



Filing Receipt

Filing Date - 2023-10-27 11:03:09 AM

Control Number - 53385

Item Number - 1623

HUSCH BLACKWELL

Dakota Parish
Associate

111 Congress Avenue
Suite 1400
Austin, TX 78701
Direct: 512.370.3318
Fax: 512.479.1101
dakota.parish@huschblackwell.com

October 27, 2023

VIA ONLINE SUBMISSION

Filing Clerk
Public Utility Commission of Texas
1701 North Congress Avenue, Suite 8-100
Austin, Texas 78701

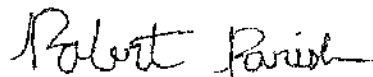
Re: Project No. 53385, *Project to Submit Emergency Operations Plans and
Related Documents Under 16 TAC § 25.53*

Dear Filing Clerk:

Please accept for filing in the above-referenced proceeding the updated Emergency Operations Plan ("EOP") for Engie Resources, LLC ("Engie"). This updated EOP replaces the EOP filed by Engie on April 18, 2022.

Sincerely,

HUSCH BLACKWELL LLP



Dakota Parish



ENGIE Resources LLC

EMERGENCY OPERATIONS PLAN

Version No. 2.0

Table of Contents

Executive Summary.....	2
Introduction	2
Reference to Specific Sections that Correspond to the Requirements	2
Affidavit.....	3
I. Approval and Implementation.....	4
1. Emergency Contacts	4
2. Revision Control.....	4
3. Record of Distribution.....	5
4. EOP Version and History	5
II. Communication Plan.....	6
III. Emergency Response Supplies.....	6
IV. Staffing During Emergencies.....	7
V. Identification of Weather-Related Hazards	7
VI. Training Drills	7
VII. Annexes.....	8
Annex A – Pandemic and Epidemic Plan.....	9
Annex B – Hurricane Plan.....	10
Annex C – Cyber Security Plan	11
Annex D – Physical Security Incident Plan	12

EXECUTIVE SUMMARY

ENGIE Resources LLC ("ENGIE") is a wholly-owned subsidiary of ENGIE North America, Inc. ("NORAM") and licensed in the State of Texas as a Retail Energy Provider ("REP").

Additionally, ENGIE is an affiliate of ENGIE Energy Marketing NA, Inc. ("EEMNA"), which has a full staff supporting wholesale power.

At this time, ENGIE is licensed as an REP and does not own any transmission, distribution or generation facilities.

The purpose of this Emergency Operations Plan ("Plan") is to ensure a stable, reliable, and robust operating environment protected from operational disruptions caused by natural or manmade hazards and/or threats and related emergencies. This Plan is submitted to the Public Utility Commission of Texas ("PUCT") and to the Electric Reliability Council of Texas ("ERCOT") in compliance with the requirements of 16 Tex. Admin. Code ("TAC") § 25.53.

Item	§ Requirement	Page No.
Description of Contents and Policies	C.1.A.i.I	2
Reference to Specific Sections in 25.53	C.1.A.i.II	2
Affidavit	c.4.C.	3
Approval and Implementation Section	d.1.	4
Emergency Contacts	c.4.B.	4
Revision Control and History	d.1.C.	4
Record of Distribution	d.1.B.	5
Communication Plan	d.2.	6
Emergency Response Supplies	d.3.	6
Staffing During Emergency Response	d.4.	7
Identification of Weather Related Hazards	d.5.	7
Training and Drills	f.	7
Annexes	e.3.	8
Pandemic and Epidemic Annex	e.3.A.	9
Hurricane Annex	e.3.B.	10
Cyber Security Annex	e.3.C.	11
Physical Security Annex	e.3.D.	12

AFFIDAVIT

STATE OF TEXAS §
 §
COUNTY OF HARRIS §

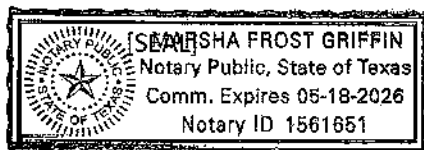
BEFORE ME, the undersigned authority, on this day personally appeared the undersigned, who, after being duly sworn, states as follows on behalf of ENGIE Resources LLC ("ENGIE"):

1. My name is GEOFFREY DUDA. I am the Vice President of Business Control for ENGIE.
2. All relevant operating personnel are familiar with and have received training on the applicable contents and execution of the EOP, and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate because of specific circumstances during the course of an emergency.
3. The EOP has been reviewed and approved by the appropriate executives of its Leadership Team.
4. Drills that test this EOP have been, or will be, conducted to the extent required by the PUCT rules.
5. The EOP or an appropriate summary has been distributed to local jurisdictions, as needed.
6. ENGIE maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident.
7. ENGIE has emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events who have received, or will receive, the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System training.
8. I further swear and affirm that all statements and representations made in this report are true and correct to the best of my knowledge.

