Filing Receipt

Filing Date - 2024-02-01 01:30:28 PM

Control Number - 53385

Item Number - 1679

Greasewood II LLC Low Impact CIP Cyber Security Incident Response

X

Signature

Revision	Revision Date	Summary of Changes	Prepared By
v1	12/15/2023	Initial Version	Electric Power Engineers (EPE)

Table of Contents

1. Purpose

The purpose of this procedure is to provide Greasewood II LLC (Greasewood) written guidance on how to comply with NERC Standard CIP-003, Attachment 1, Section 4 for their Low Impact BES Cyber Systems.

This procedure shall be used to develop, implement, and maintain a Cyber Security Incident Response Plan (CSIRP) to respond to Cyber Security Incidents at all NERC CIP designated Facilities owned by Greasewood.

2. Applicability

Greasewood's low impact BES Cyber Systems are subject to the processes herein.

3. Responsibilities

Below are the roles and responsibilities associated with Cyber Security Incident Response:

- Greasewood personnel and contractors shall notify the Site Management of any actual or suspected Cyber Security Incidents.
- Site Management must:
    - Take appropriate actions to respond to Cyber Security Incidents
    - Notify the Asset Manager and CIP Senior Manager (or delegate) of all Cyber Security Incidents.
    - Coordinate with the Asset Manager and CIP Senior Manager (or delegate) on Cyber Security Incident investigation, classification, reporting, response, recovery, and mitigation.
- Site security personnel and Greasewood 's Technical/IT Support team (if any) shall assist in the investigation, classification, reporting, response, recovery, and mitigation of Cyber Security Incidents as requested.
- The CIP Senior Manager (or delegate) and Operations Supervisor shall collaborate on Cyber Security Incident investigations to classify, report, respond, recover and mitigate identified incidents.
- Managed Security Service Provider (MSSP)
    - Provide assistance in the investigation, classification, reporting, response, recover and mitigation of identified incidents.
- CIP Senior Manager or Delegate shall:
    - Coordinate Cyber Security Incident investigation, classification, reporting, response, recovery, and mitigation with appropriate individuals.
    - Ensure that a Cyber Security Incident Response Exercise is performed at least:
        - once every 36 months for sites without Medium Impact BES Cyber Systems. (See the Low Impact CIP Cyber Security Policy) and
        - and that the Cyber Security Incident Plan is updated with any changes or updates within 60 calendar days of the change.
    - Ensure that, if need, the CSIRP is updated within 180 calendar days after completion of a Cyber Security Incident Response Plan test or action Reportable Cyber Security Incident.

4. Procedure Details

Identification & Classification

Cyber Security Events will typically be identified through automated system monitoring, notification, or direct observation. Refer to the "Incident Management & Classification" section (below) for examples of events that qualify as Cyber Security Incidents.

Based on the NERC glossary of terms for a Cyber Security Incident and Reportable Cyber Security Incident, Greasewood has identified the categories in the table below for incident identification. The identification of an incident is based on the outcome determined in the table below considering the BES Cyber System affected by the event.

Outcome	Incident Descriptions	Low Impact BCS Applicability ?	Reportable OR Non-Reportable?
Event	Security Event (Cyber or Physical) An event has occurred	Yes	Non-Reportable
Not a compromise or disruption	Non-Reportable Cyber Security Incident A malicious act or suspicious event that IS NOT found to be an attempt to compromise a BES Cyber System and/or associated Electronic Access Control or Monitoring System (EACMS)	Yes	Non-Reportable
Actual compromise or disruption	Reportable Cyber Security Incident A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity	Yes	Reportable

Incident Response (Reference Appendix 1: Low Impact CSIRP Diagram)
The following activities outline the actions Greasewood complete when responding to potential Cyber Security Incidents:

Immediate Response
Attempts should be made to contact and consult with appropriate site management personnel prior to determining whether a Cyber Security Incident is Reportable or Not Reportable. In all cases, regulatory reporting criteria and timeframes must be met. *Some reporting requirements for Cyber Security Incidents are within 1 hour.*

Upon Identification that an event is a Cyber Security Incident (or suspected Incident), Greasewood personnel shall immediately report the Incident to the Operations Supervisor and any other appropriate management personnel.

Cyber Security Incidents
For Cyber Security Incidents, Site Management must contact and coordinate with the CIP Senior Manager or Delegate on the appropriate Cyber Security Incident Report and Response actions.

Physical Security Breach/Threat
For a physical security breach or threat, Site Management must formulate an immediate response that includes:

a. Alerting on-site personnel of any existing safety issues. If personnel safety is threatened, personnel may be directed to take shelter or further actions as the situation evolves.

b. Determine if additional assistance is immediately needed from local law enforcement.

i. Fort Stockton Police Department: (432) 336-4600

ii. Fort Stockton Fire Department: (432) 336-8971

c. Take actions to mitigate the immediate risk to reliable operation of the Bulk Electric System.

Incident Response Cont.

Site Management and the CIP Senior Manager or Delegate initiate response and communication to mitigate Cyber Security Incidents. During the initial response and investigation, as much detail as possible shall be collected including (but not limited to) the following:

- Description of the event; including how and when it was discovered
- Impact, or expected possible impact, to Operations and/or components of the Bulk Electric System
- Availability of backup or redundant systems
- Physical areas and/or systems affected
- Actions already taken to respond
- Estimated restoration timeline

The Site Management, CIP senior Manager or Delegate, or other designated personnel will begin documenting the incident in an Incident Report (See: Appendix 2: Cyber Security Incident Reporting Form).

CIP Exceptional Circumstances (CEC)

Greasewood shall determine if the Incident classification meets the definition of a CEC (Reference Section 5. Glossary of Terms). If so:

- The CIP Senior Manager or Delegate must make the declaration of a CEC for which the date and time shall be logged.
- Status notifications, including initiation and termination, of the declared CEC shall be made to senior management personnel by the CIP Senior Manager or Delegate.
- Once the CEC has been resolved, the CEC shall be declared complete for which the date and time shall be logged.

See CIP Exceptional Circumstance Form for additional details of processing a CEC.

Incident Management & Classification

The following identifies scenarios and actions taken by Greasewood to classify and respond to Cyber Security Incidents. These actions are not intended to be all-inclusive, and any additional actions are determined by the Site Management and/or CIP Senior Manager or Delegate on a case-by-case basis.

Events & Suspected Activities

An event (Cyber or Physical) can occur during normal operations. Most have trivial causes requiring a routine maintenance action or other corrective actions that are not the result of malicious activity. These Events will not be considered or handled as Cyber Security Incidents.

All events & suspected activities should be treated as breaches until an initial investigation has been completed. The Site Management must be notified of the suspected activity. If a suspected physical/electronic breach or attack is determined to be invalid, normal operations should continue. Suspected activities may include:

- Unknown devices, equipment, packages within the Facility
- Unknown (abnormal) personnel
- Unexplained equipment malfunctions
- Abnormal behavior of Cyber Assets or absence in logging

Breaches

Physical Security Breaches – Physical security breaches must be investigated, and the security perimeter secured. If determined to be a malicious act or potentially malicious act, responses include:

- Ensuring the safety of on-site personnel
- Notifying law enforcement (as necessary)
- Determining whether the attack has caused damage to equipment that could compromise or disrupt reliable operations of the BES.

Electronic Security Breaches – The immediate response must focus on containment of the event to minimize its effects on equipment and prevent the spread to other parts of the system. This may include:

- Disabling all suspected network connectivity
- Confirmation of physical access controls
- Removing equipment or programs from service (provided its removal does not itself compromise or disrupt stable operations of the BES).
- Requesting necessary technical support as needed (engineering, maintenance, IT) to ensure appropriate response and for the backup and storage of information required to recover BES Cyber System functionality. Identify the teams to be contacted – engineering, maintenance, IT, etc.

Note: Data preservation should not impede or restrict recovery, but Cyber data, such as corrupted drives or recorded data, should, to the extent possible, be preserved for follow-up investigations and full recovery.

