Filing Receipt

Filing Date - 2024-04-19 09:33:44 AM

Control Number - 53385

Item Number - 2429

docVerify

0_PPM-STD-EOP Affidavit_1.pdf

DocVerify ID:	320FE54D-AB2A-42ED-B5C0-54D5ACC8C1E0
Created:	April 19, 2024 06:57:34 -8:00
Pages:	1
Remote Notary:	Yes / State: TX

This document is a DocVerify VeriVaulted protected version of the document named above. It was created by a notary or on the behalf of a notary, and it is also a DocVerify E-Sign document, which means this document was created for the purposes of Electronic Signatures and/or Electronic Notary. Tampered or altered documents can be easily verified and validated with the DocVerify veriCheck system. This remote online notarization involved the use of communication technology.

Go to www.docverify.com at any time to verify or validate the authenticity and integrity of this or any other DocVerify VeriVaulted document.

E-Signature Summary

E-Signature 1: Robert Dowd (RD)
April 19, 2024 07:09:42 -8:00 [200CE03EB881] [172.124.74.85]
robertdowd@bkv-bpp.com (Principal) (Personally Known)

E-Signature Notary: SANDY FELONE JOHNSON (sfj)
April 19, 2024 07:09:42 -8:00 [0927836EF5E9] [97.77.183.141]
sandyfelone@gmail.com
I, SANDY FELONE JOHNSON, did witness the participants named above electronically sign this document.

2. Affidavit

STATE OF ___TEXAS_____§

COUNTY OF ___BELL _____§

BEFORE ME, the undersigned authority, on this day personally appeared the undersigned, who, after being duly sworn, stated on their oath that they are entitled to make this Affidavit, and that the statements contained below and in the foregoing are true and correct.

I swear or affirm that the attached report was prepared under my direction, and that I have the authority to submit this report on behalf of the reporting party. I further swear or affirm that all statements made in the report are true, correct and complete and that any substantial changes in such information will be provided to the Public Utility Commission of Texas in a timely manner.

Robert Dowd

Signature of Authorized Representative

Robert Dowd

Printed Name

Name of Reporting Party

Sworn and subscribed before me this _____ day of 04/19/2024, _____.

Month Year

Sandy Felone Johnson
Commission # 129085130
Notary Public
STATE OF TEXAS
My Comm Exp. Jan 26, 2026

Notarial act performed by audio-visual communication

Notary Public in and for the State of _____

Emergency Operations Plan ("EOP")

Executive Summary

TABLE OF CONTENTS

EOP SECTIONS

1. Purpose

1.1 Priority Power Management, on behalf of BKV-BPP Ponder Solar, has developed this Emergency Operations Plan in accordance with TAC Rule §25.53 Electric Service Emergency Operations Plans, describing the actions to be taken by the organization in response to emergency scenarios outlined by this plan. This Emergency Operations Plan and its associated subsections will be used in conjunction with other facility specific procedures when responding to these emergencies. It also sets forth the specific actions to be taken by staff and support personnel during an emergency.

1.2 BKV-BPP Ponder Solar LLC Facility Location:

1.2.1 GPS Coordinates: 33.0920.30 N, 97.1516.67 W, 911 Address: 4285 Florance Road, Ponder TX 76259

2. Affidavit

STATE OF _____§

COUNTY OF _____§

BEFORE ME, the undersigned authority, on this day personally appeared the undersigned, who, after being duly sworn, stated on their oath that they are entitled to make this Affidavit, and that the statements contained below and in the foregoing are true and correct.

I swear or affirm that the attached report was prepared under my direction, and that I have the authority to submit this report on behalf of the reporting party. I further swear or affirm that all statements made in the report are true, correct and complete and that any substantial changes in such information will be provided to the Public Utility Commission of Texas in a timely manner.

_____

Signature of Authorized Representative

_____

Printed Name

_____

Name of Reporting Party

Sworn and subscribed before me this _____ day of _____, _____.

Month Year

_____

Notary Public in and for the State of _____

3. Record of Distribution

Copies of this Emergency Operations Plan have been copied to the following internal and external entities:

- Priority Power Management (PPM) Team
- BKV-BPP JV Corporate Leadership Team
- Public Utility Commission of Texas (PUCT)
- Electric Reliability Council of Texas (ERCOT)

Name	Job Title
Robert Dowd	Managing Director
Sean Hausman	Vice President of Operations
William Petersen	Regulatory Compliance Manager
Rick Bory	Priority Power Management
Todd Nickens	Priority Power Management
Kirsten Wood	Priority Power Management

PriorityPower

Emergency Response Overview

Contents

Emergency Response Protocol

1.1 If an Emergency Operations Plan event occurs the following response organization shall be implemented:

	Initial	Subsequent (If Required)
Emergency Coordinator	Network Operations Center (NOC) Operator	Site Emergency Manager (SEM)
Communications	Network Operations Center Operator	Operations Manager (with EHS Manager assistance)

1.2 Typical Operations Shift staffing consists of: The NOC and Operations Team will evaluate any immediate impacts to the facility and add additional in-house and/or contract staffing as required for event response.

