SCADA kaybı gibi felaket senaryolarında dahi; OSB'nin kritik tesislerine (Arıtma, İtfaiye, Güvenlik) %100, sanayi katılımcılarına ise kademeli olarak en az %50 kapasiteyle enerji arzını **en geç 4 saat (RTO)** içinde yeniden sağlamaktır.

En Önemli Kritik Süreçler ve Hedefler:

#	Kritik Süreç Adı	RTO	MTPD	MBCO (Asgari İş Sürekliliği Hedefi)
1	**Elektrik Arıza/Kesinti Tespiti ve Müdahalesi**	**4 Saat**	4 Saat	Kritik katılımcılara ve OSB temel tesislerine enerji sağlanması. Diğerlerine kademeli %50 kapasite.
2	**Elektrik Şebekesi Rutin İzleme ve Kontrolü**	**2 Saat**	8 Saat	Şebekenin temel izleme fonksiyonlarının (gerilim, ana hat yükleri, kritik alarm takibi) çalışır duruma getirilmesi.
3	**Elektrik Şebekesi Planlı Bakım Faaliyetleri**	**3 İş Günü**	5 İş Günü	Kritik bakım planlarının oluşturulması ve ekiplere iletilmesi.
4	**Elektrik Hizmeti Faturalandırma ve Tahsilatı**	**5 İş Günü**	10 İş Günü	Bir önceki ayın faturalarının %95'inin oluşturulması. (Veri kaybı toleransı: 24 saat).
5	**Yeni Bağlantı ve Kapasite Artırım Talepleri**	**10 İş Günü**	15 İş Günü	Acil ve/veya yasal süresi yaklaşan yeni bağlantı/kapasite artış taleplerinin teknik değerlendirmesinin tamamlanması.

Öncelikli Tehdit Senaryoları (Risk Kayıt Formu Özeti):

1. **TEK-ELK-001 (Yüksek):** Ana Elektrik İndirici Trafosu Arızası.
2. **SIBER-SCD-001 (Yüksek):** SCADA Sistemine Fidye Yazılımı Saldırısı.
3. **ALTYP-ELK-002 (Yüksek):** TEİAŞ Kaynaklı Bölgesel Elektrik Kesintisi.
4. **N-DRN-001 (Yüksek):** Deprem Sonrası Şebeke Hasarı.
5. **MH-ZINCIR-001 (Yüksek): Zincirleme Altyapı Çöküşü.** Elektrik kesintisinin SCADA'yı, SCADA kaybının su pompalarını durdurması ve AAT'nin taşarak çevre felaketine yol açması senaryosu.

Plan Aktivasyon Kriteri:

OSB genelinde veya kritik bir bölgede enerji kesintisinin 4 saatten uzun süreceği öngörüldüğünde veya SCADA sistemine 1 saatten fazla erişilemediğinde plan aktive edilir.

Temel Stratejiler:

- **Altyapı:** Yedek Trafo (Manuel Transfer) ve Mobil Jeneratör Kiralama.
- **Operasyon:** Yük Atma (Load Shedding) Protokolü.
- **Teknoloji:** SCADA için Sıcak Bekleme (Hot-Standby) ve Manuel Saha Operasyonu.

BÖLÜM 1: PLAN YÖNETİŞİMİ

1.1 Planın Amacı

Bu planın temel amacı, "Dirençli OSB"nin en kritik altyapı hizmeti olan elektrik dağıtımının; ana trafo arızası, doğal afet veya siber saldırı gibi kesinti durumlarında dahi, belirlenen RTO süreleri (4 Saat) içinde yeniden başlatılmasını ve kritik katılımcılara asgari seviyede (MBCO) enerji arzının sürdürülmesini sağlamaktır.

1.2 Kapsam

- **Dahil Olanlar:** OSB'ye ait Ana İndirici Merkez (TM), Dağıtım Merkezleri (DM), Orta Gerilim (OG) ve Alçak Gerilim (AG) şebekesi, SCADA sistemi ve Teknik Birim personeli.
- **Hariç Olanlar:** Katılımcı firmaların kendi parsel sınırları içindeki (sayaçtan sonraki) elektrik arızaları ve TEİAŞ'ın sorumluluğundaki iletim hattı onarımları (ancak TEİAŞ ile koordinasyon bu planın parçasıdır).

1.3 İş Sürekliliği Politikası

Bu plan, "İSY-POL-001 İş Sürekliliği Politikası"ndaki "Sanayicimizin çarklarının dönmesi için kesintisiz enerji sağlama" taahhüdünü operasyonel seviyede hayata geçirir.

1.4 Referans Çerçeve

- **Yasal:** 4628 Sayılı Elektrik Piyasası Kanunu, Elektrik Kuvvetli Akım Tesisleri Yönetmeliği, 4562 Sayılı OSB Kanunu.
- **Standartlar:** ISO 22301:2019, ISO 27001 (SCADA Güvenliği).
- İç Düzenlemeler: OSB Elektrik Dağıtım Yönergesi, Bütünleşik Olay Yönetim Planı.

1.5 Organizasyonun Anlık Görüntüsü (Bağlam)

- **Kritik Varlıklar:** 1 adet Ana İndirici Trafo (T1 - 50 MVA), 1 adet Yedek Trafo (T2 - 40 MVA), SCADA Kontrol Odası.
- **Bağımlılık:** Tüm dağıtım operasyonu SCADA sistemine ve Yüksek Gerilim (YG) yetki belgesine sahip uzman personele tam bağımlıdır.

1.6 Roller & Sorumluluklar (Üst Düzey)

- **Kriz Lideri (Bölge Müdürü):** Büyük çaplı kesintilerde stratejik kararları (örneğin, OSB geneli yük atma, basın açıklaması) verir.
- **Plan Sahibi (Elektrik İşletme Müdürü):** Bu planın güncelliğinden ve kriz anında teknik ekiplerin sevk ve idaresinden sorumludur.

1.7 Plan Bakımı ve Dağıtımı

Bu plan, Elektrik İşletme Müdürü tarafından yılda en az bir kez ve her büyük şebeke değişikliğinde (yeni DM eklenmesi vb.) güncellenir. Basılı bir kopyası "SCADA Kontrol Odası"nda ve "Nöbetçi Amiri Odası"nda bulundurulur.

BÖLÜM 2: İŞ SÜREKLİLİĞİ ORGANİZASYONU & KOMUTA YAPISI

Bu plan aktive edildiğinde (Seviye 3 Kesinti), normal işletme hiyerarşisi askıya alınır ve aşağıdaki kriz organizasyonu devreye girer.

2.1 Olay Yönetim Hiyerarşisi

- **Stratejik Seviye (KYE): Bölge Müdürü**; enerji krizinin sanayiciye etkisini, yasal bildirimleri ve dış kurumlarla (TEİAŞ, Valilik) üst düzey iletişimi yönetir.
- **Taktiksel Seviye (OKE): İSYS Yöneticisi**; Elektrik ekibinin diğer birimlerle (İtfaiye, Güvenlik, İdari) koordinasyonunu ve lojistik ihtiyaçlarını (yakıt, yemek) sağlar.
- **Operasyonel Seviye (ESE): Elektrik Süreklilik Ekibi (ESE)**; sahada arızayı onarır, manevraları yapar ve şebekeyi yeniden enerjilendirir.

2.2 Elektrik Süreklilik Ekibi (ESE) Rolleri ve Sorumlulukları

Rol	Sorumlu (Yedek)	Kriz Anındaki Görevi
Ekip Lideri	Elektrik İşletme Müdürü (Bakım Şefi)	Planı aktive eder. Arıza tespit ve onarım stratejisini belirler. Saha ekiplerine manevra emri verir.
SCADA Sorumlusu	SCADA Operatörü (Otomasyon Müh.)	Şebekeyi izler. Uzaktan açma/kapama yapar. Sistem çökerse manuel moda geçişi koordine eder.
Saha Operasyon Şefi	Vardiya Amiri (Nöbetçi Teknisyen)	Sahadaki ekiplerin güvenli çalışmasını (EKAT) sağlar. Arızalı bölgeyi izole eder.
Bakım/Onarım Ekibi	Teknisyenler (A/B Vardiyası)	Fiziksel onarımı (kablo başlığı, trafo değişimi) yapar. Mobil jeneratörleri bağlar.
Dış İlişkiler Sor.	Abone İşleri Şefi (Sayaç Okuma Per.)	Katılımcı firmaların "Ne zaman elektrik gelecek?" sorularını yanıtlar ve bilgilendirir.

2.3 Olağanüstü Yetki Matrisi

Kriz anında enerji arzını hızlandırmak için aşağıdaki yetkiler tanımlanmıştır:

Fonksiyon	Normal Yetki	Kriz Yetkisi (İSP Aktifken)
Yük Atma (Kesinti)	Bölge Müdürü Onayı	**Elektrik İşl. Md.** (Doğrudan yetkili)
Acil Malzeme Alımı	Satın Alma Prosedürü	**Elektrik İşl. Md.** (50.000 TL'ye kadar doğrudan alım)
Mobil Jeneratör	İhale / Teklif	**Sözleşmeli Firmayı Çağırma** (Tek telefonla)
Personel Mesaisi	İK Onayı	**Ekip Lideri** (Tüm teknik personeli göreve çağırma)

2.4 Yetki Devri Sırası

Elektrik İşletme Müdürü'ne (Ekip Lideri) ulaşılamazsa veya iş göremez durumdaysa, komuta yetkisi şu sırayla devredilir:

Elektrik Bakım Şefi → En Kıdemli Vardiya Mühendisi → SCADA Yöneticisi

BÖLÜM 3: ANALİTİK TEMEL ÖZETİ

Bu plan, kurumun iş etki analizi ve risk değerlendirmesi çalışmalarından elde edilen somut verilere ve belirlenen önceliklere dayanmaktadır.

3.1 Kritik Süreçler ve Kurtarma Hedefleri

Elektrik Dağıtımı ve Bakımı hizmetinin sürekliliğini sağlamak için yürütülen 5 temel süreç analiz edilmiş ve kurtarma öncelikleri aşağıdaki gibi belirlenmiştir.

Tablo 3.1: Kritik Süreçler ve Hedefler

Öncelik	Kritik Süreç Adı	RTO	MTPD	MBCO (Asgari İş Sürekliliği Hedefi)
1	**Elektrik Arıza/Kesinti Tespiti ve Müdahalesi**	**4 Saat**	4 Saat	Kritik katılımcılara ve OSB temel tesislerine (Arıtma, Güvenlik) %100, diğer sanayi katılımcılarına kademeli olarak %50 kapasiteyle enerji sağlanması.
2	**Elektrik Şebekesi Rutin İzleme ve Kontrolü**	**2 Saat**	8 Saat	Şebekenin temel izleme fonksiyonlarının (gerilim, ana hat yükleri, kritik alarm takibi) çalışır duruma getirilmesi.
3	**Elektrik Şebekesi Planlı Bakım Faaliyetleri**	**3 İş Günü**	5 İş Günü	Kritik ve acil bakım planlarının oluşturulması ve ilgili ekiplere iletilmesi.
4	**Elektrik Hizmeti Faturalandırma ve Tahsilatı**	**5 İş Günü**	10 İş Günü	Bir önceki ayın faturalarının %95'inin oluşturulup gönderilmeye hazır hale getirilmesi.
5	**Yeni Bağlantı ve Kapasite Artırım Talepleri**	**10 İş Günü**	15 İş Günü	Acil ve yasal süresi yaklaşan yeni bağlantı veya kapasite artış taleplerinin teknik değerlendirmesinin tamamlanması.

3.2 Kritik BT Sistemleri Kurtarma Hedefleri

Elektrik dağıtım operasyonlarının sürdürülebilmesi için bağımlı olunan teknolojik altyapının kurtarma hedefleri şöyledir:

Tablo 3.2: Kritik BT Sistemleri

BT Sistemi / Uygulama	Desteklediği Süreç	RTO	RPO	Kritiklik Gerekçesi
SCADA Sistemi	Arıza Tespiti ve İzleme	**1 Saat**	5 Dk	Şebekenin uzaktan izlenmesi ve kontrolü için hayati öneme sahiptir.
GIS (Coğrafi Bilgi Sis.)	Arıza Yeri Tespiti	**4 Saat**	24 Saat	Yeraltı kablo arızalarında müdahale süresini kısaltır.
OSOS Sunucusu	Faturalandırma	**4 Saat**	1 Saat	Sayaç verilerinin kaybı finansal risk oluşturur.
E-Posta Sunucusu	İletişim ve Koordinasyon	**4 Saat**	1 Saat	Katılımcı ve tedarikçi iletişimi için gereklidir.

3.3 Risk Değerlendirmesi Özeti

Bu planın aktivasyonunu tetikleyebilecek ve elektrik altyapısını tehdit eden öncelikli riskler şunlardır:

1. **TEK-ELK-001 (Yüksek):** Ana Elektrik İndirici Trafosu Arızası. Tek nokta hatası olması nedeniyle tüm OSB'yi enerjisiz bırakma potansiyeli vardır.

2. **SIBER-SCD-001 (Yüksek):** SCADA Sistemine Yönelik Fidye Yazılımı Saldırısı. Şebeke üzerindeki kontrolün ve izlenebilirliğin kaybına yol açar.
3. **ALTYP-ELK-002 (Yüksek):** TEİAŞ Kaynaklı Bölgesel Elektrik Kesintisi. OSB dışından kaynaklanan ve uzun sürebilecek enerji arzı kaybıdır.
4. **N-DRN-001 (Yüksek):** Şiddetli Deprem. Yeraltı ve yerüstü şebeke unsurlarında yaygın fiziksel hasar riski taşır.
5. **MH-ZINCIR-001 (Yüksek - Zincirleme Etki):** Deprem Tetiklemeli Altyapı Çöküşü. Elektrik kesintisinin SCADA kaybına, bunun da su pompalarının durmasına ve nihayetinde Atık Su Arıtma Tesisi'nin (AAT) taşarak çevre felaketine yol açmasına neden olduğu domino etkisi senaryosudur.

3.4 Kritik Bağımlılıklar

Bu süreçlerin kurtarılabilmesi için aşağıdaki kaynaklara mutlak bağımlılık vardır. Planın başarısı bu bağımlılıkların yönetilmesine bağlıdır.

Tablo 3.4: Bağımlılık Matrisi

Kritik Süreç	İç Bağımlılıklar (Olmazsa Çalışamaz)	Dış Bağımlılıklar (Tedarikçi/Kurum)
Elektrik Arıza/Kesinti Tespiti ve Müdahalesi	**BT Birimi** (SCADA/Haberleşme) **Güvenlik Birimi** (Saha Erişimi)	**TEİAŞ** (Ana Enerji Beslemesi) **Akaryakıt Tedarikçisi** (Jeneratör Yakıtı) **Vinç/Nakliye Firması** (Ağır Ekipman)
Elektrik Şebekesi Rutin İzleme ve Kontrolü	**BT Birimi** (Ağ Altyapısı) **İdari Birim** (Nöbet Düzeni)	**SCADA Yazılım Firması** (Teknik Destek) **Telekom Operatörü** (Veri Hattı)
Elektrik Şebekesi Planlı Bakım Faaliyetleri	**Satın Alma Birimi** (Yedek Parça) **Mali İşler** (Bütçe Onayı)	**Malzeme Tedarikçileri** (Kablo, Başlık) **Kalibrasyon Firması** (Test Cihazları)
Elektrik Hizmeti Faturalandırma ve Tahsilatı	**Teknik Birim** (OSOS Verisi) **BT Birimi** (Sunucu)	-
Yeni Bağlantı ve Kapasite Artırım Talepleri	**İmar Birimi** (Ruhsat Bilgisi) **İdari Birim** (Evrak Akışı)	-

BÖLÜM 4: İŞ SÜREKLİLİĞİ STRATEJİLERİ VE ÇÖZÜMLERİ

Bu bölüm, İEA ve RD analizleri sonucunda belirlenen riskleri yönetmek ve RTO hedeflerine ulaşmak için Dirençli OSB'nin benimsediği temel yaklaşımları tanımlar.

4.1 Genel Stratejik Yaklaşım

Dirençli OSB Teknik Birimi, elektrik dağıtım hizmetinin sürekliliği için **"Yedekli Altyapı ve Esnek Operasyon"** felsefesini benimser. Amacımız, tek bir ekipmanın (Trafo) veya sistemin (SCADA) kaybının, tüm OSB'yi karanlıkta bırakmasını engellemektir.

4.2 Olay Öncesi Stratejiler (Önleme ve Hazırlık)

Bu stratejiler, risk gerçekleşmeden önce sistemin direncini artırmak için uygulanır.

- **Altyapı Stratejisi (Yedeklilik):**
  - **Strateji:** Ana enerji besleme noktasındaki tek nokta hatasını (T1 Trafosu) yönetmek.
  - **Çözüm:** Mevcut **Yedek Trafo (T2 - 40 MVA)**'nun periyodik bakımlarının yapılması ve manuel transfer prosedürlerinin hazır tutulması. Uzun vadede Otomatik Transfer Sistemi (ATS) yatırımı planlanması.
  - **Aksiyonlar:** T2 trafosunun ayda bir boşta çalıştırılarak test edilmesi ve manevra talimatlarının güncel tutulması.
- **Operasyonel Strateji (Yük Yönetimi):**
  - **Strateji:** Kısıtlı enerji durumunda (T2 kapasitesi veya Ulusal Kısıntı) öncelikleri belirlemek.
  - **Çözüm: "Yük Atma (Load Shedding) Protokolü"**.
  - **Aksiyonlar:** Tüm fiderlerin "Kritik" (AAT, İdari, Gıda) ve "Kesilebilir" (Demir-Çelik, Tekstil) olarak sınıflandırılması ve bu listenin (Ek-A) SCADA odasında asılı tutulması.
- **Teknoloji ve Veri Stratejisi (Siber Hazırlık ve Yedekleme):**
  - **Strateji:** SCADA ve OSOS (Faturalandırma) sistemlerini siber tehditlerden korumak ve veri kaybını önlemek.
  - **Çözüm: "İzole Ağ (Air-Gap)"** ve **"Sık Yedekleme (High Frequency Backup)"**.
  - **Aksiyonlar:**
    - ❑ SCADA ağının idari ağdan fiziksel olarak ayrılması.
    - ❑ OSOS faturalandırma verilerinin günlük olarak harici diske ve buluta şifreli yedeklenmesi (RPO: 1 Saat).
    - ❑ Felaket Kurtarma Merkezi'nde yedek bir sunucunun hazır tutulması.
- **Kaynak Stratejisi (Alternatif Güç):**
  - **Strateji:** Şebeke tamamen çöktüğünde kritik noktaları (Arıtma, Güvenlik) beslemek.
  - **Çözüm: "Mobil Jeneratör Kiralama Çerçeve Sözleşmesi"**.

- **Aksiyonlar:** Tedarikçi ile "4 Saatte Teslim" garantili sözleşme imzalanması ve dağıtım merkezlerinde bağlantı noktalarının (konnektörlerin) hazır edilmesi.

- **Entegre Altyapı Stratejisi (Zincirleme Etki Kontrolü):**
  - **Strateji:** Elektrik kesintisinin su ve atıksu sistemlerini çökertmesini (Domino Etkisi) önlemek.
  - **Çözüm: "Kritik Altyapı Önceliklendirme Protokolü"**.
  - **Aksiyonlar:** AAT ve Su Pompaları besleme fiderlerinin "Kesilemez Yük" olarak işaretlenmesi ve bu birimlerle telsiz iletişim kanalının (Kanal 4) tanımlanması.

4.3 Olay Sırası Stratejileri (Müdahale ve Süreklilik)

Kesinti anında hizmetin RTO süreleri (4 Saat) içinde yeniden başlatılmasını hedefler.