Attacks

Physical Security attacks – The immediate response must focus on ensuring the safety of on-site personnel and mitigating the risk to reliable operations of the BES by protecting, restoring, or securing equipment or by otherwise stabilizing or securing site operations.

Electronic Security attacks – The immediate response must focus on ensuring the LIBES is still secure and that the attack did not result in a breach of the LIBCS. Responses may include:

- Reviewing LIBCS configurations (firewall settings, intrusion detection logs, etc.)
- Validation that suspected Cyber Assets have not been compromised
- Requesting technical support as needed (engineering, maintenance, IT) to ensure appropriate response and for the backup and storage of information required to recover BES Cyber System functionality. Identify the teams to be contacted – engineering, maintenance, IT, etc.

Threats

Verbal Threats – Obtain all available information regarding the threat so that appropriate notifications and actions may begin.

- If a live caller is involved, obtain and document any available details that can be collected. If possible, remain on the phone with the caller to support call tracing.
- Notify the Site Management and other appropriate management so that reporting requirements may be considered.

Physical Security threats (bombs, sabotage, weaponry, etc...) – Notify Site Management and local law enforcement immediately. Conduct a review of protective measures that are in place to ensure mitigation capability is intact.

- Implement increased security measures such as more frequent security patrols or additional security personnel (as appropriate).
- Conduct searches of security perimeters and site areas for signs of ingress or attempted ingress and report to the Operations Supervisor and other appropriate management.
- Once the threat window has passed, consider returning measures and controls to the baseline security posture.

Electronic Security threats – while uncommon, threats to the ESP should be responded to using the same measures above for ESP attacks.

Note: CIP Exceptional Circumstance actions may be in exception to previously defined CIP related procedures and/or regulations. Exceptions to defined procedures should be noted for future review.

Cyber Security Incident Reporting

Greasewood is obligated to notify the E-ISAC of Reportable Cyber Security Incidents. Greasewood also reports such incidents to the appropriate Independent System Operator (ISO) and Reliability Entity (RE) as a best practice.

E-ISAC & DOE Reporting

As soon as practicable, and with consideration of the severity of the Cyber Security Incident and the filing horizon, the CIP Senior Manager and/or Site Management will contact the E-ISAC at (404) 446-9780 (Press 2) within one (1) hour from the time the Response Team concludes that functionality essential to performing reliability tasks has been compromised or disrupted (Reportable Cyber Security Incident).

Depending on the nature of the situation, Form OE-417 must be filed to the DOE either within one hour; six hours; or by the later of 24 hours after the recognition of the incident OR by the end of the next business day of the incident. The DOE reporting website provides provisions to include NERC and/or E-ISAC as additional recipients of the OE-417 submittal. For detailed procedure on reporting and filing OE-417 refer to filing instructions in the link:

https://www.oe.netl.doe.gov/OE417/Form/Home.aspx

Reporting Updates

Greasewood will provide updates to the initial report, if any, within seven (7) calendar days of determination of new or changes attribute information. Attribute information under this requirement include: the functional impact, the attack vector used and the level of intrusion that was achieved or attempted. If any of these attributes receive new or updated information, they must be reported to both E-ISAC and NCCIC and indicated as an "Update" to the initial and/or prior updates.

CSIRP Review and Maintenance

The Site Management is responsible for initiating updates to the CSIRP as necessary. Any changes to the roles or responsibilities, response groups or technology that would impact the ability to execute the plan will be reflected in the plan and communicated to respondents no later than 60 calendar days after the change. The Site Management will facilitate the documentation and communication of any such changes. A review of the Cyber Security Incident Response Plan will be completed at least once every 15 calendar months.

CSIRP Testing

Greasewood will schedule and execute tabletop testing of the CSIRP for Low Impact BES Cyber Systems with representatives of those facilities at least once every 36 calendar months. Any such test can include an actual Reportable Cyber Security Incident, an attempted compromise of a Cyber Security Incident, a paper drill or tabletop exercise of a Reportable Cyber Security Incident. CSIRP testing does not require removing a component or system from service during the test.

It is important to treat the test as if it were a real incident; including completion of a "Drill" Incident Response Report, Executive Report, and/or completion of a "Drill" OE-417, if required by the scenario. Tests should also include validating contact numbers, email addresses and weblinks.

No later than 180 calendar days after completion of a Cyber Security Incident Response Plan test or actual Reportable Cyber Security Incident, Greasewood shall update the CSIRP if needed.

5. Glossary of Terms

Bulk Electric System (BES)
See NERC "Glossary of Terms Used in NERC Reliability Standards" definition.

BES Cyber Asset (BCA)
A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

BES Cyber System (BCS)
One or more BES Cyber Asset logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

CIP Senior Manager
A senior management official with overall authority and responsibility for leading and managing the implementation of and continuing adherence to the requirements within the NERC CIP Standards.

Control Center
One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data center, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Cyber Asset
Programmable electronic devices, including the hardware, software, and data in those devices.

Cyber Security Incident
A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or- Disrupts or attempts to disrupt the operation of a BES Cyber System. ***Note that for low impact BES Cyber Systems the only applicable portion of the definition of Cyber Security Incident is "A malicious act or suspicious event that: …Disrupts or attempts to disrupt the operation of a BES Cyber System."*

Interconnection Reliability Operating Limit (IROL)
A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System.

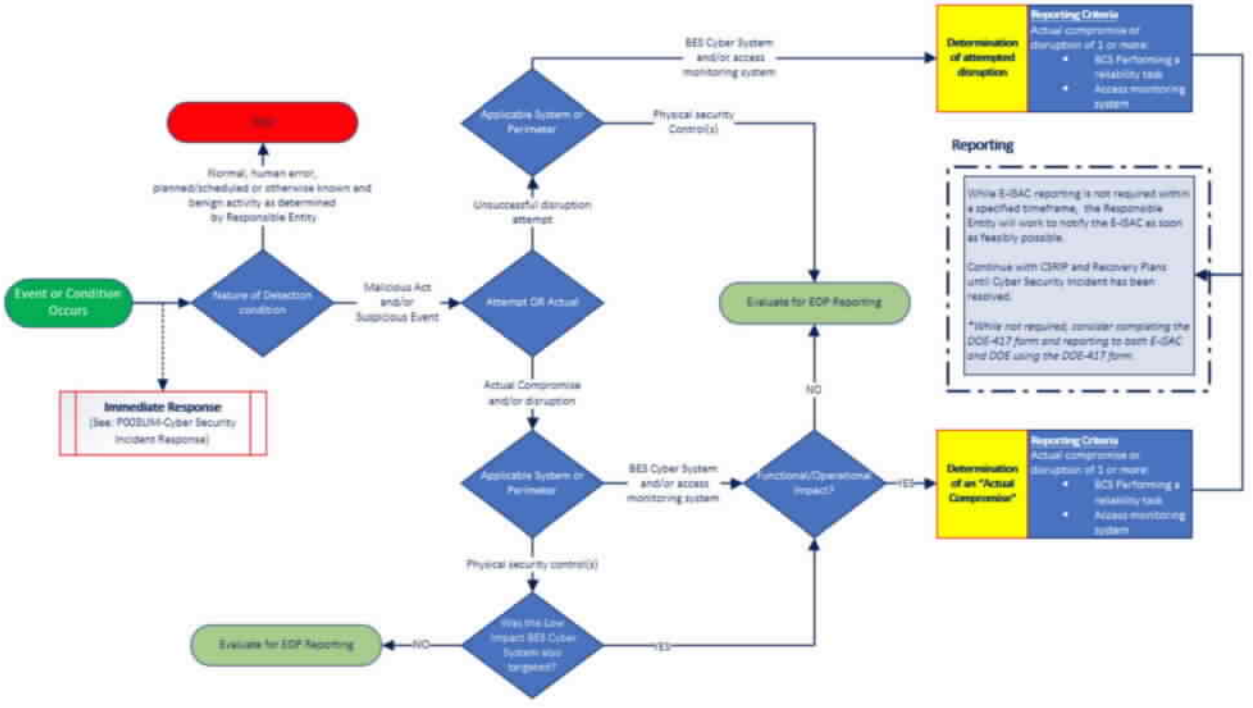
Special Protection Systems (SPS) / Remedial Action Scheme (RAS)
See "NERC Glossary of Terms Used in NERC Reliability Standards"