1.3 The NOC Operator is responsible for initiating the immediate response action(s) and ensuring the facility remains in safe condition. If the NOC Operator is unable to initiate an immediate response a designated employee will act on behalf of the NOC Operator until one is available to relieve them.

1.4 During an emergency event, the NOC Operator immediately assumes the duties of the SEM, Site Emergency Manager until a member of the Operations Team is onsite.

1.5 The NOC Operator or designee shall:

1.5.1 Take necessary actions to stabilize operations if affected.

1.5.2 Evaluate operational & physical impact to the facility.

1.5.3 Request emergency services if required.

1.5.4 Notify Operations Manager and Team

1.5.5 Take the necessary corrective action to restore systems if the facility has been impacted.

1.6 General Response

1.6.1 Refer to specific applicable Emergency Operations Plan sections to guide emergency response actions.

1.6.2 Notify site personnel of facility event and any safety concerns that may exist.

1.6.3 NOC initiates phone calls for necessary off-site notification.

1.6.4 All other on-site personnel will monitor communications and support the appropriate response as directed by the SEM.

1.7 Emergency Response Plan Staffing Plan

1.7.1 Priority Power **(PPM)** will evaluate the staffing needs of the Emergency Event and will determine the appropriate staffing needs to manage the response, including the following:

- Notifying additional PPM Staff and employees to respond to the site to support the response.
- Procuring contracted support companies to support the response with additional resources and equipment as required.

1.7.2 There shall be continuous and unobstructed way of exit travel from any point at the facility for active means of egress.

1.7.3 Exits will be marked with an exit sign and illuminated by a reliable light source.

1.7.4 Areas will have directions to exits when not immediately apparent with visible signage.

1.7.5 Areas that are not meant as an exit will be clearly marked "NOT AN EXIT".

1.7.6 All exit signs will be provided with the word "EXIT" in letters at least 5 inches high and ½ inches wide.

1.7.7 All exit doors must be side-hinged and kept free of obstructions.

1.7.8 There must be at least (2) means of egress provided.

1.7.9 There must be sufficient exits to permit escape in case of emergency.

1.8 Emergency Response Supplies

1.8.1 PPM maintains inventory of supplies for response to all reasonable events that have the probability to occur to support O&M personnel needs. PPM maintains inventory of spare parts and consumables to support maintenance and replacement of critical facility equipment to minimize the impact.

1.8.2 All exit doors will operate in the direction of exit travel without use of a key or any special knowledge or effort.

1.8.3 All exit doors opening directly onto an alley or other areas where vehicles may be operated will have adequate barriers and warnings to prevent employees from stepping into the line of traffic.

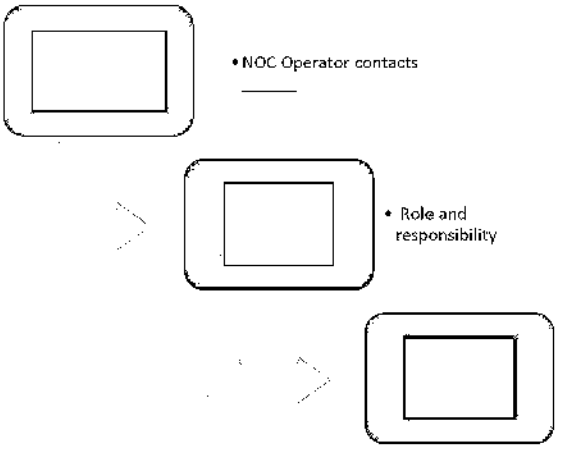
1.8.4 Exterior exit access ways must be kept clear of snow and ice to allow for egress.

1.9 Recovery

1.9.1 Upon conclusion of an Emergency Response Event the NOC and Operations Staff will give the approval and direction to restore facility operations to restore generation capability as allowed through communication with the qualified scheduling entity.

Communications Plan

2.1 Upon activation of the EOP due to an event covered under this plan, the active NOC Operator will notify the Operations Team of the event. The chain of command is as follows:



2.2 The PPM Operations Team with the assistance of the EHS Manager and Legal will manage all communications with outside regulatory entities as appropriate including the news media and public inquiries. A spokesperson shall be appointed by the leadership at the time of the event. This PPM spokesperson will handle immediate media inquiries.

2.3 The NOC Operator will make appropriate communications to ERCOT via documented email and or CoServ (Transmission Operator) if facility status has been immediately impacted by the event.

2.4 Any written communications in response to inquiries from outside entities should be routed and reviewed by the appropriate members of the Corporate Leadership Team and Legal. All other employees shall not respond to outside inquires.

