Filing Receipt

Received - 2022-04-18 02:31:51 PM
Control Number - 53385
ItemNumber - 336

BROAD REACH POWER

Broad Reach Power Energy Services
Emergency Operations Plan Executive Summary

Executive Summary:

As a registered REP, in the ERCOT footprint, Broad Reach Power Energy Services (BRPES) is required to develop, maintain, and utilize (when necessary) an Emergency Operations Plan, pursuant to the requirements set forth in the PUCT Rule §25.53. As such, BRPES has developed this plan to comply with the PUCT Substantive rule, as well as ensure a greater likelihood of continued operations during an emergency. This plan must be filed with the PUCT either (a) concurrently with submission of its REP application, (b) for calendar year 2022, by April 18th if it has been granted REP approval by that time (as the April 15, 2022 deadline has been extended by the Commission), or (c) beginning in 2023, annual updates to the EOP must be filed by March 15th in the circumstances outlined by § 25.53(c)(3). At all times, the most recent approved copy of the BRPES Emergency Operations Plan must be available at the main office for PUCT inspection.

For Broad Reach Power Energy Services, a REP, the PUCT has ordered the following information be included and/or addressed in the Emergency Operations Plan:

- **(d)(1)(A-D) Approval and Implementation (p. 1)** Section that:
    - Introduces the EOP and outlines its applicability;
    - Lists the individuals responsible for maintaining and implementing the EOP, and those who can change the EOP;
    - **Provides a revision control summary that lists the dates of each change made to the EOP since the initial EOP filing pursuant to** § 25.53(c)(1); and
    - **States the date the EOP was most recently approved by the REP.**
- **(d)(2)(B) Communication Plan (p. 1)** describing the procedures during an emergency for communicating with the public, media, customers, the commission, and OPUC, and the procedures for handling complaints during an emergency.
- **(d)(3) Plan for Maintenance of Pre-identified Supplies (p. 4)** for Emergency Response
- **(d)(4) Plan that Addresses Staffing (p. 5)** during Emergency Response
- **(d)(5) Plan that Addresses how the REP identifies weather-related hazards (p. 5)**, including tornadoes, hurricanes, extreme cold weather, extreme hot weather, drought, and flooding, and the process the REP follows to activate the EOP
- **(c)(4)(B) List of primary and, if possible, backup emergency contacts (p. 1)**

- **(c)(1)(A)(i)(IV) and (c)(4)(C) Affidavit** from the REP's highest-ranking representative, official, or officer with binding authority over the REP stating the following:
    - 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 as a result of specific circumstances during the course of an emergency;
    - The EOP has been reviewed and approved by the appropriate executives;
    - Drills have been conducted to the extent required by subsection (f) of the rule;
    - The EOP or an appropriate summary has been distributed to local jurisdictions as needed;
    - The entity maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident; and
    - The entity's emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events have received the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System training

- **Annexes to be included in the EOP -** A REP must include
    - **((e)(2)(D) Pandemic and epidemic annex (p. 6)**;
    - **(e)(2)(E) Hurricane annex (p. 6)** that includes evacuation and re-entry procedures if facilities are located within a hurricane evacuation zone, as defined by TDEM;
    - **(e)(2)(F) Cyber security annex (p. 6)**;
    - **(e)(2)(G) Physical security incident (p. 6)** annex; and
    - **(e)(2)(H) Any additional annexes** as needed or appropriate to the entity's particular circumstances
- Drills

As a registered REP, it is Broad Reach Power Energy Services' intent to fully comply with all drill requirements and expectations of the Public Utility Commission of Texas as outlined in § 25.53(f).

Record of Distribution:

Pursuant to § 25.53(c)(1)(A)(III) and (c)(4)(A), Broad Reach Power Energy Services will provide access to and training on the EOP during the week of April 18, 2022.

Affidavit:

Broad Reach Power Energy Services attaches the affidavit required by § 25.53(c)(1)(A)(i)(IV) and (c)(4)(C), signed by Steve Vavrik, its highest-ranking representative, official, or officer with binding authority over Broad Reach Power.

AFFIDAVIT

STATE OF TEXAS §
§
COUNTY OF HARRIS §

Before me, the undersigned notary public, on this day personally appeared Steve Vavrik, to me known to be the person whose name is subscribed to the foregoing instrument, who being duly sworn according to law, deposes and says:

"1. My name is Steve Vavrik. I am over the age of eighteen and am a resident of the State of Virginia. I am competent to testify to all the facts stated in this Affidavit, and I have the authority to make this Affidavit on behalf of Broad Reach Power Energy Services LLC ("BRPES").

2 I swear or affirm that in my capacity as President of BRPES, I have personal knowledge of the facts stated in the Emergency Operations Plan ("EOP") submitted to ERCOT and filed into Project No. 53385.

3. I further swear or affirm that I have personal knowledge of the facts stated below:

- Relevant operating personnel are familiar with and will receive training the week of April 18, 2022 on the applicable contents and execution of the EOP, and such personnel will be instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency;
- The EOP has been reviewed and approved by the appropriate executives;
- The EOP or an appropriate summary will be distributed to local jurisdictions as needed;
- BRPES maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident; and

4. BRPES intends to conduct a drill consistent with subsection (f) of PUC Subst. R. § 25.53 by June 15th, 2022, and will provide notice to the Commission at least 30 days before that drill is conducted. Once that drill is conducted, BRPES will notify the Commission.