NERC Glossary of Terms
https://www.nerc.com/files/glossary_of_terms.pdf

6. Reference Documents

Appendix A: Low Impact CSIRP Diagram
Appendix B: Cyber Security Incident Response Form
CIP Exceptional Circumstance Form

Appendix A: Low Impact CSRIP Diagram



Appendix B: Cyber Security Incident Response Form

General Information	
Date Updated:	Incident Response #:

Respondent Information	
Incident Response Lead:	Title:
Incident Support Lead:	Title:

Additional Participants/Respondents		

Dates and Times Associated with Incident	
Initial Notification:	By:
Start of Incident:	*End of Incident:
Actual Initiation of Malicious Behavior (complete this section following root cause identification, if known):	

**In the "End of Incident" field, enter the date on which containment and eradication activities ended.*

Overall Description of Incident

Root Cause

Containment Activities

Eradication & Recovery Activities

Lessons Learned

Threat Source (Attack Vector)		
☐ Unknown	☐ Email	☐ Improper Usage

☐ Attrition	☐ External/Removable Media	☐ Loss of Theft of Equipment
☐ Web/Cloud	☐ Impersonation/Spoofing	☐ Unmanaged Devices
☐ Other:		
Additional Information:		

Incident Classification & Associated Impact				
Incident Classification:	☐ Reportable Cyber Security Incident	☐ NON-Reportable Cyber Security Incident		
Functional Area Impact:	☐ Corporate	☐ Generation	☐ Transmission	☐ Other:
Impact to Operations?	☐ NO	☐ YES (provide details):		

Information Sharing	
☐ Legal	
☐ Communications	
☐ Human Resources	
☐ Physical Security	
☐ Law Enforcement	
☐ Regulatory Agencies	
☐ External Partners	
☐ Additional Contacts:	

Associated Documents	
☐ OE-417	Electric Emergency Incident and Disturbance Report
☐ E-ISAC	
☐ FBI	
☐ DHS	
☐ NCCIC	
☐ Additional Contacts:	

Near-Term Action Items (3-6 months)

#	Description	Respondent	Due Date	Status
1				
2				
3				
4				

Long-Term Action Items (6+ months)				
#	Description	Respondent	Due Date	Status
1				
2				
3				
4				

Incident Log (Use this section to log incident activities. When respondents have the same initial, establish method to distinguish unique ID)			
Date	Time	Initial	Description of Activity

Greasewood Solar II
Emergency Operations Drill

Introduction:
It is imperative to consider as many operational and weather-related issues as possible when developing the tasks for your Emergency Operations Drill (Drill). Equally as important is determining the appropriate staff to address these issues, timing, contracts and dependencies on external entities, all while executing clear and unambiguous instructions. This Drill is designed to ensure Greasewood Solar II addresses as many of these issues as possible, supporting the continued operations of its generating facilities during extreme weather conditions.

Staffing:
All Greasewood Solar II personnel participating in the Drill will be notified directly, with a clear set of tasks to be completed. Should the tasks need to be performed in a sequential order, appropriate personnel shall be instructed on the timing and order of tasks, stressing clear, concise communication throughout the process. Example - If a switchyard operator is required to open a breaker, he/she must have the proper switching order as a prerequisite and abide by the Lock-out/Tag-out process for Greasewood Solar II. It is important to identify adequate staff to complete the necessary tasks to ensure continuous operation of the generating facility, to the extent possible.

Task Identification:
For Greasewood Solar II facilities, the weatherization tasks may require less barriers and portable heaters than a conventional generation site; however, these measures can be utilized to keep exposed equipment above freezing temperatures or sheltered from precipitation where necessary.

Carefully list all tasks to be performed in Attachment B of *Greasewood Solar II-PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*, as well as assigning the tasks to the appropriate personnel. It is important to note that severe conditions may warrant more resources to execute a task than normal operating conditions, so it is imperative that equipment like snow chains, de-icing solution(s), extra fuel, etc., are available. Attachment B will require an action item to be assigned to personnel (listed by name), a description of the task, date, completion status (for tracking purposes), and any notes or comments taken during the drill.

Sample Tasks:
- Procurement and distribution of fuel for emergency generators, if applicable.
- Procurement and distribution of spare SF6, nitrogen, or oil for switchyard equipment.
- Management of transportation for personnel participating in the Drill.
- Establishment of emergency operations communications, cell phones, satellite phones, radios, etc.
- Communication of tasks and continual updates via the communication platforms used in the Drill.
- Erection of temporary barriers
- Procurement and placement of portable heaters and extra fuel.
- Inspection of plant and balance of plant equipment to ensure heaters (breaker panels, for example) and instrumentation are serviceable and properly insulated, where applicable.
- All necessary PPE is on hand and available for staff.
- Establish communication with ERCOT, QSE, and appropriate transmission entities, to keep them informed of any developing issues that may impact operation of the facility.
- Ensure proper equipment is on hand and available for clearing paths to the facility, should there be downed vegetation or obstructions.

Review and Correction:
In the event that vulnerabilities or issues were identified during the Drill, appropriate Greasewood Solar II staff shall conduct a review of the Drill, corrective actions to be taken, and document those corrective actions in Attachment B of *Greasewood Solar II-PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*. This review should include an extent of conditions assessment and root cause analysis in order to address any latent issues that may exist in other areas.

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

Name	Title	Permission(s)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to the EOP Drill Instructions since the initial EOP Drill Instructions adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0	12/XX/2023	12/XX/2023	EOP Drill Instructions

As of 12/XX/2023, EOP Version 1.0, approved on 12/XX/2023, supersedes all previous EOP Drill Instructions.

The following files are not convertible:

Greasewood Solar II-PGCEOP-1.0-Emergency Operations Plan - Attachments B-E.xlsx

Please see the ZIP file for this Filing on the PUC Interchange in order to access these files.

Contact centralrecords@puc.texas.gov if you have any questions.

Emergency Operations Plan

Greasewood Solar II

Power Generation Company (PGC)

Version 1.0
Effective Date:
12/XX/2023

Contents

Approval and Implementation

Introduction:

- This EOP is developed to help ensure Greasewood Solar II 's continued power generation 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)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to the EOP since the initial EOP filing pursuant to paragraph (1) of this subsection.

Version	Approval Date	Effective Date	Revision Summary
1.0	12/XX/2023	12/XX/2023	Initial Emergency Operations Plan

As of 12/XX/2023, EOP Version 1.0, approved on 12/XX/2023, supersedes all previous EOPs.

Communication Plan

An entity with generation operations must describe the procedures during an emergency for communicating with,

- the media
- PUCT
- OPUC
- QSE
- fuel suppliers
- Local and state governmental entities, officials, and emergency operations centers, as appropriate in the circumstances for the entity
- and ERCOT, as the Reliability Coordinator.