PriorityPower

Emergency Contacts

Contents

Emergency Contacts

Directions to Texas Health Presbyterian Hospital (from site) Head north on Florance Rd toward Seaborn Rd (1.4 mi), Turn right onto FM2449 E (5.1 mi), Turn right to merge onto I-35W N (3.3 mi), Take exit 85B to merge onto I-35 Frontage Rd (0.5 mi), Turn Right, Destination will be on the left.
CALL 911: Give emergency responders your location OR location of the emergency and provide a call back number
YOU ARE HERE: 4285 Florance Road, Ponder TX 76259
HOSPITALS
Texas Health Presbyterian Hospital [13 miles]: 3000 I-35 Denton, TX 76201 (940) 898-7000 I Trauma Center
Occupational Health Solutions [38 miles]: 4775 S. FWY at Felix Fort Worth, TX 76115 (817) 921-2500
AIR FLIGHT
Call 800-600-9015 and XstremeMD will coordinate an air flight.
EMERGENCY CONTACTS
Ponder Fire Dept.: 102 E Bailey St. Ponder, TX 76259 (940) 479-2488, (call 911 if emergency/fire)
Denton County Sheriff: 127 N Woodrow Lane Denton, TX 76205 (940) 349-1600 (call 911 if emergency)
Texas Poison Control: (800) 222-1222
SAFETY CONTACTS

PPM EHS Manager	Kirsten Wood	432-305-5959
PPM Medical Manager	XstremeMD	800-600-9015
PPM NOC	Available 24/7	855-776-6621
BKV EHS	Richard Miller	817-757-0765

Accident/ Incident Protocol

1. Find A Safe Place: And contact your supervisor. If your supervisor is not available, contact another employee or the NOC. DO NOT REMAIN ALONE. If Fire or Hazardous Release call 911 and provide location.
2. Call Safety: With your supervisor or with assistance from the NOC Operator, Priority Power's EHS Manager shall be notified.
3. Medical Manager: With EHS Manager, you will contact Medical Management service to coordinate care if necessary.
4. Life Threatening: If the situation is life threatening (loss of limb, eye or unconsciousness) contact 911 First, then medical management service. If help cannot be reached in time contact Air Flight or transport the person to nearest medical facility.
5. Safety Must be Notified: Notify EHS of incident and investigation will take place. DO NOT resume work until the site has been deemed safe and approved by EHS and the Operations Team.
6. All incidents must be reported to PPM and BKV-BPP. All workplace injuries/ illnesses must be coordinated using medical management services.

PriorityPower

Weather Emergencies

Contents

Introduction

1.1 Priority Power (PPM) utilizes **Windy.com** and other reputable news stations to initiate warnings.

1.2 When the facility receives a Tornado Alert, all steps applicable to this procedure are to be entered into the Network Operations Center (NOC) control logbook by the NOC Operator.

Lightning

2.1 The NOC operator will monitor radar for lightening strikes.

2.2 If a lightning strike is observed within a 10-mile radius, a Microsoft Teams Message alert is sent to PPM technicians.

2.3 Monitoring may be discontinued once all alerts/ warnings have been terminated or expired and not further threats are imminent.

Tornadoes

3.1 If a Tornado Watch is issued for the facility, a Microsoft Teams Message alert is sent to the PPM technicians:

"A Tornado Watch has been issued for the area. Anyone in the area is instructed to proceed to ground level. Ground work is permitted but limited to storm preparation and basic maintenance activities."

3.1.1 Repeat the message above.

3.1.2 Any personnel, contractors, and visitors working above ground level will proceed immediately to the ground level.

3.1.3 Once personnel are at ground level they will begin readiness work for a potential storm.

3.2 If a Tornado Warning is issued for the facility, a Microsoft Teams Message alert is sent to the PPM technicians:

"A Tornado Warning has been issued for the area. Anyone in the area is instructed to secure all portable equipment and proceed immediately to a safe area and await further instructions."

3.2.1 Repeat the message above.

3.2.2 All personnel, contractors, and visitors will secure portable equipment and proceed to a safe area. All personnel, contractors and visitors must be mustered and accounted for by the NOC.

3.2.3 The NOC operator shall notify the Operations Manager and the Qualified Scheduling Entity and Transmission/Distribution Service Provider that a Tornado Warning has been issued for the site and proceed with actions as directed by those sources.

3.3 If a Tornado is spotted or the facility receives a notification that a tornado is likely, a Microsoft Teams Message alert is sent to PPM technicians:

"A tornado is approaching the facility. Take cover immediately. The site is being evacuated."

3.3.1 A phone call will additionally be made to all PPM technicians immediately following the Teams message.

3.3.2 Repeat the Teams announcement above.

3.3.3 Leave the facility in its current configuration.

3.3.4 Onsite personnel will collect communications devices and proceed immediately to a storm shelter.

3.3.5 The NOC Operator will notify the Qualified Scheduling Entity and Transmission/Distribution Service Provider that the control room has been evacuated and provide an update on the configuration of the facility.

3.3.6 No personnel shall leave the shelter areas without "All Clear" from the NOC.

3.4 Once the storm has cleared, the following shall be performed:

3.4.1 The NOC Operator will notify all personnel, contractors and visitors it is safe to leave shelter. It may be necessary to perform this action at each shelter if communication systems are not available.

3.4.2 A muster shall be performed to account for all personnel that were onsite. Any missing person must be located. Medical emergencies shall be managed in accordance with PPM's Medical Management Plan.

3.4.3 Plant personnel will survey the site to assess damage, exercising extreme caution while navigating the area. Verbal updates will be provided to the NOC Operator as conditions are evaluated.

3.4.4 Any damage found will be documented and evaluated prior to return of service. Spills, fires and any other damage shall be addressed and followed per PPM's ERP and BCP Plan.

3.4.5 The NOC Operator with the Operations Team shall update the BKV-BPP Corporate Leadership Team on plant status and site condition.