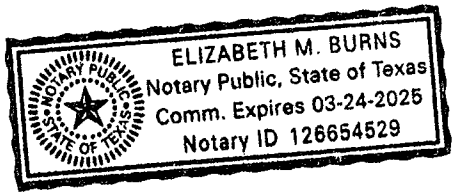
5. BRPES intends for emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events to receive the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management Systems training by June 15th, 2022. Once the training is completed, BRPES will notify the Commission.

6. I further swear or affirm the information, statements and/or representations contained in the Emergency Operations Plan are true, complete, and correct to the best of my knowledge and belief."

Further affiant sayeth not.

[Name] Steve Vaurik
[Title] President
[Entity] Broad Reach Power Energy Services LLC

SWORN TO AND SUBSCRIBED TO BEFORE ME on the 14 day of April 2022.



Notary Public in and for the
State of Texas

My Commission Expires: 03-24-2025

BROAD REACH POWER

Emergency Operations Plan

Broad Reach Power Energy Services LLC

Retail Electric Provider (REP)

Version 1.0
Effective Date: 04/18/2022

BROAD REACH POWER

Contents

BROAD REACH POWER

Approval and Implementation

This Emergency Operations Plan (EOP) is developed to help ensure Broad Reach Power Energy Services' continued Retail Electric Provider (REP) operations in the event of emergency conditions, including, but not limited to pandemic(s) or severe weather. This plan includes the necessary elements, pursuant to PUCT Rule §25.53.

The following individuals are responsible for maintaining, implementing, and revising the EOP.

Name	Title	Permission(s)
Luke Butler	Sr. Associate, Asset Management	Maintain
Mike Dubois	Manager of Real-time Operations	Implement
Luke Butler	Sr. Associate, Asset Management	Revise

Revision Control History

Version	Approval Date	Effective Date	Revision Summary
1.0	04/15/2022	04/18/2022	Initial Emergency Operations Plan

As of 04/18/2022, EOP Version 1.0, most recently approved on 04/15/2022, supersedes all previous EOPs.

Emergency Contacts

The following primary and backup emergency contacts are those who can immediately address urgent requests and questions from the Commission during an emergency:

Primary:

- Steve Vavrik, Chief Executive Officer, svavrik@broadreachpower.com, 401-497-7566
- Doug Moorehead, Chief Operating Officer, dmoorehead@broadreachpower.com, 757-328-3309

Backup:

- Narsimha Misra, Chief Commercial Officer, nmisra@broadreachpower.com, 832-458-2831

Communication Plan

During emergency operations, Broad Reach Power Energy Services (BRPES) will use the contact information provided in the table below.

Please see Attachment C, Emergency Staffing Schedule, for a list of BRPES internal contact information.

EMERGENCY OPERATIONS CONTACT LIST (EXTERNAL)		
NAME	ENTITY	PHONE NUMBER
Shift Supervisor	ERCOT	512-248-3105
QSE Agent	APX	408-878-1852
PUCT Infrastructure Staff	PUC	512-936-7197
OPUC	OPUC	512-936-7500
TNMP Real-time Operations	TNMP	281-581-4762

Additionally, BRPES will use the following procedures for communicating with the specified entities during an emergency:

- **Public**: BRPES Legal department will review and coordinate all incoming and outgoing public communications.
- **Media**: BRPES Legal department will review and coordinate all incoming and outgoing media communications.
- **Customers**: BRPES real-time operations will serve as the point of communication with customers.
- **PUCT**: The identified BRPES contacts listed in the section "Emergency Contacts" are those who can immediately address urgent requests and questions from the Commission during an emergency. If further information or review is required during this communication, the identified Emergency Contacts can request BRPES Legal department to initiate and coordinate with the appropriate departments. The BRPES Legal department will then serve as the point of contact for the remainder of that specific request.
- **OPUC**: BRPES Legal department will review and coordinate all incoming and outgoing communications to OPUC.
- **Complaints**: As an Option 2 REP, BRPES has a limited list of customers, each of which is specifically identified with contact information maintained with BRPES real-time operations. In the case of a complaint, the customer will reach out directly to BRPES. In the case of the customer experiencing an outage, the customer will first reach out to their connecting Transmission/Distribution Service Provider, followed by a call to the BRPES real-time operations desk who will have open communication with our QSE Agent (APX).

Definitions and Acronyms

TERM	ACRONYM	DEFINITION
Annex		A section of an emergency operations plan that addresses how an entity plans to respond in an emergency involving a specified type of hazard or threat.
Drill		An operations-based exercise that is a coordinated, supervised activity employed to test an entity's EOP or a portion of an entity's EOP. A drill may be used to develop or test new policies or procedures or to practice and maintain current skills.
Electric Reliability Council of Texas	ERCOT	Independent System Operator for approximately 90% of the state of Texas.
Emergency		A situation in which the known, potential consequences of a hazard or threat are sufficiently imminent and severe that an entity should take prompt action to prepare for and reduce the impact of harm that may result from the hazard or threat. The term includes an emergency declared by local, state, or federal government, or ERCOT or another reliability coordinator designated by the North American Electric Reliability Corporation and that is applicable to the entity.
Entity		An electric utility, transmission and distribution utility, PGC, municipally owned utility, electric cooperative, REP, or ERCOT.
Hazard		A natural, technological, or human-caused condition that is potentially dangerous or harmful to life, information, operations, the environment, or property, including a condition that is potentially harmful to the continuity of electric service.
Retail Electric Provider	REP	A Retail Electric Provider (REP) sells electric energy to retail customers in the areas of Texas where the sale of electricity is open to retail competition. A REP buys wholesale electricity, delivery service, and related services, prices electricity for customers, and seeks customers to buy electricity at retail.
Public Utility Commission of Texas	PUCT	The PUCT is the regulatory body for energy entities in the state of Texas.