Greasewood Solar II Emergency Operations Contact List

EMERGENCY OPERATIONS CONTACT LIST (EXTERNAL)			
NAME	ENTITY	PHONE NUMBER	EMAIL
Shift Supervisor	ERCOT	512-248-6804	shiftsupv@ercot.com
QSE REPRESENTATIVE	QSE NAME	XXX-XXX-XXXX	XX
PUCT Infrastructure Staff	PUCT	512-936-7197	
JC Culberson	Electric Power Engineers, LLC	817-688-9114	jculberson@epeconsulting.com
RADIAN REPRESENTATIVE	RADIAN	XXX-XXX-XXXX	XX

Greasewood Solar II Internal Emergency Operations Contact List

INTERNAL GREASEWOOD SOLAR II EMERGENCY OPERATIONS CONTACT LIST			
NAME	ENTITY	PHONE NUMBER	EMAIL
Zahi Harel	Ashtrom Renewable Energy	737-351-3522	zahih@ashtrom.co.il
Dikla Fhima	Ashtrom Renewable Energy	+ 972-544838283	diklaf@ashtrom.co.il

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.
Power Generation Company	PGC	Generates electricity intended to be sold at wholesale and does not own a transmission or distribution facility in this state (with some exceptions, see PUC Substantive Rule 25.5(23) and 25.5(45)).
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 & FILING REQUIREMENTS

As a registered PGC, in the ERCOT footprint, Greasewood Solar II 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, Greasewood Solar II 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) before COD if it is a new facility or (b) within 30 days of a substantive change to the plan. A substantive change that is made to the plan between November 1st and April 30th must be filed no later than June 1st of that year. If a substantive change is made to the plan between May 1st and October 31st, the submission date is no later than December 1st of that same year. At all times, the most recent approved copy of the Greasewood Solar II Emergency Operations Plan (Greasewood Solar II -PGCEOP-1.0) must be available at the main office for PUCT inspection.

- For Greasewood Solar II, a PGC, the PUCT has ordered the following information be included and/or addressed in the Emergency Operations Plan:

Maintenance of Pre-identified Supplies for Emergency Response

A plan to maintain pre-identified supplies for emergency response.

Greasewood Solar II staff shall identify any supplies necessary for continued operations during an extreme weather event, and must procure, to the extent possible, those supplies. A list of some of these supplies is contained below:

- Fuel for generator (if applicable)
- Fuel for heaters
- Gas for breakers or load-interrupting switches (if applicable)

- Oil and nitrogen for transformers (if applicable)
- Parts used for maintenance or repair of equipment
- Fuel for vehicles (if applicable)
- Etc.

See Attachment D for a listing of supplies required for emergency response.

Evidence - Any evidence that supplies were requested and procured prior to the extreme weather event. Please use the appropriate details from the bulleted list above for supplies. Completed Attachment D.

Staffing During Emergency Response

A plan that addresses staffing during emergency response. Greasewood Solar II will identify appropriate staff and staffing levels to respond to emergency conditions, including, but not limited to severe weather events, physical threats or physical damage, and cyber security events.

Greasewood Solar II shall identify operational and management staff that will remain on call or on stand-by for the duration of the emergency (Attachment C of Greasewood Solar II-PGCEOP-1.0 Emergency Operations Plan-Attachments B-E). This list may be dynamic and will be subject to change should conditions warrant it.

Evidence - Attachment C of Tierra Bonita Solar -PGCEOP-1.0 Emergency Operations Plan - Attachments B-E). should be completed to reflect a staffing plan for severe weather events. Secondary evidence would consist of dated emails or documented evidence that staff was notified and understood their expectations during this event.

Weather-related Hazards

A plan that addresses how an entity identifies weather-related hazards, including tornadoes, hurricanes, extreme cold weather, extreme hot weather, drought, and flooding, and the process the entity follows to activate the EOP.

Greasewood Solar II staff shall actively monitor all potential extreme weather events that may affect their facilities, to include sever weather and operational circumstances arising from those

events. Greasewood Solar II staff will continue monitoring weather forecasts and ERCOT operational data aid in predicting conditions on the BES that may impact operations.

Evidence - Screenshots of ERCOT site and weather site, complete with timestamps. Any dated correspondence to reflect communication of the potential or forecasted extreme weather event to staff.

Additional Annexes

Greasewood Solar II, in its operational capacity as a PGC, must include the following annexes for its generation resources other than generation resources authorized under PURA §39.918:

Weather Emergency

- operational plans for responding to a cold or hot weather emergency, distinct from the weather preparations required under §25.55 of this title;
- verification of the adequacy and operability of fuel switching equipment, if installed; and
- a checklist for generation resource personnel to use during a cold or hot weather emergency response that includes lessons learned from past weather emergencies to ensure necessary supplies and personnel are available through the weather emergency.

For severe cold weather, Greasewood Solar II shall identify, through inspection, areas of the generating facility that may be most vulnerable to malfunction during extreme cold events. Greasewood Solar II staff shall ensure the following:

- Greasewood Solar II staff will ensure, where applicable, heat tracing is present and functional for all appropriate exposed instrumentation and/or equipment, where applicable.
- Where appropriate and necessary, temporary barriers shall be erected to shield sensitive or exposed equipment and instrumentation from wind and freezing precipitation.
- Temporary barriers may be constructed of plastic sheeting or other material that is sufficient to protect exposed equipment and instrumentation, and may contain, if conditions warrant, a portable heat source to keep temperatures above freezing in the designated area.
- Other measures may be taken, as the generation facility staff see fit, to protect the facility during an extreme cold weather event.

For severe hot weather, Greasewood Solar II staff shall ensure the following:

- Proper ventilation is present and functional for any areas where extreme hot temperatures may negatively impact generator output.
- In addition to this, portable fans may be mobilized to force air around potentially affected areas.
- Ensure normal facility cooling measures are maintained and operational.

In all cases, Greasewood Solar II staff will ensure that any substation or switchyard equipment that it owns is properly weatherized. This includes the following:

- Ensuring all breaker and transformer oil levels, SF6 levels, nitrogen levels, and air compressor tank levels are adequate for that equipment manufacturer and model.
- Heaters in breaker and transformer cabinets are functioning properly
- Adequate supply of spare gas and oil is available to be used during an emergency Evidence - Maintenance records, records of inspection at generating sites, photos of erected temporary barriers, portable heaters in service, heat trace application photos, photos of unobscured ventilation, photos of any cooling measures deployed photos of any other weatherization measures with dates. If any breakers or transformers fall under the facility's purview, dated inspection and maintenance records detailing heater functionality and oil and gas levels and a list of any spare bottles of gas or stores of oil.

A water shortage annex that addresses supply shortages of water used in the generation of electricity;

Not applicable as Greasewood Solar II assets do not use water to generate power.

An attestation declaring this portion of the plan is not applicable should suffice as evidence.

A restoration of service annex that identifies plans intended to restore to service a generation resource that failed to start or that tripped offline due to a hazard or threat;

Greasewood Solar II 's plan for emergency operation addresses its process for recovering generation capacity, should an emergency force a derate, a unit trip, or inability to generate and fulfill its MW obligations. These actions are listed in *Annex E-Greasewood Solar II -PGCEOP-*

1.0 - Generation Restoration Instructions and Attachment E of *Greasewood Solar II -PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*.

Evidence - By completing Attachment E of *Tierra Bonita Solar -PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*, document all actions taken to address any inability to generate MW along with a detailed description of communications to QSE and/or

A pandemic and epidemic annex;

Greasewood Solar II 's existing pandemic/epidemic plan for business continuity is listed in Annex F.

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

In the event of a hurricane, the first priority is always the health and safety of Greasewood Solar II personnel. The Greasewood Solar II hurricane response process is listed below:

- Ensure all Greasewood Solar II personnel and any potentially affected public personnel are not in danger.
- By using the evacuation routes contained in the HRP (Greasewood Solar II -EOP-1.0 Hurricane Response Plan), Greasewood Solar II personnel must evacuate at a time recommended by local authorities.
- The Greasewood Solar II facility should be hardened, to the extent possible, against lasting damage from a hurricane. Some of these hardening details are listed below:
    - Ensure all loose material or equipment is secured.
    - Ensure proper draining channels exist and are functional

Greasewood Solar II is in Region 7, as specified by TDEM, and shall use the hurricane evacuation routes published by the Texas Department of Transportation.

A cyber security annex;

- The Greasewood Solar II Cyber Security Incident Response Policy (*Annex G-Greasewood Solar II -Cyber Security Incident Response Plan*) contains this information.

A physical security incident annex;

This section contains reporting for physical threats to any COBO, as well as actual damage to or destruction of any COBO, per NERC Reliability Standard EOP-004. The DOE digital form, OE-417 shall be used to communicate physical attacks and cyber security incidents.

