d. VERIFY lube oil filter differential pressure is less than 15 psid. SHIFT filters if necessary or if faulty D/P indication is suspected.

e. If the cause of the abnormal temperature indication is not readily identified and lube oil pressure is within the normal range, REDUCE turbine load in order to limit heat input to bearing(s). Monitor temperatures. If temperatures continue to increase, completely unload the turbine. Shut down the unit and correct the problem as necessary.

f. Return unit to service as soon as possible.

ac NAES	RELIABILITY COMPLIANCE MANUAL	
Reference Organization: **NERC**	**Quail Run Energy Center**	
Reference Standard Name: **Cyber Security - Security Management Controls**		
Reference Standard Number: **CIP-003-8**	Reliability Compliance Manual Procedure Number: **RCP-NERC-CIP-003-8**	
Approved for Use by:	Current Issue: **Rev. 2**	Issue Date: **March 28, 2022**

1. INTRODUCTION

This Reliability Compliance Procedure is intended to address the Requirements of **Generator Owners** and **Generator Operators** only. Refer to the Standard referenced below for additional Requirements related to all other Entities, as well as the Measures of Compliance, Monitoring of Compliance and Levels of Non-compliance applicable to all Entities.

Reference Organization: NERC
Reference Standard Title: Cyber Security - Security Management Controls
Reference Standard No.: CIP-003
Standard Effective Date: July 1, 2016

CIP-003, Requirement 2:
- April 1, 2017
- Att 1, Section 1:
  - April 1, 2017
- Att 1, Section 2:
  - January 1, 2020
- Att 1, Section 3:
  - January 1, 2020
- Att 1, Section 4:
  - April 1, 2017
- Att 1, Section 5:
  - January 1, 2020
- Att 1, Section 5.2.2:
  - April 1, 2020

Other Reference Documents:
RCP-NAES-GEN-001 - Reliability Compliance Program Guide

Procedure Attachments:
RCP-NERC-CIP-003-ATT-A-Cyber Security Policy
RCP-NERC-CIP-003-ATT-B-Cyber Security Awareness
RCP-NERC-CIP-003-ATT-C-Physical Security Controls
RCP-NERC-CIP-003-ATT-D-Electronic Access Controls
RCP-NERC-CIP-003-ATT-E-Cyber Security Incident Response Plan
RCP-NERC-CIP-003-ATT-F-Cyber Security Incident Attestation Form
RCP-NERC-CIP-003-ATT-G-CSIRP Test and Review
RCP-NERC-CIP-003-ATT-H-Leadership
RCP-NERC-CIP-003-ATT-I-Access Control List
RCP-NERC-CIP-003-ATT-J-TCA & RM Plan
RCP-NERC-CIP-003-ATT-K-TCA-RM Form
RCP-NERC-CIP-003-ATT-L-CIP Exceptional Circumstances
RCP-NERC-CIP-003-ATT-M-CIP Exceptional Circumstances Form

2. PURPOSE:

To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber System against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

3. APPLICABILITY:

Functional Entities:

For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

Balancing Authority

Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

- is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
- performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

Reliability Coordinator	ERCOT
Balancing Authority	ERCOT
Transmission Owner	Oncor
Transmission Operator	Oncor
Generator Owner	Quail Run Energy Partners, LP
Generator Operator	**NAES Corporation - Quail Run Energy Center**

Facilities:
For the purpose of the requirements contained herein, the following Facilities, systems and equipment owned by each Responsible Entity listed below are those to which these requirements are applicable. For requirements in this standard where specified type of Facilities, systems, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly below.

Distribution Provider
One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES.

Each UFLS or UVLS System that:

- is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

- performs automatic Load shedding under a common control system owned by the Responsibility Entity, without human operator initiation, of 300 MW or more.

Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

Each Protection System (Excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

Each Cranking Path and group of Elements meeting the initial switching requirements from Blackstart Resources up to and including the first interconnecting point of the starting station service of the next generation unit(s) to be started.

Responsible Entities listed other than Distribution Providers:
All BES Facilities.

Exemptions:
The following are exempt from Standard CIP-003-7:

Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

For Distribution Providers, the systems and equipment that are not included above.

4. RESPONSIBILITIES:

Procedure Review and Approval: The Plant Manager is responsible for the review and approval of this procedure.

Procedure Implementation: The Compliance Manager is responsible for implementing this procedure.

Procedure Compliance: All Plant Personnel are responsible for complying with this procedure.

5. REQUIREMENTS

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004);

1.1.2 Electronic Security Perimeter (CIP-005) including Interactive Remote Access;

1.1.3 Physical security of BES Cyber Systems (CIP-006);

1.1.4 System security management (CIP-007);

1.1.5 Incident reporting and response planning (CIP-008);

1.1.6 Recovery plans for BES Cyber Systems (CIP-009);

1.1.7 Configuration change management and vulnerability assessments (CIP-010);

1.1.8 Information protection (CIP-011); and

1.1.9 Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness;

1.2.2 Physical security controls;

1.2.3 Electronic access controls;

1.2.4 Cyber Security Incident response

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances. Requirement Actions and Documentation

The **Generator Owner** and **Generator Operator** at Quail Run Energy Center has not identified any High or Medium Impact BES Cyber Systems and therefore requirements 1.1-1.1.9 are not applicable at this time.

The Generator Owner and Generator Operator at Quail Run Energy Center has a Cyber Security Policy documented as RCP-NERC-CIP-003-ATT-A.

The Cyber Security Policy collectively addresses cyber security awareness, physical security controls, electronic access controls and dial-up connectivity, Cyber Security Incident response, Transient Cyber Assets and Removable Media malicious code risk mitigation, and declaring and responding to CIP Exceptional Circumstances. (M1)

The Cyber Security Policy for Quail Run Energy Center's low impact facilities shall be reviewed and approved by the CIP Senior Manager at least once every fifteen (15) calendar months.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber

security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

REQUIREMENT ACTIONS AND DOCUMENTATION

The **Generator Owner and Generator Operator** at Quail Run Energy Center has documented and implemented a plan for each section in CIP-003, R2, Attachment 1, including:

RCP-NERC-CIP-003-ATT-B - Cyber Security Awareness Plan that reinforces cyber security practices at least once every fifteen (15) calendar months.