3.4.6 The Operations Team with the communication coordination of the NOC will initiate cleanup efforts and system restoration shall be performed in accordance with facility procedures.

Winter Storms

4.1 If forecasted temperatures are expected to be less than 20 degrees F at any point or forecasted to be below freezing for more than 24 hours, the NOC will discuss with the Operations Team a plan to prepare for cold weather operations.

4.2 For long duration forecasted winter events, evaluate the necessity of site or local housing and food accommodations for PPM Technicians and make arrangements as necessary.

4.3 Evaluations should be made to determine if additional winterization shall be implemented. Evaluations at minimum shall include:

4.3.1 Insulation and lagging integrity

4.3.2 Water leaking or piping systems

4.3.3 Verify all instrument sensing lines are adequately covered with insulation and heat tracing.

4.3.4 Determine if additional temporary or permanent wind breaks are required to protect critical equipment or instrumentation.

4.4 Supplies utilized in response to an event should be staged in strategic locations to expedite response times from personnel and reduce risk of travel.

4.5 Electrical heat trace should be verified to be in proper working order prior to event. (Not Applicable for Solar Facilities)

4.6 During snow and ice storms, attention should be paid to snow and ice accumulation around equipment, doorways, buildings and tanks. Consider blocking pathways in areas where ice can accumulate.

4.7 Evaluate walkways for ice accumulation. Remove as necessary for access. If ice is forecasted, consider pre-salting.

4.8 Tracker Motor and Drivelines visual inspection and confirm operation after storm ends. Solar modules visual inspection for damage and if necessary drone thermal infrared scan)

Heavy Winds

5.1 During periods of heavy winds, caution should be exercised. Outside activities shall be suspended and personnel shall avoid being in the highest elevation onsite.

5.2 Ensure there are no loose materials exposed that could cause hazard to personnel or equipment.

5.3 Place overhead cranes in storage position and lock in place.

5.4 During periods of high winds it will be necessary to monitor Tracker tilt angle

Flooding

6.1 The site should be monitored for rising water.

6.2 No personnel should enter or cross suspected high water level areas.

6.3 Any equipment exposed to rising water shall be shut down prior to water immersion. The NOC shall notify a PPM Technician if equipment shutdown shall be initiated.

6.4 All personnel shall proceed to high ground and stay out of flood waters.

Hail

7.1 If hail is forecasted for the facility: verify tracker is tilted 52 degrees to the east(away from prevailing winds) and NOC operator shall confirm angle.

Extreme Heat

8.1 Prior to extreme heat events, inspections shall be performed on temperature control units on location.

8.2 Evaluations of critical equipment shall be made to determine if additional measures can or should be taken to minimize the effects of extreme heat exposure.

8.3 Temporary cooling equipment will be made available in convenient locations to expedite the response to an extreme heat event.

8.4 Evaluations shall be made to determine if additional staffing resources are needed during extreme heat to allow for frequent breaks and schedule adjustments.

8.5 All maintenance activities will be evaluated to determine potential risks to operability during extreme heat conditions and will be deferred to off peak hours or following the extreme heat incident if warranted depending on the severity of the event, all maintenance activities may be limited to emergent work only.

8.6 Screen equipment deficiencies for potential impact and prioritize their resolution as required to ensure reliable operation.

8.7 The NOC Operator shall monitor operations during extreme heat to identify and communicate weaknesses. Items will be logged to create work orders for resolution.

PriorityPower

Hurricane

Hurricane Procedure

1.1 The BKV-BPP Ponder Facility is located in Denton County, Texas and is not located in a designated evacuation zone as outlined by the Texas Division of Emergency Management. Based on this location, a Hurricane Procedure is not applicable to this facility.

1.2 Any weather impacts experienced on location from a hurricane that makes landfall on the gulf is covered under Section 3 (weather) of this Emergency Operations Plan (EOP).

PriorityPower

Restoration of Service

Priorities for Recovery of Generation Capacity

1.1 The BKV-BPP Ponder Solar facility is registered as a Generation Resource.

1.2 If the Generation Resource has experienced a reduction of generating capability due to a "Failed Start" or "Generator Trip" attributable to a Hazard or Threat, an investigation will be initiated to determine the direct cause of the failure. An assessment will be completed to determine if the initiating Hazard or Threat can be mitigated or eliminated to allow a return to service without further risk to plant equipment and capability.

1.3 During this investigation and recovery phase the Operations Team will provide updates to ERCOT through the Qualified Scheduling Entity on assessment findings and estimated return to service.

1.4 The Plant Management team will initiate the appropriate response actions to perform any necessary corrective actions to restore generation capability of the plant.

1.5 Once the threat or hazard that caused impact to the generating capability of the plant has passed or has been mitigated to reduce the risk to reliable operation of the facility, the SEM and the Solar Management Staff will determine if any corrective action is necessary. Once any required corrective actions have been completed the Plant Management Team will request a return to service via the Qualified Scheduling Entity and attempt to restore the full generation capability of the facility.

PriorityPower

Pandemic Plan

Contents

Pandemic Plan

A roster of employees volunteering for pandemic duty will be posted if Phase Two of the Priority Power (PPM) Pandemic Plan is initiated.