Qualified Scheduling Entity	QSE	Submit bids and offers on behalf of resource entities (REs) or load serving entities (LSEs) such as retail electric providers (REPs).
State Operations Center	SOC	The SOC is operated by TDEM on a 24/7 basis and serves as the state warning point.
Texas Department of Energy Management	TDEM	coordinates the state emergency management program, which is intended to ensure the state and its local governments respond to and recover from emergencies and disasters and implement plans and programs to help prevent or lessen the impact of emergencies and disasters.
Threat		The intention and capability of an individual or organization to harm life, information, operations, the environment, or property, including harm to the continuity of electric service.

Purpose and Filing Requirements

As a registered REP, in the ERCOT footprint, Broad Reach Power Energy Services (BRPES) is required to develop, maintain, and utilize (when necessary) an Emergency Operations Plan, pursuant to the requirements set forth in the PUCT Rule §25.53. As such, BRPES has developed this plan to comply with the PUCT Substantive rule, as well as ensure a greater likelihood of continued operations during an emergency. This plan must be filed with the PUCT either (a) concurrently with submission of its REP application, (b) for calendar year 2022, by April 18th if it has been granted REP approval by that time (as the April 15, 2022 deadline has been extended by the Commission), or (c) beginning in 2023, annual updates to the EOP must be filed by March 15th in the circumstances outlined by § 25.53(c)(3). At all times, the most recent approved copy of the BRPES Emergency Operations Plan must be available at the main office for PUCT inspection.

Maintenance of Pre-identified Supplies for Emergency Response

In the case an emergency that requires evacuation of the Houston real-time operations control-center, BRPES maintains a “go-box” that contains additional monitors and a wireless hotspot so that control-room personnel can remotely work from anywhere in the United States. The primary contact number for BRPES control-room operations is a web-based number that only requires an internet connection, therefore communication channels with external entities is maintained. This scenario has been tested and proved effective.

Staffing During Emergency Response

Broad Reach Power Energy Services (BRPES) shall identify operational and management staff that will remain on call or on stand-by for the duration of the emergency (Attachment C). This list may be dynamic and will be subject to change should conditions warrant it.

Critical business functions are those functions and critical activities that BRPES must maintain in a continuity situation, when there has been a disruption to normal operations, in order to sustain the mission of the organization. They are the backbone of business and must be continued in order for BRPES to continue to meet its mission. Refer to Attachment E for a description of these critical business functions

Weather-related Hazard Identification and EOP Activation

Broad Reach Power Energy Services (BRPES) staff shall actively monitor all potential extreme weather events that may affect their facilities, to include severe weather and operational circumstances arising from those events. BRPES uses a variety of services that provide monitoring and alerting capabilities for extreme weather conditions on a 24/7 basis, including Accuweather Pro, Windy.com, and Stormvista. These services provide appropriate monitoring capability for tornado, hurricane, extreme hot weather, extreme cold weather, drought, and flooding conditions.

Hurricane or tropical storm. Notifications can be called when there is a probability of landfall in the ERCOT Region. ERCOT Meteorologist will provide the forecasts to supplement other Weather Service data information. ERCOT's operations support and Outage Coordination will analyze the situation and make recommendations as to Resource requirements and transmission topology.

Extreme Cold Weather. Extreme cold weather notifications can be issued when temperatures are forecasted to be 25 degrees (Fahrenheit) or below in the North Central and in the South-Central weather zones. Wind chill also has an impact on how the temperature feels due to the flow of lower temperature air. When the wind chill is forecasted to be 20 degrees or below in the North Central and in the South-Central weather zones, a notification may be issued. For such events, additional reserves may be necessary and the sequence of actions and/or notifications may vary due to system conditions or other operational issues.

Extreme Hot Weather. Extreme hot weather notifications can be issued when temperatures are forecasted to be 103 degrees (Fahrenheit) or above in the North Central and South-Central weather zones. Notifications can also be issued when temperatures are forecasted to be 94 degrees or above in the North Central and South-Central weather zones during the following

months (October-May). For such events, additional reserves may be necessary and the sequence of actions and/or notifications may vary due to system conditions or other operational issues.

Other Significant Weather Events. Significant weather events are those that do not meet the criteria of the extreme hot, extreme cold, hurricane, or tropical storm procedures. Significant weather events can consist of, but are not limited to the following:

(1) Tornadoes
(2) Strong straight-line winds
(3) Hail
(4) Severe lightning
(5) Flooding
(6) Freezing precipitation
(7) Hard freeze

Upon notification of an ERCOT declared OCN for approaching extreme weather conditions, BRPES will initiate an internal notification and briefing with those listed in the Emergency Staffing Schedule (Attachment C). The BRPES internal briefing will include a review of potential impacts and a decision on EOP activation.

Annexes Required for a Retail Electric Provider

The following annexes must be included in the Emergency Operations Plan for a Retail Electric Provider.

A pandemic and epidemic annex;

The Broad Reach Pandemic Response Plan (Attachment F) contains this information.

A hurricane annex that includes evacuation and re-entry procedures if facilities are located within a hurricane evacuation zone, as defined by TDEM;

The Broad Reach Hurricane Plan (Attachment K) contains this information.

A cyber security annex;

The Broad Reach Cyber Security Incident Response Policy (Attachment G) contains this information.

A physical security incident annex;

This section contains reporting for physical threats to any Broad Reach facility, as well as actual damage to or destruction of any Broad Reach facility, per NERC Reliability Standard EOP-004.