RCP-NERC-CIP-003-ATT-C - Physical Security Controls Plan that requires granting of access to locations of the low impact BES Cyber Systems within Quail Run Energy Center and the low impact BES Cyber System electronic access control devices are based on need by personnel role. Visitors to Quail Run Energy Center are granted temporary access at the main gate by personnel in the control room or administration office. (Ref: Section 2 of CIP-003 – Attachments 1 & 2)

RCP-NERC-CIP-003-ATT-D - Electronic Access Controls Plan, that addresses all bi-directional routable protocol access that enters or leaves Quail Run Energy Center and the need for such access. Cyber Assets used in the access control shall deny access by default for inbound and outbound traffic. Quail Run Energy Center deems bi-directional routable protocol access that is needed for normal and emergency operation as necessary. Quail Run Energy Center does not have any Dial-up connectivity to Low Impact BES Cyber Systems. (Ref: Section 3 of CIP-003 – Attachments 1 & 2)

The Cyber Security Incident Response Plan - RCP-NERC-CIP-003-ATT-E includes: identification, classification and response to Cyber Security Incidents, roles and responsibilities, subsequent notification to Electricity Sector Information Sharing and Analysis Center (E-ISAC), testing the Cyber Security Incident response plan, and updating the Cyber Security Incident Response Plan(s), as needed. (Ref: Section 4 of CIP-003 – Attachments 1 & 2)

Exercise of the Cyber Security Incident Response Plan is documented in RCP-NERC-CIP-003-ATT-G (CSIRP Test and Review).

RCP-NERC-CIP-003-ATT-F - Cyber Security Incident Attestation Form which can be filled out annually indicates that there were no Cyber Security Incidents during that period. Each completed RCP-NERC-CIP-003-ATT-F shall be retained for the duration of the audit period.

Transient Cyber Assets and Removable Media malicious code risk mitigation - RCP-NERC-CIP-003-ATT-J identifies mitigating measures that reduces the risk of the introduction of malicious code to low impact BES Cyber Systems. Quail Run Energy Center shall complete RCP-NERC-CIP-003-ATT-K-TCA-RM Form prior to allowing any TCA or RM use on a BES Cyber System. (Ref: Section 5 of CIP-003 – Attachments 1 & 2)

R3. Each **Responsible Entity** shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.

REQUIREMENT ACTIONS AND DOCUMENTATION

The **Generator Owner** and **Generator Operator** at Quail Run Energy Center has identified a CIP Senior Manager by name with overall responsibility for leading and managing the implementation of, and adherence to, Standards CIP-002 through CIP-011. The CIP Senior Manager or delegate authorized is documented in RCP-NERC-CIP-003-ATT-H. Changes to the CIP Senior Manager shall be documented within thirty (30) calendar days of the effective change by using this same document. (M3)

R4. The **Responsible Entity** shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

REQUIREMENT ACTIONS AND DOCUMENTATION

The **Generator Owner** and **Generation Operator** at Quail Run Energy Center has implemented a process to delegate authority documented in RCP-NERC-CIP-003-ATT-H. Where allowed by the CIP Standards, the CIP Senior Manager has delegated authority for specific actions to delegates documented in RCP-NERC-CIP-003-ATT-H. The delegates are identified by name or title, date of designation and approved by the CIP Senior Manager. Changes to the delegation shall be documented within thirty (30) days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. (M4)

6. PROCEDURE

Refer to referenced attachments for quail run's cybersecurity and physical security policies to address each of the requirements by the NERC standard

7. REGIONAL DIFFERENCES

None identified.

Latest Revision Approval:

Written By: NAES Corp Date: 1/21/2020

Approved By: Andy Duncan Date: 3/28/2022

REVISION HISTORY LOG RCP-NERC-CIP-003				
Rev.	Date	Description	By Initials	Approval Initials
0	3/25/2020	Updated CIP-003-7 to CIP-003-8	MJS	AD
1	3/5/2021	Annual review	ECN	AD
2	3/24/2022	Annual Review	ECN	AD
3				

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or

- Other method(s) to mitigate the introduction of malicious code.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:

a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and

b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus

update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

CYBER SECURITY POLICY

CYBER SECURITY POLICY

1. INTRODUCTION

A. PURPOSE

The purpose of this document is to specify consistent and sustainable security policies that establish responsibility and accountability to protect Quail Run Energy Center's Low Impact BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

B. SCOPE

CIP-003 R1.2 applies to Quail Run Energy Center as an entity with Low Impact BES Cyber Systems which may have External Routable Connectivity and Electronic Access Point Cyber Assets. Quail Run Energy Center does not have any Medium or High Impact BES Cyber Systems.

C. DEFINITIONS AND DEFINED TERMS

Capitalized terms included in this policy statement are defined in the NERC *Glossary of Terms Used in NERC Reliability Standards*, which is periodically updated, or are listed below in this section as Quail Run Energy Center specific terms. The most current version of the Glossary can be accessed by clicking the following link:

http://www.nerc.com/pa/Stand/Glossary of Terms/Glossary_of_Terms.pdf

2. POLICY STATEMENTS

A. GENERAL

Low Impact BES Cyber Security configurations, plans, programs, processes, and procedures shall comply with all existing Quail Run Energy Center policies and standards as well as the NERC Reliability Standards CIP-002 & CIP-003 (i.e. "the Standards"). Where there is a conflict, the NERC Reliability Standards shall prevail.

Quail Run Energy Center shall have a documented "CIP Senior Manager" responsible for ensuring the organization is meeting the requirements of the Standards and of this Policy. The CIP Senior Manager shall be appointed in accordance with CIP-003 R3.

Where reviews and approvals are required, the CIP Senior Manager or delegate(s) shall determine the appropriate level of management if not specified in the Standards.

B. VIOLATION OF POLICY

An employee found to have intentionally violated any part of this policy document shall be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor, or vendor may result in the termination of their contract or assignment with Quail Run Energy Center.

C. CYBER SECURITY AWARENESS (ATT 1, SECTION 1 OF THE STANDARD)

Cyber Security practices shall be reinforced at least once every 15 calendar months (which may include associated physical security practices). Reinforcement may occur through direct or indirect communications such as emails, system wide publications, intranet postings and at various meetings and training modules. The evidence could be documentation through one or more of the following methods:

1. Direct communications (for example, e-mails, memos, or computer-based training);

2. Indirect communications (for example, posters, intranet, or brochures); or

3. Management support and reinforcement (for example, presentations or meetings).

Quail Run Energy Center shall ensure that any employee, contractor, or vendor, who has a need for physical and/or electronic access to a Low Impact BES Cyber System be subject to the Cyber Security Awareness Program.

See RCP-NERC-CIP-003-ATT-B Cyber Security Awareness for Quail Run's Procedure on Cyber Security Awareness.

D. PHYSICAL SECURITY CONTROLS (ATT 1, SECTION 2)

The Physical Security plan will be based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented to comply with Section 3.1 of CIP-003, Attachment 1, if any.

Quail Run Energy Center shall control physical access in accordance with its Physical Security Controls plan documented in RCP-NERC-CIP-003-ATT-C Physical Security Controls.