PPM will attempt to staff the Pandemic Team with volunteers. If there are not enough volunteers, the operators and technicians scheduled to work the shifts (that are not replaced with volunteers) will be expected to stay through operations.

Purpose

The Pandemic Operations Plan has been developed to assure that the facility and support staff to the facility are prepared in the event a Pandemic should threaten PPM Operations and the Denton County area.

This procedure provides information and outlines steps to protect personnel and is a guideline to follow. The Pandemic Operations Plan is split into three phases.

Three stages of Preparation:

1. **Stage One:** Threat of Pandemic – prepare for subsequent stages.
2. **Stage Two:** Threat to facility and operations due to infection elevation – essential personnel onsite only
3. **Stage Three**: Facility Lockdown – Personnel remain in place

2.1 Stage One

- Confirm VPN access for NOC Operators and technicians.
- Purchase disinfectant products, hand sanitizer and other disinfectants.
- Hire a professional cleaning service that specializes in pandemic cleanup and agree upon a schedule for cleaning.
- Implement a program to ensure surfaces and equipment are disinfected after use.
- Ensure adequate food and sleeping accommodations are available to cover Stage 3
    - If supply chain is threatened confirm there is adequate supply until resources can be ordered again (food, bottled water, breads etc).
    - Cots, air mattresses, blankets, pillows, linens, restrooms
- Develop lists of Essential Personnel and what their duties will be
- Only perform maintenance required to keep the facility operational
    - Minimize contractor access to Essential Personnel and notify non-essential personnel that their service shall be discontinued until further notice.
    - Monitor any personnel onsite for symptoms, and request anyone exhibiting symptoms to leave site immediately and contact Medical Management Services.

2.1 Stage Two

- Stage Two will be declared after careful consideration by the Operations Lead, Human Resources and PPM's EHS Manager.

    - Notification of Level 2 will be sent via Microsoft Teams and email to all affected employees.
- Only Essential Personnel will be onsite.
- Onsite Safety requirements:
    - Personnel will don a facemask whenever working with another person
    - Complete virus threat/exposure checklist with anyone onsite
    - Maintain approach distances whenever possible
        - Per the Center for Disease Control (CDC), maintain a least 6 feet from other people.
        - If 6 foot distancing is not possible, don a facemask
- Institute a 4-6 hour schedule for sanitizing surfaces and equipment in the work area.
- Emphasize and provide training to all personnel on the importance of hand washing for at least 20 seconds, If soap/water is not available, use a hand sanitizer that contains at least 60% alcohol.
- Request anyone exhibiting symptoms to notify leadership and leave site immediately.
- Management to conduct daily meetings to discuss the current events of the pandemic and update executive leadership as needed.

2.3 Stage Three

- A stage three will be declared after careful consideration by the Operations Lead, Human Resources and PPM's EHS Manager.
    - Notification of Level 3 will be sent via Microsoft Teams and email to all affected employees.
- Employees should be prepared for potential lockdown.
- Restrict access to facility to only essential personnel. All other employees shall work from home.
- Continue Stage Two cleaning process
- Continue Stage Two daily meetings

Duties and Responsibilities

Responsibilities during a Pandemic will follow normal operations. Exceptions to normal operations are detailed below:

3.1 Employees:

- Report to work as scheduled until Stage 3 of this plan is declared and implemented.
- Any affected employee or employee that has had reasonable exposure to an affected person should continue to stay home until they are cleared by a medical professional.

3.2 Operations Management

- Direct onsite activities
- Initiate processes of this plan as necessary with the assistance of Human Resources and EHS Manager.
- Release all non-essential personnel to work remotely where appropriate.

Pandemic Lockdown Crew

Name	Responsibility	Alternate

Exposure Checklist (Questionnaire)

During Stages Two and Three employees and personnel shall be required to complete this checklist/ questionnaire prior to being physically onsite.

Name: _____ ☐PPM Employee ☐Contractor ☐Other: _____

Date: _____ **Location:** _____

Duration at Location: _____

In the past (48) hours have you experienced the following symptoms:

☐Fever or chills

☐Cough

☐Shortness of breath or difficulty breathing

☐Fatigue

☐Muscle or Body aches

☐Headache

☐New loss of taste or smell

☐Sore throat

☐Congestion or runny nose (not related to allergy)

☐Nausea or vomiting

☐Diarrhea

If any of the boxes above are checked, further screening shall take place prior to being allowed onsite.

PriorityPower

Cyber Security Incident

Contents

Purpose

1.1 This plan addresses the actions and reporting procedures to be followed by BKV-BPP Ponder Solar, LLC in the event of a Cyber Security Incident. This Plan ensures that an incident response plan is in place to detect and mitigate incidents and restore identified Bulk Electric System Cyber Systems (BCS) computing services.

Scope

2.1 This plan applies to all BKV-BPP Ponder Solar, LLC employees, contract, and vendor personnel responsible for the operation, protection and maintenance of Bulk Electric System Cyber Systems (BCS) that support Bulk Electric Systems, including those having authorized cyber or authorized unescorted physical access to BCSs.