- **Manuel Transfer Stratejisi:**
  - **Senaryo:** Ana Trafo (T1) Arızası (Risk: TEK-ELK-001).
  - **Aksiyon:** Arıza tespit edildiğinde T1 izole edilir. Yük Atma prosedürü uygulanarak talep T2 kapasitesine düşürülür. Ekipler manuel manevra ile yükü Yedek Trafo (T2)'ye aktarır.
- **Ada Modu Stratejisi (Island Mode):**
  - **Senaryo:** Ulusal Şebeke (TEİAŞ) Kesintisi (Risk: ALTYP-ELK-002).
  - **Aksiyon:** Şebeke dışarıdan izole edilir. Kiralanan mobil jeneratörler kritik Dağıtım Merkezlerine (DM) bağlanır ve sadece öncelikli tesisler (Arıtma, Güvenlik) beslenir.
- **Manuel Operasyon Stratejisi:**
  - **Senaryo:** SCADA Sisteminin Çökmesi veya Siber Saldırı (Risk: SIBER-SCD-001).
  - **Aksiyon:** "Teknoloji Yoksa Telsiz Var" prensibi uygulanır. SCADA sistemi kapatılır. Saha ekipleri trafo merkezlerine dağılır. Merkezden telsizle verilen emirlerle manevralar manuel olarak yapılır.
- **Veri Koruma ve Manuel Kayıt Stratejisi:**
  - **Senaryo:** OSOS Sunucusunun Erişilemez Olması (Siber Saldırı/Bina Kaybı).
  - **Aksiyon:** Otomatik okuma yapılamıyorsa, son endeks verileri güvene alınır (Yedekten Dönüş). Yeni okumalar saha ekipleri tarafından **manuel (gözle okuma)** yapılarak kayıt altına alınır ve faturalandırma süreci manuel verilerle işletilir.
- **Çapraz Koordinasyon Stratejisi:**
  - **Senaryo:** Zincirleme Altyapı Riski (Risk: MH-ZINCIR-001).
  - **Aksiyon:** Elektrik Ekibi, Su ve Çevre birimleriyle anlık koordinasyon kurar. Enerji kısıtlıysa, sanayi yerine öncelikle AAT pompaları beslenerek çevre felaketi önlenir.

4.4 Olay Sonrası Stratejileri (Kurtarma ve İyileştirme)

Bu stratejiler, geçici çözümlerden normal operasyonlara dönüşü sağlar.

- **Normalleşme:** Arızalı ana trafonun onarımı veya yenilenmesi sonrası yükün tekrar T1'e aktarılması. Jeneratörlerin devreden çıkarılması.
- **Veri Kurtarma (Failback):** SCADA ve OSOS verilerinin Felaket Kurtarma Merkezi'nden veya yedek disklerden ana sunucuya geri yüklenmesi. Manuel tutulan kayıtların sisteme işlenmesi.
- **Analiz:** Kesintinin kök neden analizi (RCA) yapılarak bakım planlarının ve siber güvenlik kurallarının güncellenmesi.

4.5 Strateji Özeti ve Prosedür Eşleşme Tablosu

Aşağıdaki tablo, hangi risk senaryosunda hangi stratejinin devreye gireceğini ve Bölüm 6'daki hangi prosedürle uygulanacağını özetler.

Risk Senaryosu	Seçilen Strateji	İlgili Uygulama Prosedürü (Bölüm 6)
Ana Trafo Arızası **(TEK-ELK-001)**	**Altyapı Yedekliliği** (Manuel Transfer)	**İSP-ELK-01:** Arıza Tespiti ve Müdahale
Kapasite Yetersizliği **(T2 Kullanımı)**	**Operasyonel Yönetim** (Yük Atma)	**İSP-ELK-03:** Yük Atma Operasyonu
Ulusal Kesinti / Afet **(ALTYP-ELK-002)**	**Acil Güç** (Ada Modu)	**İSP-ELK-01:** Arıza Tespiti ve Müdahale
SCADA Kaybı / Siber **(SIBER-SCD-001)**	**Manuel Operasyon** (Telsizle Yönetim)	**İSP-ELK-02:** SCADA Kaybı ve Manuel Yönetim
Faturalama Sistemi Kaybı **(SIBER-SCD-001)**	**Veri Koruma ve Manuel Kayıt**	**İSP-FAT-01:** Faturalandırma ve Manuel Kayıt
Zincirleme Altyapı Riski **(MH-ZINCIR-001)**	**Entegre Altyapı Yönetimi**	**İSP-ELK-04:** Zincirleme Altyapı Koordinasyonu

BÖLÜM 5: AKTİVASYON VE OLAY YÖNETİM PROSEDÜRLERİ

Bu bölüm, bir elektrik kesintisi veya arıza anında müdahale felsefesini, planın hangi kriterlere göre aktive edileceğini, komuta merkezinin nasıl çalışacağını ve iletişim protokollerini tanımlar.

5.1 Aktivasyon Kriterleri ve Yükseltme Akışı (Olay Seviyeleri)

Olaylar, etkilerine ve çözüm sürelerine göre 4 seviyede sınıflandırılır. Planın aktivasyonu bu seviyelere bağlıdır.

Seviye 1: Rutin Arıza (Incident):

- **Tanım:** Tek bir aboneyi, bir sokak aydınlatma hattını veya tali bir dağıtım panosunu etkileyen, yedekli sistemlerin otomatik devreye girdiği veya nöbetçi ekibin 2 saatten kısa sürede çözebileceği durumlar.
- **Örnek:** Bir fabrikanın girişindeki sigortanın atması, AG (Alçak Gerilim) kablosunda lokal kopukluk.
- **Aksiyon: İSP Aktive Edilmez.** Arıza, Standart İşletme Prosedürleri (SOP) ile Nöbetçi Teknisyen tarafından yönetilir.

Seviye 2: Acil Durum (Emergency):

- **Tanım:** Can veya mal güvenliğini tehdit eden (yangın, patlama riski) veya kritik bir tesisi (Arıtma, İtfaiye) besleyen tekil bir hattın kaybı.
- **Örnek:** Bir dağıtım merkezinde (DM) trafo yangını, direk devrilmesi, AAT'yi besleyen kablonun kopması.
- **Aksiyon: Acil Durum Müdahale Planı (ADMP)** derhal aktive edilir. İtfaiye ve Bakım ekibi sahaya sevk edilir. İSP "Beklemede" moduna geçer.

Seviye 3: İş Kesintisi / Felaket (Disruption):

- **Tanım:** RTO sürelerinin aşılma riskinin olduğu büyük çaplı kesintiler.
  - ❑ **Süre Kriteri:** OSB genelinde veya geniş bir bölgede enerjinin **4 saatten fazla** kesileceği öngörülürse.
  - ❑ **Varlık Kriteri:** Ana İndirici Trafo (T1) kaybı veya TEİAŞ kaynaklı tam kesinti yaşanırsa.
  - ❑ **Teknoloji Kriteri:** SCADA sistemi **1 saatten fazla** erişilemez olursa.
- **Aksiyon: Bu Plan (İSP)** resmen aktive edilir. Tüm teknik personel göreve çağrılır. Yük Atma veya Jeneratör prosedürleri devreye girer.

Seviye 4: Kriz (Crisis):

- **Tanım:** Kesintinin OSB'nin itibarını, yasal statüsünü (Lisans İptali riski) veya finansal yapısını tehdit etmesi.
- **Örnek:** 24 saati aşan tam kesinti, çevre felaketine yol açan trafo patlaması, siber saldırı sonucu sistemlerin ele geçirilmesi.
- **Aksiyon: Kriz Yönetim Planı (KYP)** ve **Kriz İletişim Planı (KİP)** devreye girer. Komuta Bölge Müdürü'ne geçer.

5.2 Komuta Merkezi (ADOM - Acil Durum Operasyon Merkezi)

Elektrik arızalarında komuta merkezi, olayın teknik niteliğine göre belirlenir.

- **Birincil ADOM (Teknik Merkez): SCADA Kontrol Odası (Yönetim Binası).**
  - **Gerekçe:** Şebekenin izlendiği, manevra emirlerinin verildiği ve iletişim altyapısının (Telsiz/Telefon) en güçlü olduğu yerdir.
- **İkincil ADOM (Alternatif): İtfaiye Binası Toplantı Salonu.**
  - **Gerekçe:** Yönetim Binası'nın (veya SCADA odasının) yangın/deprem nedeniyle kullanılamaz olması durumunda, yedek SCADA terminalinin bulunduğu bu alana geçilir.
- **Saha Komuta: Mobil Araç Telsizi.**
  - **Gerekçe:** Arıza bölgesindeki Ekip Lideri, sahadaki operasyonu (onarım, izolasyon) buradan yönetir.

5.3 Genel Olay Yönetim Döngüsü

İSP aktive edildiğinde (Seviye 3), süreç şu adımları izler:

- **Tespit ve Değerlendirme:**
  - SCADA alarmı veya katılımcı ihbarı ile kesinti tespit edilir.
  - Vardiya Amiri, arızanın boyutunu (Etkilenen MW gücü ve Abone sayısı) ve tahmini onarım süresini (ETR) belirler.
  - Eğer ETR > 4 Saat ise Elektrik İşletme Müdürü'ne "Aktivasyon" önerir.
- **Aktivasyon ve Strateji Seçimi:**
  - Elektrik İşletme Müdürü, **Adaptif Müdahale Matrisi (Bölüm 5.5)**'ne bakarak stratejiyi belirler (Örn: "Yük Atma Başlat" veya "Manuel Moda Geç").
  - İlgili prosedür (6.1, 6.2 veya 6.3) başlatılır.
- **Müdahale ve Kurtarma:**
  - Saha ekipleri arızayı izole eder ve alternatif besleme (Ring) yapar.
  - Gerekirse Mobil Jeneratörler kritik noktalara bağlanır (Ada Modu).
  - **Amaç:** RTO (4 saat) içinde kritik yüklere %100, diğerlerine %50 enerji vermektir.
- **Normale Dönüş:**
  - Ana arıza giderildikten sonra şebeke normal besleme düzenine (Normal Open Point) döndürülür.
  - Mobil jeneratörler devreden çıkarılır.

5.4 İletişim Prosedürleri

Elektrik kesintilerinde bilgi akışı hayati önem taşır.

Tablo 5.1: Elektrik Kesintisi İletişim Matrisi

Kiminle İletişime Geçilecek	İletişim Sorumlusu	Kullanılacak Yöntem	Zamanlama
İÇ: Saha Ekipleri	SCADA Operatörü	Telsiz (Kanal 3)	Anlık (Manevra Emirleri)
İÇ: Kriz Yönetimi (KYE)	Elektrik İşl. Müdürü	Telefon / Yüz Yüze	Her saat başı
DIŞ: TEİAŞ Yük Tevzi	Elektrik İşl. Müdürü	Direkt Hat (Kırmızı Telefon)	Kesinti anında ve değişimde
DIŞ: Katılımcı Firmalar	Abone İşleri / İdari	Toplu SMS / E-posta	İlk 30 dakikada ("Kesinti Bilgisi") ve RTO aşıldığında
DIŞ: Kritik Tedarikçi	Satın Alma Sor.	Telefon	Yakıt/Parça ihtiyacında

5.5 ADAPTİF MÜDAHALE SENARYOLARI (ZAMAN VE TÜR BAZLI AKIŞ)

Aşağıdaki tablolar, elektrik kesintisinin **türüne** (Teknik Arıza, Ulusal Kesinti, Siber Saldırı) ve **zamanına** (Mesai İçi/Dışı) göre ilk tepkinin ve kararların nasıl değişeceğini detaylandırır.

Tablo 5.2: Adaptif Müdahale Akışı - Faz 1: Anlık Müdahale (İlk 5-60 Dakika)

OLAY TÜRÜ & ZAMANI	LOKAL TEKNİK ARIZA (Trafo/Kablo Arızası) MESAİ SAATLERİ İÇİNDE	BÖLGESEL/ULUSAL KESİNTİ (TEİAŞ Kaynaklı) HER ZAMAN	LOKAL TEKNİK ARIZA MESAİ DIŞINDA (GECE)	SİBER SALDIRI / SCADA KAYBI HER ZAMAN
SAHA PERSONELİNİN İLK EYLEMİ	**1. Tespit:** SCADA alarmını teyit et. **2. İzolasyon:** Arızalı fideri uzaktan (veya sahada) aç. **3. Hazırlık:** Arıza arama aracını hazırla.	**1. Teyit:** TEİAŞ Yük Tevzi'yi ara, durumu sor. **2. Kontrol:** İndirici Merkezdeki (TM) giriş kesicilerini kontrol et. **3. Jeneratör:** Kritik tesis jeneratörlerini kontrol et.	**1. İhbar:** Nöbetçi teknisyen alarmı görür. **2. İlk Müdahale:** Tek başına müdahale etme, ekibi bekle. **3. Bildirim:** İşletme Müdürünü ara.	**1. Tespit:** Ekran donması veya fidye mesajı. **2. İzolasyon:** İnternet kablosunu fiziksel olarak çek. **3. Manuel Mod:** Telsizle "Manuel Operasyon" anonsu geç.
YÖNETİMİN İLK EYLEMİ	**1. Ekip Sevk:** Bakım ekibini arıza bölgesine gönder. **2. Analiz:** Tahmini Onarım Süresini (ETR) hesapla. **3. Karar:** "4 saati geçerse mobil jeneratör iste."	**1. Bilgilendirme:** Üst yönetime "Bizden kaynaklı değil" bilgisini ver. **2. SMS:** Katılımcıya "Ulusal şebeke arızası" mesajı at. **3. Yük Atma:** Şebeke gelince "Blackstart" için yükleri ayır.	**1. Çağrı:** İcapçı (on-call) ekibi evden çağır. **2. Güvenlik:** Gece bekçisini trafo merkezine yönlendir.	**1. BT Çağrısı:** BT Müdürü ve Siber Ekibi çağır. **2. Saha Yönetimi:** Ekipleri kritik Dağıtım Merkezlerine (DM) gönder. **3. Karar:** "Sistemi kapat, telsizle manevra yapacağız."

Tablo 5.3: Adaptif Müdahale Akışı - Faz 2: Değerlendirme & İletişim (Saat 1-12)

OLAY TÜRÜ & ZAMANI	LOKAL TEKNİK ARIZA (Mesai İçi)	ULUSAL KESİNTİ (Her Zaman)	LOKAL TEKNİK ARIZA (Gece)	SİBER SALDIRI (Her Zaman)
EKİP AKTİVASYONU	**Tam Kadro:** Tüm bakım ekibi sahada aktif çalışır.	**Kritik Kadro:** Sadece ana kumanda ve kritik tesis nöbetçileri kalır.	**İcapçı Ekip:** Evden gelen ekip sahaya çıkar.	**Manuel Ekip:** Her DM'ye bir teknisyen yerleştirilir (Telsizli).
HASAR DEĞERLENDİRME	**Fiziksel Test:** Kablo test aracı ile arıza noktası bulunur.	**Bekleme:** TEİAŞ'tan enerji gelmesi beklenir. Hasar yoktur.	**Görsel Kontrol:** Fener ile hatlar kontrol edilir. Test gündüze bırakılabilir.	**Siber Analiz:** BT ekibi logları inceler. Saha ekibi şalter durumlarına bakar.
RESMİ İLETİŞİM	**SMS:** "Arıza tespit edildi, onarım sürüyor."	**SMS/Web:** "Ulusal kesinti devam ediyor."	**SMS:** "Bölgesel arıza var, ekip çalışıyor."	**İç Bilgi:** "Sistem kapalı, manuel çalışıyoruz." (Dışarıya detay verilmez).

Tablo 5.4: Adaptif Müdahale Akışı - Faz 3: İş Sürekliliği (İSP) Aktivasyonu (Saat 12-72)

OLAY TÜRÜ & ZAMANI	LOKAL TEKNİK ARIZA	ULUSAL KESİNTİ	LOKAL TEKNİK ARIZA (Gece)	SİBER SALDIRI
AKTİVASYON KARARI	**İSP AKTİF:** Onarım 4 saati aştı. Yedek trafo/hat devrede.	**YÜK ATMA AKTİF:** Kısmi enerji gelirse sadece kritiklere verilir.	**İSP AKTİF:** Sabaha kadar jeneratörle besleme kararı.	**MANUEL İSP AKTİF:** SCADA açılana kadar telsizle yönetim.
KAYNAK TAHSİSİ	**Lojistik:** Mobil jeneratörler kiralanır ve bağlanır.	**Tasarruf:** Jeneratör yakıtları idareli kullanılır.	**Güvenlik:** Arıza bölgesinde güvenlik nöbeti.	**BT Desteği:** Dış siber güvenlik firmasından destek alınır.

BÖLÜM 6: İŞ KURTARMA PROSEDÜRLERİ (KONTROL LİSTELERİ)

Bu bölüm, İSP aktive edildikten sonra, Elektrik Süreklilik Ekibi (ESE) tarafından uygulanacak olan adım adım kurtarma talimatlarını içerir. Her prosedür, ilgili sürecin RTO hedefine ulaşmasını sağlamak üzere tasarlanmıştır.

6.1 Prosedür İSP-ELK-01: Elektrik Arıza/Kesinti Tespiti ve Müdahalesi

İlgili Süreç:	**Elektrik Arıza/Kesinti Tespiti ve Müdahalesi**
RTO (Hedef Süre):	**4 Saat**
MBCO (Asgari Hedef):	Kritik katılımcılara ve OSB temel tesislerine (Arıtma, Güvenlik) %100, diğerlerine %50 enerji sağlanması.
Sorumlu:	Saha Operasyon Şefi (Vardiya Amiri)

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
1	**Güvenli İzolasyon:** Arızalı bölgeyi (Trafo, Kablo veya Dağıtım Merkezi) giriş/çıkış kesicilerini açarak izole et. "Çalışma Var" kartı as ve topraklama yap.	[ ]	*EKAT yönetmeliğine ve İSG kurallarına tam uyulmalıdır.*
2	**Hasar Analizi:** Arızanın fiziksel nedenini (kablo patlağı, buşing hasarı, trafo yanığı) tespit et. Onarım süresi **4 saati geçecekse** derhal "B Planı"na (Jeneratör/Yedek Hat) geç.	[ ]	*Kriz Liderine ETR (Tahmini Onarım Süresi) bilgisini ver.*
3	**Ring Besleme (Varsa):** Arıza kabloda ise, ring şebeke üzerindeki diğer Dağıtım Merkezlerinden (DM) tersten besleme manevrasını planla ve uygula.	[ ]	*Yük akış analizine dikkat et.*
4	**Yedek Trafo (T2) Devreye Alma:** Eğer Ana Trafo (T1) arızalıysa; • T1 giriş/çıkışını ayır. • T2 boşta testini yap. • T2'yi devreye al ve yükü kademeli olarak aktar.	[ ]	*T2 kapasitesi (40MVA) yetmezse önce **Prosedür 6.3 (Yük Atma)** uygula.*
5	**Mobil Jeneratör (Ada Modu):** Şebeke onarılamıyorsa, sözleşmeli tedarikçiyi (Güçsan Enerji) ara. Jeneratörleri Kritik DM'lere bağlayarak "Ada Modu"na geç.	[ ]	*Öncelik: Arıtma Tesisi Pompaları ve İdari Bina.*
6	**Enerjilendirme ve Kontrol:** Güvenlik önlemleri alındıktan sonra hattı enerjilendir. SCADA'dan veya sahada ampermetre ile yük durumunu kontrol et.	[ ]	*Dengesiz yüklenmeyi önle.*

6.2 Prosedür İSP-ELK-02: Elektrik Şebekesi Rutin İzleme ve Kontrolü (SCADA Kaybı Durumu)

İlgili Süreç:	**Elektrik Şebekesi Rutin İzleme ve Kontrolü**
RTO (Hedef Süre):	**1 Saat** (Manuel kontrole geçiş süresi)
MBCO (Asgari Hedef):	Şebekenin kör uçuş yapmadan, telsiz koordinasyonu ile güvenli yönetilmesi.
Sorumlu:	SCADA Sorumlusu ve Saha Ekipleri
Tetikleyici:	SCADA sistemine siber saldırı veya sunucu arızası.

Adım No	**Eylem**	**Tamamlandı mı?**	**Notlar / Kritik Detay**
1	**Bağlantı Kesme (İzolasyon):** Siber saldırı şüphesi varsa, SCADA sunucusunun dış ağ (internet) kablosunu fiziksel olarak çek (Air-Gap).	[ ]	*Virüsün yayılmasını önle.*
2	**Felaket Kurtarma Merkezi Denemesi:** Felaket Kurtarma Merkezi'ndeki (YDK-IT-01) yedek SCADA sunucusuna bağlanmayı dene. Başarılıysa operasyona oradan devam et.	[ ]	*BT Birimi ile koordineli ol. (Bkz. BT-FKP)*
3	**Manuel Moda Geçiş:** Felaket Kurtarma Merkezi çalışmıyorsa "Manuel Mod" ilan et. Saha ekiplerini kritik Dağıtım Merkezlerine (DM) ve İndirici Merkeze (TM) gönder.	[ ]	*Her kritik DM'de en az 1 teknisyen olmalı.*
4	**Telsizle Koordinasyon:** Tüm manevra emirlerini telsiz üzerinden **"Sesli Teyit" (Read-back)** usulüyle ver.	[ ]	*Örn: "DM-3 Kesicisini AÇ" → "Anlaşıldı, DM-3 Kesicisini AÇIYORUM."*
5	**Fiziksel İzleme:** Teknisyenler, trafo sıcaklıklarını, yağ seviyelerini ve sayaç değerlerini saat başı merkeze telsizle raporlasın.	[ ]	*Körlüğü gidermek için şarttır. Verileri "Manuel Kayıt Defteri"ne işle.*

6.3 Prosedür İSP-ELK-03: Yük Atma (Load Shedding) Operasyonu

İlgili Süreç:	**Elektrik Dağıtımı (Kapasite Yönetimi)**
RTO (Hedef Süre):	**2 Saat**
MBCO (Asgari Hedef):	Mevcut kısıtlı kapasite ile kritik tesislerin (AAT, Güvenlik) beslenmesi.
Sorumlu:	Elektrik İşletme Müdürü
Tetikleyici:	Yedek Trafo (T2) kullanımı veya Ulusal Şebeke (TEİAŞ) kısıntısı.