The DOE digital form, OE-417 shall be used to communicate physical attacks and cyber security incidents.

The Broad Reach Cyber Security Incident Response Policy (Attachment G) contains this information.

PUC Filing Requirements

An entity must file an emergency operations plan (EOP) and executive summary by April 15, 2022.

A. An entity must file with the commission:
   i. an executive summary that:
      I. describes the contents and policies contained in the EOP;
      II. includes a reference to specific sections and page numbers of the entity's EOP that correspond with the requirements of this rule;
      III. includes the record of distribution required under paragraph (4)(A) of this subsection; and
      IV. contains the affidavit required under paragraph (4)(C) of this subsection; and
   ii. a complete copy of the EOP with all confidential portions removed.

B. For an entity with operations within the ERCOT power region, the entity must submit its unredacted EOP in its entirety to ERCOT.

C. In accordance with the deadlines prescribed by paragraphs (1) and (3) of this subsection, an entity must file with the commission the following documents:
   i. A record of distribution that contains the following information in table format:
      I. titles and names of persons in the entity's organization receiving access to and training on the EOP; and
      II. dates of access to or training on the EOP, as appropriate.
   ii. A list of primary and, if possible, backup emergency contacts for the entity, including identification of specific individuals who can immediately address urgent requests and questions from the commission during an emergency.
   iii. An affidavit from the entity's highest-ranking representative, official, or officer with binding authority over the entity affirming the following:
      I. 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 as a result of specific circumstances during the course of an emergency;
      II. the EOP has been reviewed and approved by the appropriate executives;

III. drills have been conducted to the extent required by subsection (f) of this section;
IV. the EOP or an appropriate summary has been distributed to local jurisdictions as needed;
V. the entity maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident; and
VI. the entity's emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events have received the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System training.

Annual Review

An entity must continuously maintain its EOP. Beginning in 2023, an entity must annually update information included in its EOP no later than March 15 under the following circumstances:

A. An entity that in the previous calendar year made a change to its EOP that materially affects how the entity would respond to an emergency must:
    a. file with the commission an executive summary that:
        i. describes the changes to the contents or policies contained in the EOP;
        ii. includes an updated reference to specific sections and page numbers of the entity's EOP that correspond with the requirements of this rule;
        iii. includes the record of distribution required under paragraph (4)(A) of this subsection; and
        iv. contains the affidavit required under paragraph (4)(C) of this section;
    b. file with the commission a complete, revised copy of the EOP with all confidential portions removed; and
    c. submit to ERCOT its revised unredacted EOP in its entirety if the entity operates within the ERCOT power region.
B. An entity that in the previous calendar year did not make a change to its EOP that materially affects how the entity would respond to an emergency must file with the commission:
    a. a pleading that documents any changes to the list of emergency contacts as provided under paragraph (4)(B) of this subsection;
    b. an attestation from the entity's highest-ranking representative, official, or officer with binding authority over the entity stating the entity did not make a change to its EOP that materially affects how the entity would respond to an emergency; and
    c. the affidavit described under paragraph (4)(C) of this subsection.

Annual Drill

An entity must conduct or participate in at least one drill each calendar year to test its EOP. Following an annual drill, the entity must assess the effectiveness of its emergency response and revise its EOP as needed. If the entity operates in a hurricane evacuation zone as defined by TDEM, at least one of the annual drills must include a test of its hurricane annex. An entity conducting an annual drill must, at least 30 days prior to the date of at least one drill each calendar year, notify commission staff, using the method and form prescribed by commission staff on the commission's website, and the appropriate TDEM District Coordinators, by email or other written form, of the date, time, and location of the drill. An entity that has activated its EOP in response to an emergency is not required, under this subsection, to conduct or participate in a drill in the calendar year in which the EOP was activated.

By applying the Emergency Operations Drill Instructions and completing Attachment B, Broad Reach Energy Services (BRPES) Emergency Operations Plan shall be tested each year, no later than February 15th, and includes a review section, to identify and correct any vulnerabilities in the Emergency Operations Plan. Broad Reach Energy Services (BRPES) Emergency Operations Drill Procedure has a section dedicated to any facility that is located within a defined hurricane evacuation zone.

Broad Reach, as a registered RE, shall provide ERCOT with any updated versions of their emergency operations plan by **June 1** *for any updates made between November 1 and April 30*, and by **December 1** *for any updates made between May 1 through October 31*. Broad Reach shall submit all updated plans electronically.

ATTACHMENT B - EMERGENCY OPERATIONS DRILL
Section 2.2.1

BROAD REACH POWER

ACTION ITEM	NAME	TASK	COMPLETE	DATE	NOTES
1					

VULNERABILITIES AND ISSUES IDENTIFIED & CORRECTIVE ACTIONS

ACTION ITEM	NAME	CORRECTIVE ACTION TASK	COMPLETE	DATE	NOTES
1					

ATTACHMENT C - EMERGENCY STAFFING SCHEDULE

BROAD REACH POWER

NAME	LOCATION	CONTACT INFORMATION	DUTIES
Mike Dubois	Houston - Remote Office	412-527-1780	Real-time Operations and Dispatching
Carlis Miller	Houston - Field Services	832-287-0029	Field Services
Gabriel Roy Liguori	Houston - Remote Office	617-633-2080	Asset Management
Cody Morgan	Houston - Remote Office	325-829-7309	IT
Casey Kopp	Houston - Remote Office	585-748-9378	Trading
Guillaume Dufay	Houston - Remote Office	346-561-4123	Asset Management
Doug Moorehead	Houston - Remote Office	757-328-3309	Asset Management
Ashley Waggoner	Houston - Remote Office	785-979-1544	Human Resources
Sally Shaw	Houston - Remote Office	713-962-3719	Legal