E. ELECTRONIC ACCESS CONTROLS (ATT 1, SECTION 3)

All low impact External Routable Connectivity shall be through an identified low impact Electronic Access Point and restricted to only the communication with a need. Access to or through the Electronic Access Point device shall only be granted to those employees, contractors, or vendors who have a need for access.

For each low impact Electronic Access Point, inbound and outbound access shall be documented with reason for access and deny all other access by default. This is for any communications that are:

1. Between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

2. Using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

3. Not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Dial-up connectivity is prohibited within Quail Run Energy Center's BES Cyber Systems. In the event dial-up connectivity to a Low Impact BES Cyber System is permitted, per Cyber Asset capability shall be set to one of the following:

Dial out only (no auto-answer) to a preprogrammed number to deliver data.

1. Incoming Dial-up Connectivity is configured to dial back.

2. A modem that must be remotely controlled by the control center or control room.

3. The low impact BES Cyber System that includes the Dial-up devices enforces authentication.

4. See RCP-NERC-CIP-003-ATT-D Electronic Access Controls

RCP-NERC-CIP-003-ATT-I Access Control List

NOTE:
Quail Run Energy Center prohibits dial-up connections of any kind.

F. CYBER SECURITY INCIDENT RESPONSE (ATT 1, SECTION 4)

Quail Run Energy Center shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

1. Identification, classification, and response to Cyber Security Incidents;

2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

3. Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4. Incident handling for Cyber Security Incidents;

5. Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by:

   a. Responding to an actual reportable Cyber Security Incident;

   b. Using a drill or tabletop exercise of a Reportable Cyber Security Incident; or

   c. Using an operational exercise of a Reportable Cyber Security Incident; and

6. Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident. Quail Run Energy Center shall invoke its Cyber Security Incident Response Plan to rapidly detect incidents to minimize loss and destruction, mitigate exploited weaknesses, restore computing services, and identify and report Cyber Security Incidents to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law.

7. See RCP-NERC-CIP-003-ATT-E CSI Response Plan

   RCP-NERC-CIP-003-ATT-F CSI Response Attestation Form

   RCP-NERC-CIP-003-ATT-G CSI Evaluation Form

G. CIP SENIOR MANAGER DELEGATE

The formal assignment and duty of a CIP Senior Manager delegate is limited to the review and approval of RCP-NERC-CIP-002-ATT-A BES Cyber System Identification that identifies the Low Impact facility location(s) at least once every 15 months, as permitted by CIP-002-5.1a, Requirement 2.2.

Changes to the CIP Senior Manager shall be documented within thirty (30) calendar days of the effective date of the change.

QUAIL RUN'S CIP SENIOR MANAGER IS DOCUMENTED IN RCP-NERC-CIP-003-ATT-H

H. TRANSIENT CYBER ASSET AND REMOVABLE MEDIA (ATT 1 SECTION 5)

Quail Run Energy Center shall maintain processes for appropriate use of Transient Cyber Assets (TCAs) and Removable Media to prevent unauthorized access or malware propagation to BCSs; and prevent unauthorized access to BCS Information.

All TCAs managed by Quail Run Energy Center shall require use and documentation of one or more of the following safeguards in an ongoing or on-demand manner per TCA capability:

1. Antivirus software, including manual or managed updates of signatures or patterns;

2. Application whitelisting; or

3. Other method(s) to mitigate the introduction of malicious code.

All TCAs **not** managed by Quail Run Energy Center shall use of one or more of the following safeguards which must be documented and reviewed by the System Administrator prior to allowing connection of the TCA to a BCS:

1. Antivirus update level;

2. Antivirus update process used;

3. Application whitelisting;

4. Use of live operating system and software executable only from read-only media;

5. System hardening used;

6. Other method(s) to mitigate the introduction of malicious code.

Quail Run Energy Center shall require documentation and use of method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BCS; and documentation and mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a BES Cyber System.

Quail Run's TCA & RM plan is maintained in RCP-NERC-CIP-003-ATT-J TCA & RM plan. Documentation is maintained IAW RCP-NERC-CIP-003-ATT-K TCA & RM Form

I. DECLARING AND RESPONDING TO CIP EXCEPTIONAL CIRCUMSTANCES

Quail Run Energy Center's CIP Senior Manager or delegate shall have the authority to declare CIP Exceptional Circumstances when it cannot conform to this Policy.

Quail Run Energy Center shall document an explanation as to why the exception is necessary and any compensating measures authorized by the CIP Senior Manager or delegate.

J. CIP EXCEPTIONAL CIRCUMSTANCES

The NERC Glossary of Terms defines a CIP Exceptional Circumstance as

"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."

Refer to the following attachments for instructions on declaring an exceptional circumstance and associated requirements.

RCP-NERC-CIP-003-ATT-L-CIP Exceptional Circumstances

RCP-NERC-CIP-003-ATT-M-CIP Exceptional Circumstances Form

3. REVIEW

This policy shall be updated as needed or when the Standards addressed by this policy are modified.

4. POLICY RESPONSIBILITY

The CIP Senior Manager shall review and approve the Cyber Security Policy at least once every fifteen (15) calendar months.

Andy Duncan
CIP Senior Manager Signature

3/30/22
Date

CYBER SECURITY POLICY

Latest Revision Approval:

Written By: NAES Corp Date: 2/15/2019

Approved By: Andy Duncan Date: 3/24/2022

REVISION HISTORY LOG RCP-NERC-CIP-003-ATT-A				
Rev.	Date	Description	By Initials	Approval Initials
0	<Month DD, YEAR>	Revised to make policy statements supportive of CIP-003-7 implementation.	MJS	
1	03/08/2019	Adopted for Plant Use	WC	SR
2	3/25/2020	Removed reference to CIP-003 version 7 in Section 2 paragraph D	NC	AD
3	3/31/2021	Annual review.	ECN	AD
4	3/28/2022	Annual Review. Minor edits to refer to attachments for each applicable section	ECN	AD

CYBER SECURITY AWARENESS

CYBER SECURITY AWARENESS

1. INTRODUCTION

A. PURPOSE

This document defines Quail Run Energy Center's Cyber Security Awareness program. The purpose of this program is to ensure that Quail Run Energy Center's personnel with physical and/or electronic access to Low Impact BES Cyber Systems receive on-going reinforcement in sound security practices. Quail Run Energy Center shall provide this reinforcement, at least once every fifteen (15) calendar months.

B. SCOPE

CIP-003 R2 applies to Quail Run Energy Center as an entity with Low Impact BES Cyber Systems. Quail Run Energy Center does not have any Medium or High-Impact BES Cyber Systems.