Adım No	**Eylem**	**Tamamlandı mı?**	**Notlar / Kritik Detay**
1	**Kapasite Analizi:** Mevcut güvenli kapasiteyi (örn. T2 Trafosu: 40 MVA) ve anlık talebi (örn. 55 MVA) karşılaştır. Atılması gereken yük miktarını (15 MVA) belirle.	[ ]	*Trafo aşırı yüklenmemelidir.*
2	**Öncelik Listesi Kontrolü:** "Ek-A: Yük Atma Öncelik Listesi"ni aç. Kesilecek fiderleri sırasıyla belirle (Örn: 1. Grup: Demir-Çelik, 2. Grup: Tekstil).	[ ]	*Kritik tesisler (AAT, Gıda, İlaç) listede "Korunacak" statüsündedir.*
3	**Kesinti Uygulama:** Seçilen fiderlerin kesicilerini SCADA'dan (veya manuel olarak) aç.	[ ]	*Ani yük değişimine (ark oluşumu) dikkat et.*

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
4	**Katılımcı Bilgilendirmesi:** Enerjisi kesilen firmalara SMS/E-posta ile "Zorunlu Yük Kısıtlaması" yapıldığı bilgisini ve tahmini süreyi ilet.	[ ]	*İletişim Sorumlusu ile koordine ol.*
5	**Rotasyon:** Kesinti 4 saati aşarsa, adil kullanım için kesilen fiderleri devreye alıp diğer grubu keserek **"Dönüşümlü (Rotasyonlu) Veriş"** uygula.	[ ]	*Her firmaya belirli süre enerji ver (Örn: 4 saat var, 4 saat yok).*

6.4 Prosedür İSP-FAT-01: Faturalandırma Veri Koruma ve Manuel Kayıt

Bu prosedür, siber saldırı veya sunucu arızası nedeniyle **OSOS (Otomatik Sayaç Okuma Sistemi)** ve faturalandırma yazılımına erişilemediği durumlarda, gelir kaybını önlemek ve veri bütünlüğünü sağlamak için uygulanır.

İlgili Süreç:	Elektrik Hizmeti Faturalandırma ve Tahsilatı
RTO (Hedef Süre):	**5 İş Günü** (Fatura kesimi için) / **24 Saat** (Veri kurtarma için)
MBCO (Asgari Hedef):	Sayaç endeks verilerinin kaybolmaması ve manuel takibi.
Sorumlu:	Abone İşleri Şefi (Destek: Teknik Saha Ekipleri)
Tetikleyici:	OSOS Sunucusunun veya İletişim Hattının 24 saatten fazla kesilmesi.

Adım No	Eylem	Tamamlandı mı?	Notlar / Kritik Detay
1	**Veri Güvenliği (Snapshot):** Arıza veya siber saldırı anında, eğer erişim mümkünse, son güncel endeks verilerinin yedeğini al ve ağdan bağımsız (Offline) bir diske kaydet.	[ ]	*Veri kaybını (RPO: 1 Saat) minimize et.*
2	**Manuel Okuma Kararı:** OSOS sistemi 24 saat içinde düzelmezse, **"Manuel Okuma (Gözle Okuma)"** planını devreye al.	[ ]	*Kriz Lideri onayı ile.*
3	**Önceliklendirme (Pareto):** Okuma listesini hazırla. Önceliği, OSB toplam tüketiminin %80'ini oluşturan **"Büyük Tüketicilere" (İlk 20 Firma)** ver.	[ ]	*Gelir akışını garantiye al.*
4	**Saha Operasyonu:** Saha ekiplerini sayaç okumaya gönder. Okunan her endeksin **fotoğrafını çekmelerini** ve "Manuel Sayaç Okuma Formu"na (Kâğıt) işlemelerini sağla.	[ ]	*Fotoğraf, itiraz durumunda kanıttır.*
5	**Veri Konsolidasyonu:** Sahadan gelen kağıt formlardaki verileri, elektrik/internet olmayan ortamda çalışabilen bir laptopta "Acil Durum Excel Tablosu"na işle.	[ ]	*Hesaplama hatalarını önle.*
6	**Geçici Fatura/Bilgilendirme:** Sistemler 5 günü aşan sürede gelmezse, katılımcılara Excel üzerinden hesaplanan **"Tahmini/Avans Tutar"** bilgisini resmi yazıyla bildir.	[ ]	*Nakit akışını sürdür.*
7	**Sisteme Giriş (Recovery):** ERP/OSOS sistemi açıldığında, manuel okunan endeksleri ve fotoğrafları sisteme geriye dönük tarihle işle.	[ ]	*Veri bütünlüğünü sağla.*

6.5 Prosedür İSP-ELK-04: Zincirleme Altyapı Arızası ve Koordinasyon

Bu prosedür, elektrik kesintisinin diğer kritik altyapıları (Su, Atık Su) etkileyerek **çevre felaketi** gibi daha büyük krizlere (Domino Etkisi) yol açmasını önlemek için uygulanır.

İlgili Süreç:	**Teknik Koordinasyon (Entegre Altyapı Yönetimi)**
RTO (Hedef Süre):	**1 Saat** (Kritik altyapı koordinasyonu için)
MBCO (Asgari Hedef):	Elektrik kesintisine rağmen AAT ve Su Pompalarının çalışır tutulması veya güvenli duruşun sağlanması.
Sorumlu:	Elektrik İşletme Müdürü
Tetikleyici:	Elektrik kesintisinin Su/Atık Su operasyonunu tehdit etmesi (Risk: MH-ZINCIR-001).

Adım No	**Eylem**	**Tamamlandı mı?**	**Notlar / Kritik Detay**
1	**Çapraz Durum Sorgusu:** Kesinti başlar başlamaz Su ve Çevre (AAT) birim yöneticileriyle **Telsiz (Kanal 1)** veya Dahili hat üzerinden temasa geç. Durumlarını (Taşma riski var mı? Su deposu seviyesi ne?) sor.	[ ]	*Domino etkisini erken tespit etmek hayati önem taşır.*
2	**Önceliklendirme:** Eğer AAT taşma riski varsa veya su depoları kritik seviyedeyse, eldeki tüm enerjiyi (T2 veya Jeneratör) öncelikle **Fider-01**'e (Altyapı Besleme Hattı) yönlendir.	[ ]	*Sanayiye enerji verme, altyapıyı kurtar.*
3	**Jeneratör Desteği:** Şebeke besleyemiyorsa, boştaki mobil jeneratörleri derhal AAT ve Su Pompa istasyonlarına yönlendir ve bağlantısını yap.	[ ]	*Elektrik ekibini desteğe gönder.*
4	**SCADA Koordinasyonu:** Elektrik SCADA'sı çalışmıyorsa, Su/Atık Su SCADA'sının durumunu sor. Ortak körlük varsa (iletişim altyapısı da çöktüyse), tesisler arasında manuel haberleşme zincirini (kurye/araç) kur.	[ ]	*Bilgi akışını kesme.*
5	**Kriz Liderine Raporlama:** Altyapıdaki zincirleme risk durumunu (örn. "Elektrik yok, AAT taşmak üzere") Kriz Liderine bildir ve acil destek iste.	[ ]	*Çevre felaketi riski raporlanmalıdır.*

BÖLÜM 7: PLAN SÜRDÜRÜLEBİLİRLİĞİ (PUKÖ)

Bu bölüm, bu İSP'nin statik bir doküman olarak kalmamasını; sürekli olarak test edilmesini, güncellenmesini ve teknik personelin kriz anında "kas hafızası" ile hareket etmesini sağlayan PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) döngüsünü tanımlar. Bu sürecin yönetiminden **Elektrik İşletme Müdürü** sorumludur.

7.1 Eğitim ve Yetkinlik Programı

Amaç: Saha ve merkez ekiplerinin, kriz anında prosedürleri (manevra, yük atma vb.) hatasız uygulayacak yetkinliğe sahip olması.

Hedef Kitle (Kim?)	Eğitim Konusu (Ne?)	Sıklık	Sorumlu
Tüm Teknik Personel	**İSP Farkındalığı:** Planın genel yapısı, aktivasyon kriterleri, toplanma yerleri ve iletişim zinciri.	İşe Girişte & Yılda 1	İK / İSG
Saha Ekipleri (Teknisyenler)	**Manuel Operasyon:** SCADA olmadan telsizle manevra yapma, EKAT (Yüksek Gerilim) güvenlik prosedürleri, Jeneratör bağlama.	6 Ayda 1	Bakım Şefi
SCADA Operatörleri	**Siber/Teknik Kriz:** Fidye yazılımı durumunda sistem izolasyonu, Felaket Kurtarma Merkezi'ne (Yedek Merkez) geçiş ve manuel veri işleme.	6 Ayda 1	BT / Otomasyon
Yedek Personel (Deputies)	**Gölge (Shadowing):** Asıl sorumlunun (Vardiya Amiri vb.) yokluğunda komuta etme pratiği.	Yılda 1	Elektrik İşl. Md.

7.2 Test ve Tatbikat Programı

Amaç: Planın masa başında değil, sahada (veya simülasyonda) çalıştığını doğrulamak.

Dönem	Tatbikat Türü	Senaryo / Kapsam	Katılımcılar
Ç1 (Mart)	**Haberli İletişim Testi**	**Çağrı Zinciri:** Mesai saati dışında tüm teknik ekibin "Acil Görev" çağrısına yanıt verme süresinin ölçülmesi.	Tüm ESE Üyeleri
Ç2 (Haziran)	**Masa Başı Tatbikatı**	**Siber Saldırı:** SCADA ekranlarının kararması senaryosu üzerinden karar alma ve manuel moda geçiş simülasyonu.	Kriz Lideri & Operatörler
Ç3 (Eylül)	**Teknik Test (Fonksiyonel)**	**Yük Atma & Jeneratör:** Kritik bir DM'nin şebekeden izole edilerek Mobil Jeneratör ile beslenmesi ve yük atma prosedürünün (sanal) uygulanması.	Saha Ekipleri
Ç4 (Aralık)	**Tam Ölçekli Tatbikat**	**Ana Trafo Arızası:** T1 trafosunun kaybı senaryosunda, T2'ye manuel yük aktarımı ve Kriz İletişiminin (SMS) test edilmesi.	Tüm Ekipler & İdari Birim

7.3 Planın Gözden Geçirilmesi ve Güncellenmesi

Bu plan, aşağıdaki durumlar (Tetikleyiciler) oluştuğunda derhal gözden geçirilir:

- **Periyodik:** Yılda bir kez (Ocak ayı) tam gözden geçirme.
- **Değişiklik Bazlı:**
  - Şebeke topolojisinde önemli değişiklik (Yeni İndirici Merkez, yeni DM eklenmesi).
  - Kritik tedarikçilerin (Jeneratör, SCADA firması) değişmesi.
  - Yasal mevzuat (EPDK, OSB Kanunu) değişikliği.

- **Olay Sonrası:** Her gerçek kesinti veya tatbikat sonrasında yapılan "Kök Neden Analizi" çıktısına göre prosedürlerin iyileştirilmesi.

Dağıtım ve Erişim Kontrolü:

- **Basılı Kopyalar:** Planın "Kontrollü Kopya"sı (Islak İmzalı), SCADA Kontrol Odası ve İtfaiye Binası'ndaki (Ilık Alan) **"Kırmızı Dosya"** içinde bulundurulur.
- **Dijital Kopyalar:** Planın güncel PDF versiyonu, **Ek-E**'de belirtilen güvenli sunucu dizinlerinde ve çevrimdışı yedekleme ünitelerinde (USB) saklanır. Dijital kopyaların güncelliğinden ve erişim güvenliğinden (Sadece Okunabilir) Plan Sahibi sorumludur.

BÖLÜM 8: EKLER LİSTESİ

Bu planın etkin bir şekilde uygulanabilmesi için aşağıdaki ek dokümanlar ve listeler hazır bulundurulmalıdır. Bu ekler, planın ayrılmaz bir parçasıdır.

Ek No	Ek Adı	İçerik ve Amaç
Ek-A	**Yük Atma (Load Shedding) Öncelik Listesi**	Kapasite yetersizliğinde veya ulusal kısıntı durumunda, hangi fiderlerin hangi öncelik sırasına göre (Kesilebilir, Hassas, Kritik) enerjisiz bırakılacağını tanımlayan liste.
Ek-B	**Kritik Teknik İletişim Listesi**	Kriz anında teknik koordinasyon için aranacak iç ve dış paydaşların (TEİAŞ, Jeneratör Firması, Bakım Ekibi vb.) 7/24 iletişim bilgileri.
Ek-C	**Tek Hat Şemaları ve Şebeke Haritaları**	Arıza tespiti ve manevra planlaması için kritik olan OG/AG şebeke topolojisi, trafo ve hücre detaylarını gösteren güncel şemaların referansları ve fiziksel/dijital konumları.
Ek-D	**Mobil Jeneratör Bağlantı Noktaları**	Ada modu (Island Mode) beslemesi için mobil jeneratörlerin bağlanabileceği uygun Dağıtım Merkezleri (DM) ve bağlantı tiplerini (Bara/Konnektör) gösteren harita/tablo.
Ek-E	**Plan Dağıtım ve Dijital Erişim Listesi**	Bu planın güncel basılı kopyalarının kimlerde bulunduğu ve dijital kopyalarına (Sunucu, USB, Bulut) güvenli erişim yöntemlerini tanımlayan liste.
Ek-F	**Yedek Personel (Deputy) Listesi**	Kritik teknik rollerin (Ekip Lideri, SCADA Sorumlusu, Saha Şefi) asil ve yedek (A/B Takımı) personelini ve yetkinlik durumlarını gösteren liste.
Ek-G	**Ek-G Eylem Kartları (Görev Kartları)**	Kriz anında Ekip Lideri, Saha Şefi ve Operatörün uygulayacağı adım adım pratik talimatlar.

EK-A: YÜK ATMA (LOAD SHEDDING) ÖNCELİK LİSTESİ

Amaç: Kapasite yetersizliğinde (T2 kullanımı veya Ulusal Kısıntı) hangi fiderin hangi sırada kesileceğini belirlemektir.

ÖNCELİK	FİDER ADI / BÖLGE	YÜK (MVA)	AÇIKLAMA / KESİNTİ KURALI
1. GRUP **(İlk Kesilecekler)**	**Fider-05 (Demir-Çelik Bölgesi)**	8 MVA	Ark ocakları nedeniyle en yüksek yük. İlk etapta kesilir.
2. GRUP **(İkinci Kesilecekler)**	**Fider-08 (Tekstil Bölgesi)**	5 MVA	Üretim süreçleri kesintiye daha toleranslıdır.
3. GRUP **(Hassas)**	**Fider-02 (Gıda/Soğuk Hava)**	4 MVA	Sadece çok acil durumda ve **rotasyonlu** (maks. 2 saat) kesilir.
KORUNACAK **(Kesilemez)**	**Fider-01 (Arıtma/İdari)**	2 MVA	AAT pompaları ve Yönetim Binası bu hattadır. Asla kesilmez.

EK-B: OSB İÇİ VE DIŞI KRİTİK İLETİŞİM LİSTELERİ

Tablo B.1 OSB DIŞI İLETİŞİM LİSTESİ

Amaç: Kriz anında teknik koordinasyon için aranacak numaralar.

KURUM / ROL	İLGİLİ KİŞİ	TELEFON (7/24)	NOTLAR
TEİAŞ Yük Tevzi	Nöbetçi Mühendis	0312 XXX XX XX	Ulusal şebeke durumu için.
Mobil Jeneratör	Güçsan Enerji (Ali Bey)	0532 XXX XX 10	Sözleşme No: J-2025-01.
SCADA Destek	ABC Otomasyon	0850 XXX XX XX	Uzaktan bağlantı desteği.
Trafo Bakım	Yüksek Gerilim Ltd.	0533 XXX XX 11	Arıza onarım ekibi.
Akaryakıt	XYZ Petrol	0542 XXX XX 12	Jeneratör yakıt ikmali.

Tablo B.2 ELEKTRİK İŞLETME VE BAKIM PERSONELİ İLETİŞİM LİSTESİ

Amaç: Arıza anında teknik personeli göreve çağırmak ve diğer altyapı birimleriyle (Zincirleme Etki Yönetimi) koordinasyon sağlamak.

ROL	ADI SOYADI	CEP TELEFONU	TELSİZ KODU	EV KONUMU
İşletme Müdürü	Ali Yılmaz	0532 XXX XX 01	Merkez-1	Merkez
Bakım Şefi	Veli Demir	0533 XXX XX 02	Bakım-1	OSB Lojman
Vardiya Amiri A	Ahmet K.	0542 XXX XX 03	Saha-1	İlçe
Vardiya Amiri B	Mehmet T.	0544 XXX XX 04	Saha-2	Merkez
SCADA Operatörü 1	Ayşe S.	0535 XXX XX 05	Scada-1	Merkez
SCADA Operatörü 2	Can B.	0536 XXX XX 06	Scada-2	İlçe
Teknisyen (Kablo)	Hasan V.	0537 XXX XX 07	Ekip-1	OSB Yakını
Teknisyen (Trafo)	Hüseyin G.	0538 XXX XX 08	Ekip-2	Merkez

Tablo B.3 DİĞER OSB BİRİMLERİ İLETİŞİM LİSTESİ (KOORDİNASYON LİSTESİ)

Amaç: Elektrik kesintisinden etkilenecek ve koordine olunması gereken birimlerle iletişim kurmak.

BİRİM	KONTAK KİŞİ	DAHİLİ	CEP TELEFONU	KOORDİNASYON NEDENİ
Su İşleri	Su Şefi	1120	053X XXX XX 20	Pompaların durması / Jeneratör ihtiyacı.
Arıtma (AAT)	Tesis Sorumlusu	1130	053X XXX XX 30	**KRİTİK:** Taşma riski. Öncelikli enerji verilecek.
Doğalgaz	RMS Sorumlusu	1140	053X XXX XX 40	Isıtma/Kazan daireleri.
İtfaiye	Nöbetçi Amir	1110	053X XXX XX 10	Yangın riski / Asansörde kalma.
Güvenlik	Güvenlik Amiri	1150	053X XXX XX 50	Saha güvenliği / Giriş-Çıkış kontrolü.
BT / IT	Sistem Yöneticisi	1160	053X XXX XX 60	Sunucu odası soğutma / UPS durumu.

EK-C: TEK HAT ŞEMALARI VE ŞEBEKE HARİTALARI (REFERANS)

Amaç: Arıza tespiti ve manevra planlaması için şebeke topolojisine erişim.

- **Basılı Kopyalar:**
  - 1 Takım A0 Boyutunda Güncel Şema: **SCADA Kontrol Odası Duvarı**
  - 1 Takım A3 Kitapçık: **Saha Ekip Araçlarında**
  - 1 Takım A3 Kitapçık: **İtfaiye Binası (Ilık Alan) Dolabı**
- **Dijital Kopyalar:**
  - **Çevrimdışı:** İtfaiye Binası'ndaki SCADA Laptopu masaüstünde ("ACİL_SEMALAR" klasörü).
  - **Bulut:** Güvenli Bulut Alanı (Erişim: Teknik Müdür ve Şefler).

EK-D: MOBİL JENERATÖR BAĞLANTI NOKTALARI

Amaç: Ada modu (Island Mode) beslemesi için jeneratörlerin bağlanacağı uygun noktalar.

LOKASYON	BAĞLANTI TİPİ	KAPASİTE	BESLEDİĞİ KRİTİK YÜK
DM-01 (Merkez)	**Harici Konnektör (Powerlock)**	**1000 kVA**	**Yönetim Binası, Güvenlik, Sunucular.**
DM-04 (Arıtma)	**Bara Bağlantısı (Kablo ile)**	**1600 kVA**	**AAT Giriş Pompaları ve Blowerlar.**
İtfaiye Binası	**Sabit Jeneratör Mevcut**	**500 kVA**	**Kriz Masası ve İtfaiye Operasyonu.**

EK-E: PLAN DAĞITIM VE DİJİTAL ERİŞİM LİSTESİ

Amaç: Planın güncel versiyonunun kimde olduğunu ve dijital yedeğine nasıl ulaşılacağını belirlemek.