Broad Reach Power Company Critical Business Function			
Critical Business Function 1: Monitoring and Dispatching Assets			
Business Process To Complete: Monitor and dispatch assets to meet market obligations			
Supporting Elements			
Supporting Activities (Describe)	**Lead POC** **Alternate**	**Vendors and External Contacts**	**Maximum Allowed Down Time** **Criticality**
Monitor and dispatch	**Manager, Real-time Operations**	**APX (QSE Agent)**	**0**
	Associate, Real-time Operations		**High**
Communication with TDSPs and ERCOT	**Manager, Real-time Operations**	**APX (QSE Agent)**	**0**
	Associate, Real-time Operations		**High**
Internal Communication	**Manager, Real-time Operations**	**N/A**	**0**
	Associate, Real-time Operations		**High**
Implications if not Conducted: Interruption and/or loss of this function would disrupt ability to control assets and meet market obligations. This could lead to compliance and market penalities.			
Calendar Dependent: This function is always occurring.			
Required Resources: Staff, equipment, supplies, Information Technology, and other resources. Broad Reach maintains a "go-box" that contains additional monitors and a wireless hotspot so that control-room personnel can remotely work from anywhere in the United States. This scenario has been tested and proved effective.			
Facilities: This function can be completed through a work-from-home setting with a standard office space with traditional office equipment and space for phones, computers, scanners, printers, etc., with network access to Internet.			

Broad Reach Power Company Critical Business Function			
Critical Business Function 2: Trading			
Business Process To Complete: Submit Day-Ahead Market bids			
Supporting Elements			
Supporting Activities (Describe)	**Lead POC** **Alternate**	**Vendors and External Contacts**	**Maximum Allowed Down Time** **Criticality**
Daily Bid Submission	**Manager, Trading**	**APX (QSE Agent)**	**1**
	Associate, Trading		**Med**
Implications if not Conducted: Interruption and/or loss of this function would disrupt ability to submit Day-Ahead Market bids and receive awards.			
Calendar Dependent: This function is always occurring.			
Required Resources: Staff, equipment, supplies, Information Technology, and other resources.			
Facilities: This function can be completed through a work-from-home setting with a standard office space with traditional office equipment and space for phones, computers, scanners, printers, etc., with network access to Internet.			

Broad Reach Power Company Critical Business Function
Critical Business Function 3: Information Technology
Business Process To Complete: Maintain and troubleshoot network connectivity for all critical business functions

Supporting Elements			
Supporting Activities (Describe)	**Lead POC**	**Vendors and External Contacts**	**Maximum Allowed Down Time**
	Alternate		**Criticality**
Network Maintenance Troubleshooting	**Director, Critical Asset Operations**	**Triumphus**	**0**
	Associate, Network and Cyber Security		**High**
Implications if not Conducted: Interruption and/or loss of this function would disrupt ability for all critical business functions.			
Calendar Dependent: This function is always occurring.			
Required Resources: Staff, equipment, supplies, Information Technology, and other resources.			
Facilities: This function can be completed through a work-from-home setting with a standard office space with traditional office equipment and space for phones, co			

BROAD REACH POWER

Pandemic Response Plan

Broad Reach Power Energy Services LLC

Retail Electric Provider (REP)

Version 1.0
Effective Date: 04/18/2022

BROAD REACH POWER

Contents

BROAD REACH POWER

Executive Summary and Approval

Introduction:

In light of recent responses to pandemics and epidemics, Broad Reach Power Energy Services (BRPES) has developed this plan (PRP) to address the subject of business continuity, in the face of a widespread medical event, such as a pandemic or an epidemic. This Plan provides a framework, guidance, and concept of operations to support BRPES's efforts to continue and/or rapidly restore critical business functions in the event of a disruption to normal operations. This plan includes an overview of continuity operations, outlines the approach for BRPES's critical business functions, and defines the roles and responsibilities of staff. It also outlines the orders of succession, notification procedures and communication methods, plan activation and deactivation protocols, provisions for alternate work locations, and the plan for maintaining and restoring access to vital records.

This plan establishes procedures and processes to maintain operational continuity for businesses based on the loss of services due to a reduction in workforce (e.g., during pandemic influenza).

The following individuals are responsible for maintaining, implementing, and revising the PRP.

Name	Title	Permission(s)
Luke Butler	Sr. Associate, Asset Management	Maintain
Mike Dubois	Manager of Real-time Operations	Implement
Luke Butler	Sr. Associate, Asset Management	Revise

Version	Approval Date	Effective Date	Revision Summary
1.0	04/15/2022	04/18/2022	Initial Pandemic and Epidemic Response Plan

As of 04/18/2022, PRP Version 1.0, approved on 04/15/2022, supersedes all previous PRPs.

BROAD REACH POWER

Introduction

Overview:

Continuity of Operations planning ensures Broad Reach Power Energy Service (BRPES) is able to continue or quickly resume performing critical business functions, which are the functions that support the organization's mission, comply with legal requirements, and support life-safety, under all circumstances, to the extent possible. The benefit of this planning includes the ability to anticipate response actions following a pandemic or epidemic and ensure timely recovery.

Plan Scope & Applicability:

The BRPES Pandemic Response Plan (PRP) is applicable once the safety of employees, customers, and guests has been verified. It can be active during normal business hours and after hours, with and without warning.