DocuSigned by:

E00FDD0054864FF...
GEOFFREY DUDA, VP of Business Control

Sworn and subscribed before me on this 25th day of October, 2023.




ffin, Notary Public

EMERGENCY OPERATIONS PLAN

I. APPROVAL AND IMPLEMENTATION

The approval and implementation section of the EOP introduces the EOP and outlines its applicability. This EOP, including the annexes hereto, establishes ENGIE's common and operational functions relevant across emergency types and outlines ENGIE's response to specific types of emergencies. This EOP applies to ENGIE Resources LLC (REP No. 10053). The EOP also lists the emergency contacts, those individuals responsible for maintaining and implementing the EOP and those who can change the EOP. It also provides a revision control summary that lists the dates of each change made to the EOP since the initial EOP filing on April 15, 2022. It provides a dated statement that the current EOP supersedes previous EOPs, and also states the date the EOP was most recently approved by ENGIE.

1. EMERGENCY CONTACTS

ENGIE provides the below list of primary and backup contacts who can immediately address urgent requests and questions by the PUCT:

Level of Contact	Name	Title	Email	Phone
Primary	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Primary	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Primary	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Primary	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Backup	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Backup	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

2. REVISION CONTROL

Change control for the EOP is managed and owned by the Head of Operations for ENGIE. A summary of revisions and individuals responsible for maintaining, implementing, and changing the EOP is listed below.

Employee	Title	Authority
[REDACTED]	[REDACTED]	To maintain and implement EOP
[REDACTED]	[REDACTED]	To maintain and implement EOP

Employee	Title	Authority
[REDACTED]	[REDACTED]	To implement EOP
[REDACTED]	[REDACTED]	To implement EOP
[REDACTED]	[REDACTED]	To implement EOP
[REDACTED]	[REDACTED]	To modify, change, or edit EOP
[REDACTED]	[REDACTED]	To modify, change, or edit EOP
[REDACTED]	[REDACTED]	To modify, change or edit EOP

3. RECORD OF DISTRIBUTION

The following table provides the titles and names of persons in ENGIE's organization receiving access to the EOP and the dates of access and distribution of the EOP. No training has yet occurred for the current version of the EOP as training is under development. Employee training is expected to occur by March 15, 2024. The below table will be updated to reflect employee training dates as necessary.

Name	Title	Action (Distribution, Access or Training on the EOP)	Date of Distribution, Access, or Training
[REDACTED]	[REDACTED]	Access, Distribution & Training	
[REDACTED]	[REDACTED]	Access, Distribution & Training	
[REDACTED]	[REDACTED]	Access, Distribution & Training	
[REDACTED]	[REDACTED]	Access, Distribution & Training	
[REDACTED]	[REDACTED]	Access, Distribution & Training	
[REDACTED]	[REDACTED]	Access, Distribution & Training	
[REDACTED]	[REDACTED]	Access, Distribution & Training	
[REDACTED]	[REDACTED]	Access, Distribution & Training	

4. EOP VERSION AND HISTORY

The below table discloses the dates of each change made to the EOP since the initial EOP was submitted in accordance with § 25.53(c)(1), meaning April 15, 2022 or a later time as provided by the PUCT's extension of the April 15, 2022 deadline.

EOP Section	Version	Date of Change	Description of Change
Entire EOP	2.0	October 24, 2023	Update existing EOP to comply with 16 TAC 25.53 updates and personnel changes.

As of October 24, 2023, version 2.0 of the EOP (which is the current version) supersedes previous ENGIE EOPs. Version 2.0 was most recently approved by ENGIE on October 25, 2023.

II. COMMUNICATION PLAN

ENGIE will handle potentially affected stakeholders and its own operations in the event of an emergency as follows below. ENGIE may modify its approach depending on the specific facts, circumstances, and needs of the situation with the most updated information available and accessible.