1. Basılı Kopyalar (Kontrollü Dağıtım):

Kopya No	Lokasyon / Kişi	Sorumlu
01 (Ana Kopya)	SCADA Kontrol Odası (Kriz Masası)	Nöbetçi Amir
02	İtfaiye Binası (Acil Durum Dolabı)	İFSE Lideri
03	Bölge Müdürü Ofisi	Yönetici Asistanı

2. Dijital Kopyalar (Güvenli Erişim):

Ortam	Erişim Yolu / Konum	Güvenlik
Kurumsal Sunucu	\\OSB-FILE\Ortak\IS_SUREKLILIGI\Planlar\Elektrik_ISP.pdf	Sadece Yöneticilere Açık (Read-Only)
Çevrimdışı USB	İtfaiye Binası "Acil Durum Dolabı" (Kırmızı USB)	Şifreli (BitLocker) - Şifre Zarfı Kasada
Bulut (Cloud)	OSB Güvenli Bulut Hesabı	Çift Faktörlü Doğrulama (MFA) ile Erişim
Mobil Cihazlar	Teknik Müdür ve Şeflerin Tabletleri	Çevrimdışı PDF olarak yüklü

EK-F: ELEKTRİK SÜREKLİLİK EKİBİ (ESE) YEDEK PERSONEL LİSTESİ

Amaç: Kritik rollerdeki personelin (hastalık, izin vb. nedenlerle) bulunamadığı durumlarda veya vardiyalı çalışma (A/B Takımı) gerektiğinde yetkiyi devralacak kişileri belirlemektir.

KRİTİK ROL	ASİL SORUMLU (A Takımı)	1. YEDEK (B Takımı)	YEDEK İLETİŞİM	YETKİNLİK DURUMU
Ekip Lideri	**Elektrik İşletme Md.**	**Bakım Şefi**	0532 XXX XX 20	Tam Yetkili (EKAT Var)
SCADA Sorumlusu	**SCADA Mühendisi**	**Otomasyon Teknikeri**	0533 XXX XX 21	Sistem Erişim Yetkisi Var
Saha Operasyon Şefi	**Vardiya Amiri A**	**Vardiya Amiri B**	0542 XXX XX 22	Saha Tecrübesi > 5 Yıl
Arıza Bakım Ekibi	**Ekip Şefi (Ahmet Y.)**	**Ekip Şefi (Mehmet K.)**	0535 XXX XX 23	YG Müdahale Sertifikalı
İdari Koordinasyon	**Abone İşleri Şefi**	**İdari İşler Personeli**	0536 XXX XX 24	Katılımcı İletişimi Yapabilir

EK-G: EYLEM KARTLARI (GÖREV KARTLARI)

(Not: Bu kartlar lamine edilerek ilgili personelin yaka kartında veya baretinde taşınmalıdır.)

KART 1: ELEKTRİK İŞLETME MÜDÜRÜ (EKİP LİDERİ)

ROL: ELEKTRİK SÜREKLİLİK EKİP LİDERİ	SORUMLULUK: STRATEJİ, KOORDİNASYON VE ONAY
FAZ 1: İLK 15 DAKİKA (TESPİT VE KARAR)	**DURUM**
[ ] 1. Durum Teyidi: **SCADA Odası veya Vardiya Amirinden kesintinin boyutunu (Lokal/Genel) ve kaynağını (OSB/TEİAŞ) öğren.**	☐
[ ] 2. ETR Analizi: **Onarım süresi** 4 saati geçecekse **veya TEİAŞ "uzun süreli kesinti" bilgisi verdiyse** İSP'yi Aktive Et.	☐
[ ] 3. Ekip Aktivasyonu: **Tüm bakım personelini, icapçıları ve destek ekiplerini (Test, Kablo) göreve çağır.**	☐
[ ] 4. İlk Bildirim: **Kriz Lideri'ne (Bölge Müdürü) "Enerji kesildi, tahmini süre X saattir, İSP'yi başlattım" bilgisini ver.**	☐
FAZ 2: İLK 1 SAAT (STRATEJİ VE LOJİSTİK)	
[ ] 5. Strateji Belirleme: **Duruma uygun stratejiyi seç ve uygulat:** • ***Yük Atma*** **(Kapasite yetersizse)** • ***Manuel Transfer*** **(Trafo arızasıysa)** • ***Ada Modu*** **(Ulusal kesintiyse)**	☐
[ ] 6. Dış Kaynak: **Onarım için dış kaynak (Vinç, Kablo Ekibi) veya Mobil Jeneratör gerekiyorsa tedarikçileri ara. (Sözleşme No: J-2025-01)**	☐
[ ] 7. Yük Atma Onayı: **Eğer yük atılacaksa, **"Ek-A: Öncelik Listesi"**ne göre hangi fiderlerin kesileceğini onayla.**	☐
SÜREKLİ GÖREVLER (KRİZ BOYUNCA)	
[ ] 8. Koordinasyon: **Her saat başı Kriz Yönetim Ekibi'ne (KYE) ve Katılımcı İlişkilerine durum raporu ver.**	☐
[ ] 9. Güvenlik: **Saha ekiplerinin yorgunluk durumunu izle, İSG kurallarına (EKAT) uyulduğunu denetle.**	☐
İLETİŞİM BİLGİLERİ	
KRİZ LİDERİ: **Mehmet Demirtaş - 0532 XXX XX 01** YEDEK LİDER: **Bakım Şefi - 0533 XXX XX 02**	**TELSİZ:** Kanal 1

KART 2: SAHA OPERASYON ŞEFİ (VARDİYA AMİRİ)

ROL: SAHA OPERASYON ŞEFİ	SORUMLULUK: SAHA GÜVENLİĞİ VE MANEVRA YÖNETİMİ
FAZ 1: İLK 30 DAKİKA (GÜVENLİK VE İZOLASYON)	**DURUM**
[ ] 1. İSG Kontrolü: **Sahaya çıkacak tüm personelin** EKAT **belgesini ve** KKD **(Eldiven, Baret, Çizme, Ark Kıyafeti) durumunu kontrol et.**	☐
[ ] 2. İzolasyon: **Arızalı bölgeyi (Trafo/Hat) izole et, giriş-çıkış kesicilerini aç, kilitle ve üzerine** "Çalışma Var" **levhası as.**	☐
[ ] 3. Topraklama: **Çalışma yapılacak noktanın her iki ucundan** Mahalli Topraklama **yapıldığını bizzat gör.**	☐
[ ] 4. Teyit: **Merkeze (SCADA) "Saha güvenli, çalışmaya başlıyoruz" teyidini ver.**	☐
FAZ 2: İLK 2 SAAT (ONARIM VE BESLEME)	
[ ] 5. Hasar Tespiti: **Arızanın fiziksel nedenini (kablo başlığı, buşing patlağı) bul ve fotoğrafla. Malzeme listesini depoya bildir.**	☐
[ ] 6. Ring Besleme: **Arızalı kısmı by-pass ederek diğer aboneleri tersten beslemek için manevra ekibini yönlendir.**	☐
[ ] 7. Jeneratör Bağlantısı: **Gelen mobil jeneratörü** DM-01 veya DM-04**'e bağla. (Faz sırasına ve voltaj seviyesine dikkat et!)**	☐
SÜREKLİ GÖREVLER	
[ ] 8. Denetim: **Ekiplerin çalışma alanını gez, emniyet şeritlerini ve topraklamaları sürekli kontrol et.**	☐
İLETİŞİM BİLGİLERİ	
EKİP LİDERİ: **Elektrik Md. - 0542 XXX XX 03** SCADA MERKEZ: **Dahili 1150**	**TELSİZ:** Kanal 3

KART 3: SCADA OPERATÖRÜ (KONTROL MERKEZİ)

ROL: SCADA SORUMLUSU	SORUMLULUK: İZLEME, UZAKTAN KONTROL VE HABERLEŞME
FAZ 1: İLK 15 DAKİKA (TESPİT VE İLK TEPKİ)	**DURUM**
[ ] 1. Alarm Analizi: **Hangi fiderin açtığını, rölelerin hangi hata kodunu (Aşırı Akım, Toprak, Buchholz) verdiğini belirle ve Lidere oku.**	☐
[ ] 2. Yük Durumu: **Mevcut yükü ve trafo kapasitesini kontrol et. (T2'ye geçilecekse yükün 40 MVA altına düşmesi gerekir).**	☐
[ ] 3. Siber Tehdit Kontrolü: **Ekran donması, yetkisiz mouse hareketi veya fidye mesajı var mı? Varsa **"Acil Durum Butonu"**na bas ve fişi çek.**	☐
FAZ 2: SÜREKLİLİK (MANEVRA VE YÜK ATMA)	
[ ] 4. Manuel Mod: **SCADA çalışmıyorsa telsizden tüm ekiplere** "SCADA KAPALI. MANUEL YÖNETİME GEÇİYORUZ" **anonsu yap.**	☐
[ ] 5. Yük Atma: **Liderden emir gelirse, **"Ek-A: Öncelik Listesi"**ndeki fiderleri (Demir-Çelik vb.) sırayla aç.**	☐
[ ] 6. Teyit: **Sahadan gelen "Manevra Tamam" bilgisini almadan hatta enerji verme.**	☐
SÜREKLİ GÖREVLER	

ROL: SCADA SORUMLUSU	SORUMLULUK: İZLEME, UZAKTAN KONTROL VE HABERLEŞME
[ ] 7. Kayıt: **Yapılan tüm manevraları, arıza saatini ve enerji verme saatini **"Olay Kayıt Defteri"**ne (Logbook) dakika dakika işle.**	☐
İLETİŞİM BİLGİLERİ	
EKİP LİDERİ: **Elektrik Md. - 0542 XXX XX 03** BT DESTEK: **Can Öztürk - 0536 XXX XX 06**	**TELSİZ:** Kanal 3

ONAY

Bu plan ve ekleri, Dirençli OSB'nin elektrik dağıtım hizmetinin sürekliliğini garanti altına almak için hazırlanmıştır.

Hazırlayan:	Onaylayan:
(İmza)	*(İmza)*
Elektrik İşletme Müdürü	**Mehmet Demirtaş**
Plan Sahibi	Bölge Müdürü
Tarih: 01/07/2025	Tarih: 01/07/2025

Ek E.3.1: "Dirençli OSB" İçin Tamamlanmış BT Felaket Kurtarma (İş Sürekliliği) Planı

"Dirençli OSB" İçin Tamamlanmış BT Felaket Kurtarma (İş Sürekliliği) Planı

DOKÜMAN KONTROL

Plan Adı:	Dirençli OSB - Bilişim Teknolojileri (BT) Felaket Kurtarma Planı
Doküman No:	İSY-PLAN-BTKP-001
Versiyon:	1.0
Yürürlülük Tarihi:	01/10/2025
Plan Sahibi:	İKE Lideri - Teknik/BT (Bilgi Teknolojileri Müdürü)
Onaylayan:	Mehmet Demirtaş (Bölge Müdürü - Olay Yöneticisi)
Gizlilik:	YÜKSEK - Sadece Yetkili Personel (İçerdiği IP ve topoloji bilgileri nedeniyle)
Bir Sonraki Gözden Geçirme:	01.10.2026

0. YÖNETİCİ ÖZETİ

0.1 Kurumsal Bağlam:

Dirençli OSB; elektrik, su, doğalgaz ve atıksu gibi kritik altyapı hizmetlerini yöneten, 150 katılımcı firmaya hizmet veren teknoloji bağımlı bir organizasyondur. Operasyonların

sürekliliği, SCADA (Altyapı Kontrolü), OSOS (Sayaç Okuma) ve ERP (Finans/Abone) sistemlerinin kesintisiz çalışmasına bağlıdır.

0.2 Planın Amacı:

Bu planın amacı, OSB'nin Veri Merkezi'nde meydana gelebilecek fiziksel bir felaket (yangın, su baskını) veya sistemleri kilitleyen kapsamlı bir siber saldırı (fidye yazılımı) durumunda; kritik BT hizmetlerini ve verilerini, İş Etki Analizi (İEA) raporunda belirlenen Kurtarma Süresi Hedefleri (RTO) ve Kurtarma Noktası Hedefleri (RPO) doğrultusunda alternatif bir ortamda (Afet Kurtarma Merkezi) yeniden çalışır hale getirmektir.

0.3 Kritik Sistemler ve Kurtarma Hedefleri (İEA Özeti):

Plan, aşağıdaki öncelik sırasına göre işletilecektir:

Öncelik	Kritik Sistem / Altyapı	RTO (Hedef Süre)	RPO (Veri Kaybı)	Kurtarma Stratejisi
P-1	**Ağ Altyapısı (Network)**	**2 Saat**	-	Yedek Donanım (Cold Standby)
P-2	**SCADA Sistemi**	**1 Saat**	5 Dk	Felaket Kurtarma Merkezi - Sıcak Bekleme
P-3	**OSOS / Faturalandırma**	**4 Saat**	1 Saat	Felaket Kurtarma Merkezi - Sanal Sunucu Replikasyonu
P-4	**E-Posta / İletişim**	**4 Saat**	1 Saat	Bulut Tabanlı Kurtarma

0.4 Temel Kurtarma Stratejisi:

Dirençli OSB, BT sürekliliği için "Hibrit Bulut ve Afet Kurtarma Merkezi" stratejisini benimsemiştir:

- **SCADA:** OSB dışındaki bir Felaket Kurtarma Merkezi'nde (YDK-IT-01) sürekli replike edilen "Sıcak Yedek" (Hot Standby) sunucusu üzerinden çalıştırılacaktır.

0.5 Aktivasyon Kriteri:

Ana SCADA sunucusuna veya Veri Merkezi'ne 1 saatten uzun süre erişilemeyeceğinin veya sistemlerin siber saldırı sonucu kilitlendiğinin teyit edilmesi.

BÖLÜM 1: GİRİŞ

1.1 Amaç

Bu BT Felaket Kurtarma Planı'nın (BT-FKP) temel amacı; Dirençli OSB'nin kritik altyapı yönetimini (Elektrik, Su, Atık Su) ve idari operasyonlarını destekleyen bilgi teknolojileri altyapısında meydana gelebilecek bir kesinti veya felaket sonrasında; sistemleri ve verileri, **İş Etki Analizi (İEA)** raporunda belirlenen **Kurtarma Süresi Hedefi (RTO)** ve **Kurtarma Noktası Hedefi (RPO)** doğrultusunda yeniden çalışır hale getirmek için izlenecek teknik adımları tanımlamaktır.

1.2 Kapsam

Bu plan, İEA çalışması sonucunda "Kritik" olarak tanımlanan aşağıdaki BT sistemlerini, donanımları ve bunları destekleyen ağ altyapısını kapsar:

- **P-1: Ağ ve Güvenlik Altyapısı:** İnternet erişimi, Firewall, Omurga Switchler ve VPN altyapısı.
- **P-2: SCADA Sistemi (Kritik Altyapı):** Elektrik ve Su şebekesi izleme/kontrol sunucuları ve saha haberleşme üniteleri.
- **P-3: OSOS ve Faturalandırma Sistemi:** Sayaç okuma sunucuları ve fatura veri tabanı.
- **P-4: E-Posta ve İletişim Sistemi:** Kurumsal e-posta sunucusu ve IP telefon santrali.
- **P-5: ERP / Kurumsal Kaynak Planlama:** Muhasebe, Finans, Satın Alma ve Abone Yönetim modülleri.

Not: Katılımcı firmaların kendi iç BT sistemleri ve kişisel kullanıcı cihazları (dizüstü bilgisayarlar hariç) bu planın kapsamı dışındadır.

1.3 Bütünleşik Planlarla İlişkisi (Aktivasyon Bağlantısı)

Bu plan, taktiksel bir alt plandır ve tek başına çalışmaz. Diğer planlarla ilişkisi şöyledir:

- **Aktive Eden Plan (Tetikleyici):** Bu plan, **İş Sürekliliği Planı (İSY-İSP-GENEL-001)** kapsamında, **Olay Yöneticisi** veya **Kriz Lideri**'nin talimatıyla aktive edilir.
- **Raporlama:** Bu planın sorumlusu (BT Müdürü), kurtarma operasyonunun ilerleme durumunu doğrudan **Olay Koordinasyon Ekibi'ne (OKE)** raporlar.
- **Ön Koşul (Siber Saldırı):** Eğer kesintinin nedeni bir **Siber Saldırı (Örneğin, Fidye Yazılımı)** ise; bu plan uygulanmadan önce **Siber Olaylara Müdahale Planı (SOP)** devreye girmelidir.
  - *Kural:* Sistemler izole edilmeden ve temizlenmeden (Siber Olaylara Müdahale Planı tamamlanmadan), BT-FKP (Yedekten Dönüş) başlatılamaz. Aksi takdirde yedekler de enfekte olabilir.

BÖLÜM 2: ORGANİZASYON (BT KURTARMA EKİBİ)

2.1. Ekip Yapısı

Bu planın uygulanmasından, İş Sürekliliği Planı'nda (İSP) tanımlanan ve **Bilgi Teknolojileri Müdürü** liderliğinde çalışan **BT Felaket Kurtarma Ekibi (BT-FKE)** sorumludur. Bu ekip, kriz anında Olay Koordinasyon Ekibi'ne (OKE) raporlama yapar.

2.2. Ekipler, Roller ve Sorumluluklar

Rol (Plandaki Adı)	Sorumlu Kişi / Birim	Temel Görev ve Sorumluluklar (BTKP Sırasında)
BT-FKE Lideri - Teknik/BT	**BT Müdürü**	Bu planın genel komutasını alır. Sistemlerin kurtarma önceliklerini (P-1, P-2...) yönetir. Olay Yöneticisi'ne (OYE) düzenli durum raporu verir. Dış destek firmalarını aktive eder.

Rol (Plandaki Adı)	Sorumlu Kişi / Birim	Temel Görev ve Sorumluluklar (BTKP Sırasında)
Sistem ve Ağ Sorumlusu	**Sistem Yöneticisi**	Felaket Kurtarma Merkezi'ndeki sunucuların, sanal makinelerin ve ağ altyapısının (VPN, Firewall) fiziksel ve mantıksal olarak ayağa kaldırılmasını sağlar.
OT/SCADA Sorumlusu	**Otomasyon Teknikeri**	SCADA sunucusunun çalışırlığını, saha cihazları (RTU/PLC) ile veri iletişimini ve endüstriyel ağın güvenliğini kontrol eder.
Uygulama Sorumlusu	**Yazılım Uzmanı**	OSOS (Sayaç Okuma) ve ERP (Muhasebe) yazılımlarının veritabanı tutarlılığını ve uygulama katmanının çalışırlığını test eder.
Dış Destek (SCADA)	**ABC Otomasyon Firması**	*(SLA Kapsamında)* SCADA yazılımının yeniden kurulumu, lisanslama sorunları ve karmaşık veri tabanı kurtarma işlemlerinde uzaktan/yerinde destek verir.
Dış Destek (Siber)	**Siber Güvenlik Firması**	*(Siber Saldırı Durumunda)* Sistemin temizlenmesi, delillerin korunması ve güvenli geri yükleme onayı verilmesi konularında uzman desteği sağlar.

BÖLÜM 3: AKTİVASYON VE ÖNCELİKLER

3.1. BTKP Aktivasyon Kriterleri

Bu plan, BT-FKE-Teknik/BT Lideri (BT Müdürü) tarafından aşağıdaki durumlardan birinin tespit edilmesi ve Olay Yöneticisi'ne bildirilerek İSP'nin aktive edilmesiyle devreye girer:

- **Erişim Kaybı:** Kapsamdaki kritik bir sunucuya (SCADA, OSOS) veya ana omurga ağ anahtarına (Core Switch) **30 dakikadan uzun süre** erişilememesi ve ilk müdahalenin başarısız olması.
- **Siber Saldırı:** RD-03 (Siber Saldırı) şüphesi veya teyidi (Örneğin, SCADA ekranlarında fidye notu görülmesi). *Bu durumda önce Siber Olay Müdahale Planı (SOMP) uygulanır.*
- **Veri Bütünlüğü:** Kritik bir sistemde (Örneğin, OSOS veritabanı) geri döndürülemez bir veri bozulması tespit edilmesi.
- **Fiziksel Felaket:** Yönetim Binası Sistem Odası'nın yangın, su baskını veya deprem nedeniyle kullanılamaz hale gelmesi.