Plan Objectives:

The objective of the BRPES PRP is to facilitate the resumption of critical operations and functions in a timely and organized manner to ensure a viable and stable organization. In doing this it is critical to ensure the safety and well-being of employees, customers, and guests. The primary objectives of the plan are to:

- Maintain Critical Business Functions during the pandemic or epidemic
- Adjust business functions to address staffing issues
- Ensure employees are able to perform work remotely, where applicable and appropriate

Plan Assumptions:

The following assumptions were used while creating this plan:

- An event has occurred that affects normal business operations.
- Access to BRPES facilities may be limited.
- Qualified personnel are available to continue operations.

Critical Business Functions

Overview:

Critical business functions are those functions and critical activities that Broad Reach Power Energy Services (BRPES) must maintain in a continuity situation, when there has been a disruption to normal operations, in order to sustain the mission of the organization, comply with legal requirements and support life-safety. They are the backbone of business and must be continued in order for BRPES to continue to meet its mission. Refer to **Attachment E of the BRPES-EOP-1 Emergency Operations Plan, Critical Business Functions**, for a description of these critical business functions

Identification of Staff Required to Continue Business Operations:
In the event of a pandemic or epidemic, work absences, due to medical issues attributed to the widespread medical event, can lead to dramatic decreases in productivity, potentially leading to the shutdown of facilities. To maintain the best possible operational posture, it is imperative to communicate duties to the appropriate personnel, helping to ensure BRPES's facilities can remain operational to the greatest extent possible. In many cases, employees may log in remotely and perform their duties, fostering as much of an illness-free atmosphere possible, however, there will be the need for onsite staff to maintain and operate facilities, leading to the identification of mission essential staff and reporting structures. BRPES senior management will identify those mission essential individuals and will communicate tasks to them. As each case may differ, there will be no "One-size-fits-all" approach, and each response to a pandemic or epidemic will require its own set of responsible personnel and tasks. It is imperative that all possible measures are taken to keep BRPES staff from contracting or spreading the illness. Maintaining social distancing, where appropriate and possible, wearing proper PPE, and maintaining hygienic work and living spaces is crucial to combatting a widespread medical event. Depending on the nature of the event, the measures below may serve to facilitate the continued operations of BRPES facilities:

- Wearing of PPE
  - Masks
  - Social distancing
  - Proper hygiene
  - Eye, face, or other protection (as applicable)
- Remote work, where appropriate and possible
- Encourage the use of approved medications and/or vaccine(s)

Plan Activation Procedures

Plan Activation During Normal Business Hours:
If it is determined that the facility cannot be re-inhabited, the Business Owner or designee will inform personnel on next steps. Employees may be instructed to go home to await further instructions or move to an alternate site. Further communications, such as instructions on where and when to report for work will be made using communication methods such as email, phone calls, texts, or other communication methods.

Plan Activation Outside Normal Business Hours:
If an event occurs outside normal business hours that renders a facility uninhabitable, the Business Owner or designee will activate the PRP using email, phone calls, texts, or other communication methods.

Actions upon Activation:
Upon activation of the PRP, the Business Owner or designee will be responsible for notifying all affected personnel of their duties and where they will be performing those duties (remotely or at a site).

Plan Deactivation Procedures

Overview:
PRP deactivation is the process of demobilizing the alternate facility and restoring critical business functions to the primary facility or a new facility that will permanently replace the damaged facility. Plan deactivation may not consist of an exact replacement of lost facilities, equipment or processes. The goal of plan deactivation is to reestablish full capability in the most efficient manner. In some continuity incidents, extensive coordination may be necessary to backfill staff, procure a new operating facility, and re-establish vital records. When it is determined the PRP activation has ended, all personnel should be informed that the necessity for continuity operations no longer exists and the return to normal operations will begin.

Criteria for PRP Deactivation:
The business owner or designee will determine, based on input from medical authorities, staff, or other entities when it is safe and when the organization is prepared to restore or transfer critical business functions to a facility for long term usage. Critical business functions must be restored in priority sequence based upon the classification and criticality of the function. The following elements are typically completed prior to plan deactivation.

- Purchase and acquire equipment, supplies and travel arrangements needed for the resumption effort.
- Temporarily suspend non-critical functions, as necessary, to support the resumption efforts.
- As applicable, utilize other personnel, such as contract personnel, to support the resumption efforts.

Table 1 details the restoration process that must be completed during plan deactivation.

Table 1

Item	Function	Supplies	Required Resources
1	Monitor current CDC guidelines for indication of safe plan deactivation	N/A	HR in coordination with senior leadership will monitor CDC guidelines to determine when it is safe to restore critical business functions to standard operating locations.
2	Purchase and acquire equipment, supplies and travel arrangements needed for the resumption effort	Medical supplies, such as face coverings, hand washing stations, as well as proper arrangement of office seating to meet CDC guidelines for social distancing.	HR in coordination with senior leadership
3	Conduct return to normal operations briefing	N/A	HR coordinate and present briefing on return-to-work procedures with all employees
4	Continue to monitor CDC guidelines and adherence to latest revisions	N/A	HR in coordination with senior leadership will continue to monitor CDC guidelines and adjust procedures as needed.