C. DEFINED TERMS

Capitalized terms included in this policy statement are defined in the NERC Glossary of Terms Used in NERC Reliability Standards, which is periodically updated, or are listed below in this section as Quail Run Energy Center specific terms. The most current version of the Glossary can be accessed by clicking the following link:

http://www.nerc.com/pa/Stand/Glossary of Terms/Glossary_of_Terms.pdf

2. AWARENESS PROGRAM

For Quail Run Energy Center to appropriately protect the confidentiality, integrity, and availability of its assets, it must ensure that personnel receive reinforcement of cyber security practices at least once every fifteen (15) calendar months or more frequently.

Quail Run Energy Center shall provide periodic awareness information to plant employees and contractors with access to BES Cyber Assets through one or more of the following methods:

1. Emails or bulletins with information on current events and security news.
2. Posted informational signs that focus on cyber security. Signs will include the use of posters reminding staff of the need for cyber security as they carry out their daily activities.
3. Brief security awareness topics covered during staff or other types of meetings.
4. Scheduled informal meetings to discuss computer and network security for home and office systems. The topics may include, but are not limited to, the awareness topics in the following table:
5. Other methods as appropriate

Sample Cyber Security Awareness Topics
Classified material identification and handling

CYBER SECURITY AWARENESS

Sample Cyber Security Awareness Topics
Password use and management—including creation, frequency of changes, and protection
Internet safety and security risks (Unknown e-mail/attachments, spam, phishing)
Protection of personal information and social engineering
Desktop security—use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems
Use of encryption and the transmission of sensitive/confidential BES Cyber System Information over the Internet - corporate security policy, procedures, and technical contact for assistance
Secure Transient Cyber Asset and Removable Media use
Web usage—allowed versus prohibited; monitoring of user activity
Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions
Visitor control and physical access to spaces—applicable physical security policy and procedures, e.g., challenging strangers, tailgating, reporting unusual activity
Appropriate use of personal devices (smart phones, tablets, etc…) both physical and wireless security issues
Laptop security while on travel—both physical and information security issues

Evidence of all distributed awareness materials shall be kept for the duration of the audit period. The evidence could be documentation through one or more of the following methods:

1. Direct communications (for example, e-mails, memos, or computer-based training);
2. Indirect communications (for example, posters, intranet, or brochures); or
3. Management support and reinforcement (for example, presentations or meetings).

3. REVIEWS AND UPDATES

This program shall be reviewed and updated as needed and upon the approval of any new versions of the CIP Standards.

4. PROGRAM RESPONSIBILITY

The CIP Senior Manager is responsible for this program and for saving the evidence that awareness materials were distributed.

CYBER SECURITY AWARENESS

Latest Revision Approval: (Revision History)

Written By: NAES Corporation Date: 2/15/2019

Approved By: Andy Duncan Date: March 29, 2022

REVISION HISTORY LOG
RCP-NERC-CIP-003-ATT-B

Rev.	Date	Description	By Initials	Approval Initials
0	<Month DD, YEAR>	Updated RCP language for clarity	MJS	
1	03/11/2019	Updated for Plant Use	WC	SR
2	3/31/2021	Annual Review	ECN	ACD
3	3/29/2022	Annual Review	ECN	ACD

RCP-NERC-CIP-003-ATT-C
QUAIL RUN ENERGY CENTER - ODESSA, TX

Referencing Documents:	Revision: Rev 3
NERC-CIP-003	Revision Date: March 29, 2022

PHYSICAL SECURITY CONTROLS

PHYSICAL SECURITY CONTROLS

1. INTRODUCTION

A. PURPOSE

This document defines Quail Run Energy Center's Physical Security Controls program. The purpose of this program is to ensure that Quail Run Energy Center's Low Impact BES Cyber Systems have adequate physical security controls.

B. SCOPE

CIP-003 R2 applies to Quail Run Energy Center as an entity with Low Impact BES Cyber Systems. Quail Run Energy Center does not have any Medium or High Impact BES Cyber Systems. Quail Run Energy Center shall control physical access, based on need as determined by the plant, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for CIP-003-8 R2, Attachment 1, Section 2, if any.

C. DEFINED TERMS

Capitalized terms included in this policy statement are defined in the NERC Glossary of Terms Used in NERC Reliability Standards, which is periodically updated, or are listed below in this section as Quail Run Energy Center specific terms. The most current version of the Glossary can be accessed by clicking the following link:

http://www.nerc.com/pa/Stand/Glossary of Terms/Glossary_of_Terms.pdf

2. CONTROLLING PHYSICAL ACCESS

Quail Run Energy Center has defined a number of operational and procedural controls to restrict physical access to the Quail Run Energy Center's perimeter and Low Impact Electronic Access Point(s), if any. Additional physical security controls may protect the immediate area surrounding the Low Impact BES Cyber Systems (LIBCS).

A. PHYSICAL ACCESS CONTROLS & MONITORING

Quail Run Energy Center has implemented physical access controls at the access point into each physical security area and the protected locations housing the physical access control system. The access controls consist of:

- Approximately 6' cyclone fencing with three rung barbed wire surrounds the facility. The facility's access gates are locked.
- Card Readers are used on site. The card is issued to active employees. The card is revoked upon termination of employment at the facility.

[redacted]

- Access controlled at the main entry gate by a card reader and call box. Employees with a valid card may open the gate, while visitors must request entry from the control room. The Control Room Operator ensures access is needed and has visual capability of the gate. Once inside the facility, the person signs the visitor's log which is located in the Administration Building and signs out when departing the facility.
- All visitors performing work have a site sponsor and they are issued a work permit which is approved by the CRO. This tracks the work and the visitors onsite (the permit lists the work crew and their supervisor).
- The control room is manned around the clock and maintains visual contact of all equipment in the control room.

B. PROCEDURES FOR GRANTING AND REVOKING PHYSICAL ACCESS

Granting Access

Physical access to Low Impact BES Cyber Systems and Electronic Access Points are granted by the CIP Senior Manager based on need. Quail Run Energy Center shall retain evidence that access is controlled per this procedure. Examples of evidence may include, but are not limited to, access lists, forms documenting access requests/revocations, periodic reviews, etc.

Identified Roles Requiring Access:

- Operating personnel require access to the asset in order to ensure proper operation of the facility.
- Plant management staff including engineers, require access to supervise plant employees.
- Technicians require access to ensure proper operation and maintenance of the facility.
- Asset Managers – require access to ensure Assets are maintained to the Asset owner's satisfaction and ensure proper operation and management decisions.
- Project Managers – ensure that the plant staff are maintaining the asset per contract requirements.
- Plant Admin Staff – while these employees do not need access to BES Cyber Systems, they ensure plant payroll and other essential paperwork is completed including accounts payable and billing and need access to the Plant Facility.
- Contractors – are granted plant access via the main gate. They must confirm their identity prior to entry. Contractors are then given an orientation which includes instructions not to operate any equipment without a plant operator present. Entry into areas such as switch rooms requires specific permission from the Control Room Operator.
- Other positions as dictated by plant needs.