Public – ENGIE will accommodate public communications through its digital/social presence and telecommunication capabilities.

Media – The media can contact ENGIE through its website, social media pages, and business phone numbers. All inquiries will be referred to NORAM’S communications and external affairs team.

Customers – ENGIE will handle customer communications through its digital/social presence, email, and telecommunication capabilities. These capabilities are all internet-based.

Commission/OPUC – The Public Utility Commission of Texas (“Commission”) and Office of Public Utility Counsel (“OPUC”) can communicate with ENGIE personnel through readily available email, internet-based video/conference calls, and phone numbers. These capabilities are all internet-based.

Complaint Handling – ENGIE operates its customer care center through readily available email, internet-based video/conference calls, and phone numbers and can also maintain all complaints handling via work-from-home, if required. ENGIE customer information is managed via a cloud-based information platform that supports remote access, if required.

III. EMERGENCY RESPONSE SUPPLIES

The facility provider for ENGIE maintains first aid equipment kits on all floors of the facility to assist in the event of a local medical emergency.

IV. STAFFING DURING EMERGENCIES

ENGIE currently maintains a disaster recovery location at a backup location that is geographically separate from the primary location and where all activities can be maintained and monitored on a 24x7 basis. The back-up location is maintained to ensure functionality and redundancy.

ENGIE'S backup location is as follows:



ENGIE utilizes an internal Business Continuity Plan group comprised of senior level staff who will initiate the mobilization of business personnel and activities when a situation arises that could render the primary location inoperable.

In the event it becomes necessary to move ENGIE from the primary to the backup location, a representative from ENGIE will notify ERCOT. ENGIE personnel will then be deployed to the backup location where all ERCOT QSE and LSE responsibilities will be managed.

ENGIE is required to submit its Business Continuity Plan ("BCP") to ERCOT on an annual basis as required by *ERCOT Operating Guides Section 3.2.1(2)*. The BCP is attached hereto.

V. IDENTIFICATION OF WEATHER-RELATED HAZARDS

ENGIE's BCP provides basic business continuity guidance applicable to all Trading teams, supporting functions and related co-located teams. Notifications of an incident (including tornadoes, hurricanes, extreme cold weather, extreme hot weather, drought, flooding, etc.) that could impact the business continuity may come from building facility management or local public emergency notification systems, managers, leadership team, or from the automated ENGIE alert system via SMS messaging. ENGIE will coordinate with NORAM to utilize this system, if needed.

VI. TRAINING/DRILLS

ENGIE will perform its 2023 drill on November 16, 2023 and annually thereafter. Prior to conducting its annual drills, ENGIE will provide advanced 30-day notice of the drill to the Commission and to the appropriate TDEM District Coordinators of the date, time, and location of the drill.

ENGIE "realtime" personnel have been assigned to either a primary or secondary role when the staff is deployed to a backup location. The primary roles are required to travel to the backup location to perform all ERCOT duties and participate in the testing during a yearly practice drill. The secondary roles remain in the primary location as the transition team when the event has ended, and the primary personnel are returning from ENGIE's backup location.

The BCP is reviewed annually by the Head of Operations and approved by the ENGIE Leadership Team.

VII. ANNEXES

ENGIE submits the following annexes as required by the rule.

Annex A

Pandemic and Epidemic

In the event of a pandemic outbreak or health event in which personal contact needs to be restricted in an effort to reduce potential human-to-human transmission, and the health and wellbeing of personnel are impacted, ENGIE may close its primary location and instruct personnel to work remotely from home. This event may also prohibit ENGIE personnel from traveling and working from the ENGIE backup locations, in which case the following exceptional circumstance procedures will apply:

- ENGIE will notify ERCOT Operations Desk via phone and email that all personnel will be working remotely from home until further notice;
- ERCOT will need to deactivate the OPX Hotline temporarily, until ENGIE personnel can return to work to the primary or backup locations;
- ENGIE will continuously maintain its 24/7 realtime phone line for all ERCOT communications; and
- ENGIE will continue to manage and perform all operational functions from remote locations.

Annex B

Hurricane Plan

ENGIE maintains procedures for emergencies, evacuations, and utility outages in coordination with the facility management personnel, in conjunction with its Business Continuity Plan attached hereto, and as referenced in Annex D herein.