Definitions and Defined Terms

3.1 Cyber Security Incident: A malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Cyber Security Incident: A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

NERC Glossary of Terms can be accessed by clicking the following link:
https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Cyber Security Incident Response Procedure (Identification)

4.1 Upon discovery of a potential Cyber Security Incident, immediately notify the On-Shift Operator. The On-Shift Operator shall then contact the Shift Supervisor, who will alert the CIP Sr. Manager and work with the organization's technical support staff or vendor to determine if there is a Cyber Security Incident or other issue affecting the system.

4.2 A Cyber Security Incident (CSI) is defined as a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, disrupts or was an attempt to disrupt, the operation of a BES Cyber System. The following conditions may indicate a CSI has occurred:

a. Routine systems monitoring detects a known or potential incident such as:

i. Endpoint Protection alerts

ii. Intrusion Detection System (IDS) alerts

iii. Security Information and Event Management (SIEM) alerts

iv. Policies changed (firewall, Group Policy Object (GPO), etc.)

v. System hardening settings changed

vi. Physical Security Perimeter breach

b. Unexplainable behavior of a BCS and/or BES Cyber Assets (BCAs) within a BCS.

c. Unexplainable loss of BCA or BCS functionality

d. Notification of a potential CSI by an external entity, including law enforcement, CERT or E-ISAC.

e. Notification of a potential CSI by an employee, contractor, or vendor.

Cyber Security Incident Response Procedure (Assessment and Clarification)

5.1 Record the following information as applicable in the initial assessment and investigation on RCP-NERC-CIP-003-ATT-G. Please note that the following list is not exhaustive:

a. When, how, and by whom was the event reported (from Section 3.A)?

b. What system functionality is affected?

c. Are generation or transmission assets affected?

d. How many BCAs and/or BCSs are possibly affected?

e. Indicate results of log(s) examination on all access and monitoring devices and suspect systems.

f. Was unauthorized electronic and/or physical access gained?

g. Was there a compromise or disruption of one or more of reliability tasks? Reliability tasks are listed in Attachment B and defined in NERC Standard CIP-002-5.1a.

Based on the assessment above, the CSIRT shall classify the event as a Reportable CSI if the CSI has compromised or disrupted one or more reliability tasks of BKV-BPP Ponder Solar, LLC.

If the CSI is determined to be Reportable (also review EOP-004 & DOE reporting requirements), then proceed to Section D, Communication Protocol, and initiate the reporting process, then return to Section C. Some incident types have a limited reporting window starting (within 1 hour) from when the CSI was determined to be reportable.

If the event is determined not to be a Reportable CSI, continue to document the investigation on the RCP-NERC-CIP-003-ATT-G, retain that form and any other evidence, and skip Section D.

Cyber Security Incident Response Procedure (Response and Incident Handling)

6.1 The incident response process will be initiated when there is an event that requires further investigation. The CIP Senior Manager, Delegate(s) or assigned Incident Coordinator will assemble the CSIRT, initiate measures to contain the incident, implement measures to eradicate the threat and determine whether the incident is resolved or to implement device recovery.

6.1.2 Containment

Containment must be performed at the earliest possible stage to avoid cascading incidents. If the threat is internal from a compromised system or device, the device should be isolated from the network to reduce the threat to unaffected systems. If the threat is external such as an attempt to access the low impact physical security

area or electronic security area, steps should be taken to sever or block the external accessibility to the extent possible.

Prevent future electronic or physical access that could cause additional damage.

Engage internal and external support resources as needed.

If the event involved physical access to a PSP or system, investigate how access was obtained.

Reassess damage and capabilities of impacted systems per Section B.

Engage local law enforcement as required. Phone numbers can be found in procedure RCP-NERC-EOP-004-3-ATT-A.

6.1.3 Evidence Collection and Documentation

Document the identification, assessment and/or actions taken in response to the event. Examples may include any of the following:

Dated Documentation

Security Logs

Police Reports

Emails

Checklists

Forensic Analysis Results

Restoration Records

Post-Incident Review Notes

OE-417 Form

Document any deviations from the plan taken during the response.

6.1.4 Data Preservation

Collection of information from the target system should be conducted in accordance with the appropriate forensic practices, where possible. Other relevant data that may correlate with the evidence of unauthorized access, including intrusion detection alerts and firewall logs, should be collected. Collected evidence should be securely stored.

Preserve records of electronic and physical access to the cyber assets

Data on disk drives of cyber assets shall be copied, mirrored, or replaced prior to recovering the asset where possible.

Configuration files of firmware based cyber assets shall be saved to a secure location.

Eyewitness accounts shall be documented.

Restoration of the BES and the safety of employees, contractors, and the public will take priority over the preservation of CSI data preservation.

Record chain of custody of all evidence collected.

6.1.5 Eradication, Recovery and Resolution

Successful attackers frequently install root kits, which modify or replace system binaries and other files. Root kits hide much of what they do, making it tricky to identify what was changed.

If an attacker appears to have gained root access to a system:

a. Restore the system from a known good backup or reinstall the operating system and applications

b. Change all passwords on the system, and possibly on all systems that have trust relationships with the victim system.

If an attacker only gains a lesser level of access than administrator-level, eradication and recovery actions should be based on the extent to which the attacker gained access.