Temporary Access

Other positions as dictated by plant needs may include:

- Delivery Personnel/contractors - Control Room Operators are authorized to grant temporary plant access via the main gate. The contractor must confirm their purpose and identity prior to entry, including the plant personnel who will be their escort while on site. The contractor shall proceed to the administration building to sign in and out, noting the date, time, and name of Quail Run Energy Center.
- Visitors - Control Room Operators are authorized to grant temporary plant access via the main gate. The visitor must identify plant personnel they are visiting and who will be their escort while on-site. The visitor shall be instructed to proceed to the administration building to sign in and out on the visitors' log. The visitors' log will document each visitor's name, point of contact/ escort, time of initial entry and time of last exit of the day.

Revoking Access

Access shall be removed due to any of the following events, as appropriate: termination of employees, contract termination, transfer of duties, extended leaves of absence, or change in contract personnel. Revocation will also occur for any individuals who are deemed to no longer require access to LIBCS.

All access shall be revoked as soon as practical when it is determined that access is no longer required. Possible methods to remove access include:

- Removing access in card-control system
- Change of padlock combinations
- Obtain plant ID, physical keys and fobs
- Removing electronic access in electronic access control or other firewall devices &/or by changing of user or shared account passwords and collecting fobs.

3. INTERNAL CONTROLS/EVIDENCE

Quail Run Energy Center has implemented the following, additional physical security controls:

- Operators check the locked access gate twice a day as part of the plant required rounds therefore ensuring the facility remains secured.

- The Administrative Building/Control Room is locked after hours and accessible by card readers. The facility's security system activates automatically locking the doors at approximately 1700 and remain locked until approximately 0600 the next morning.

[redacted]

PHYSICAL SECURITY CONTROLS

4. REVIEWS AND UPDATES

This program shall be reviewed and updated as needed and upon the approval of any new versions of the CIP Standards.

5. PROGRAM RESPONSIBILITY

The Quail Run Energy Center's CIP Senior Manager is the responsible person for this program and shall approve revisions.

PHYSICAL SECURITY CONTROLS

Latest Revision Approval: (Revision History)

Written By: NAES Corp Date: 2/15/2019

Approved By: Andy Duncan Date: March 29, 2022

REVISION HISTORY LOG
RCP-NERC-CIP-003-ATT-C

Rev.	Date	Description	By Initials	Approval Initials
0	<Month DD, YEAR>	Updated for CIP-003-7 and added Internal Controls Section	MJS	
1	03/11/2019	Updated for Plant Use	WC	SR
2	3/31/2021	Annual Review	ECN	ACD
3	3/29/2022	Annual Review	ECN	ACD

CYBER SECURITY INCIDENT RESPONSE PLAN

Contents

CYBER SECURITY INCIDENT RESPONSE PLAN

1. INTRODUCTION

A. PURPOSE

This plan addresses the actions and reporting procedures to be followed by Quail Run Energy Center in the event of a Cyber Security Incident. This Plan ensures that an incident response plan is in place to detect and mitigate incidents and restore identified Bulk Electric System Cyber Systems (BCS) computing services.

B. SCOPE

This plan applies to all Quail Run Energy Center employees, contract and vendor personnel responsible for the operation, protection and maintenance of Bulk Electric System Cyber Systems (BCS) that support Bulk Electric Systems, including those having authorized cyber or authorized unescorted physical access to BCSs.

C. DEFINITIONS AND DEFINED TERMS

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

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

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

2. ROLES AND RESPONSIBILITIES

Detection by direct observation and internal reporting of a Cyber Security Incident are the responsibilities of each Quail Run Energy Center employee and vendor. These personnel are entrusted with the responsibility of safeguarding the physical or cyber security of CIP-related assets, which includes all identified Low Impact BCSs.

The following roles collectively comprise the Cyber Security Incident Response Team (CSIRT). These job titles have specific roles and responsibilities assigned to them. It is understood that all plants are different and may have various job titles that meet these roles.

A. Quail Run Energy Center CIP SENIOR MANAGER OR DELEGATE(S)

Functions as the onsite incident responder providing overall direction and authority during a Cyber Security Incident, leading the classification and response to the incident, and coordinating other communication as necessary. The CIP Senior Manager or Delegate(s) assists in the determination of a Reportable Cyber Security Incident.

B. Quail Run Energy Center STAFF

The incident response team consists of senior plant management, physical security specialists, network and control specialists, and applicable personnel. Other Quail Run Energy Center business units, information technology, business analysts, and contractors may also be part of these teams depending on the issue and recovery required.

Position	Role	Responsibility
I&C Technician	Recovery team	Support recovery efforts
Operations Manager	Plant expert, Recovery Team Lead	Lead recovery efforts
CRO	Operations expert	Assist Operations Manager in assessment
Maintenance Manager/Plant Manager	Alternate Recovery Team Lead	Responsible for coordinating labor needs, lead recovery efforts
IT Manager/IT personnel	IT SME	Responsible for technical insight, device log collection, review, and preservation
NERC Compliance Manager	Physical Security Expert	Responsible for support of Incidents involving Physical Security

C. VENDORS

CIP-related asset vendors may have an essential role in ensuring the CSIRT understands how to resolve or work around equipment failures and how to resume operations when necessary. CIP-related asset vendors may also be called upon for the supply of replacement software and hardware.

3. CYBER SECURITY INCIDENT RESPONSE PROCEDURE

A. IDENTIFICATION

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

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

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

(1) Endpoint Protection alerts
(2) Intrusion Detection System (IDS) alerts
(3) Security Information and Event Management (SIEM) alerts
(4) Policies changed (firewall, Group Policy Object (GPO), etc.)
(5) System hardening settings changed
(6) Physical Security Perimeter breach

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

c. Unexplainable loss of BCA or BCS functionality

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

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

NOTE:

Appendix A has other example conditions that may indicate a potential CSI has occurred.

B. ASSESSMENT AND CLASSIFICATION

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

a. When, how, and by whom was the event reported (from Section 3.A)?
b. What system functionality is affected?
c. Are generation or transmission assets affected?
d. How many BCAs and/or BCSs are possibly affected?
e. Indicate results of log(s) examination on all access and monitoring devices and suspect systems.
f. Was unauthorized electronic and/or physical access gained?
g. Was there a compromise or disruption of one or more of Quail Run Energy Center's reliability tasks? Reliability tasks are listed in Attachment B and defined in NERC Standard CIP-002-5.1a.

2. Based on the assessment above, the CSIRT shall classify the event as a Reportable CSI if the CSI has compromised or disrupted one or more reliability tasks of Quail Run Energy Center.