Annex C

Cyber Security Plan

ENGIE maintains detailed cyber security procedures within its Business Continuity Plan attached hereto on pages 20-22. The purpose is to protect ENGIE's people and assets from a cyber threat that would disrupt ENGIE's operations.

Annex D

Physical Security Plan

ENGIE maintains procedures for emergencies, evacuations, and utility outages in coordination with the facility management personnel and in conjunction with its Business Continuity Plan. Examples of emergencies and/or threats:

- Fire;
- Safety emergencies;
- Hazardous materials spills;
- Building collapse;
- Unauthorized or disorderly persons;
- Outside incidents, such as natural disasters or gas leaks;
- Bomb threats;
- Active shooters/Hostage situations; and
- Robbery, extortion or other threats.

FIRE EMERGENCIES

If you see flames, smell smoke or see smoke, immediately call the local fire department or follow local protocol for such incidents. If the building is equipped with a fire alarm system, it can be used to alert occupants to evacuate the building. The fire alarm may also alert the emergency team members that there is an emergency in progress.

EVACUATIONS

Should an alarm occur, all staff must immediately evacuate the facility. Evacuation plans are posted at all exterior doors and conference rooms (or other predetermined locations) and should be reviewed periodically by all staff at least annually.

DO NOT use the elevator during an emergency. Help those who may need assistance.

Examples of when evacuations should occur:

- i) Danger is obvious;
- ii) The fire alarm sounds;
- iii) Directed to do so by a safety team member, human resources or company manager; or
- iv) Directed by the local fire or police departments.

UTILITY OUTAGES, SEVERE WEATHER AND EMERGENCY CLOSINGS

ENGIE will always make every attempt to be open for business. However, there will be times when emergencies such as severe weather, fires, utility outages, power failures or other declarations of weather emergency from the local government that can disrupt company operations and may require the closing

of the offices. Severe weather is defined as weather that significantly impedes the normal flow of traffic, such as snow and/or ice, flooding, rain or wind damage. Heavy rains unaccompanied by flooding or low temperatures unaccompanied by snow and/or ice do not constitute as severe weather.

Where this is a decision to close the offices during these situations, employees will receive official notification from their immediate manager and/or from ENGIE's automated alert system.

SECURITY

ENGIE strives to provide a safe and comfortable work environment for all employees and authorized visitors to its premises.

In addition to restricting unauthorized access, ENGIE takes preventative measures to keep our premises safe and secure, by using security alarms, access cards, access pin codes, sign-in sheet or systems and armed security, whenever practical, to support our safety and visitors' policies. Access cards or access pin codes (if used) are disabled upon termination of employment. Employees should take care to avoid "tailgating" by unauthorized individuals, and should report suspicious individuals or behavior to building security.

To further protect and control sensitive or confidential information access, and help prevent theft of assets, employees should take the following precautions: (i) lock up information and computers, during non-working hours; (ii) keep desks and work areas clean and clear, if they are not in active use during working hours; (iii) position computer screens whenever possible in such a way that unauthorized people cannot see information displayed onscreen; (iv) using the screen lock feature when not at their desk; and (v) taking other measures as needed to guard against unauthorized disclosure.



Business Continuity Plan

ENGIE Resources LLC


Version: 2.0

Last Updated: 10/25/2023



TABLE OF CONTENTS

I.	FOR IMMEDIATE USE.....	2
II.	PLAN OVERVIEW.....	4
	A. Purpose.....	4
	B. Objectives	4
	C. Emergency Situations	4
	D. Key Participants.....	5
	E. Plan Activation	6
	F. References and Related Documents.....	6
III.	ASSESSMENT.....	6
IV.	EMERGENCY PROCEDURES	8
	A. Emergency Contact Information.....	9
	B. Emergency Notification Plan.....	9
	C. Evacuation of Corporate Offices.....	11
	D. Migration to Alternate Site.....	11
	E. IT Disaster Recovery ("DR Plan")	16
V.	TESTING	17
	A. Overview.....	17
	B. Testing Schedule.....	17
VI.	TRAINING AND AWARENESS.....	18
	A. Training.....	18
	B. Awareness	19
VII.	MAINTENANCE AND REVISION	20
VIII.	CYBER SECURITY	20