- **Talimat:** Doğrudan Kriz Yönetim Ekibi (KYE) veya Olay Yöneticisi'nden aktivasyon talimatı gelmesi.

3.2. Kurtarma Öncelikleri ve Hedefleri (İEA Odaklı)

Kurtarma operasyonu, İEA sonuçlarına göre belirlenen aşağıdaki kritiklik sırasına (P-1'den P-5'e) göre yapılacaktır. En kritik sistem (Altyapı ve SCADA), ilk kurtarılır.

Öncelik	BT Sistemi / Altyapı	Sistem RTO (Hedef Süre)	Veri RPO (Veri Kaybı)	İlgili Prosedür
P-1	**Ağ ve Güvenlik Altyapısı**	**2 Saat**	-	**BTKP-NET-01**
P-2	**SCADA Sistemi (Elektrik/Su)**	**1 Saat**	**5 Dakika**	**BTKP-SCADA-01**
P-3	**OSOS ve Faturalandırma**	**4 Saat**	**1 Saat**	**BTKP-OSOS-01**
P-4	**İletişim (E-posta/IP Tel)**	**4 Saat**	**1 Saat**	**BTKP-MAIL-01**
P-5	**ERP / Muhasebe Yazılımı**	**8 Saat**	**1 Saat**	**BTKP-ERP-01**

3.3. İş Sürekliliği Stratejileri ve Çözümleri

BT Birimi, riskleri yönetmek ve RTO hedeflerine ulaşmak için aşağıdaki stratejileri **Olay Öncesi (Hazırlık)**, **Olay Sırası (Müdahale)** ve **Olay Sonrası (Kurtarma)** olmak üzere üç fazda uygular.

3.3.1. Olay Öncesi Stratejiler (Önleme ve Hazırlık)

Amaç, risk gerçekleşmeden önce sistemin direncini artırmak ve yedekliliği sağlamaktır.

- **Veri Koruma Stratejisi (Yedeklilik):**
  - **Strateji:** Veri kaybını RPO hedefleri (1 Saat) içinde tutmak ve fidye yazılımına karşı bağışıklık kazanmak.
  - **Çözüm: "3-2-1 Yedekleme Kuralı"**. (3 Kopya, 2 Farklı Medya, 1 Tesis Dışı/Çevrimdışı).
  - **Aksiyon:** SCADA ve ERP verilerinin her gece otomatik olarak hem yerel NAS ünitesine hem de şifreli olarak Bulut'a yedeklenmesi. Haftalık yedeğin **LTO Tape** ünitesine alınarak ağdan fiziksel olarak koparılması (Air-Gap).
- **Donanım Hazırlık Stratejisi (Altyapı):**
  - **Strateji:** Fiziksel arıza anında parça temin süresini ortadan kaldırmak.
  - **Çözüm: "Soğuk Yedek (Cold Standby)"** ve **"Sıcak Bekleme (Hot Standby)"**.
  - **Aksiyon:** Kritik Omurga Switch ve Firewall cihazının birebir yedeğinin İtfaiye Binası'ndaki (Ilık Alan) dolapta hazır tutulması. Ankara Kurtarma Merkezi'ndeki sanal sunucuların "Hazır" modda bekletilmesi.
- **Siber Savunma Stratejisi (Sıkılaştırma):**
  - **Strateji:** Kritik altyapıya (OT) yetkisiz erişimi engellemek.
  - **Çözüm: "Ağ Segmentasyonu ve İzolasyon"**.
  - **Aksiyon:** SCADA ağının (VLAN 100) İdari ağdan (VLAN 10) Firewall kuralları ile katı bir şekilde ayrılması.

3.3.2. Olay Sırası Stratejileri (Müdahale ve Süreklilik)

Amaç, kesinti anında hizmetin alternatif yöntemlerle sürdürülmesini sağlamaktır.

- **Yük Devretme Stratejisi (Failover):**
  - **Strateji:** Ana merkez (İstanbul) kaybedildiğinde operasyonu sürdürmek.
  - **Çözüm: "Felaket Kurtarma Merkezi Aktivasyonu"**.
  - **Aksiyon:** Kriz anında Ankara Felaket Kurtarma Merkezi'ndeki sanal sunucuların "Power On" yapılması ve DNS yönlendirmelerinin değiştirilmesi.
- **Erişim Stratejisi (Bağlantı):**
  - **Strateji:** Personelin ofis dışında güvenli çalışabilmesi.
  - **Çözüm: "Güvenli VPN Tüneli"**.
  - **Aksiyon:** Kullanıcıların ve Ilık Alanın (İtfaiye Binası), SSL VPN üzerinden doğrudan Ankara Felaket Kurtarma Merkezi'ne bağlanması.
- **Manuel İşletim Stratejisi (B Planı):**
  - **Strateji:** Teknoloji tamamen çökerse (RTO aşıldığında) işin durmamasını sağlamak.
  - **Çözüm: "Kâğıt Tabanlı Süreçler"**.
  - **Aksiyon:** Sayaçların gözle okunması, faturaların Excel'de hesaplanması ve SCADA yerine telsizle saha yönetimine geçilmesi (Prosedür İSP-MAN-01).

3.3.3. Olay Sonrası Stratejileri (Kurtarma ve Normalleşme)

Amaç, kriz bittikten sonra normal düzene dönüşü sağlamaktır.

- **Geri Dönüş Stratejisi:**
  - **Strateji:** Veri tutarlılığını bozmadan ana merkeze dönmek.
  - **Çözüm: "Tersine Replikasyon ve Planlı Geçiş"**.
  - **Aksiyon:** Ankara'da biriken yeni verilerin İstanbul'daki onarılmış sunuculara senkronize edilmesi ve planlı bir kesintiyle hizmetin tekrar İstanbul'a alınması.

3.4. Strateji Özeti ve Prosedür Eşleşme Tablosu

Risk Senaryosu	Seçilen Strateji	Uygulama Aracı (Prosedür Ref.)
Donanım Arızası **(Ağ/Güvenlik)**	Yedek Donanım (Cold Standby)	**4.2.1 Prosedür BTKP-NET-01**
Veri Merkezi Kaybı **(SCADA)**	Sıcak Bekleme (Hot Standby)	**4.2.2 Prosedür BTKP-SCADA-01**
İletişim Sistemi Kaybı **(E-posta)**	Bulut Yönlendirme	**4.3.3 Prosedür BTKP-MAIL-01**
Uygulama Sunucusu Kaybı **(OSOS)**	Sanal Sunucu Replikasyonu	**4.3.1 Prosedür BTKP-OSOS-01**
Siber Saldırı **(Fidye Yazılımı)**	Temiz Yedekten Dönüş	**SOP-PB-01** *(Bkz. Ek E.4)* →**4.3.2 Prosedür BTKP-ERP-01**
Teknoloji Kurtarılamıyor **(>8 Saat)**	Manuel İşletim Desteği	**4.4.1 Prosedür İSP-MAN-01**

BÖLÜM 4: DETAYLI KURTARMA PROSEDÜRLERİ (FAZLARA GÖRE)

Kurtarma operasyonu, sistemlerin birbirine olan bağımlılığı (Örneğin, Ağ olmadan SCADA çalışmaz) nedeniyle aşağıdaki fazlar ve sıra ile yürütülecektir.

4.1. Faz 1: Anlık Müdahale ve Teşhis (İlk 0-60 Dakika)

Amaç: Sorunun kök nedenini anlamak ve güvenli ortamı hazırlamak.

Adım	Eylem	Sorumlu	Kontrol
1	**Ekip Toplanması:** BT-FKE üyelerini (Ağ, Sistem, SCADA) acil durum grubu üzerinden topla.	BT Müdürü	[ ]
2	**Kök Neden Analizi:** Sorun fiziksel mi (Yangın/Su) yoksa siber mi (Fidye/Saldırı)?	Sistem Yöneticisi	[ ]
3	**KRİTİK GÜVENLİK KONTROLÜ:** Eğer neden **Siber Saldırı** ise, bu planı **DURDUR**. Önce **Siber Olay Müdahale Planı (SOP)**'nı uygula. Sistemler temizlenmeden geri yükleme yapma!	**Tüm Ekip**	[ ]
4	**Fiziksel Güvenlik:** Neden fiziksel ise, Veri Merkezi'ne girişin güvenli olduğunu İSG/Güvenlik biriminden teyit et.	BT Müdürü	[ ]
5	**Raporlama:** Olay Yöneticisi'ne (OYE) "Teşhis tamamlandı, kurtarmaya başlıyoruz" bilgisini ver.	BT Müdürü	[ ]

4.2. Faz 2: Kritik Altyapı Kurtarma (Saat 1 - 2)

Amaç: Şebeke yönetimi (SCADA) ve erişim (Ağ) altyapısını ayağa kaldırmak.

4.2.1 Prosedür BTKP-NET-01: Ağ ve Güvenlik Altyapısının Kurtarılması *(Strateji: Soğuk Yedek Donanım / Felaket Kurtarma Merkezi VPN)*

Adım	Teknik Eylem	Notlar	Durum
1	**Donanım Değişimi:** Arızalı Omurga Switch/Firewall yerine, İtfaiye Binası'ndaki dolaptan **Yedek Cihazı (Cold Standby)** çıkar ve rack kabinime tak.	Yedek Cihaz Envanter No: BT-NET-Y01	[ ]
2	**Konfigürasyon Yükleme:** USB bellekteki son "Switch Config" dosyasını cihaza yükle.	Dosya Adı: conf_backup_latest.bin	[ ]
3	**DR Tüneli:** Felaket Kurtarma Merkezi (YDK-IT-01) ile aradaki **Site-to-Site VPN** bağlantısını test et.	Ping testi: 192.168.10.1 (DR Gateway)	[ ]
4	**Kullanıcı Erişimi:** İdari personelin evden bağlanabilmesi için **Client VPN** havuzunu aktif et.	35 Lisans	[ ]

4.2.2 Prosedür BTKP-SCADA-01: SCADA Sisteminin Kurtarılması *(Strateji: Sıcak Bekleme / Hot Standby)*

Adım	Teknik Eylem	Notlar	Durum
1	**Erişim:** VPN üzerinden Felaket Kurtarma Merkezindeki **Yedek SCADA Sunucusu (SVR-SCD-DR)** konsoluna bağlan.	IP: 10.20.30.50	[ ]
2	**Servis Aktivasyonu:** Sunucu üzerindeki SCADA servislerini (SQL, Runtime, Poll) "Start" konumuna getir.	Servis Adı: SCADA_Core_Service	[ ]
3	**Veri Kontrolü:** Son gelen verinin tarih/saatini kontrol et. **RPO (5 dk)** hedefi tutuyor mu?	Veritabanı Log: Last_Transaction_Time	[ ]
4	**Saha Testi:** Rastgele 3 adet Dağıtım Merkezi (DM) ile ping/veri testi yap.	RTU bağlantılarını kontrol et.	[ ]
5	**Teslim:** Sistemi Elektrik İşletme Müdürü'ne teslim et.	"Sistem izlemeye açık."	[ ]

4.3. Faz 3: Destek Sistemleri Kurtarma (Saat 2 - 8)

Amaç: Faturalandırma ve idari işlerin devamlılığını sağlamak.

4.3.1 Prosedür BTKP-OSOS-01: OSOS ve Faturalandırma Sisteminin Kurtarılması *(Strateji: Sanal Sunucu Replikasyonu)*

Adım	Teknik Eylem	Notlar	Durum
1	**Failover:** Sanallaştırma platformundan (VMware/Hyper-V) OSOS sunucusunu Felaket Kurtarma Merkezi üzerinde "Power On" yap.	Sunucu: SVR-OSOS-DR	[ ]
2	**IP Yönlendirme:** DNS kayıtlarını değiştirerek osos.direncliosb.org.tr adresini Kurtarma Merkezi IP'sine yönlendir.	TTL süresini düşür.	[ ]
3	**Veri Bütünlüğü:** Sayaç okuma loglarında eksik olup olmadığını sorgula. Eksik varsa **İSP-FAT-01 (Manuel Okuma)** talimatı ver.	Veri Kaybı > 1 Saat ise bildir.	[ ]

4.3.2 Prosedür BTKP-ERP-01: ERP / Muhasebe Sisteminin Kurtarılması *(Strateji: Çevrimdışı Yedekten Dönüş - Siber Saldırı Senaryosu)*

Adım	Teknik Eylem	Notlar	Durum
1	**Temiz Ortam:** Felaket Kurtarma Merkezi'nde izole edilmiş, ağa kapalı (Air-Gapped) yeni bir sanal sunucu oluştur.	"Clean Room" prosedürü.	[ ]
2	**Yedek Getirme:** Tesis dışı kasadan **LTO Teyp** veya **Çevrimdışı Disk** yedeğini getir.	En son temiz yedek tarihi: _____	[ ]
3	**Geri Yükleme (Restore):** Veritabanını ve uygulama dosyalarını bu temiz sunucuya yükle.	Süre: Yaklaşık 4-6 saat.	[ ]
4	**Kullanıcı Testi:** Mali İşler Müdürü'ne sisteme giriş yetkisi ver ve bir deneme faturası kestir.	MBCO: Fatura Kesebilme.	[ ]

4.3.3. Prosedür BTKP-MAIL-01: E-Posta ve İletişim Sisteminin Kurtarılması (Strateji: Bulut Tabanlı Yönlendirme)

Amaç, kurum içi ve dışı haberleşmeyi (RTO: 4 Saat) sağlamaktır.

Adım	Teknik Eylem	Notlar	Durum
1	**DNS Yönlendirme:** Hosting paneline girerek direncliosb.org.tr alan adının **MX Kayıtlarını** Bulut Yedekleme (DR) sunucusuna yönlendir.	TTL süresini 300 saniyeye düşür.	[ ]
2	**Webmail Aktivasyonu:** Kullanıcılara mail-dr.direncliosb.org.tr üzerinden Webmail erişimini aç.	Kullanıcı adı/şifre aynıdır (AD Sync).	[ ]
3	**Duyuru:** Personele SMS atarak "E-postalarınız Webmail üzerinden çalışmaktadır, Outlook kullanmayın" bilgisini ver.		[ ]
4	**Geçmiş Veri:** Son 1 saate kadar olan e-postaların arşivden (Mail Gateway) geri yüklenmesini başlat.	RPO: 1 Saat.	[ ]

4.4: ALTERNATİF VE MANUEL SÜREÇLER

Teknoloji RTO süreleri içinde geri getirilemezse veya siber saldırı devam ediyorsa bu bölüm uygulanır.

4.4.1 Prosedür İSP-MAN-01: BT Destekli Manuel Çalışma Operasyonu

- **Senaryo:** Tüm sistemlerin kapalı olduğu veya güvenilmez olduğu durum (Blackout).
- **Amaç:** İş birimlerinin kâğıt-kalem ile çalışabilmesi için gerekli **"Teknolojik Lojistiği"** sağlamak.

Adım	Teknik Eylem	Sorumlu	Durum
1	**Acil Durum Kitinin Dağıtımı:** İtfaiye Binası'ndaki (Ilık Alan) dolaptan şu ekipmanları çıkar ve birimlere dağıt: • 3 Adet "Standalone" (Ağa bağlanmayan) Laptop. • 2 Adet USB Yazıcı (Toner dolu). • 1 Kutu "Boş USB Bellek" (Temiz).	Sistem Yöneticisi	[ ]
2	**İnternet Erişimi (4G):** Yönetim binasındaki internet kesik olduğu için, Kriz Masasına **4G/5G Mobil Modemleri (Superbox)** kur ve Wi-Fi şifresini sadece Kriz Yöneticilerine ver.	Ağ Uzmanı	[ ]

Adım	Teknik Eylem	Sorumlu	Durum
3	**Form Basımı:** Standalone laptoptaki "Manuel Formlar Klasörü"nden (Fatura şablonu, Sayaç okuma formu) gerekli evrakları USB yazıcıdan 100'er kopya bas.	BT Destek	[ ]
4	**Şablon Paylaşımı:** Mali İşler birimine, fatura hesabı yapabilmeleri için içinde formüller olan boş Excel şablonlarını USB ile ver.	BT Destek	[ ]
5	**Manuel Kayıt:** Bu süreçte yapılan işlemlerin (dağıtılan laptop zimmeti vb.) kaydını kağıt üzerindeki log defterine tut.	BT Müdürü	[ ]

NOT: SOP-PB-01 (FİDYE YAZILIMI) HAKKINDA

SOP-PB-01, bu planın (BT-FKP) bir parçası değil, **Ek E.3.2: Siber Olay Müdahale Planı**nın içindeki bir prosedüsdür.

Ancak, BT-FKP içindeki akışın bozulmaması için **Bölüm 4.1 (Faz 1)** içine şu kontrol adımı zaten eklenmiştir:

Adım 3 (KRİTİK GÜVENLİK KONTROLÜ): *Eğer neden Siber Saldırı ise, bu planı DURDUR. Önce **SOP-PB-01 (Fidye Yazılımı Müdahalesi)** prosedürünü uygula. Sistemler temizlenmeden geri yükleme yapma!*

BÖLÜM 5: NORMALE DÖNÜŞ PROSEDÜRLERİ

Ana Yönetim Binası'ndaki sistem odası veya birincil sunucular tekrar güvenli ve çalışır hale geldiğinde (Örneğin, Yangın sonrası tadilat bittiğinde veya siber tehdit tamamen temizlendiğinde), operasyonlar kontrollü bir şekilde ana merkeze geri taşınır. Bu süreç, **planlı bir kesinti** ile yürütülür.

5.1. Hazırlık ve Ön Koşullar

Normale dönüş kararını **Kriz Yönetim Ekibi (KYE)** verir. İşlem başlamadan önce BT Müdürü şu koşulların sağlandığını teyit eder:

Kontrol Maddesi	Durum	Sorumlu
Fiziksel Ortam: **Ana sistem odasının enerjisi, soğutması ve fiziksel güvenliği (kapı/kamera) tam olarak çalışıyor.**	[ ]	Altyapı Müdürü
Donanım: **Arızalı sunucu veya ağ cihazları onarıldı/yenilendi ve "Hazır (Standby)" konumunda bekliyor.**	[ ]	Sistem Yöneticisi
Siber Temizlik: ***(Siber saldırı sonrası ise)* Ana sistemlerin tamamen temizlendiği ve güvenlik açıklarının kapatıldığı "Siber Güvenlik Firması" raporuyla teyit edildi.**	[ ]	BT Müdürü
Bağlantı: **Felaket Kurtarma Merkezi ile Ana Merkez arasındaki veri replikasyon hattı (Fiber/VPN) aktif ve stabil.**	[ ]	Ağ Yöneticisi

5.2. Veri Senkronizasyonu (Ters Replikasyon)

Felaket süresince, Kurtarma Merkezi üzerinde oluşan yeni verilerin (yeni faturalar, SCADA logları), ana sisteme aktarılması işlemidir.

1. **Replikasyonu Başlat:** Kurtarma Merkezindeki sanal sunuculardan Ana Merkezdeki sunuculara doğru **"Tersine Replikasyon"** işlemini başlat.
2. **Senkronizasyon Takibi:** Veri farkının (Delta) sıfırlanmasını bekle. Bu süreçte sistemler Kurtarma Merkezi üzerinden hizmet vermeye devam eder.

5.3. Kesinti ve Geçiş (Cutover)

Veriler eşitlendikten sonra, hizmetin yönünü değiştirmek için kısa süreli bir kesinti planlanır.

- **Zamanlama:** Operasyonel etkinin en az olduğu saat (Genellikle 02:00 - 05:00 arası veya Hafta Sonu).
- **Duyuru:** Tüm personele ve katılımcılara "Planlı Bakım Çalışması" duyurusu yapılır.

Adım Adım Geçiş (Kontrol Listesi):

Sıra	İşlem	Sistem	Sorumlu
1	Felaket Kurtarma Merkezi üzerindeki servisleri (SCADA, OSOS, ERP) durdur. (Veri girişi engellenir).	Tümü	Sistem Yöneticisi
2	Son veri "Delta"sının ana sisteme aktarıldığını (%100 Sync) teyit et.	Storage	Veritabanı Yöneticisi
3	Ana Merkezdeki sunucuları ve servisleri "Başlat (Power On)".	Tümü	Sistem Yöneticisi
4	DNS ve Ağ yönlendirmelerini Ana Merkez IP'lerine geri çevir.	Network	Ağ Yöneticisi
5	**Test:** Ana sistem üzerinden SCADA verisi geldiğini ve fatura kesilebildiğini test et.	Uygulama	Kullanıcılar
6	**Onay:** Sistemlerin kararlı çalıştığı görüldüğünde "Normale Dönüş Tamamlandı" bilgisini ver.	Tümü	BT Müdürü

5.4. Felaket Kurtarma Merkezinde Sistemin Sıfırlanması

Ana merkeze geçiş başarılı olduktan 24 saat sonra:

- Kurtarma Merkezindeki sunucular kapatılır veya "Pasif Bekleme" moduna alınır.
- Replikasyon yönü tekrar "Ana Merkez → Kurtarma Merkezi" olarak ayarlanır.
- Acil durum için kullanılan yedek donanımlar (Dizüstü Bilgisayar, Switch) temizlenir ve İtfaiye Binası'ndaki dolaba kilitlenir.