Please see *Annex H - Greasewood Solar II -PGCEOP-1.0 Physical Security Plan* for more details.

Checklist(s) for generating facility personnel to address emergency events

Greasewood Solar II shall use the checklist in Attachment C of *Greasewood Solar II -PGCEOP-1.0 Emergency Operations Plan - Attachments B-E* to identify which personnel shall address events that arise during the emergency.

Evidence - Complete Attachment C and document any actions taken to address any vulnerabilities found and addressed while completing the checklist.

A plan for alternative fuel testing if the facility has the ability to utilize alternative fuels

As a solar generating facility, measures for securing alternative fuels are not applicable.

> Evidence - If the facility is capable of burning alternative fuel, dated proof that the fuel was tested prior to its use as the fuel source for the generator. If not applicable, state so in an attestation.

Affidavit from an owner, partner, officer, manager, or other official with responsibility for Greasewood Solar II's operations affirming that all relevant Greasewood Solar II operating personnel are familiar with the contents of the emergency operations plan; and such personnel are committed to following the plan except to the extent deviations are appropriate under the circumstances during the course of an emergency.

Completed, executed, and notarized *Annex A- Greasewood Solar II -PGCEOP-1.0 Emergency Operations Plan Affidavit*.

PUC Filing Requirements

An entity must file an emergency operations plan (EOP) and executive summary by April 15, 2022, or upon registration date, if after 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 of *Greasewood Solar II -PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*, Greasewood Solar II Emergency Operations Plan shall be tested each year, no later than December 31, and includes a review section, to identify and correct any vulnerabilities in the Emergency Operations Plan. Greasewood Solar II Emergency Operations Drill Procedure has a section dedicated to any generation facility that is located within a defined hurricane evacuation zone.

Evidence - Emergency Operations Drill documentation, instructions, Attachment B of *Tierra Bonita Solar -PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*, attendance/participation records with dates and names.

Greasewood Solar II, 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*. Greasewood Solar II shall submit all updated plans electronically. *Attachment I - Greasewood Solar II - PGCEOP-1.0 ERCOT Protocols Section 22(O) - Declaration of Generation Resource Winter Weather Preparations* is the attestation ERCOT requires for notification, along with the EOP.

Evidence - Electronic copy or screenshot of successful submittal to ERCOT (Attachment I and complete plan, should there be any updates).

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

Name	Title	Permission(s)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to the EOP since the initial EOP adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0	12/XX/2023	12/XX/2023	General Restoration Instructions

As of 12/XX/2023, EOP Version 1.0, approved on 12/XX/2023, supersedes all previous EOPs.

Greasewood Solar II
Emergency Operations Plan Executive Summary

Executive Summary:

As a registered PGC, Greasewood Solar II 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. Greasewood Solar II has developed this plan to comply with the PUCT Substantive rule and applicable NERC Reliability Standards, as well as ensure a greater likelihood of continued operations during an emergency. This plan must be filed with the PUCT either (a) before COD if it is a new facility or (b) within 30 days of a substantive change to the plan. Any substantive change to the plan, made between November 1st and April 30th must be filed no later than June 1st of that year. If a substantive change is made to the plan between May 1st and October 31st, the submission date is no later than December 1st of that same year. At all times, the most recent, approved copy of the Greasewood Solar II Emergency Operations Plan must be available at the Ashtrom Renewable Energy LLC main office for PUCT inspection.

For Greasewood Solar II, a PGC, the PUCT has ordered the following information be included and/or addressed in the Emergency Operations Plan:

- Maintenance of Pre-identified Supplies for Emergency Response
- List of primary and, if possible, backup emergency contacts
- Affidavit 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 training.
- Annexes to be included in the EOP - A Generation resource/PGC must include
    - A weather emergency annex that includes
        - Operational plan for responding to a cold and hot weather emergency, distinct from the weather preparations required under § 25.55
            - EOP-001, page 7 and Annex W
        - Verification of the adequacy and operability of fuel switching equipment, if installed; and
            - EOP-001, page 9. It is not applicable to this site.
        - A checklist for generation resource personnel to use during a cold or hot weather emergency response that includes lessons learned from past

weather emergencies to ensure necessary supplies and personnel are available through the weather emergency
    - Annex D
  - A water shortage annex that addresses supply shortages of water used in the generation of electricity;
    - EOP-001, page 8. This is not applicable to this site.
  - A restoration of service annex that identifies plans intended to restore to service a generation resource that failed to start or that tripped offline due to a hazard or threat;
    - Annex E
  - A pandemic and epidemic annex;
    - Annex F
  - A hurricane annex that include evacuation and re-entry procedures if facilities are located within a hurricane evacuation zone, as defined by TDEM;
    - Annex L
  - A cyber security annex;
    - Annex G
  - A physical security incident annex; and
    - Annex H
  - Any additional annexes as needed or appropriate to the entity's particular circumstances
- Drills
  - Attachment B of *Greasewood Solar II -PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*

As a registered PGC, it is the intent of Greasewood Solar II to fully comply with all requirements and expectations of the Public Utilities Commission of Texas, all applicable ERCOT protocols, Operating Guides, and Planning Guides, and Applicable NERC Reliability Standards.

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

Name	Title	Permission(s)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to Executive Summary adoption since the initial Executive Summary adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0	12/XX/2023	12/XX/2023	Executive Summary

As of 12/XX/2023, Executive Summary Version 1.0, approved on 12/XX/2023, supersedes all previous Executive Summary adoptions.

Annex E- Greasewood Solar II
General Restoration Instructions

Introduction:

When the Greasewood Solar II facility trips offline, or is taken offline for any reason, there will be a set of details to consider. In the case of Tierra Bonita, consultation with the OEM provider, third-party consultants, ERCOT Operations staff, FERC staff, DOE, and internal operations staff may be necessary, depending on the nature of the incident that caused the generation Facility to go offline. This Annex, along with Attachment E of *Greasewood Solar II-PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*, will serve to support Greasewood Solar II management and operations personnel in recovery efforts.

Staffing:

Depending on the reason for the outage, various Greasewood Solar II staff may be needed to address the incident. There can be many causes for a generator to trip, or be forced into an outage situation, requiring nuanced approaches to restoring power to the Facility. The following circumstances are meant to provide examples for different scenarios but is not an exhaustive list.

Operational Instruction from RC, BA, or TOP:

As a solar generating facility, Tierra Bonita must comply with any Operating Instruction from ERCOT (as the BA, RC, and TOP), as well as the operational TOP, Garland Power and Light (GPL). If there is a problem with complying with the Operating Instruction, Tierra Bonita operations personnel must communicate this to ERCOT or GPL operations staff, immediately. If the Operating Instruction was given by ERCOT, as the RC, BA, or TOP the communication shall be made with ERCOT, if the Operating Instruction was issued by GPL, as the Transmission Operator (TOP), the communication shall be with GPL staff. If the Operating Instruction violates safety or may damage Facility equipment, this must be communicated to the entity issuing the Operating Instruction.

Physical damage:

If it is determined that the damage sustained by the Facility is not due to malicious and intentional damage to the Facility, normal operations checks should be conducted on the equipment, to ensure it is possible to begin generating again. This may include consultation with the OEM, contract engineers, and internal maintenance and operations staff.

If the physical damage is determined to be a direct result of intentional damage to the Facility, please refer to *Annex H-Greasewood Solar II-PGCEOP-1.0 Physical Security Plan*. After completing the reporting process, communication with internal, ERCOT, and GPL operations staff is vital. Tierra Bonita staff should refer to restoration procedures when restoring power.

Cyber Security:

In any case that involves cyber security, threat of cyber damage, or actual damage to the Facility from a cyber security perspective, please refer to *Annex G-Greasewood Solar II-PGCEOP-1.0 Cyber Security Incident Response Plan (CSIRP)*. Careful investigation must be carried out at the Facility to determine how to restore power.