[illegible]

Task	Status	Action Taken
[REDACTED]		
[REDACTED]		
[REDACTED]		
[REDACTED]		
Post 24 hours		
[REDACTED]		
[REDACTED]		
[REDACTED]		
Post Recovery		
[REDACTED]		
[REDACTED]		



Task	Status	Action Taken
[REDACTED]		

II. PLAN OVERVIEW

A. Purpose

[REDACTED]

B. Objectives

[REDACTED]

[REDACTED]

C. Emergency Situations

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

D. Key Participants

[REDACTED]

[REDACTED]

Role	Name(s)	Summary of Responsibilities
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Role	Name(s)	Summary of Responsibilities
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

E. Plan Activation

[REDACTED]

F. References and Related Documents

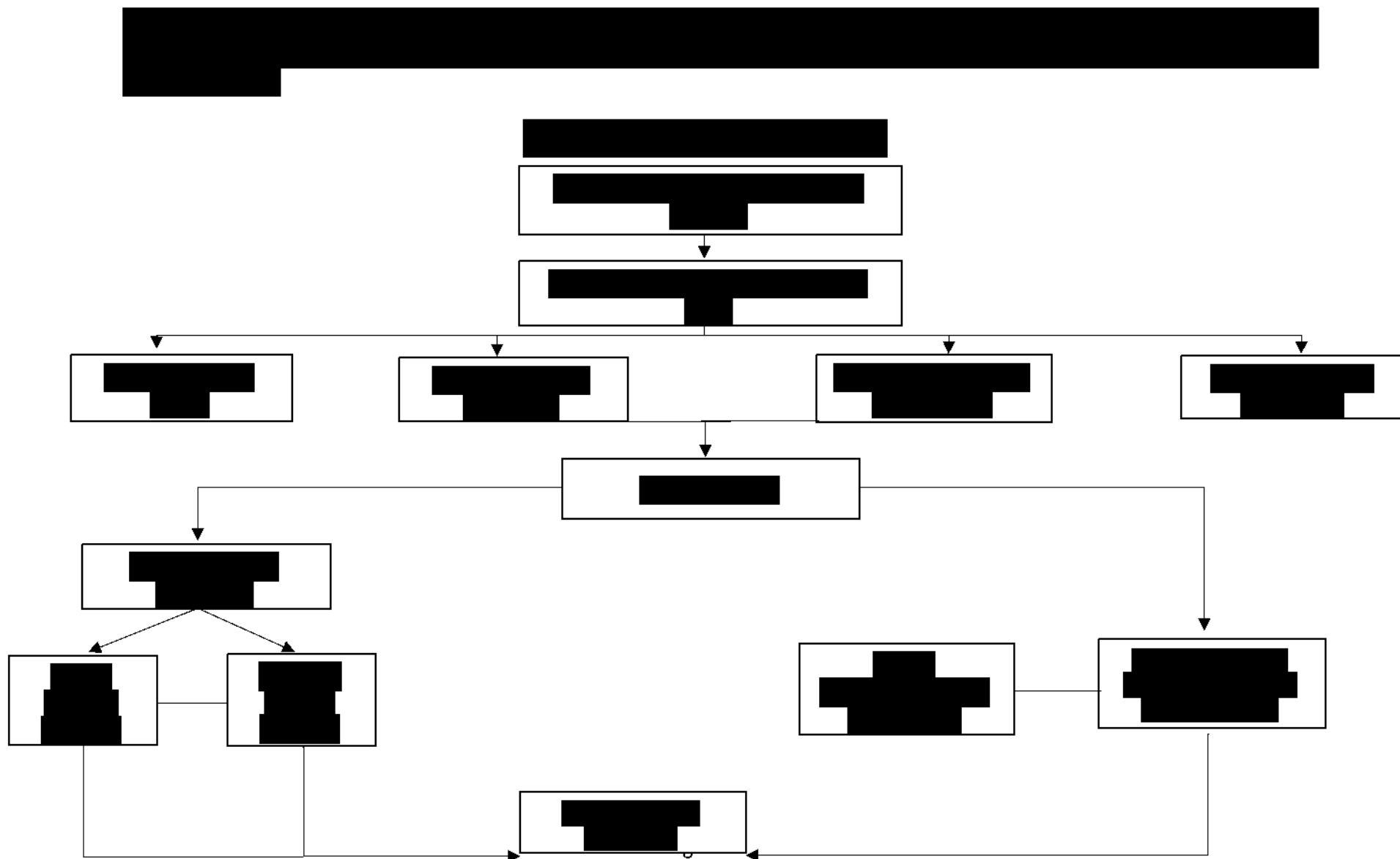
Document Name	Owner
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