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

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

C. RESPONSE AND INCIDENT HANDLING

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

Containment

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

1. Prevent future electronic or physical access that could cause additional damage.
2. Engage internal and external support resources as needed.
3. If the event involved physical access to a PSP or system, investigate how access was obtained.
4. Reassess damage and capabilities of impacted systems per the Section B.
5. Engage local law enforcement as required.

Evidence Collection and Documentation

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

1. Dated Documentation
2. Security Logs
3. Police Reports
4. Emails
5. Checklists
6. Forensic Analysis Results
7. Restoration Records
8. Post-Incident Review Notes
9. OE-417 Form
10. Document any deviations from the plan taken during the response.

Data Preservation

Collection of information from the target system should be conducted in accordance with the appropriate forensic practices, where possible. Other relevant data that may correlate

with the evidence of unauthorized access, including intrusion detection alerts and firewall logs, should be collected. Collected evidence should be securely stored.

1. Preserve records of electronic and physical access to the cyber assets
2. Data on disk drives of cyber assets shall be copied, mirrored, or replaced prior to recovering the asset where possible.
3. Configuration files of firmware based cyber assets shall be saved to a secure location.
4. Eyewitness accounts shall be documented.
5. Restoration of the BES and the safety of employees, contractors, and the public will take priority over the preservation of CSI data preservation.
6. Record chain of custody of all evidence collected.

Eradication, Recovery and Resolution

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

1. If an attacker appears to have gained root access to a system:
    a. Restore the system from a known good backup or reinstall the operating system and applications
    b. Change all passwords on the system, and possibly on all systems that have trust relationships with the victim system
2. If an attacker only gains a lesser level of access than administrator-level, eradication and recovery actions should be based on the extent to which the attacker gained access.

D. COMMUNICATION PROTOCOL

1. Initial Identification Notification – Immediately upon detection of a possible CSI, notify the CIP Senior Manager or Delegate(s). Notifications may originate from any of the personnel listed in the CSIRT roles that receives alerts from applicable sources, including any employee or vendor who is entrusted with the responsibility of safeguarding the physical and/or cyber security of Quail Run Energy Center's CIP-related Cyber Assets.
2. Vendor Support - If required, the CSIRT is responsible for initiating vendor support services. Such communication may be appropriate to enable a deeper investigation of the incident or resumption of services.
3. Required Reporting
    a. E-ISAC & DOE

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

http://www.oe.netl.doe.gov/oe417.aspx

(2) Alternative methods for reporting an incident to the E-ISAC can be found through this link

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

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

b. Regional Entity

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

c. Reliability Coordinator, Balancing Authority and Transmission Operator

(1) The Quail Run Energy Center operating personnel on duty will make notifications to the other parties in the interchange via phone or email as directed by the CIP Sr. Manager

4. EVIDENCE RETENTION

Quail Run Energy Center will retain data or evidence to show compliance with each requirement for three calendar years unless directed by its Compliance Enforcement Authority ("CEA") to retain specific evidence for a longer period.

5. TESTING AND REVIEWS

The Quail Run Energy Center CIP Senior Manager or delegate is the responsible person for this Plan. This Plan will be reviewed and updated by the CIP Senior Manager or delegate upon the approval of any new versions of the CIP Standards.

A. TESTING

1. This plan shall be tested at least once every 36 calendar months using one of the following mechanisms:

a. Responding to an actual Reportable Cyber Security Incident; or

b. Using a drill or table top exercise of a Reportable Cyber Security Incident; or
c. Using an operational exercise of a Reportable Cyber Security Incident

2. For a paper drill, tabletop exercise or operational exercise, the CSIRT will create a scenario, documenting the effect on systems, facilities, and personnel under that scenario. **The scenario must be one that results in a Reportable Cyber Security Incident.**

3. Follow the Cyber Security Incident Response Plan, documenting each step on RCP-NERC-CIP-003-ATT-G, and maintain a list of issues encountered or deviations from the plan while executing the response plan.

4. Document any lessons learned, or lack thereof, during the execution of the Cyber Security Incident Response Plan.

B. REVIEW AND UPDATES

1. Review the Cyber Security Incident Response Plan to identify:

a. Any opportunities to improve the incident response process.
b. That appropriate roles and responsibilities have been assigned to personnel.
c. The need for additional roles and responsibilities, or personnel involved.
d. The procedures for Identification, Assessment, Response, and Follow up are still appropriate.
e. If training is sufficient for the process.

2. This plan shall be updated by the CIP Senior Manager or delegate if needed, within 180 calendar days after completion of a Cyber Security Incident Response Plan test or actual Reportable Cyber Security Incident.

a. Distribute the updated plan.

(1) Document date of distribution, recipients, and communicated summary of changes.

APPENDIX A- EXAMPLES OF CONDITIONS INDICATING POSSIBLE CSI

- abnormal response time or non-responsiveness
- unexplained account lockouts
- passwords not working
- programs not running properly
- running unexpected programs
- lack of disk space or memory
- bounced-back emails
- inability to connect to the network
- constant or increasing crashes
- abnormal hard drive activity
- connecting to unfamiliar sites
- browser settings changed
- extra toolbars that cannot be deleted

CYBER SECURITY INCIDENT RESPONSE PLAN

APPENDIX B - BES Reliability Operating Service (Reliability Tasks)

[NERC Standard CIP-002-5.1a, pages 17-18]

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5.1. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

RCP-NERC-CIP-003-ATT-E
QUAIL RUN ENERGY CENTER- ODESSA, TX

Referencing Documents:	Revision: Rev. 3
RCP-NERC-CIP-003	Revision Date: March 29, 2022

CYBER SECURITY INCIDENT RESPONSE PLAN

Latest Revision Approval: (Revision History)

Written By: NAES Corporation Date: 2/15/2019

Approved By: Andy Duncan Date: March 29, 2022

REVISION HISTORY LOG
RCP-NERC-CIP-003-ATT-E

Rev.	Date	Description	By Initials	Approval Initials
0	02/15/2019	Updated to template format, added table of contents, section 5.B.2.a and inserted footer	MJS	
1	03/11/2019	Updated for Plant Use	WC	SR
2	3/31/2021	Annual Review	ECN	ACD
3	3/29/2022	Annual Review	ECN	ACD

TRANSIENT CYBER ASSET PLAN AND REMOVABLE MEDIA MALICIOUS CODE RISK MITIGATION

1. INTRODUCTION

A. PURPOSE

The purpose of this document is to prescribe the processes to be followed to avoid the damage to Quail Run Energy Center's in-scope Cyber Assets that could be caused by the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. This plan shall be followed except under CIP Exceptional Circumstances.

B. SCOPE

CIP-003-7 R2, Attachment 1, Section 5 applies to Quail Run Energy Center as an entity with Low Impact BES Cyber Systems.