BÖLÜM 6: PLANIN SÜRDÜRÜLEBİLİRLİĞİ (PUKÖ)

Bu bölüm, BT-FKP'nin güncel kalmasını, teknik personelin müdahale yetkinliğine sahip olmasını ve yedek sistemlerin (Felaket Kurtarma Merkezi) her an çalışır durumda olmasını sağlayan **Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ)** döngüsünü tanımlar. Bu sürecin yönetiminden **BT Müdürü (BT-FKE Lideri)** sorumludur.

6.1 Eğitim ve Farkındalık Programı

Amaç: Teknik ekibin kriz anında donanım ve yazılım kurtarma adımlarını ezbere bilmesini, son kullanıcıların ise siber hijyen kurallarına uymasını sağlamak.

Hedef Kitle	Eğitim Konusu	Sıklık	Sorumlu
BT-FKE (Teknik Ekip)	**Teknik Kurtarma Prosedürleri:** Felaket Kurtarma Merkezi aktivasyonu (Failover), Çevrimdışı (Tape) yedekten geri dönme, SCADA izolasyon prosedürü ve donanım değiştirme pratikleri.	6 Ayda 1	BT Müdürü
Tüm Personel	**Siber Güvenlik Farkındalığı:** Oltalama (Phishing) e-postalarını tanıma, şüpheli durumlarda "Acil İhbar" yapma ve parola güvenliği.	Yılda 1 (Simülasyonlu)	İK / BT
SCADA Operatörleri	**Manuel Mod ve Güvenlik:** Siber saldırı belirtilerini (ekran donması vb.) tanıma ve "Acil Durum Bağlantı Kesme (Fiş Çekme)" prosedürü.	İşe Girişte & Yılda 1	Otomasyon Sor.
Yedekler (Deputies)	**Gölge (Shadowing):** Asıl sistem yöneticisiyle birlikte bir "Yedekten Dönüş" işlemini baştan sona izleme ve uygulama.	Yılda 1	BT Müdürü

6.2 Test ve Tatbikat Programı

Amaç: "Yedeklerin çalıştığını sanmak" yerine "Çalıştığını bilmek". Test edilmemiş bir yedek, yedek değildir.

Dönem	Tatbikat Türü	Senaryo / Kapsam	Katılımcılar
Ç1 (Mart)	**Teknik Test (Restore)**	**Veri Kurtarma:** Rastgele seçilen bir sunucunun (Örn: ERP-Test) çevrimdışı teyp yedeğinden "Sıfırdan" kurulması ve veri bütünlüğünün teyidi.	Sistem Yöneticisi
Ç2 (Haziran)	**Masa Başı Tatbikatı**	**Siber Karar Alma:** "Fidye Yazılımı Saldırısı" senaryosu üzerinden; İzolasyon kararı, Fidye ödememe kararı ve Yasal bildirim süreçlerinin simülasyonu.	KYE & BT-FKE
Ç3 (Eylül)	**Fonksiyonel Test**	**SCADA Failover:** Ana SCADA sunucusunun ağ bağlantısının kesilmesi ve Felaket Kurtarma Merkezi'ndeki "Sıcak Yedek" sunucunun kontrolü devraldığının (Heartbeat) doğrulanması.	Otomasyon / Saha Ekibi
Ç4 (Aralık)	**Tam Ölçekli Tatbikat**	**Felaket Kurtarma Merkezi Aktivasyonu:** Hafta sonu planlı kesinti yapılarak; tüm kritik sistemlerin (ERP, E-posta) Felaket Kurtarma Merkezi üzerinden çalıştırılması ve kullanıcıların oradan erişim sağlaması.	Tüm BT Ekibi

6.3 Planın Gözden Geçirilmesi ve Güncellenmesi

Bu plan statik değildir. Teknoloji ve tehditler değiştikçe güncellenir.

Gözden Geçirme Tetikleyicileri:

- **Periyodik:** Yılda bir kez (Ekim ayı) tam gözden geçirme.
- **Donanım/Yazılım Değişikliği:**
  - Yeni bir sunucu veya depolama ünitesi alındığında.
  - ERP veya SCADA yazılım sürümü yükseltildiğinde.
  - Ağ topolojisi değiştiğinde (Yeni VLAN, Yeni Switch).
- **Personel Değişikliği:** BT Müdürü veya Sistem Yöneticisi değiştiğinde (Şifreler ve yetkiler dahil).
- **Olay Sonrası:** Herhangi bir gerçek kesinti veya başarısız test sonrası yapılan "Kök Neden Analizi"ne göre.

Dağıtım ve Versiyon Kontrolü:

- **Güncelleme Yetkisi:** Sadece BT Müdürü değişiklik yapabilir.
- **Onay:** Büyük değişiklikler Olay Yöneticisi (Üretim/Bölge Müdürü) tarafından onaylanır.
- **Saklama:** Güncel planın basılı kopyası "Sistem Odası" ve "İtfaiye Binası (Ilık Alan)"ndaki şifreli kasada; dijital kopyası ise "Çevrimdışı USB"de saklanır.

PLAN EKLERİ LİSTESİ

Ek No	Ek Adı	İçerik ve Kullanım Amacı
Ek-A	**Kritik BT İletişim Listesi**	BT Felaket Kurtarma Ekibi (BT-FKE), Dış Tedarikçiler (SCADA, ERP, Sunucu), ISP ve Siber Güvenlik firmalarının 7/24 acil durum iletişim bilgileri.
Ek-B	**Kritik BT Varlık Envanteri ve Konfigürasyonlar**	Kurtarılacak sunucuların (Fiziksel/Sanal) IP adresleri, İşletim Sistemi versiyonları, Kritiklik seviyeleri (P1-P5) ve yedekleme konumları.
Ek-C	**Ağ Topolojisi ve Felaket Kurtarma Merkezi Bağlantı Şemaları**	VLAN yapıları (İdari/SCADA ayrımı), Felaket Kurtarma Merkezi VPN tünel ayarları ve kritik ağ cihazlarının (Switch/Firewall) fiziksel konumları.
Ek-D	**Parola Kasası ve Acil Erişim Prosedürü**	BT yöneticilerinin ulaşılamaz olduğu durumlarda (Key Person Risk), sistemlere "Admin/Root" seviyesinde erişim sağlayan **"Çift Zarf (Two-Man Rule)"** prosedürü.
Ek-E	**BT Olay Kayıt Formu (Teknik Log)**	Kurtarma sırasında yapılan teknik müdahalelerin (Komutlar, Resetleme, Geri Yükleme) zaman damgalı olarak kaydedildiği form.
Ek-F	**Eylem Kartları (Teknik Roller İçin)**	Sistem Yöneticisi, Ağ Uzmanı ve SCADA Sorumlusu için krizin ilk anlarında uygulanacak "Hızlı Başvuru" kontrol listeleri.

EK-A: KRİTİK BT İLETİŞİM LİSTESİ

Doküman No: İSY-PLAN-BTKP-001 (Ek-A)

Son Güncelleme: 01/07/2025

Gizlilik: YÜKSEK (Kişisel ve Ticari Veri İçerir)

A.1 İÇ PAYDAŞLAR - BT FELAKET KURTARMA EKİBİ (BT-FKE)

(Siber saldırı veya sistem çökmesi anında ilk aranacak kişiler)

KRİTİK ROL	İSİM SOYİSİM	CEP TELEFONU (7/24)	YEDEK İLETİŞİM	GÖREVİ
İKE Lideri (BT Müdürü)	**Can Öztürk**	0536 XXX XX 01	Telsiz Kanal 2	Kurtarma Yöneticisi
Sistem Yöneticisi	**Emre Su**	0536 XXX XX 02	0236 XXX XX 12	Sunucu/Yedekleme
Ağ/Güvenlik Uzmanı	**(Dış Danışman)**	0532 XXX XX 03	-	Firewall/VPN
SCADA Sorumlusu	**Hasan Demir**	0530 XXX XX 05	Telsiz Kanal 3	OT/Saha Entegrasyonu
Olay Yöneticisi	**Üretim Müdürü**	0533 XXX XX 02	Telsiz Kanal 1	Üst Yönetim Raporlama

A.2 DIŞ PAYDAŞLAR - YAZILIM VE DONANIM TEDARİKÇİLERİ

(Sistemlerin teknik kurtarılması için SLA kapsamında destek verecek firmalar)

HİZMET TÜRÜ	FİRMA ADI	KONTAK KİŞİ	ACİL DESTEK HATTI	SLA SÜRESİ
SCADA Yazılımı	**ABC Otomasyon A.Ş.**	Mühendis Veli	**0850 XXX XX 10**	2 Saat (Uzaktan)
ERP Destek	**Yazılım Çözümleri Ltd.**	Destek Masası	**0850 XXX XX 11**	4 Saat
Sunucu/Storage Donanım	**TeknoNet Bilişim**	Burak Tekin	**0532 XXX XX 15**	4 Saatte Parça Değişimi
Siber Güvenlik (IR)	**CyberSavunma A.Ş.**	Olay Müdahale Ekibi	**0212 XXX XX 20**	1 Saat (Analiz)
OSOS (Sayaç) Sistemi	**Enerji Yazılım A.Ş.**	Proje Yöneticisi	**0312 XXX XX 30**	4 Saat

A.3 DIŞ PAYDAŞLAR - ALTYAPI VE HİZMET SAĞLAYICILAR

(Veri merkezinin çalışması ve bağlantı için gerekli kurumlar)

HİZMET TÜRÜ	KURUM ADI	MÜŞTERİ / ABONE NO	ARIZA TELEFONU	NOTLAR
Metro Ethernet (ISP)	**Türk Telekom**	888XXXXXXX	**444 X XXX** (Kurumsal)	Statik IP Blokları
Felaket Kurtarma Merk.	**Bulut Bilişim A.Ş.**	CRM-2025-OSB	**0850 XXX XX 50**	Felaket Kurtarma Merkezi Aktivasyonu İçin
Veri Merkezi Elektrik	**GDZ Elektrik**	-	**186**	Bölgesel Kesinti Teyidi
Klima/Soğutma	**İklimsa Servis**	-	**0542 XXX XX 40**	Sistem Odası Kliması

EK-B: KRİTİK BT VARLIK ENVANTERİ VE KONFİGÜRASYONLAR

Doküman No: İSY-PLAN-BTKP-001 (Ek-B)

Son Güncelleme: 01/07/2025

Gizlilik Derecesi: ÇOK GİZLİ (Kritik IP ve Topoloji Bilgisi İçerir)

Saklama Koşulu: Şifreli Dijital Ortam ve Kilitli Kasa (Basılı)

B.1 SUNUCU VE SANALLAŞTIRMA ALTYAPISI (SERVERS)

Sistem Odası'nda çalışan ve Kurtarma Merkezine replike edilen kritik sunucular.

HOSTNAME	IP ADRESİ	ROL / FONKSİYON	OS / VERSİYON	CPU/RAM/DISK	KRİTİKLİK	YEDEKLEME DURUMU
HOST-01	192.168.10.10	Sanallaştırma Ana Sunucusu 1 (VMware ESXi)	vSphere 8.0	2xXeon / 256GB / -	**P-1**	Config Yedeği (NAS)
HOST-02	192.168.10.11	Sanallaştırma Ana Sunucusu 2 (VMware ESXi)	vSphere 8.0	2xXeon / 256GB / -	**P-1**	Config Yedeği (NAS)

HOSTNAME	IP ADRESİ	ROL / FONKSİYON	OS / VERSİYON	CPU/RAM/DISK	KRİTİKLİK	YEDEKLEME DURUMU
SVR-DC-01	192.168.10.20	Domain Controller (AD) & DNS	Win Svr 2022	4 vCPU / 16GB / 100GB	**P-1**	DR Replika + Günlük
SVR-SCADA	**10.0.0.5**	**SCADA Ana Sunucusu** (Elektrik/Su)	Win Svr 2019	16 vCPU / 64GB / 1TB	**P-2**	**Hot-Standby (Kurtarma Merkezi)**
SVR-SQL-01	192.168.10.30	Veritabanı Sunucusu (ERP/OSOS)	Win Svr 2022	16 vCPU / 128GB / 2TB	**P-3**	Transaction Log (15dk)
SVR-APP-ERP	192.168.10.31	ERP Uygulama Sunucusu	Win Svr 2022	8 vCPU / 32GB / 500GB	**P-5**	Günlük Snapshot
SVR-OSOS	192.168.10.32	OSOS (Sayaç Okuma) Head-End	Linux RHEL 9	8 vCPU / 32GB / 1TB	**P-3**	Günlük Snapshot
SVR-FILE	192.168.10.40	Ortak Dosya Sunucusu	Win Svr 2022	4 vCPU / 16GB / 4TB	**P-4**	Haftalık LTO Tape

B.2 AĞ VE GÜVENLİK DONANIMLARI (NETWORK)

İletişimi sağlayan ve güvenliği kuran omurga cihazlar.

CİHAZ ADI	MARKA / MODEL	YÖNETİM IP	LOKASYON	FONKSİYON	YEDEK DURUMU
FW-MAIN-01	Fortigate 200F	192.168.10.1	Sistem Odası	Ana Firewall / VPN Gateway	**Cold Standby** (İtfaiye Dolabı)
SW-CORE-01	Cisco Catalyst 9300	192.168.10.2	Sistem Odası	Omurga Switch (L3)	**Cold Standby** (İtfaiye Dolabı)
SW-SCADA-01	Cisco IE-4000	**10.0.0.1**	Sistem Odası	**Endüstriyel Switch (İzole)**	Yedek Yok (Manuel Yama)
SW-DR-01	Fortigate 60F	(DR IP'si)	**DR SITE**	DR Tünel Sonlandırma	Aktif

B.3 DEPOLAMA VE YEDEKLEME ÜNİTELERİ (STORAGE)

Verilerin tutulduğu fiziksel alanlar.

CİHAZ KODU	MARKA / TÜR	KAPASİTE	RAID YAPISI	KULLANIM AMACI	ERİŞİM
SAN-01	Dell PowerStore	20 TB (SSD)	RAID 6	Canlı Sanal Makineler	Fiber Channel
NAS-BK-01	Synology	40 TB (HDD)	RAID 5	**Veeam Yerel Yedek**	İzole VLAN
TAPE-01	HP LTO-8 Drive	30 TB / Kartuş	-	**Çevrimdışı (Offline) Yedek**	Fiziksel (USB)

B.4 YAZILIM VE LİSANS BİLGİLERİ

Sistemleri yeniden kurmak için gereken lisans anahtarları.

(Not: Lisans anahtarlarının tam listesi "Ek-D: Parola Kasası" içindedir, burada özet verilmiştir.)

YAZILIM	TEDARİKÇİ	LİSANS TÜRÜ	DESTEK BİTİŞ	KRİTİK NOT
SCADA (Wonderware)	ABC Otomasyon	USB Dongle (Donanım Kilidi)	31.12.2026	**Dongle kaybolursa sistem çalışmaz.** Yedeği kasadadır.
ERP (Logo/Netsis)	Yazılım Çözümleri	Sanal Lisans	31.12.2025	MAC adresine kilitlidir.
Veeam Backup	Distribütör	Abonelik	01.06.2026	Kurtarma için gereklidir.
Firewall (UTM)	TeknoNet	Yıllık Lisans	15.08.2025	VPN lisansı dahildir (50 Kullanıcı).

B.5 BAĞIMLILIK VE KURTARMA SIRASI

Sistemleri açarken izlenecek teknik sıralama (Dependency Map).

- **AŞAMA 1 (Altyapı):** FW-MAIN-01 → SW-CORE-01 → SAN-01 → HOST-01/02
- **AŞAMA 2 (Çekirdek):** SVR-DC-01 (Active Directory olmadan kimse login olamaz).
- **AŞAMA 3 (Operasyon - OT):** SVR-SQL-01 → **SVR-SCADA** (Elektrik yönetimi için en acil).
- **AŞAMA 4 (İdari - IT):** SVR-FILE → SVR-APP-ERP.

EK-C: AĞ TOPOLOJİSİ VE DR SITE BAĞLANTI ŞEMALARI

Doküman No: İSY-PLAN-BTKP-001 (Ek-C)

Son Güncelleme: 01/07/2025

Gizlilik: ÇOK GİZLİ (Siber güvenlik riski nedeniyle şifreli saklanmalıdır)

C.1 GENEL AĞ MİMARİSİ VE GÜVENLİK BÖLGELERİ (ZONES)

Dirençli OSB ağı, güvenlik ve performans için 4 ana bölgeye (Zone) ayrılmıştır. Kriz anında, bu bölgeler arasındaki geçişler Firewall üzerinden yönetilir.

- **WAN (Dış Dünya):** Türk Telekom Metro Ethernet (500 Mbps) ve Yedek VDSL hatları.
- **DMZ (Arındırılmış Bölge):** Web sunucusu ve E-posta Gateway'in bulunduğu, dışarıya kontrollü açık alan.
- **LAN (İdari İç Ağ):** ERP, Dosya Paylaşımı ve Ofis kullanıcılarının bulunduğu güvenli alan.
- **SCADA/OT (Kritik Altyapı):** Elektrik, Su ve Doğalgaz yönetim sistemlerinin bulunduğu **Yüksek Güvenlikli/İzole** alan.

C.2 VLAN VE IP ADRESLEME PLANI (SUBNETTING)

Sistem kurtarma sırasında IP çakışmalarını önlemek için aşağıdaki plan uygulanır.

VLAN No	AĞ ADI	IP BLOĞU	AĞ GEÇİDİ (GATEWAY)	AÇIKLAMA
VLAN 10	**SERVER_FARM**	192.168.10.0/24	192.168.10.1	Ana sunucular (DC, ERP, SQL) buradadır.
VLAN 20	**CLIENT_PC**	192.168.20.0/24	192.168.20.1	İdari personel bilgisayarları.
VLAN 30	**VOIP_PHONE**	192.168.30.0/24	192.168.30.1	IP Telefonlar.
VLAN 40	**KAMERA_CCTV**	192.168.40.0/24	192.168.40.1	Güvenlik kameraları ve NVR.
VLAN 100	**SCADA_OT**	**10.0.0.0/24**	**10.0.0.1**	**Kritik Altyapı.** İdari ağdan tamamen izoledir.
VLAN 99	**MGMT_OOB**	172.16.1.0/24	172.16.1.1	Switch/Firewall yönetim arayüzleri (Out-of-Band).

C.3 FELAKET KURTARMA MERKEZİ BAĞLANTI ŞEMASI

Ana merkez (Yönetim Binası) kaybedildiğinde veya siber saldırı altında olduğunda, veriye erişim bu topoloji üzerinden sağlanır.

Bağlantı Yöntemi: Site-to-Site IPSec VPN

Şifreleme: AES-256

Replikasyon Yazılımı: Veeam Backup & Replication (Sürekli)

Veri Akış Şeması:

ANA MERKEZ - İSTANBUL (Yönetim Binası)		BULUT KURTARMA MERKEZİ - ANKARA (Veri Merkezi)
FW-MAIN-01 (Firewall)	**IPSec Tünel**	**FW-DR-01** (Firewall)
VLAN 10 - Sunucular SVR-ERP (Aktif)		**VLAN 10 - Replika Sunucular SVR-ERP** (Pasif/Standby)
VLAN 100 - SCADA SVR-SCADA (Aktif)		**VLAN 100 - SCADA DR SVR-SCADA** (Hot-Standby)

Acil Durum Erişim Yolu:

- **Kullanıcılar:** Evden veya Ilık Alan'dan "SSL VPN" ile Felaket Kurtarma Merkezi Firewall'una (FW-DR-01) bağlanır.
- **Yönlendirme:** FW-DR-01, gelen trafiği Felaket Kurtarma Merkezi içindeki aktif edilen sunuculara yönlendirir.
- **DNS:** erp.direncliosb.org.tr adresi Felaket Kurtarma Merkezi dış IP'sine yönlendirilir.