III. ASSESSMENT

[REDACTED]

[illegible]

IV. EMERGENCY PROCEDURES





A. Emergency Contact Information

Organization	Contact Number
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

B. Emergency Notification Plan

[REDACTED]

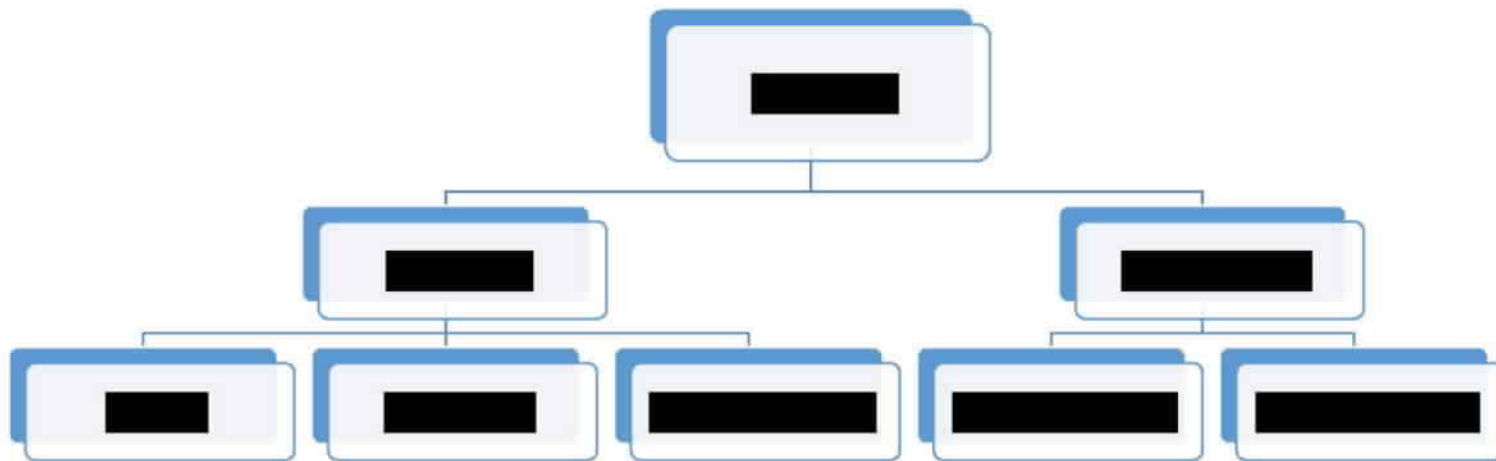
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Name	Designation	Office Phone	Mobile Phone	E-mail
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Emergency Notification System

[Redacted]



C. Evacuation of Corporate Offices

[REDACTED]

[REDACTED]

[REDACTED]

D. Migration to Alternate Site

[REDACTED]

[REDACTED]

[REDACTED]



Essential Personnel

[illegible]

[illegible]

Name	Team	Role	Backup
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

Preparations for Alternate Site (ongoing)

Task	Details	Responsible Person(s)
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Task	Details	Responsible Person(s)
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Migration to Alternate Site (in response to, or in immediate preparation for emergency event)

Task	Details	Responsible Person(s)
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Task	Details	Responsible Person(s)
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Migration back to Primary Site (after emergency event has concluded)

Task	Details	Responsible Person(s)
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

E. IT Disaster Recovery ("DR Plan")

[REDACTED]

[REDACTED]

V. TESTING

A. Overview

[REDACTED]

B. Testing Schedule

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]		[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]
[REDACTED]		[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]
[REDACTED]		[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]					[REDACTED]	

VI. TRAINING AND AWARENESS

[REDACTED]

[REDACTED]

[REDACTED]

A. Training

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

VII. MAINTENANCE AND REVISION

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

VIII. CYBER SECURITY

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

i

[REDACTED]

|

[REDACTED]

|

[REDACTED]

|

|

[REDACTED]