The processes below must be followed for each in-scope Cyber Asset to the fullest capability of the device.

C. DEFINITIONS AND DEFINED TERMS

Many capitalized terms included in this document are defined in the NERC *Glossary of Terms Used in NERC Reliability Standards*, which is periodically updated. Listed below in this section are Quail Run Energy Center-specific terms, if any.

Access the most current version of the NERC Glossary by clicking the following link:

http://www.nerc.com/pa/Stand/Glossary of Terms/Glossary_of_Terms.pdf

Additional capitalized terms are either defined in the NERC CIP standards or listed below:

Malware (short for "Malicious Software"): This software consists of programming (code, scripts, active content, and other software) that is designed to disrupt or deny operation, gather information, or gain unauthorized access to system resources, or that otherwise exhibits abusive behavior. Malware is not the same as defective software, i.e., software that has a legitimate purpose but contains harmful "bugs."

Transient Cyber Assets (TCA) Defined: A Cyber Asset that is:

i. capable of transmitting or transferring executable code;
ii. not included in a BES Cyber System;
iii. not a Protected Cyber Asset (PCA), and
iv. 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:
    - BES Cyber Asset,
    - network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or
    - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of TCAs include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Removable Media (RM) Defined: 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 are directly connected for 30 consecutive calendars days or less to a:
    - BES Cyber Asset,
    - Network within an Electronic Security Perimeter (ESP) containing high or medium impact BCS, or
    - Protected Cyber Asset associated with high or medium impact BCS.

Examples of RM include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

2. TCA MANAGED BY QUAIL RUN ENERGY CENTER

Quail Run Energy Center shall manage all authorized Transient Cyber Assets in an ongoing manner to ensure compliance with applicable requirements. Quail Run Energy Center will also manage all authorized Transient Cyber Assets in an on-demand manner applying the applicable requirements before connection to a BES Cyber System.

A. TCA AUTHORIZATION

Prior to connecting a TCA to an Applicable System Quail Run Energy Center the TCA owner must obtain approval through the RCP-NERC-CIP-003-ATT-K - Transient Cyber Asset & Removable Media Authorization Record Form and indicate the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

1. Antivirus software, including manual or managed updates of signatures or patterns;

    a. Prior to connection to the BCS, review of AV signatures, patterns and rules sets will be performed to ensure the most current updates have been applied.

2. Application white listing; or

3. Other method(s) to mitigate the introduction of malicious code such as:

   a. Security patching;

   b. System hardening;

   c. Manual alert response;

   d. Rule tuning to provide more granular alerting detail to more closely monitor detected events to expose additional mitigation strategies;

   e. Restrict physical access to TCAs

      (1) Transient Cyber Assets will be secured in locked file cabinets prior to departure for the workday.

      (2) Individuals must not attempt to access authorized Transient Cyber unless they have been granted access rights

      (3) Full-disk encryption with authentication

      All authorized Transient Cyber Assets that connect to Quail Run Energy Center's BES Cyber Systems will have full-disk encryption with authentication. Full disk encryption encrypts 'data at rest'. i.e., all the data on the hard drive and the module which authorizes software installation at the boot up. With this technology, only authenticated users can access the system, using a password, token or a combination of these.

      (4) Multi-factor authentication

      The architecture for Quail Run Energy Center's Transient Cyber Asset connections to the BES Cyber Systems includes multi-factor authentication. All Transient Cyber Asset access requires the use of a username, PIN and RSA SecureID Token combination. The RSA SecureID server used for this access is dedicated to authenticating access for only the BES Cyber Systems and their associated PCAs.

3. TCA MANAGED BY A VENDOR OR CONTRACTOR

A. TCA AUTHORIZATION

Prior to allowing a non-Quail Run Energy Center TCA to connect to an Applicable System Quail Run Energy Center shall have the TCA owner obtain approval through the RCP-NERC-CIP-003-ATT-K - Transient Cyber Asset & Removable Media Authorization Record Form and attest to the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability). Additionally, Quail Run Energy Center's System Administrator or other designated personnel shall perform the following based on the TCA owner's attestation of method(s) of malicious code prevention:

1. Review of antivirus update level;
2. Review of antivirus update process used by the party;
3. Review of application whitelisting used by the party;
4. Review use of live operating system and software executable only from read-only media;
5. Review of system hardening used by the party; or
6. Other method(s) to mitigate the introduction of malicious code:

    a. If a transient Cyber asset is not fully capable of any of the methods above, then verify the Transient Cyber Asset capabilities and the implementation of those capabilities up to the requirement.

    b. For any method used to mitigate software vulnerabilities or malicious code as specified in this section Quail Run Energy Center will verify the following actions:

        (1) Quail Run Energy Center will determine whether any additional mitigation actions are necessary

        (2) If any additional mitigation actions are necessary, Quail Run Energy Center will verify that such actions are implemented prior to connecting the Transient Cyber Asset.

4. RM AUTHORIZATION

For Removable Media, the following items must be documented prior to initial connection to a BCS. Use the applicable RCP-NERC-CIP-003-ATT-K - Transient Cyber Asset & Removable Media Authorization Record Form and indicate the use of one or a combination of the following.

A. METHOD(S) USED TO DETECT MALICIOUS CODE

1. All removable media to be used on a BES Cyber System will be scanned for malware before use
2. The system to be used for scanning the removable media will be kept up-to-date with OS and application upgrades and patches
3. The Cyber Asset used for detection will not be a BES Cyber Asset and shall be identified; and
4. AutoRun or AutoPlay operating system features will be disabled for removable media drives on all BES Cyber Assets where possible.

B. RM USER AUTHORIZATION

For each individual or group of Removable Media, Quail Run Energy Center shall consider the following as authorized RM Users: System Administrator(s), CIP Sr. Manager, and Third-Party Vendors as needed.

1. Authorized Removable Media shall be labeled as such, accounted for, and secured at all times.

2. All Removable Media with authorized access to BES Cyber Systems shall be documented on RCP-NERC-CIP-003-ATT-K - Transient Cyber Asset & Removable Media Authorization Record Form. A description of the roles and responsibilities and business needs for each applicant and description of the type and scope of access is required.

C. RM SECURITY AND STORAGE

RMs will be securely stored in a designated location when not in direct control by the authorized user. Current designated storage locations are listed in the Designated Storage Locations List. Key control for authorized access to the Designated Storage Locations is managed by the System Administrator.

D. RM LOSS OR THEFT

Any loss or theft of Removable Media containing BES Cyber Asset Information must immediately be reported to Quail Run Energy Center's CIP Senior Manager. This includes the loss of Removable Media that was used to transport, or store protected BES Cyber System Information.