Cyber Security Incident Response Procedure (Communication Protocol)

7.1 Initial Identification Notification – Immediately upon detection of a possible CSI, notify the CIP Senior Manager or Delegate(s). Notifications may originate from any of the personnel listed in the CSIRT roles that receives alerts from applicable sources, including any employee or vendor who is entrusted with the responsibility of safeguarding the physical and/or cyber security of Temple Generation I's CIP-related Cyber Assets.

Vendor Support - If required, the CSIRT is responsible for initiating vendor support services. Such communication may be appropriate to enable a deeper investigation of the incident or resumption of services.

Required Reporting

7.1.1 E-ISAC & DOE

(1) Reporting an incident to DOE and E-ISAC is time sensitive, in some cases within one hour of determining a Reportable CSI. Reporting should be done using the Department of Energy OE-417 form. The form and instructions are found at the link below. The report can be submitted online directly to DOE and E-ISAC with a copy being emailed back to the originator (for documentation and forwarding to additional reporting recipients, if necessary). If emailing the form, apply encryption if necessary.

http://www.nerc.com/pa/CI/ESISAC/Pages/Report-an-Incident.aspx

7.1.2 Ongoing communication with DOE and E-ISAC will be coordinated through the CIP Sr. Manager or Delegate.

Texas RE

The CIP Senior Manager or Delegate(s) will submit or direct submission of the same DOE Form OE-417, to the Regional Entity via email as required.

b. Electric Reliability Council of Texas, Inc., Electric Reliability Council of Texas, Inc. and ERCOT / ONCOR

Operating personnel on duty will make notifications to the other parties in the interchange via phone or email as directed by the CIP Sr. Manager

PriorityPower

Physical Security

Contents

Purpose

The purpose of this procedure is to describe the plan for responding to physical security events at the BKV-BPP facility. This plan will outline detecting and reacting to physical security incidents, determine their scope and risk and to respond appropriately and quickly, and communicating to appropriate stakeholders.

Scope

This plan applies to all Priority Power (PPM) employees, contractors, clients and visitors of the facility. This plan does not entail cybersecurity or data breaches. See Section (7) for detailed Cybersecurity information.

Definitions

At Priority Power, an incident is an event that is unfavorable and violates the policies, standards and Code of Conduct of the Company, regulations or law, or threatens the safety and well-being of PPM employees, contractors or visitors. This also includes damage to company assets.

Examples of incidents:

- Unauthorized breach of BKV-BPP Facility property, fence, gates, etc.
- Workplace accidents and injuries
- Health and Safety Incidents
- Environmental Incidents
- Near Misses
- Physical security breach (i.e. break-in)
- Workplace Violence
- Bomb Threat

Restricting Physical Access

4.1 PPM has defined operational and procedural controls to restrict physical access to the facility.

4.1.1 Security fencing with gates and locks

4.1.2 Fence Lines and entry ways are under 24/7 video camera surveillance

4.1.3 PPM's Network Operating Centers are equipped with a card reading system limiting access to only authorized PPM employees only.

Roles & Responsibilities

5.1 Employees are responsible for:

5.1.1 Abiding by PPM's safety and security policies and procedures

5.1.2 Reporting incidents in accordance with safety and security policies and procedures

5.1.3 Attending scheduled training by PPM

5.2 Managers are responsible for:

5.2.1 Promoting a safe work environment

5.2.2 Taking reasonable measure to protect their employees

5.2.3 Providing and updating employees on PPM's safety and security policies

5.2.4 Assisting in incident investigations

5.2.5 Reporting incidents in accordance with PPM's safety policies and procedures

5.3 The Emergency Response Team is responsible for:

5.3.1 Notifying employees of potential risks

5.3.2 Monitoring the implementation of this incident response plan

5.3.3 Conducting and leading risk assessments and root cause analysis

5.3.4 Initiating the assistance of subject matter experts

5.3.5 Conducting interviews

5.3.6 Leading employee training on this plan as well as provide updates on safety and security issues in the workplace

5.3.7 Review this response plan on an annual basis

5.3.8 Respond to all incidents where immediate assistance is required, taking steps to mitigate immediate risks and notify emergency services where required.

5.3.9 Liasing with law enforcement agencies and participating in legal processes

Incident Response Stages and Procedure

6.1 Stage One: Preparation

6.1.1 Develop and review policies and procedures

6.1.2 Train employees on the plan

6.2 Stage Two: Detection

6.2.1 Discover Incident through tips or reports

6.2.2 Discover incident using security tools (video) or other detection

6.2.3 Complete incident reporting as required

6.3 Stage Three: Containment

6.3.1 Identify, isolate/ mitigate risks associated with the incident

6.3.2 Notify affected personnel

6.3.3 Decide if investigation is necessary

6.3.4 Preserve physical and or digital evidence

6.4 Stage Four: Investigation

6.4.1 Determine the incidents impact on the organization/ facility, scope and root cause

6.4.2 Collect physical and digital evidence

6.4.3 Conduct interviews with everyone involved

6.5 Stage Five: Remediation

6.5.1 Communicate with Insurance

6.5.2 Repair affected assets

6.5.3 Communicate to and instruct all involved/ affected personnel of next steps

6.5.4 Confirm the threat has been contained and is no longer imminent

6.5.5 File formal reports per regulatory requirements

6.5.6 Create Post-Incident Report and schedule after-action review meeting with affected personnel and leadership

6.6 Stage Six: Recovery

6.6.1 Analyze the events of the incident of its procedural and policy implications

6.6.2 Gather metrics

6.6.3 Review and edit established policies and procedures following items discovered in the after-action review

PriorityPower

Water Shortage

Purpose

1.1 The purpose of this procedure is to provide guidance on actions to be taken in the event of a raw water supply interruption that could impact the generation capability of the BKV-BPP Ponder Solar facility.