Review and Correction:

After the incident, an in-depth review should be completed. This review should address communications best practices, actionable tasks for improvement of the procedures used for notification and operations, as well as addressing staff responses and actions. During this review, please use Attachment E of *Greasewood Solar II-PGCEOP-1.0 Emergency Operations Plan - Attachments B-E*.

The following individuals are responsible for maintaining, implementing, and revising the General Restoration Instructions.

Name	Title	Permission(s)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to the General Restoration Instructions adoption since the initial General Restoration Instructions adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0	12/XX/2023	12/XX/2023	General Restoration Instructions

As of 12/XX/2023, General Restoration Instructions Version 1.0, approved on 12/XX/2023, supersedes all previous General Restoration Instructions adoptions.

Hurricane Response Plan

12/XX/2023

In the event of a hurricane, the first priority is always the health and safety of Greasewood Solar II personnel. The Greasewood Solar II Hurricane Response Process/Plan (HRP) is listed below:

- Ensure all Greasewood Solar II personnel and any potentially affected public personnel are not in danger.
- By using the evacuation routes in the link below, Greasewood Solar II personnel must evacuate at a time recommended by local authorities.
- The Greasewood Solar II facility should be hardened, to the extent possible, against lasting damage from a hurricane. Some of these hardening details are listed below:
    - Ensure all loose material or equipment is secured.
    - Ensure proper draining channels exist and are functional
- Ensure all loose items and material are tied down, moored, or tethered, to reduce the likelihood of any blowing debris that may cause damage to personnel and/or equipment.

Greasewood Solar II facilities in Region 7, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

Checklist(s) for generating facility personnel to address emergency events

Greasewood Solar II shall use the checklist in Attachment C of *Greasewood Solar II-PGCEOP-1.0 Emergency Operations Plan - Attachments B-E* to identify which personnel shall address events that arise during the emergency.

When re-entry to the affected facility is safe, it is important to ensure all emergency gear and equipment that may be necessary to clear paths are available, serviceable, and on hand to be used, if necessary. This equipment may include, depending on the circumstances, saws, tire chains, etc.
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 Greasewood Solar II personnel attempting re-entry and Greasewood Solar II leadership.

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

Name	Title	Permission(s)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to the HRP since the initial HRP adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0	12/XX/2023	12/XX/2023	Initial Hurricane Plan

As of 12/XX/2023, annexes associated with EOP Version 1.0, approved on 12/XX/2023, supersede all previous HRP annexes.

Pandemic Response Plan

12/XX/2023

Contents

EXECUTIVE SUMMARY & APPROVAL

Introduction:

In light of recent responses to pandemics and epidemics, Greasewood Solar II has developed this Pandemic Response 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 the Greasewood Solar II 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 supporting the Greasewood Solar II 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)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to the PRP since the initial PRP adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0	12/XX/2023	12/XX/2023	Initial Pandemic and Epidemic Response Plan

As of 12/XX/2023, EOP Version 1.0, approved on 12/XX/2023, supersedes all previous PRPs.

INTRODUCTION

Overview:

Continuity of Operations planning ensures Greasewood Solar II 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, improve the performance of its generating and operations facilities, and ensure timely recovery.

Plan Scope & Applicability:

The Greasewood Solar II 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 Greasewood Solar II 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
- Protect vital records

Plan Assumptions:

The following assumptions were used while creating this plan:

- An event has occurred that affects normal business operations.
- Access to Greasewood Solar II facility may be limited.
- Qualified personnel are available to continue operations.

CRITICAL BUSINESS FUNCTIONS

Overview:

Critical business functions are those functions and critical activities that Greasewood Solar II 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 Greasewood Solar II to continue to meet its mission. These functions are not meant to be the name of a division, program, unit, etc. but meant to be the actual process/function that must be continued. These processes/functions can be supported or 'owned' by different divisions/units but the unit itself is not a critical business function. Each responsive action will inevitably be different, with its own unique challenges posed by the pandemic/epidemic, therefore, the following sample bullets should be used to define business practices and operations during such periods:

- Function - Enter the specific function that may need to be resumed.

- Business Process to Complete - Write a high-level description of the function process. Include any specific forms or systems that may be needed. Supporting Activities
- Supporting activities - Those tasks performed to achieve a critical business function and should be described.
- Lead Point of Contact (POC) and Alternate - Identify and include contact information, if necessary, for staff POCs for each supporting activity.
- Vendors and External Contacts - Identify and include contact information, if necessary, for vendor POCs for each supporting activity.
- Vital Records - Vital Records are those records a business needs to sustain the mission of the organization and comply with legal requirements. Vital records must be stored in multiple places in multiple formats. The identification, protection, and ready availability of vital records needed to support essential functions are critical components of a successful PRP.
- Maximum Allowed Downtime - Identify the amount of time your business could afford for the function to be down before it could cause irreparable harm. Consider using the following units:
    - Less than 24 hours
    - 1 day to 1 week
    - 1 to 2 weeks
    - 2 to 4 weeks
    - 30 days or greater
- Criticality - Enter High, Medium, or Low depending on how critical the function is to the operations of your business. Following are some considerations to use when determining criticality:
    - What business objective/goal does this function support?
    - How often does this function occur?
    - How many business units (departments) or people perform this function?
    - Does the successful completion of this function depend on any other functions?
    - Are other functions dependent on this function for its successful completion?
    - Is there a potential for revenue loss if this function is not completed?
    - Is there a potential for fines, litigation, additional downtime, or other punishment for noncompliance due to a regulatory requirement (NERC or ISO)?
    - What priority ranking would you give this function as compared to other functions?

Required Resources:

- People: Identify the number of employees required for this function. Also identify if a staggered resumption of employees is an option.
- Equipment: Identify the type of equipment and how many would be required in order to get this function back in operation.
- Supplies: Identify any unique supplies required for this function (do not list items that could be easily purchased from an office supply store). This would include any paper forms or documents needed.

- Information Technology: Identify software (e.g., Microsoft Office, QuickBooks, etc.), systems, applications, and electronic documentation needed to complete the function.
- Interdependencies: List other business functions this function relies on to be operational.

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 Greasewood Solar II facility 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. Greasewood Solar II 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 Greasewood Solar II 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 Greasewood Solar II:

- Wearing of PPE
  - Masks (N-95 or similar)
  - 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)

TABLE 1

Greasewood Solar II - Company Critical Business Function				
Critical Business Function 1:				
Business Process To Complete:				
Supporting Elements				
Supporting Activities (Describe)	Lead POC Alternate	Vendors and External Contacts	Vital Records	Maximum Allowed Down Time Criticality
Activity	Position Title Position Title	Brief list of vendors or external contacts to know for PRP purposes	Brief list of the vital records that support this activity	Time/Days High/Med/Low
Activity	Position Title Position Title	Brief list of vendors or external contacts to know for PRP purposes	Brief list of the vital records that support this activity	Time/Days High/Med/Low
Activity	Position Title Position Title	Brief list of vendors or external contacts to know for PRP purposes	Brief list of the vital records that support this activity	Time/Days High/Med/Low
Implications if not Conducted: *Interruption and/or loss of this function would interrupt...Furthermore, it would result in a delay of the capability to...*				
Calendar Dependent: *(e.g., this function is always occurring, this function only occurs in summer months, this function is active during inclement winter weather, etc.)*				
Required Resources: *Staff, equipment, supplies, Information Technology, and other resources.*				
Facilities: *Standard office space that can accommodate up to 50 people at any time. Traditional office equipment and space for phones, computers, scanners, printers, etc., with network access to Internet, radio, and other telecommunications services.*				
Supporting Partners: *List private sector or public sector supporting partners.*				
Vital Records: *List relevant vital records and their location, if appropriate.*				

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).

ORDERS OF SUCESSION AND DELEGATIONS OF AUTHORITY

Overview:
Orders of succession are prepared to provide clarity of senior leadership roles in the event that individuals in these roles, whether they be decision-making or management roles, are unavailable due to effects of a pandemic or epidemic. A delegation of authority provides successors with the legal authorization to act on behalf of critical positions within the organization for specific purposes and duties.