Document Type: Policy
Broad Reach Power Cyber Security Incident Response Policy

Version Control			
Version #	Date	Content	Justification
1.0	2021-10-22	Initial Version	n/a

Prepared by:	Reviewed by:	Reviewed by:	Approved by:
Cody Morgan	Doug Moorehead	Sally Shaw	Steve Vavrik
Cody Morgan (Jan 4, 2022 10:16 CST)	W. Doug Moorehead (Jan 4, 2022 11:18 EST)	Sally Shaw (Jan 4, 2022 10:21 CST)	
Title: Director, Critical Asset Operations Dpt.: Asset Management Date: Jan 4, 2022	Title: Chief Technology Officer Dpt.: Engineering Date: Jan 4, 2022	Title: Executive Vice President Legal & General Counsel Dpt.: Legal, Regulatory, Compliance & Policy Date: Jan 4, 2022	Title: Chief Executive Officer Dpt.: Executive Date: Jan 4, 2022

Table of Contents

1 Purpose

This policy defines Cyber Security Incident Responses for Broad Reach Power (BRP) and the entities governed by the NERC CIP Standards for Low-Risk ESS's.

BRP is committed to developing and maintaining a Cyber Security Incident response plan and to reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Any act or event that could be considered a Cyber Security Incident will be evaluated and reported as appropriate, in accordance with the steps outlined below.

2 Scope of Application

This policy applies to all BRP personnel (including contractors and service vendors) with authorized cyber or authorized unescorted physical access to covered Cyber Assets.

3 Definitions & Acronyms

- Roles and Definitions can be found in the BRP Master Definitions List.
- The use of any defined term will be capitalized.

4 Areas Involved

While no groups within BRP are exempt from this policy, the following groups have specific responsibilities and/or need to be familiar with the policy:

- Director of Information Technology
- IT Operations Manager
- IT Security Engineer
- Operation Center Manager
- SCADA Manager
- Help Desk
- Cyber Security Incident Response Team
- Cyber Security Senior Manager or Delegate

5 Compliance Requirements

5.1 Cyber Security Incident Response Plan

BRP shall develop, implement and maintain a Cyber Security Incident response plan in response to Cyber Security Incidents. This policy, along with the BRP Cyber Security Incident Response Procedure, serves as the BRP Cyber Security Incident Response Plan as called for by the NERC Cyber Security Standards for Low-Risk ESS's.

5.2 Cyber Security Incident Response Team

A Cyber Security Incident Response Team (CSIRT), comprised of the following members, will handle response to Cyber Security Incidents:

- Director of Information Technology (Lead)
  - Declares Cyber Security Incident as reportable to ES-ISAC
- IT Operations Manager
  - Notifies CSIRT of Cyber Security Incident
- IT Security Engineers
  - Primary technical advisor to the IT Operations Manager
  - Monitors systems and networks
  - Evaluates logs and other data and technical information to investigate the security incident
  - In an emergency situation may act to minimize damage to BRP systems before communicating with the IT Operations Manager
- CIP Senior Manager or Delegate
  - Perform oversight activities
  - Manage scheduling of periodic reviews
  - Schedule the annual test of the Cyber Security Incident Response Plan
- Sr. Manager, OPCENTER
  - Determine impact of the incident with regard to real-time system operations
  - Coordinate OPCENTER actions to minimize the impact to essential OPCENTER processes and applications

- SCADA Manager
  - Determine impact of the incident on OPCENTER applications and report to the Sr. Manager, OPCENTER

5.3 Discover

All BRP personnel will contact the Help Desk immediately if they suspect a cyber security incident.

5.4 Characterize, Classify, Resolve

CSIRT will use the ES-ISAC Reporting Cross Reference Matrix in Attachment A to determine the type and severity of an incident and whether or not the incident must be categorized as an ES-ISAC reportable incident. Each Cyber Security Incident will be categorized as either being a reportable incident or not.

Notification of the ES-ISAC, if needed, will be performed by the Director of Information Technology. The steps for doing so are specified in the BRP Cyber Security Incident Response Procedure.

5.5 Document

Cyber Security Incidents will be documented. Evidence will be preserved and protected per the BRP Cyber Security Incident Response Procedure. Documentation related to a defined reportable incident will be maintained for three calendar years. Non-reportable incident documentation will be maintained per the BRP Cyber Security Incident Response Procedure.

5.6 Review and Testing

The BRP Cyber Security Incident Response Policy and the BRP Cyber Security Incident Response Procedure will be reviewed annually. The policy, procedure and workflow will be tested annually. This test can take the form of a paper drill, tabletop exercise or full operational exercise and is to be scheduled by the CIP Senior Manager or delegate. This review and testing is detailed in the BRP Cyber Incident Response Annual Review and Testing Procedure.

In addition, the components of the Cyber Security Incident Response Plan will be updated and communicated to all CSIRT members within thirty (30) days of any changes, whether those changes are the result of an incident, a test or review.

Updates to the plan will be stored on a share point site to be identified later. All CSIRT members will be notified by email of the updates, and each CSIRT member will demonstrate that the member has reviewed the changes in the update.

6 Training Requirements

BRP will provide periodic training to new and existing personnel on their regulatory responsibilities. Training for the Cyber Security Incident Response Plan will be provided to the members of the CSIRT and to the document owners for the pieces of the plan. Additional training will be provided to response personnel as needs for capabilities as they are identified.

7 References

7.1 NERC CIP-008-4 – Cyber Security – Incident Reporting and Response Planning

7.2 BRP Cyber Security Incident Response Procedure

7.3 BRP Cyber Incident Response Annual Review and Testing Procedure

8 Attachments

8.1 Attachment A: ES-ISAC Reporting Cross Reference Matrix

Attachment A – ES-ISAC Reporting Cross-Reference Matrix

This cross-reference is provided for convenience. It is not intended to be inclusive.