Action

2.2 BKV-BPP Ponder Solar Facility will not be affected (NOT APPLICABLE)

2.3 Note: The only water onsite would be external water used for module cleaning which would be about 20,000 gallons brought to site in a truck

PriorityPower

EOP Compliance Requirements

Contents

Purpose

1.1 The purpose of this section is to provide guidance to maintaining compliance with Texas Administrative Code Rule §25.53 Electric Service Emergency Operations Plans, including but not limited to, the requirements for reviews and updates, training, drills, and affidavits.

Review and Updates

2.1 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:

2.1.1 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 file with the PUCT and executive summary that describes the changes to the contents or policies contained in the EOP.

2.1.2 includes an updated reference to specific sections and page numbers of the entity's EOP that correspond with the requirements of Rule §25.53 Electric Service Emergency Operations Plans

2.1.3 includes the record of distribution required under Rule §25.53 Electric Service Emergency Operations Plans

2.1.4 contains the affidavit required under Rule §25.53 Electric Service Emergency Operations Plans

2.1.5 file with the PUCT a complete, revised copy of the EOP with all confidential portions removed.

2.1.6 submit to ERCOT its revised unredacted EOP in its entirety if the entity operates within the ERCOT power region.

2.2 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 PUCT:

2.2.1 a pleading that documents any changes to the list of emergency contacts as provided under Rule §25.53 Electric Service Emergency Operations Plans

2.2.2 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.

2.2.3 the affidavit required by Rule §25.53 Electric Service Emergency Operations Plans

2.3 An Entity must update its EOP, or other documents required if PUCT staff determines that the entity's EOP or other documents do not contain sufficient information to determine whether the entity can provide adequate electric service through and emergency. If directed by PUCT staff, the entity must file its revised EOP or other documentation, or a portion thereof, with the PUCT and, for entities with operations in the ERCOT power region, with ERCOT.

Record of Distribution

3.1 A record of distribution contains the following information in table format:

3.2 titles and names of persons in the entity's organization receiving access to and training on the EOP

3.3 dates of access to or training on the EOP, as appropriate.

Emergency Contacts

4.1 An entity must file with the PUCT a list of primary and, if possible, backup emergency contacts for the entity, including identification of specific individuals who can immediately address urgent request and questions from the PUCT during an emergency.

Affidavits

5.1 An affidavit must be signed by the highest-ranking representative, official, or officer with binding authority affirming that the items in 25.53(c)(4)(C) are met.

5.2 The affidavit must affirm the following:

5.2.1 relevant operating personnel are familiar with and have received training on the applicable contents and execution of the EOP.

5.2.2 personnel have been 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.

5.2.3 the EOP has been reviewed and approved by the appropriate executives.

5.2.4 Drills have been conducted to the extent required by Rule §25.53 Electric Service Emergency Operations Plans

5.2.5 the EOP or an appropriate summary has been distributed to local jurisdictions as needed

5.2.6 the entity maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident

5.2.7 the entity's emergency management personnel who are designated to interact with local, state, and federal emergency management official during emergency events have received the lates IS-100, IS-200, IS-700, and IS-800 National Incident Management System training.

Drills

6.1 An entity must conduct or participate in at least one drill each calendar year to test its EOP.

6.2 Following an annual drill, the entity must assess the effectiveness of its emergency response and revise its EOP as needed.

6.3 An entity conducting an Annual Drill must, at least 30 days prior to the date of at least one drill each calendar year, notify PUCT staff, using the method and form prescribed by PUCT staff on the PUCT website, by email or other written form, of the date, time, and location of the drill.

6.4 An entity that has activated its EOP in response to an emergency is not required, under Rule §25.53 Electric Service Emergency Operations Plans, to conduct or participate in a drill in the calendar year in which the EOP was activated.

Reporting

7.1 Upon request by PUCT staff during an activation of the State Operations Center by TDEM, an affected entity must provide updates on the status of operations, outages, and restoration efforts.

7.2 Updates must continue until all incident related outages of customers able to take service are restored or unless otherwise notified by PUCT staff.

7.3 After an emergency, commission staff may require an affected entity to provide an after action or lessons learned report and file it with the commission by a date specified by commission staff.

Training

8.1 Relevant operating personnel must receive training on the applicable contents and execution of the EOP and subsections.

8.2 An entity's emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events must have received the latest IS-100, IS-200, IS-700, IS-800 National Incident Management System training.

Revision History

Rev.	Date	Description	By Initials	Approval Initials
0	04/18/2024	Rev. 0 for compliance with revised Rule 25.53	PPM	WAP
1				
2				
3				
4				
5				