C.4 ILIK ALAN (İTFAİYE BİNASI) BAĞLANTI ŞEMASI

Yönetim Binası'nın fiziksel kaybı durumunda (Senaryo: Yangın), İtfaiye Binası'ndaki teknik altyapı şu şekilde devreye girer.

Fiziksel Bağlantı: Yönetim Binası ile İtfaiye Binası arasında yeraltından geçen **Yedekli Fiber Optik (Multi-mode)** kablo mevcuttur. Ancak Yönetim Binası'ndaki ana switch yanarsa, bu fiber hat işlevsiz kalır.

Bu Durumda B Planı (Bağımsız Erişim):

- İtfaiye Binası'nda bağımsız bir **VDSL Modem** ve **4G Yedekleme Router**'ı bulunur.
- Ilık Alan Switch'i (SW-ILIK-01), bu bağımsız hat üzerinden internete çıkar.
- Kullanıcılar, bu internet üzerinden **Kurtarma Merkezine** VPN ile bağlanır.

Şema (Kavramsal):

İTFAİYE BİNASI - ILIK ALAN		
Acil Durum Modem/4G (Bağımsız İnternet)	**İNTERNET** VPN Bağlantısı	**BULUT KURTARMA MERKEZİ** Sunucular Aktif
SW-ILIK-01 (Yedek Switch)		
Port 1-5 Kriz Masası Laptopları	**Port 6** SCADA Yedek Terminali	**Port 7** Ağ Yazıcısı

C.5 SCADA İZOLASYON (AIR-GAP) ŞEMASI

Siber saldırı (Fidye Yazılımı) durumunda uygulanacak en kritik topoloji değişikliğidir.

Normal Durum:

SCADA Ağı ↔ Firewall (İzinli Portlar) ↔ İdari Ağ ↔ İnternet

(Veri okuma için kontrollü geçiş vardır)

SCADA AĞI (VLAN 100)	Firewall İzinli Portlar	İDARİ AĞ	İNTERNET

Saldırı Anı (İzolasyon Modu):

1. **Fiziksel Müdahale:** SCADA Switch'inden (SW-SCADA-01), Firewall'a giden **"Uplink Kablosu"** (Port 24) çekilir.
2. **Sonuç:** SCADA ağı (VLAN 100) tamamen bir adaya dönüşür. İnternet ve İdari Ağ ile bağı kesilir. Saldırgan SCADA'ya ulaşamaz.
3. **Operasyon:** Operatörler sunucu odasında veya Felaket Kurtarma Merkezi üzerinden (temiz ise) lokal konsoldan sistemi yönetir.

SCADA AĞI (VLAN 100) İZOLE	KABLO ÇEKİLDİ X	Firewall → İdari Ağ → İnternet *(SCADA'ya Erişim Yok)*

EK-D: PAROLA KASASI VE ACİL ERİŞİM PROSEDÜRÜ

Doküman No: İSY-PLAN-BTKP-001 (Ek-D)

Gizlilik Derecesi: ÇOK GİZLİ / KIRMIZI

Erişim Yetkisi: Sadece Bölge Müdürü ve Mali İşler Müdürü (Birlikte)

D.1. AMAÇ VE KAPSAM

Bu prosedürün amacı; BT Müdürü ve Sistem Yöneticisinin kriz anında ulaşılmaz olduğu veya görev yapamaz durumda olduğu "Anahtar Personel Kaybı" (Key Person Risk) senaryolarında; **Kriz Yönetim Ekibi'nin (KYE)** kritik sistemlere (Sunucular, Firewall, SCADA, Felaket Kurtarma Merkezi) en üst düzey yetkiyle (Admin/Root) erişebilmesini garanti altına almaktır.

D.2. SAKLAMA STRATEJİSİ: ÇİFT ZARF KURALI (TWO-MAN RULE)

Tek bir kişinin tek başına sisteme tam erişimini engellemek ve güvenliği sağlamak için, kritik şifreler **bölünmüş** ve **mühürlenmiş** iki ayrı zarfta saklanır.

- **Dijital Kasa:** Tüm şifreler, şifreli bir **"Master Password Vault"** (KeePass/Bitwarden - Çevrimdışı Kopya) dosyasında tutulur. Bu dosya, Felaket Kurtarma Merkezi'nde ve İtfaiye Binası'ndaki USB bellekte mevcuttur.
- **Fiziksel Anahtarlar (Zarflar):** Bu dijital kasayı açacak olan "Ana Şifre (Master Password)" ve "MFA Yedek Kodları" ikiye bölünerek saklanır.

ZARF	LOKASYON	SAKLAYAN / SORUMLU	İÇERİK
ZARF A	Yönetim Binası - Ana Kasa	**Bölge Müdürü**	• Master Password (İlk Yarısı) • BitLocker Kurtarma Anahtarı (Bölüm 1)
ZARF B	Banka Kiralık Kasa	**Mali İşler Müdürü**	• Master Password (İkinci Yarısı) • MFA (2FA) Yedek Kurtarma Kodları • BitLocker Kurtarma Anahtarı (Bölüm 2)

D.3. ACİL DURUM ERİŞİM PROSEDÜRÜ (AKTİVASYON)

Bu prosedür, sadece **Seviye 3 ve üzeri krizlerde** ve **BT Yöneticilerine ulaşılamadığının teyit edildiği** durumlarda uygulanır.

- **Teyit:** Kriz Lideri (Bölge Md.), BT Müdürü ve yedeğinin ulaşılamaz olduğunu (veya güvenilmez durumda olduğunu) teyit eder.
- **Birleşme:** Bölge Müdürü ve Mali İşler Müdürü bir araya gelir. (Biri yoksa vekili devreye girer, tutanak tutulur).
- **Zarf Açımı:**
  - Bölge Müdürü **Zarf A**'yı açar.
  - Mali İşler Müdürü **Zarf B**'yi bankadan getirtir/açar.
- **Sisteme Giriş:**
  - İtfaiye Binası'ndaki (Ilık Alan) Acil Durum Dizüstü Bilgisayarı açılır.
  - Masaüstündeki OSB_SECURE_VAULT.kdbx dosyası çalıştırılır.
  - Zarf A ve Zarf B'deki şifre parçaları birleştirilerek kasa açılır.
- **Dış Destek:** Kasa açıldıktan sonra, içindeki **"Domain Admin"** şifresi, kurtarma işlemi için çağrılan **Dış Destek Firmasına (TeknoNet/Siber Güvenlik)** imza karşılığı verilir.

D.4. PAROLA KASASI İÇERİK LİSTESİ

(Zarflar açıldığında erişilecek kritik hesaplar şunlardır)

SİSTEM	HESAP ADI	KRİTİKLİK	AÇIKLAMA
Active Directory	Administrator	**P-1**	Tüm ağın en yetkili hesabı.
Firewall (Fortigate)	admin	**P-1**	VPN ve internet erişim yönetimi.
Core Switch (Cisco)	enable (Secret)	**P-1**	Ağ omurgası yönetimi.
VMware (Hostlar)	root	**P-2**	Sanal sunucu yönetimi.
SCADA Sunucusu	scada_admin	**P-2**	Elektrik/Su dağıtım kontrolü.
Bulut DR Paneli	osb_dr_admin	**P-2**	Felaket kurtarma merkezini başlatmak için.
ERP (Veritabanı)	sa (SQL)	**P-3**	Veritabanı tam yetkili kullanıcısı.
OSOS (Sayaç)	root	**P-3**	Sayaç okuma sistemi kök hesabı.

D.5. GÜVENLİK VE YENİLEME (OLAY SONRASI)

Acil durum zarfları açıldıktan sonra **gizlilik ihlal edilmiş sayılır**. Kriz sona erdiğinde ve sistemler normale döndüğünde (Normale Dönüş Fazı):

- **Şifre Değişimi:** BT Müdürü (veya yeni atanan yönetici), kasada yer alan **TÜM** şifreleri derhal değiştirir.
- **Yeni Zarflama:** Yeni şifreler, yeni bir Master Password ile şifrelenir. Parçalar yeni zarflara konur, mühürlenir ve imzalanır.
- **Teslim:** Zarflar tekrar ilgili yöneticilere (Bölge Md. ve Mali İşler Md.) teslim edilir.
- **Tutanak:** Eski zarfların açıldığı ve yenilerinin oluşturulduğu bir tutanakla kayıt altına alınır.

EK-E: BT OLAY KAYIT FORMU (TEKNİK LOG)

Amaç: BT-FKP aktivasyonu süresince sistemler üzerinde yapılan tüm teknik müdahalelerin (komutlar, konfigürasyon değişiklikleri, fiziksel işlemler) kronolojik ve değiştirilemez bir kaydını tutmaktır. Bu kayıtlar, olay sonrası "Kök Neden Analizi" ve olası "Adli Soruşturma" için birincil delil niteliğindedir.

Kullanım Kuralı: Her satır, işlemi yapan kişi tarafından paraflanmalıdır. Dijital kayıt (Notepad/Excel) tutuluyorsa, dosya her saat başı salt okunur olarak kaydedilmelidir.

TARİH	SAAT	SİSTEM / VARLIK	YAPILAN TEKNİK İŞLEM / KOMUT / AKSİYON	SONUÇ / HATA KODU	YAPAN
01.07.25	14:15	FW-MAIN-01	disconnect interface wan1 komutu ile internet kesildi.	Bağlantı Koptu (OK)	C.Öztürk
01.07.25	14:20	SVR-SCADA	Sunucu ağ kablosu fiziksel olarak çekildi (Air-gap).	İzole Edildi	H.Demir
01.07.25	14:45	DR-VPN	Site-to-Site VPN tünel durumu kontrol edildi.	Status: UP	E.Su
01.07.25	15:00	SVR-ERP-DR	Sanal sunucu "Power On" yapıldı.	OS Boot Success	E.Su
01.07.25	15:30	SQL-DB	Veritabanı tutarlılık kontrolü (DBCC CHECKDB) başlatıldı.	Hata Yok	E.Su

EK-F: TEKNİK EYLEM KARTLARI (ACTION CARDS)

Amaç: Krizin ilk 60 dakikasında (Altın Saat), teknik personelin panik yapmadan kritik güvenlik ve kurtarma adımlarını atmasını sağlayan kontrol listeleridir.

KART 1: BT MÜDÜRÜ (BT-FKE-TEKNİK LİDERİ)

ROL: BT MÜDÜRÜ	SORUMLULUK: TEKNİK KOMUTA VE KARAR
FAZ 1: TEŞHİS VE İZOLASYON (İLK 15 DAKİKA)	**DURUM**
[ ] 1. Olay Tipi: **Sorun fiziksel mi (Yangın/Su) siber mi? Siber ise "SOMP Planı"nı başlat.**	☐
[ ] 2. İzolasyon Emri: **Siber saldırı şüphesi varsa, Ağ Uzmanına** "İnterneti Kes" **ve** "SCADA'yı İzole Et" **emrini ver.**	☐
[ ] 3. Raporlama: **Olay Yöneticisi'ne (Üretim Müdürü) "BTKP Aktive Edildi, Tahmini Kesinti: X Saat" bilgisini ver.**	☐
FAZ 2: KURTARMA YÖNETİMİ	
[ ] 4. DR Kararı: **Sistemlerin yerinde kurtarılamayacağı kesinleşirse** "Kurtarma Merkezine Geçiş (Failover)" **onayını ver.**	☐
[ ] 5. Dış Destek: **İhtiyaç varsa Siber Güvenlik veya ERP Yazılım firmasını (Ek-A) acil koduyla ara.**	☐
[ ] 6. İletişim: **Kullanıcılara "Sistemler kapalıdır, manuel prosedüre geçin" duyurusunu İK üzerinden yaptır.**	☐

KART 2: SİSTEM YÖNETİCİSİ (SERVER ADMIN)

ROL: SİSTEM YÖNETİCİSİ	SORUMLULUK: SUNUCU VE VERİ KURTARMA
FAZ 1: KORUMA (İLK 30 DAKİKA)	**DURUM**
[ ] 1. Yedek Güvenliği: **Çevrimdışı (Tape/USB) yedeklerin ağa bağlı** OLMADIĞINI **fiziksel olarak kontrol et.**	☐
[ ] 2. Durum Tespiti: **Hangi sunucuların etkilendiğini (Şifreli/Kapalı) listele.**	☐
FAZ 2: DR AKTİVASYONU (FAILOVER)	
[ ] 3. DR Login: **Bulut Felaket Kurtarma paneline osb_dr_admin hesabıyla güvenli (MFA) giriş yap.**	☐
[ ] 4. Öncelik: **Önce** Domain Controller (DC)**, sonra** SCADA**, en son** ERP **sunucularını "Power On" yap.**	☐
[ ] 5. Test: **Sunucuların açıldığını ve servislerin (SQL, IIS) çalıştığını kontrol et.**	☐
[ ] 6. Erişim: **Kullanıcıların bağlanabilmesi için Terminal Server / VPN ağ geçidini aktif et.**	☐

KART 3: SCADA VE OTOMASYON SORUMLUSU

ROL: SCADA SORUMLUSU	SORUMLULUK: KRİTİK ALTYAPI KONTROLÜ
FAZ 1: SAHA GÜVENLİĞİ	**DURUM**
[ ] 1. Manuel Mod: **SCADA ekranları donduysa veya şüpheli hareket varsa, telsizden** "SCADA GÜVENSİZ, MANUEL MODA GEÇİN" **anonsu yap.**	☐
[ ] 2. Fiziksel İzolasyon: **Sistem odasındaki Endüstriyel Switch'in (SW-SCADA-01) "Uplink" kablosunu çek.**	☐
FAZ 2: KURTARMA	
[ ] 3. Yedek Terminal: **İtfaiye Binası'ndaki (Ilık Alan) yedek SCADA laptopunu al ve D-1 portuna bağla.**	☐

ROL: SCADA SORUMLUSU	SORUMLULUK: KRİTİK ALTYAPI KONTROLÜ
[ ] 4. Veri Kontrolü: **Sahadaki RTU'lardan verinin (Akım, Voltaj, Su Seviyesi) gelip gelmediğini kontrol et.**	☐
[ ] 5. Operasyon: **Elektrik İşletme Müdürü'nün talimatlarını yedek terminalden uygula.**	☐

ONAY

Bu plan ve ekleri, Dirençli OSB'nin teknolojik varlıklarını her türlü felakete karşı korumak ve en kısa sürede yeniden çalışır hale getirmek amacıyla hazırlanmıştır.

Hazırlayan (Plan Sahibi):	**Onaylayan (Olay Yöneticisi):**
(İmza)	*(İmza)*
Can Öztürk	**Mehmet Demirtaş**
Bilgi Teknolojileri Müdürü	Bölge Müdürü
(BT-FKE Lideri)	(Kriz Lideri)
Tarih: **01/07/2025**	**Tarih:** 01/07/2025

Ek E.3.2: "Dirençli OSB" İçin Siber Olaylara Müdahale Planı

"Dirençli OSB" İçin Siber Olaylara Müdahale Planı

DOKÜMAN KONTROL

Plan Adı:	Dirençli OSB - Siber Olay Müdahale Planı (SOMP)
Doküman No:	İSY-PLAN-SOMP-001
Versiyon:	1.0
Yürürlülük Tarihi:	01/07/2025
Plan Sahibi:	BT Sorumlusu (Teknik/BT Lideri)
Onaylayan:	Mehmet Demirtaş (Kriz Lideri)
Gizlilik:	YÜKSEK - Sadece Yetkili Personel
Bir Sonraki Gözden Geçirme:	01.07.2026

BÖLÜM 1: GİRİŞ VE STRATEJİK ÇERÇEVE

1.1. Amaç

Bu planın temel amacı, Dirençli OSB'nin kritik bilgi varlıklarına (SCADA, ERP, sunucular, ağ) yönelik bir siber güvenlik olayı (fidye yazılımı, veri sızıntısı, yetkisiz erişim vb.) meydana geldiğinde, olayın etkisini en aza indirmek, olayı hızla kontrol altına almak, delilleri korumak ve sistemleri güvenli bir şekilde kurtarmak için izlenecek teknik ve koordinasyon adımlarını tanımlamaktır.

1.2. Kapsam

Bu plan, Dirençli OSB tesislerinde kullanılan tüm BT (Bilişim Teknolojileri) ve OT (Operasyonel Teknolojiler - SCADA) ağlarını, sunucuları (özellikle BT-SVR-SCADA ve BT-SVR-ERP), kullanıcı bilgisayarlarını ve bulut hizmetlerini etkileyen Seviye 2 ve üzeri tüm siber güvenlik olaylarını kapsar.

1.3. Bütünleşik Planlarla İlişkisi (Aktivasyon Bağlantısı)

Bu plan, Bütünleşik Olay Yönetim Yapısı'nın (İSP Bölüm 2) bir parçası olarak kullanılır.

- **Tetikleyici:** Bu plan, bir kesintinin nedeninin siber saldırı olduğundan şüphelenildiğinde derhal aktive edilir.
- **Koordinasyon:** Bu planın uygulanması **Teknik/BT Lideri (BT Müdürü)** tarafından yürütülür ve sonuçları Olay Yöneticisi'ne (İSYS Yöneticisi) raporlanır.
- **Entegrasyon:** Bu plandaki "Kurtarma" fazı, doğrudan **BT Felaket Kurtarma Planı'nı (BT-FKP)** tetikler. "İletişim" adımları ise **Kriz İletişim Planı (KİP)** ile koordine edilir.

1.4. Temel Müdahale İlkeleri

- **ÖNCE SINIRLA, SONRA İNCELE:** İlk öncelik, saldırının yayılmasını önlemektir (örneğin, SCADA ağını izole etmek). Analiz daha sonra yapılır.
- **FİDYE ÖDENMEZ:** Dirençli OSB'nin politikası, **SIBER-SCD-001** (Fidye Yazılımı) riskine yanıt olarak, saldırganlara fidye ödememektir. Tüm strateji, İSP'de tanımlanan "İzole Yedekleme (3-2-1 Kuralı)" stratejisine dayanır.
- **DELİLLERİ KORU:** Olayın yasal bir soruşturmaya (adli bilişim) dönüşme ihtimaline karşı, sistemleri hemen silmek yerine, mümkünse imajları (kopyaları) alınarak deliller korunmalıdır.

1.5. Temel Tanımlar

- **SOME (Siber Olay Müdahale Ekibi):** Bu planda görev alan, İKE-Teknik/BT Ekibi ve dış destek uzmanlarından oluşan özel ekip.
- **Fidye Yazılımı (Ransomware):** Verileri şifreleyerek fidye isteyen zararlı yazılım.

BÖLÜM 2: ORGANİZASYON VE ROLLER

2.1. Siber Olay Müdahale Ekibi (SOME)

Bu ekip, Teknik/BT Ekibinin siber olaylara müdahale için özelleşmiş halidir.

Tablo 2.1: SOME Rolleri ve Sorumlulukları

Rol (Plandaki Adı)	Sorumlu Kişi (Dirençli OSB)	Temel Görev ve Sorumluluklar (Siber Olay Sırasında)
SOME Lideri	**BT Müdürü** Teknik/BT Lideri)	Müdahalenin genel teknik komutasını yürütür. Olay Yöneticisi'ne sürekli raporlama yapar. Dış destek firmalarını (Ek-A) aktive eder.
Teknik Analist	**Sistem Yöneticisi**	Olayın kök nedenini analiz eder, ihlal göstergelerini toplar, sistemleri izole eder, tehdidi temizler ve sistemleri kurtarır (BTKP'yi uygular).
SCADA Güvenlik Sor.	**Otomasyon Teknikeri**	SCADA ağındaki anormallikleri izler. Operasyonel Teknolojinin (OT) güvenli duruşunu sağlar.
Dış Destek (Kritik)	**[Siber Güvenlik Firması Adı]** (Ek-A)	Olayın analiz edilmesi (adli bilişim), temizlenmesi ve kurtarılması için SOME Lideri'ne 7/24 uzman teknik destek sağlar.
Dış Destek (Yasal)	**Hukuk Müşaviri** (Ek-A)	KYE'ye KVKK ve TCK kapsamındaki yasal bildirim yükümlülükleri (örneğin, 72 saat kuralı) hakkında danışmanlık sağlar.

2.2. Dış Destek İrtibatları

Bu planın başarısı, OSB'nin sınırlı BT kaynağı nedeniyle dış desteğe hızlı erişime bağlıdır.