Orders of Succession:
These orders of succession are a formal and sequential list of senior leadership positions, written by position and not name, to identify who is authorized to assume the role of a position, should the incumbent be unavailable. The term unavailable means the incumbent of a position is not able, because of absence, disability, incapacity, or other causes, to exercise the powers and duties of an office. Pre-identifying orders of succession is critical to ensuring the continuation of effective leadership during an incident that disrupts operations.

Delegations of Authority:
Delegations of authority are the legal authorization to act on behalf of critical positions within the organization for specific purposes and duties. In order to ensure the rapid response to any situation requiring the activation of a PRP employees who serve in key senior leader positions must develop and maintain pre-delegated authorities for policy determinations and decisions, as needed. The delegations of authority should include what type of authority is being delegated, such as signatory or credit card authorization for purchasing, and also limitations of the delegated authority. All duties of each senior leader are delegated to the position in the

orders of succession when the incumbent cannot fulfil that authority for any reason, including but not limited to:

- Absence
- Illness
- Leave
- Death

Each authority is also terminated when the incumbent returns. The importance of previously delegated authorities is to ensure that important functions or authority can continue should the primary position become unavailable to complete their given functions. Staff who hold critical positions must maintain the pre-delegated authorities through effective cross-training and exercises for their successors.

How to Complete the Delegation Table (Table 2)
This table is customizable and has no limit to how much information should be in them. Please copy/paste to create a table for each position that must be continually occupied.

Position to be succeeded - This should be the title of the position that will need to be filled in the event a staff member becomes unavailable.
Successors - This should be the title of the position, not an individual, that will need to fill the position identified in the first column. They should be listed in sequential order.
Delegated authorities - These are the task and responsibilities held by the position delineated in the first column.
Activation and termination triggers - Select from incapacitated, unavailable, or selective decision as a reason for activation, per each position. Termination can be identified as sample language suggests or alternations can be made to termination thresholds.

Table 2

Position to be Succeeded	Successors	Delegated Authorities	Activation and Termination Triggers
Department Lead	*Successor 1*	*Delegated authorities or all duties as assigned*	*Activate: Incapacitated, unavailable, or selective decision* *Terminate: Return of Director*
	Successor 2	*Delegated authorities or all duties as assigned*	*Activate: Incapacitated, unavailable, or selective decision* *Terminate: Return of Director*
	Successor 3	*Delegated authorities or all duties as assigned*	*Activate: Incapacitated, unavailable, or selective decision* *Terminate: Return of Director*

PLAN DEACTIVATION

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.

Resumption Process:
Provide information as to how each function outlined in table 3 will be resumed and which staff members need to be active participants in this process.

How To Complete The Plan Deactivation Table - The following information details how to complete elements of Table 3 below. When completing this table, minimize the use of acronyms and describe actions in plain terms so that staff members who may be unfamiliar with the function will be able to use the document to resume and sustain the critical business function, if necessary.

Table 3

Item	Function	Supplies	Required Resources
1			
2			
3			
4			

Employee Contact List:

Table 4

Employee Name	Title/Responsibilities	Phone Number	Personal Email Address

Vendor Contact List:

Table 5

Vendor	Resource/Service	Phone Number	Email Address

Greasewood II LLC Low Impact CIP Physical Security Plan

X

Signature

Revision	Revision Date	Summary of Changes	Prepared By
v1	12/15/2023	Initial Version	Electric Power Engineers (EPE)

Table of Contents

1. Purpose

The purpose of this procedure is to provide Greasewood II LLC (Greasewood) written guidance on how to comply with NERC Standard CIP-003 Attachment 1, Section 2 for their Low Impact BES Cyber Systems.

This procedure shall be used to document Greasewood Physical Security Plan and Visitor Control process providing procedural controls to restrict physical access to identified BES Cyber Assets.

2. Applicability

Greasewood's low impact BES Cyber Systems and associated BES Cyber Assets are subject to the processes herein.

3. Responsibilities

The CIP Senior Manager or designee shall ensure that physical security controls are documented and implemented at Greasewood and identified secured BES Cyber Asset rooms/areas.

To maintain reliability, Greasewood personnel are responsible for the maintenance and implementation of primary physical controls such as:

- Physical site boundaries
- Keyed access
- Badge readers

Note that additional physical access controls may be utilized to augment Greasewood*'s defense-in-depth strategy.*

4. Procedure Details

Always notify site management immediately of any violation or suspected violation of Greasewood's Physical Security Plan. (See FRM-Physical Security Incident Investigation for reporting steps).

Access Authorizations

Greasewood must maintain documentation of personnel physical access authorizations. Access authorization to the facility is provided by the Site Manager or designee.

The CIP Senior Manager provides physical access authorizations to secured BES Cyber Assets rooms/areas. Tailgating anywhere in or around the facility is strictly prohibited.

Non-Employee Access Restrictions

Contractors will, upon arrival:

- check in with appropriate plant personnel.
- be instructed on Greasewood's physical access requirements.

Note: Certain Contractors, excluding Visitors, may be granted unescorted access to devices used by the site for electronic access control per CIP-003 or to other areas that contain BES Cyber Systems.

Visitors will, upon arrival:

- check in with appropriate plant personnel.
- be instructed on Greasewood's physical access requirements.

Note: Visitors are restricted from entering secure BES Cyber Asset rooms/areas unless being continuously escorted. During emergency scenarios, unescorted access permissions may be granted to Visitor(s) based on safety needs. (See Cyber Security Incident Response Plan for emergency response and CIP Exceptional Circumstance guidance)

Primary and Ancillary Physical Security Controls

Greasewood maintains the following primary physical controls:

Control	Description
Perimeter Fencing	6' Cattle fencing and 6' barbed wire topped fence around substation.

Additional defense-in-depth security controls include:

Control	Description
Hard Keys	Physical keys are used to provide an additional level of security and prevent unauthorized access to and/or within the facility

Perimeter Fencing

- Fencing is 6 feet tall, topped with barbed wire, surrounding all sides of the facility.
- There is multiple gate access points, each with key controlled access.
- All perimeter fencing is inspected as part of periodic walk down conducted by plant personnel. Plant personnel check to make sure that the fence is in good working condition and no damage, tampering, attempted subversion, or unauthorized access has occurred.

Any damage, tampering, attempted subversion, or unauthorized access to the perimeter fencing identified during the walk down is to be reported to the control room/facility management. (See FRM-Physical Security Incident Investigation)

Hard Key Management

- Distribution of hard keys and the employees and/or contractors responsible for those keys are managed in a dedicated repository.
- Hard keys are collected upon termination of employment or upon a determination that the employee or contractor no longer needs unescorted access to the facility (e.g., retirement, termination, job transfer).
- The employee and/or contractor to whom the key is assigned holds the ultimate responsibility for the key.
- Lost keys must be immediately reported to the control room or Operations Manager.
- Plant personnel utilize a logbook for checking out/checking in keys whenever a physical key is needed to perform work at the facility.
- The following areas are secured via hard keys:
    - Perimeter fence gates
    - Control house

5. Glossary of Terms

Bulk Electric System (BES)
See NERC "Glossary of Terms Used in NERC Reliability Standards" definition.

BES Cyber Asset (BCA)
A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

BES Cyber System (BCS)
One or more BES Cyber Asset logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

CIP Exceptional Circumstance
A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large-scale workforce availability.

CIP Senior Manager
A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Cyber Asset
Programmable electronic devices, including the hardware, software, and data in those devices.