Source: Appendix A from ES-ISAC's Threat and cyber security incident Reporting Guideline

Category	Sub-Category	Event Definition	Consider Reporting When:	Report Within:	Cross-Reference to Reporting Requirements
SABOTAGE/ TAMPERING/ VANDALISM (STV) – Physical or Cyber	Security Breaches:				
	Physical Perimeter Compromise	Unauthorized access of a person or a device through, circumventing, or damaging the physical perimeter, or security systems protecting the physical perimeter.	Unauthorized physical access to facilities, systems, or equipment (such as critical assets or critical cyber assets) that could impact the reliable operation of the bulk electric system; or, intentional damage to security systems that protect the physical perimeter.	1 hour of detection	
	Cyber Perimeter Compromise	Unauthorized ingress or egress through the electronic perimeter or into an electronic perimeter device.	Unauthorized electronic access to cyber assets whose impairment could impact the reliability of the	1 hour of detection	
	Information Theft or Loss	Unauthorized removal or loss of sensitive information.	Sensitive information, such as that required to be protected pursuant to NERC Standard CIP-003 is lost or is removed without authorization.	48 hours of detection	ES-ISAC
	Unauthorized Modification	Unauthorized addition or modification of software or data associated with the proper operation of cyber assets.	Malicious software or data modification is discovered on a cyber-asset or assets that may impact the reliability of the bulk power system.	4 hours of detection	DHS ES-ISAC
	Suspected Activities:				
	Attempted Physical Intrusion	A detected effort to gain unauthorized access of a person or a device through the physical perimeter but without obvious success.	Attempt to gain unauthorized physical access to facilities, systems, or equipment (such as critical assets or critical cyber assets) that could impact the reliable operation of the bulk power system is targeted, focused, or repetitive.	6 hours upon detection	
	Attempted Cyber Intrusion	A detected effort to gain unauthorized ingress or egress through the electronic perimeter or into an electronic perimeter device but without obvious success.	Attempt to gain unauthorized electronic access to cyber assets (such as critical cyber assets) whose impairment could impact bulk power system reliability is targeted, focused, or repetitive.	6 hours upon detection	
	Surveillance Activities – Intelligence Gathering:				

Social Engineering	The attempt by an unauthorized person to manipulate people into performing actions or divulging information.	Suspected or actual instance occurs.	8 hours of recognition	DHS ES-ISAC
Photography	Taking still or moving pictures.	A suspicious cyber security incident occurs.	8 hours	DHS ES-ISAC
Observation	Showing unusual interest in a facility; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility.	Activity is suspicious or unauthorized.	8 hours	DHS ES-ISAC
Flyover	Flying an aircraft over a facility; this includes any type of flying vehicle including an unmanned aerial vehicle (UAV) loitering over a site.	A suspicious or unauthorized cyber security incident occurs.	8 hours	DHS ES-ISAC
Threats:				
Expressed Threat	Communicating a threat.	Threatened action has the potential to damage or compromise a facility or personnel.	1 hour	DHS ES-ISAC
Weapons Discovery	Discovery of explosives.	Discovery occurs at or near a facility.	1 hour	ES-ISAC
Attacks:				
Actual Attack (Physical or Cyber or Communication)	Attack via physical, cyber, or communications means.	An actual attack against generation, transmission, or company-owned or operated communication facilities, cyber assets, or personnel occurs.	1 hour	
Attempted Attack (Physical or Cyber or Communication)	Attack via physical, cyber, or communications means.	A suspected attack against generation, transmission, or company-owned or operated communication facilities, cyber assets, or personnel occurs.	6 hours	

BROAD REACH POWER

Hurricane Response Plan

Broad Reach Power Energy Services LLC

Retail Electric Provider (REP)

Version 1.0
Effective Date: 04/18/2022

In the event of a hurricane, the first priority is always the health and safety of BROAD REACH POWER ENERGY SERVICES personnel. BROAD REACH POWER ENERGY SERVICES's hurricane response process is listed below:

- Ensure all BROAD REACH POWER ENERGY SERVICES personnel and any potentially affected public personnel are not in danger.
- By using the evacuation routes in the link below, BROAD REACH POWER ENERGY SERVICES personnel must evacuate at a time recommended by local authorities.

BROAD REACH POWER ENERGY SERVICES facilities in Region 1, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

BROAD REACH POWER ENERGY SERVICES facilities in Region 2, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

BROAD REACH POWER ENERGY SERVICES facilities in Region 3, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

BROAD REACH POWER ENERGY SERVICES facilities in Region 4, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

BROAD REACH POWER ENERGY SERVICES facilities in Region 5, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

BROAD REACH POWER ENERGY SERVICES facilities in Region 6, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

Checklist(s) for personnel to address emergency events

BROAD REACH POWER ENERGY SERVICES shall use the checklist in Annex C to identify which personnel shall address events that arise during the emergency.

In the event that the entry route is obstructed or compromised, ensure proper PPE is worn and utilized and normal safety measures are employed.

Always ensure communication is maintained between Broad Reach Energy Services personnel attempting re-entry and Broad Reach Power Energy Services leadership.

The following individuals are responsible for maintaining, implementing, and revising the PRP.

BROAD REACH POWER

Name	Title	Permission(s)
Luke Butler	Sr. Associate, Asset Management	Maintain
Mike Dubois	Manager of Real-time Operations	Implement
Luke Butler	Sr. Associate, Asset Management	Revise

Version	Approval Date	Effective Date	Revision Summary
1.0	04/15/2022	04/18/2022	Initial Hurricane Plan

As of 04/18/2022, annexes associated with EOP Version 1.0, approved on 04/15/2022, supersede all previous EOP annexes.