Tablo 2.2: Siber Olay Acil Durum İrtibatları (Detaylar Ek-A'dadır)

Kurum / Hizmet	Ne Zaman Aranır?	İrtibat Bilgisi
[Siber Güvenlik Firması]	Seviye 3 veya 4 (Fidye, Veri Sızıntısı) olay teyit edildiğinde (İlk 30 dk içinde).	Acil Destek Hattı: [Telefon No]
[SCADA Yazılım Destek]	SCADA sistemine müdahale veya temizlik gerektiğinde.	[Telefon No]
[Hukuk Müşaviri]	Kişisel veri sızıntısı şüphesi varsa (İlk 1 saat içinde KYE tarafından).	[Telefon No]
USOM	Geniş çaplı bir saldırı veya kritik altyapı (SCADA) etkilenirse (KYE kararı ile).	İhbar Hattı / Web Sitesi
Emniyet (Siber Suçlar)	Kasıtlı bir suç (fidye, hırsızlık) teyit edildiğinde (KYE kararı ile).	112

BÖLÜM 3: OLAY SINIFLANDIRMASI VE AKTİVASYON

Her güvenlik uyarısı bir kriz değildir. Kaynakların doğru yönetilmesi için olaylar etkilerine göre sınıflandırılır ve müdahale buna göre ölçeklenir.

3.1. Olay Seviyeleri

Seviye	Tanım	Örnek Senaryo (Dirençli OSB)	Aksiyon / Yükseltme
Seviye 1 ***(Olay / Event)***	Operasyonu etkilemeyen, otomatik engellenen basit tehditler.	• Antivirüsün bir dosyayı silmesi. • Firewall'un dışarıdan gelen port taramasını engellemesi.	**SOME Kayıt Açar.** Olay günlüğe işlenir, alarm kapatılır. Üst yönetime raporlanmaz.
Seviye 2 ***(Düşük Tehdit)***	Tekil bir cihazı etkileyen ancak ağa yayılmayan olaylar.	• Bir personelin oltalama mailine tıklaması. • Tek bir ofis bilgisayarına virüs bulaşması.	**SOME Müdahale Eder.** Cihaz ağdan koparılır, formatlanır. Kullanıcı şifresi değiştirilir.
Seviye 3 ***(Yüksek Tehdit)***	Kritik sunucuları veya SCADA ağını tehdit eden, yayılma riski olan saldırılar.	• ERP sunucusunda yetkisiz yönetici (Admin) hesabı açılması. • SCADA ağında bilinmeyen bir IP'nin taranması.	**SOME Tam Aktivasyon.** Olay Yöneticisi bilgilendirilir. Dış destek firması "Hazır Ol" durumuna geçirilir.
Seviye 4 ***(Kriz / Felaket)***	İş sürekliliğini durduran, veri sızıntısı içeren veya SCADA kontrolünü ele geçiren saldırılar.	• **Fidye Yazılımı (Ransomware):** Tüm sunucuların şifrelenmesi. • **Veri Sızıntısı:** Abone verilerinin çalınması. • **SCADA Sabotajı:** Uzaktan izinsiz manevra.	**TAM SEFERBERLİK. İSP ve KYP Aktive Edilir.** İnternet tamamen kesilir. USOM, KVKK ve Savcılık bildirimi yapılır.

3.2. Aktivasyon Kriterleri

Bu plan, SOME Lideri tarafından aşağıdaki durumlardan biri tespit edildiğinde **derhal** aktive edilir:

1. **Fidye Notu:** Herhangi bir sunucuda şifrelenmiş dosya veya fidye talep notu görülmesi.
2. **SCADA Anormalliği:** Operatörün yapmadığı bir işlemin (Kesici açma/kapama) sistemde görülmesi.
3. **Veri Çıkışı:** Firewall üzerinde yüksek miktarda ve açıklanamayan dışarı yönlü veri trafiği (Data Exfiltration) tespiti.

BÖLÜM 4: OLAY MÜDAHALE SÜRECİ (SANS / PICERL MODELİ)

Dirençli OSB, siber olayları yönetirken uluslararası kabul görmüş **PICERL** (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) döngüsünü uygular.

4.1. Faz 1: HAZIRLIK (Olay Öncesi)

Amaç, saldırı gerçekleşmeden önce savunma hattının kurulmasıdır.

- **Teknik Hazırlık:** SCADA ağının izole edilmesi (Air-Gap), 3-2-1 İzole Yedekleme, EDR/Firewall loglamasının aktif edilmesi.
- **Personel Hazırlığı:** SOME ekibinin 6 ayda bir "Masa Başı Tatbikatı" yapması.

4.2. Faz 2: TESPİT VE ANALİZ (Olay Anı)

Amaç, bir anormalliğin güvenlik olayına dönüştüğünün teşhis edilmesidir.

- **Tetikleyici:** EDR alarmı veya kullanıcı ihbarı ("Dosyalarım açılmıyor!").
- **İlk Analiz:** SOME Lideri şu soruları yanıtlar: *Saldırı türü ne? SCADA etkilendi mi? Olay Seviyesi (1-4) ne?*
- **Kayıt:** Olayla ilgili tüm bulgular "Ek-B: Siber Olay Kayıt Formu"na işlenmeye başlanır.

4.3. Faz 3: SINIRLAMA (Yayılmayı Önleme - En Kritik Faz)

Amaç, saldırganın hareket alanını kısıtlamak ve zararı durdurmaktır. Analizden önce gelir.

- **Adım 1 (Fiziksel İzolasyon):** Enfekte olduğu tespit edilen veya şüphelenilen cihazın ağ kablosu **FİZİKSEL OLARAK ÇEKİLİR**. (Kapatma yapılmaz, RAM verisi kaybolmasın diye).
- **Adım 2 (Ağ İzolasyonu):** Saldırı İdari Ağda (BT) ise, SCADA Ağı (OT) ile olan tüm bağlantı noktaları (Firewall kuralları) kapatılır.
- **Adım 3 (İnternet Kesintisi):** Saldırı dışarıdan yönetiliyorsa, Kurumsal Firewall üzerinden tüm internet trafiği kesilir.
- **Adım 4 (Hesap Dondurma):** Ele geçirildiği şüphelenilen yönetici (Admin) hesapları kilitlenir.

4.4. Faz 4: YOK ETME (Tehdidi Temizleme)

Amaç, saldırganın izlerinin silinmesi ve açığın kapatılmasıdır.

- **Kök Neden:** Saldırganın giriş noktası (Örneğin, Açık RDP portu, Yamasız Sunucu, Oltalama Maili) tespit edilir ve kapatılır.
- **Temizleme:**
  - Enfekte olmuş sunucular/diskler **FORMATLANIR**. (Sadece antivirüs ile temizlemeye güvenilmez).
  - BIOS/Firmware seviyesinde kalıcılık (Persistence) kontrolü yapılır.

- **Güvenlik Artırımı:** Tüm yönetici (Domain Admin) parolaları değiştirilir.

4.5. Faz 5: KURTARMA (Normale Dönüş)

Amaç, sistemlerin operasyona geri döndürülmesidir. Bu aşamada BT-FKP devreye girer.

- **Sıralama:** Önce Altyapı (AD/DNS), sonra SCADA, en son ERP sistemleri açılır.
- **Geri Yükleme: BT-FKP (Ek E.3)** prosedürleri uygulanır. Sistemler, olaydan önceki en son "Temiz/Çevrimdışı Yedek"ten geri yüklenir.
- **Doğrulama:** Sistem açıldıktan sonra EDR taraması yapılır ve verilerin tutarlılığı iş birimlerince teyit edilir.

4.6. Faz 6: OLAY SONRASI (Öğrenilen Dersler)

- **Raporlama:** SOME Lideri, olayın zaman çizelgesini, etkisini ve maliyetini içeren bir rapor hazırlar.
- **Hukuki Süreç:** Veri sızıntısı varsa, Hukuk Müşaviri ile birlikte 72 saat içinde KVKK Kuruluna bildirim yapılır.

BÖLÜM 5: SENARYO BAZLI EYLEM PLANLARI (PLAYBOOKS)

Bu bölüm, "Dirençli OSB"nin en yüksek riskli siber tehdit senaryoları (Risk Kaydı: SIBER-SCD-001, BT-RD-01) için hazırlanmış adım adım teknik müdahale talimatlarını içerir.

5.1. SOP-PB-01: FİDYE YAZILIMI (RANSOMWARE) SALDIRISI

(Kritiklik: SEVİYE 4 - Operasyonun Durması)

Tetikleyici:	Sunucularda şifrelenmiş dosya uzantıları (.enc, .lock) veya fidye notu görülmesi.
Hedef:	Yayılmayı durdurmak ve temiz yedekten dönmek (Fidye Ödememek).
Sorumlu:	SOME Lideri (BT Müdürü)

ADIM		EYLEM (KONTROL LİSTESİ)	SORUMLU	DURUM
1		**TAM İZOLASYON (FİŞİ ÇEK):** Etkilenen sunucunun/PC'nin ağ kablosunu fiziksel olarak çek. Sanal sunucu ise vSwitch bağlantısını kes. (Kapatma, RAM analizi için açık kalsın).	Saha Ekibi	[ ]
2		**AĞI KORU:** SCADA ve ERP ağları arasındaki Firewall kurallarını "DENY ALL" moduna alarak yanal hareketi (lateral movement) engelle.	Ağ Uzmanı	[ ]
3		**YEDEKLERİ GÜVENCEYE AL:** Çevrimdışı (Tape/USB) yedeklerin ağa bağlı **OLMADIĞINI** fiziksel olarak kontrol et. Bulut yedekleme hesabının şifresini değiştir.	Sistem Yön.	[ ]
4		**ANALİZ:** Fidye notunun fotoğrafını çek. Dosya uzantısını ID Ransomware gibi araçlarla kontrol et. Decryptor var mı araştır.	Analist	[ ]
5		**KARAR:** Kriz Lideri'ne (Bölge Md.) durumu bildir: *"Sistem kilitlendi. Fidye ödemiyoruz. Temiz yedekten döneceğiz. Kesinti süresi: 8 Saat."*	SOME Lideri	[ ]
6		**TEMİZLİK:** Enfekte diskleri tamamen formatla (Wipe). İşletim sistemini temiz kaynaktan (ISO) yeniden kur.	Sistem Yön.	[ ]
7		**KURTARMA: BT-FKP (Ek E.3)** prosedürlerini işleterek en son temiz çevrimdışı yedekten geri yükleme yap.	BT Ekibi	[ ]
8		**BİLDİRİM:** Kişisel veri etkilendiyse 72 saat içinde KVKK Kuruluna, SCADA etkilendiyse USOM'a bildirim yap.	Hukuk/Kriz Md.	[ ]

5.2. SOP-PB-02: SCADA AĞINA YETKİSİZ ERİŞİM

(Kritiklik: SEVİYE 4 - Fiziksel Güvenlik ve Altyapı Riski)

Tetikleyici:	SCADA ekranında operatör dışı hareket (mouse oynaması, kesici açılması) veya bilinmeyen IP bağlantısı.
Hedef:	Altyapının (Trafo, Pompa) fiziksel güvenliğini sağlamak.
Sorumlu:	SCADA Güvenlik Sorumlusu

ADIM	EYLEM (KONTROL LİSTESİ)	SORUMLU	DURUM
1	**ACİL DURDURMA (MANUEL MOD):** Telsizden tüm saha ekiplerine **"SCADA GÜVENSİZ. MANUEL YÖNETİME GEÇİN"** anonsu yap. Otomatik komutları yoksay.	Olay Yöneticisi	[ ]
2	**FİZİKSEL KOPARMA (AIR-GAP):** Sistem Odası'ndaki SCADA Switch'inin (SW-SCADA-01) dış dünya ile olan "Uplink" kablosunu çek.	BT/SCADA Sor.	[ ]
3	**DURDURMA:** Sistem kararsız davranıyorsa (kontrolsüz açma/kapama), SCADA sunucusunu güvenli şekilde kapat (Shutdown).	BT Müdürü	[ ]

ADIM	EYLEM (KONTROL LİSTESİ)	SORUMLU	DURUM
4	**GİRİŞ NOKTASI ANALİZİ:** VPN loglarını incele. Hangi kullanıcı hesabıyla girildiğini bul ve o hesabı kilitle.	Ağ Uzmanı	[ ]
5	**DOĞRULAMA:** Dış destek firması (ABC Otomasyon) ile sistemi tara. Temiz onayı almadan SCADA'yı tekrar ağa bağlama.	SCADA Sor.	[ ]

5.3. SOP-PB-03: VERİ SIZINTISI (DLP ALARMI)

(Kritiklik: SEVİYE 3 - Yasal ve İtibar Riski)

Tetikleyici:	Firewall üzerinde anormal miktarda dışarı yönlü veri trafiği (Data Exfiltration) veya ifşa sitesinde OSB verisi.
Hedef:	Veri çıkışını durdurmak ve yasal süreci başlatmak.
Sorumlu:	Ağ Güvenlik Uzmanı

ADIM	EYLEM (KONTROL LİSTESİ)	SORUMLU	DURUM
1	**HESABI DONDUR:** Veri sızdıran kullanıcı hesabını (Active Directory) ve VPN erişimini derhal kapat.	Sistem Yön.	[ ]
2	**TRAFİĞİ KES:** Firewall üzerinden şüpheli hedef IP adresine giden trafiği blokla. Gerekirse tüm internet çıkışını durdur.	Ağ Uzmanı	[ ]
3	**TESPİT (KAPSAM):** Hangi verilerin sızdığını loglardan belirle. (Personel TC'si mi? SCADA şeması mı? Ticari sır mı?).	Analist	[ ]
4	**DELİL TOPLAMA:** İlgili bilgisayarın disk imajını (Adli Kopya) al. Logları güvenli bir yere kopyala.	SOME Lideri	[ ]
5	**YASAL BİLDİRİM:** Hukuk Müşaviri ile görüş. Kişisel veri ise **72 Saat** içinde KVKK bildirimi hazırla.	Kriz Lideri	[ ]

BÖLÜM 6: PLANIN SÜRDÜRÜLEBİLİRLİĞİ (PUKÖ)

Siber tehditler sürekli değiştiği için, SOP planı yaşayan bir belge olmalıdır.

6.1 Eğitim ve Yetkinlik Programı

- **SOME Teknik Eğitimi:** BT ve Otomasyon personeline yılda bir kez "Olay Müdahale (Incident Response)" ve "Adli Bilişim" eğitimi verilir.
- **Farkındalık Eğitimi:** Tüm OSB personeline, işe girişte ve yılda bir kez "Oltalama (Phishing), Parola Güvenliği" eğitimi verilir.

6.2 Test ve Tatbikat Programı

Planın işlerliği aşağıdaki takvimle test edilir:

- **Ç1 (Mart): Oltalama Simülasyonu** (Tüm Personel). Tıklama oranları ölçülür.
- **Ç2 (Haziran): Masa Başı Tatbikatı (Ransomware).** SCADA'nın şifrelendiği senaryo üzerinden karar alma pratiği.
- **Ç3 (Eylül): Sızma Testi (Pentest).** Yetkili firmanın dışarıdan sisteme girmeye çalışması.
- **Ç4 (Aralık): Yedek Dönüş Testi.** Çevrimdışı yedekten veri kurtarma provası.

6.3 Planın Gözden Geçirilmesi

Bu plan; her "Seviye 3/4" siber olaydan sonra, IT/OT altyapısında majör değişiklik olduğunda ve yılda en az bir kez (Ocak ayı) gözden geçirilir.

BÖLÜM 7: EKLER (Siber Odaklı)

Eklerde yer alan formlar ve listeler, olay anında zaman kaybetmeden doldurulmalı ve kriz sonrası hukuki/teknik analizlerde (Adli Bilişim) delil olarak kullanılmalıdır.

- **Ek-A: SOME İletişim Listesi** (Siber Güvenlik Firması, USOM, Hukukçu).
- **Ek-B: Siber Olay Kayıt Formu** (Teknik detayların işlendiği log).
- **Ek-C: Delil Teslim Tutanağı** (Adli bilişim için zincirleme gözetim formu).
- **Ek-D: Sistem İzolasyon Şeması** (Hangi kablonun çekileceğini gösteren kroki).

EK-A: SOME İLETİŞİM LİSTESİ (SİBER ÖZEL)

Amaç: Siber saldırı anında teknik ve hukuki destek için aranacak öncelikli numaralar.

KATEGORİ	ROL / KURUM	KONTAK KİŞİ	ACİL DURUM TEL (7/24)	NOTLAR
İÇ EKİP (SOME)	**SOME Lideri (BT Md.)**	Can Öztürk	0536 XXX XX 01	Müdahale Yöneticisi
	SCADA Güvenlik Sor.	Hasan Demir	0530 XXX XX 05	OT/Saha Erişimi
	Hukuk Müşaviri	Av. Mehmet Y.	0532 XXX XX 99	KVKK/Savcılık Bildirimi
DIŞ DESTEK	**Siber Güvenlik (IR)**	**CyberSavunma A.Ş.**	**0850 XXX XX 20**	**SLA: 1 Saat.** (Acil Kod: OSB-SOS)
	USOM	İhbar Hattı	**Bilgi: usom.gov.tr**	Devlet İrtibat Noktası
	SCADA Yazılımı	ABC Otomasyon	0850 XXX XX 10	Lisans/Konfigürasyon
	İSS (Internet)	Türk Telekom	444 X XXX	DDoS Engelleme (Clean Pipe)

EK-B: SİBER OLAY KAYIT FORMU (INCIDENT LOG)

Amaç: Olayın başlangıcından çözümüne kadar atılan her adımın kronolojik kaydını tutmaktır. Bu form, adli süreçlerde "Olay Tutanağı" yerine geçer.

Olay No: SOP-2025-___ | **Başlangıç Tarihi:** //____ | **Tespit Eden:** _____

SAAT	GÖZLEM / OLAY	ALINAN AKSİYON / KOMUT	YAPAN	SONUÇ
14:15	Firewall'da 10.0.0.5 IP'sinden Rusya'ya aşırı trafik (Upload) tespit edildi.	Disconnect komutu ile port kapatıldı.	Ağ Uzmanı	Trafik durdu.
14:20	SCADA Sunucusu (SVR-SCADA) ekranında "Dosyalarınız Şifrelendi" notu görüldü.	Sunucunun ağ kablosu **fiziksel olarak çekildi**.	Saha Amiri	Sunucu İzole.
14:30	Kriz Lideri bilgilendirildi.	"Seviye 4 Kriz" ilan edildi.	SOME Lid.	KYE toplandı.
...	...	...	...	...

EK-C: DELİL TESLİM TUTANAĞI

Amaç: Adli bilişim analizi için toplanan dijital delillerin (Disk, USB, Log Dosyası) kimden kime, ne zaman geçtiğini belgeleyerek delil bütünlüğünü (mahkeme geçerliliğini) korumaktır.

DELİL NO	DELİLİN TANIMI	ALINDIĞI YER / CİHAZ	ALAN KİŞİ	TESLİM EDEN	TARİH / SAAT	İMZA
01	SVR-SCADA Hard Diski (S/N: 12345)	Sistem Odası Kabin 1	Polis Memuru / Adli Uzman	BT Müdürü	01.07.25 16:00	[İmza]
02	Firewall Logları (USB Bellek)	Firewall Log Sunucusu	Siber Güv. Firması	Sistem Yön.	01.07.25 16:15	[İmza]

EK-D: SİSTEM İZOLASYON ŞEMASI (ACİL DURUM)

Amaç: Siber saldırının yayılmasını engellemek için hangi kablonun çekileceğini gösteren görsel rehber.

Talimat:

1. **SCADA İzolasyonu:** Şemada **"KIRMIZI"** ile işaretli olan, SCADA Switch'inden (SW-SCADA-01) Firewall'a giden **Port 24** kablosunu çekin. Bu işlem SCADA'yı "Ada Modu"na alır.
2. **İnternet Kesintisi:** Şemada **"MAVİ"** ile işaretli olan, Firewall'dan Metro Ethernet Switch'e giden **WAN1** kablosunu çekin.

ONAY

Bu Siber Olay Müdahale Planı (SOP), Dirençli OSB'nin bilgi güvenliğini sağlamak, siber tehditlere karşı hazırlıklı olmak ve olası bir saldırı durumunda zararı minimize etmek amacıyla hazırlanmıştır.

Bu planın prosedürleri, **Kriz Yönetim Ekibi (KYE)** tarafından onaylanmış olup, siber kriz durumunda **SOME Lideri** tarafından resen uygulanır.

Hazırlayan (Plan Sahibi):	**Onaylayan (Olay Yöneticisi):**
(İmza)	*(İmza)*
Can Öztürk	**Mehmet Demirtaş**
Bilgi Teknolojileri Müdürü	Bölge Müdürü
(SOME Lideri)	(Kriz Lideri)
Tarih: **01/07/2025**	**Tarih:** 01/07/2025