Removable Media
Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact discs, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Transient Cyber Asset (TCA)
A Cyber Asset that:

a. is capable of transmitting or transferring executable code,
b. is not included in a BES Cyber System,
c. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
d. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
    a. BES Cyber Asset,
    b. network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
    c. PCA associated with high or medium impact BES Cyber Systems.
e. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

NERC Glossary of Terms
https://www.nerc.com/files/glossary_of_terms.pdf

12. Reference Documents

FRM-Physical Security Incident Investigation
Cyber Security Incident Response Plan

Annex W - Weather Related Emergencies Plan

12/XX/2023

Preparations for Operations During Extreme Cold Weather Conditions

For severe cold weather, Greasewood Solar II shall will identify, through inspection, areas of the generating facility that may be most vulnerable to malfunction during extreme cold events. This inspection shall be conducted prior to the filing requirements for ERCOT and the PUCT, and will be logged in the Greasewood Solar II-PGCEOP-1.0 Weather Inspection Worksheet. Greasewood Solar II staff shall ensure the following:

- Greasewood Solar II staff will ensure heat tracing is present and functional for all appropriate exposed instrumentation and/or equipment, where applicable.
- Where appropriate and necessary, temporary barriers shall be erected to shield sensitive or exposed equipment and instrumentation from wind and freezing precipitation.
- Temporary barriers may be constructed of plastic sheeting or other material that is sufficient to protect exposed equipment and instrumentation, and may contain, if conditions warrant, a portable heat source to keep temperatures above freezing in the designated area.
- Other measures may be taken, as the generation facility staff see fit, to protect the facility during an extreme cold weather event.

Preparations for Operations During Extreme Hot Weather Conditions

For extreme hot weather, Greasewood Solar II staff shall ensure the following:

- Proper ventilation is present and functional for any areas where extreme hot temperatures may negatively impact generator output.
- In addition to this, portable fans may be mobilized to force air around potentially affected areas.

In all cases, Greasewood Solar II staff will ensure that any substation or switchyard equipment that it owns is properly weatherized. This includes the following:

- Ensuring all breaker and transformer oil levels, SF6 levels, nitrogen levels, and air compressor tank levels are adequate for that equipment manufacturer and model.
- Heaters in breaker and transformer cabinets are functioning properly.
- Adequate supply of spare gas and oil is available to be used during an emergency.
- Tracking mechanisms are operational.

It is important, after any weather-related emergency, to analyze the performance of the generating plant, identify any equipment failures that

occurred (if any), and develop and action plan to address those issues. These issues may include the following:

- A list of equipment that failed during the last cold or hot weather event must be identified and addressed. Additionally, any critical failure points identified must be tracked through the normal maintenance processes to ensure appropriate maintenance has taken place for the identified equipment. Any facility equipment design limits that could limit generator output must be identified and addressed, to the extent possible, to ensure no interruption of operations occurs during an extreme weather event.
- Greasewood Solar II staff shall actively monitor all potential extreme weather events that may affect their facilities, to include sever weather and operational circumstances arising from those events. Greasewood Solar II staff will continue monitoring weather forecasts and ERCOT operational data aid in predicting conditions on the BES that may impact operations.
- It is imperative to ensure entry and egress routes are hardened to the extent possible. Make sure to elevate and/or secure equipment that may be subject to being carried away by flood currents, and ensure cabinets, control house, and other fixed structures are weatherproofed to extent possible.

The following individuals are responsible for maintaining, implementing, and revising the Weather-Related Emergencies Plan.

Name	Title	Permission(s)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to the Plan since the initial Weather-Related Emergencies Plan adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0	12/XX/2023	12/XX/2023	Weather-Related Emergencies Plan

As of 12/XX/2023, Weather Related Emergencies Plan Version 1.0, approved on 12/XX/2023, supersedes all previous Weather-Related Emergencies Plan.

This Plan is designed to identify Greasewood Solar II's weather critical components, which may lead to a downgrade of operations, should the component fail due to extreme weather conditions. Each year, by December 1st, the measures and steps, outlined in this plan, must be completed.

Identifying Greasewood Solar II's weather critical components, as defined by the Public Utility Council of Texas

This methodology's approach will focus on identifying components that are susceptible to failure during weather emergencies and assessing how such failures could significantly impact the solar plant's operations. Once the Weather Critical Components are identified, the list can be used to prove identification of Generator Cold Weather Critical Components, to satisfy compliance for requirements contained in NERC Reliability Standard EOP-012.

Complete the "Critical Components List" tab of the *Greasewood Solar II-Winterization Checklist-PUCT SR 25.55* document.

1. **Component Identification and Inventory**

- **Inventory Creation** - Compile a comprehensive inventory of all components in the solar generating plant, including the following equipment:
    - Solar panels
    - Batteries
    - Inverters
    - Transformers
    - Wiring systems
    - Control systems
    - Support structures
- **Categorization** - Categorize and rank (by criticality) components based on the following criteria:
    - Function
    - Location
    - Importance to the overall operation of the plant

2. **Vulnerability Assessment**

- **Weather Risk Analysis** - Conduct a thorough analysis of local weather patterns and historical weather data to understand potential weather emergencies (e.g., hailstorms, extreme temperatures, high winds, heavy snowfall). Monitor the ERCOT ISO website for any alerts or warnings regarding availability of generation and imminent weather conditions.

3. **Component Susceptibility Evaluation**

- **Assessment** - Assess each component's susceptibility to weather-related damage or failure. This will involve reviewing the following:
    - Manufacturer data
    - Inspection of equipment
        - Insulation
        - Heat Trace
        - Barriers for wind
        - Breaker and transformer cabinet heaters
        - Breaker and transformer cabinet weatherproofing

- SF6 gas (where applicable)
- Transformer oil and nitrogen levels & spare oil and nitrogen (where applicable)

- Historical performance data

4. **Impact Analysis**

   Failure Mode Analysis - For each susceptible component, determine the modes of failure that could occur during a weather emergency, to include the following:
   - Physical damage
   - Overheating
   - Electrical failure

   Operational Impact Assessment - Evaluate how the failure of each component would impact the plant's operations, focusing on the likelihood of a trip, derating, failure to start, or other significant operational hindrances.

5. **Criticality Ranking**

   Ranking Components - Based on the vulnerability and impact analysis, rank components in terms of criticality. Based on categorization and prioritization, identify the most critical components, which are those whose failure would most significantly hinder the plant's operation or reduce its output by more than five percent (5%).

6. **Mitigation Strategy Development**

   Preventative Maintenance – During the regularly scheduled maintenance activities for equipment at the site, specifically address the vulnerabilities of critical components, as identified in the Component Identification and Inventory activities, as described in Section 1.
   Mitigation Measures - Implement mitigation measures such as physical protections, redundant systems, or weatherproofing to reduce the risk of failure during weather emergencies.

7. **Emergency Response Planning**

   Response Procedures - Develop emergency response procedures to address failures of critical components during weather emergencies. This should include rapid repair and replacement strategies.
   Training and Drills - Train staff on the site's Emergency Operations Plan and conduct regular drills to ensure preparedness. This is required in PUCT §25.53.

8. **Review and Improvement**

   Data Collection and Analysis - Continuously collect data on component performance and failure rates, especially during and after weather events.
   Review and Update - Regularly review and update the assessment of weather critical components based on new data, changes in weather patterns, and technological advancements.

9. **Documentation and Compliance**

   Documentation - Maintain thorough documentation of all steps taken, including assessments, decisions made, and actions implemented. This is done by completing the site's Emergency Operations Plan.
   Regulatory Compliance – Retain all evidence of drills, training, inspections, etc., in order to prove compliance with PUCT §25.53 and §25.55.

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

Name	Title	Permission(s)
Zahi Harel	Managing Director, US	Maintain/Implement
Dikla Fhima	VP, Engineering and Projects	Maintain/Implement
JC Culberson	EPE - Director of NERC and Regulatory Compliance	Revise

- provides a revision control summary that lists the dates of each change made to the Weatherization Plan since the initial EOP Drill Instructions adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0a	12/XX/2023	12/XX/2023	Weatherization Plan

As of 12/XX/2023, EOP Version 1.0, approved on 12/XX/2023, supersedes all previous Weatherization Plan.

The following files are not convertible:

Greasewood Solar II-Winterization Checklist-PUCT SR25.55.xlsx

Please see the ZIP file for this Filing on the PUC Interchange in order to access these files.

Contact centralrecords@puc.texas.gov if you have any questions.