E. FINDING REMOVABLE MEDIA

Any Removable Media that is found and is labeled BCSI Confidential must be turned in to the CIP Senior Manager.

Any Removable Media that is found that is not labeled BCSI Confidential shall be turned over to IT personnel.

Any Removable Media that is found is prohibited from being connected to any Quail Run Energy Center's cyber system(s).

5. TCA AND RM MITIGATION OF DETECTED MALICIOUS CODE

A. Primary mitigation is removal upon detection, via software configuration of deletion policies on applicable Transient Cyber Assets and/or Removable Media with installed antivirus software

B. If malicious code is detected, document the mitigation of the threat applied to the TCA or RM

C. If malicious code is detected and cannot be reliably removed, the TCA or RM must be removed from service

D. Confirm that the malicious code has been removed from the TCA or RM before use on a BCA

E. Consider if Cyber Security Incident Response should be activated

6. TCA AND RM TRACKING

Quail Run Energy Center shall maintain documentation of authorized Transient Cyber Assets and Removable Media that connects to its BES Cyber System or that is used to access BES Cyber Asset protected information.

7. INTERNAL CONTROLS

A. Quail Run Energy Center shall control physical access to USB connections by installing tool removable plugs into all BCS USB sockets.

B. Quail Run Energy Center shall employ warning signs on/near all BCS as a reminder for personnel to follow this procedure.

Latest Revision Approval: (Revision History)

Written By: NAES Corporation Date: 2/15/2019

Approved By: Andy Duncan Date: 3/29/2022

REVISION HISTORY LOG
RCP-NERC-CIP-003-ATT-J

Rev.	Date	Description	By Initials	Approval Initials
0	9/6/2019	New plan for CIP-003-7 implementation.	MJS	SJR
1	3/31/2021	Annual review. No changes with CIP-003-8	ECN	ACD
2	3/29/2022	Annual Review	ECN	ACD
3				

CIP EXCEPTIONAL CIRCUMSTANCES PROCEDURE

1. INTRODUCTION

A. PURPOSE

This document describes the process followed at Quail Run Energy Center to request, review, approve, and track CIP Exceptional Circumstances.

B. SCOPE

CIP-003 R1.2.6 applies to Quail Run Energy Center as an entity with Low Impact BES Cyber Systems. Quail Run Energy Center does not have any Medium or High-Impact BES Cyber Systems.

C. DEFINITIONS AND DEFINED TERMS

Capitalized terms in this policy statement are defined in the NERC *Glossary of Terms Used in NERC Reliability Standards*, which is periodically updated, or are listed below in this section as Quail Run Energy Center-specific terms. The most current version of the Glossary can be accessed by clicking the following link:

http://www.nerc.com/pa/Stand/Glossary of Terms/Glossary_of_Terms.pdf

2. CIP EXCEPTIONAL CIRCUMSTANCES PROCESS

A. IDENTIFYING AN EXCEPTIONAL CIRCUMSTANCE

The NERC Glossary of Terms defines a CIP Exceptional Circumstance as

"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."

B. DECLARATION OF A CIP EXCEPTIONAL CIRCUMSTANCE

Declaration of a CIP Exceptional Circumstance - shall occur orally until any immediate impact to safety is resolved. Restoration of the BES and the safety of employees, contractors, and the public will take priority over the documentation of the CIP Exceptional Circumstance.

C. DOCUMENTING A CIP EXCEPTIONAL CIRCUMSTANCE

COMPLETE RCP-NERC-CIP-003-ATT-M, Exceptional Circumstances Form

1. RCP-NERC-CIP-003-ATT-M, CIP Exceptional Circumstances Form, must be completed for each CIP Exceptional Circumstance. Form instructions are attached to the form itself.

2. Include an explanation of why the exception is necessary and any compensating measures, or a statement accepting risk.

3. Identify Applicable Requirements that were exempted from adherence must be identified on the form under Section 3, Description of Exception and Alternative.

4. Document all CIP Exceptional Circumstances within 30 days of being declared

D. APPLICABLE REQUIREMENTS

Only the following requirement can be considered exempt in the case of an Exceptional Circumstance:

- CIP-003 R2, Att 1, Section 5 – Transient Cyber Assets & Removable Media Malicious Code Risk Mitigation

- CIP-012 R1 - Implementation of one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.

E. REVIEWING A CIP EXCEPTIONAL CIRCUMSTANCE

1. Upon the closure or completion of a CIP Exceptional Circumstance, a review meeting shall be conducted with all appropriate subject matter experts for comments and acceptance.

2. The exception form shall be reviewed by the Compliance Specialist, Operations Manager, Maintenance Manager, Lead Control Room Operator, and/or Plant Manager affected by the exception and the designated CIP Senior Manager or delegate.

3. Acceptance of the exception results is verified in periodic reviews by Quail Run Energy Center until the exception is removed or retired.

3. PROCEDURE RESPONSIBILITY

The Quail Run Energy Center CIP Senior Manager is responsible for this Procedure.

Latest Revision Approval: (Revision History)

Written By: NAES Corporation Date: 2/15/2019

Approved By: Andy Duncan Date: 3/29/2022

REVISION HISTORY LOG
RCP-NERC-CIP-003-ATT-L

Rev.	Date	Description	By Initials	Approval Initials
0	9/6/2019	New plan for CIP-003-7 implementation.	MJS	SJR
1	3/31/2021	Annual Review	ECN	ACD
2	3/29/2022	Annual Review	ECN	ACD
3				

Approved for use by:

3/9/23

Plant Manager / Date

TABLE OF CONTENTS

EXHIBITS

8. PURPOSE

The purpose of this Safety Manual Procedure is to establish guidelines for responding to plant emergencies. The instructions in this procedure apply to all plant personnel, contractors, and any others who may be on the plant site during a plant emergency including a fire, chemical release or spill, medical emergency, severe weather, or bomb threats.

Quail Run Energy Center is defined as a Power Generation Company per §25.5(82). To ensure compliance with Chapter 25 of the Public Utility Commission of Texas, Substantive Rules Applicable to Electric Service Providers, Subchapter C, Quality of Service. §25.53. Electric Service Emergency Operations Plans Quail Run developed this ERP-01 Emergency Response Plan.

9. RESPONSIBILITIES

B. The Plant Manager has overall responsibility for the development, revision, and implementation of this plan and for assigning the title and associated responsibilities of Emergency Coordinator to selected employees so that emergencies shall be effectively managed at all times.

C. The Control Room Operator (CRO) is the primary person in charge of the facility until relieved by management. All plant status or change in emergency status must be reported to the control room operator at all times

D. The Environmental, Health and Safety Manager is responsible for the execution of this plan.

E. The Environmental, Health and Safety Manager is responsible for conducting fire and evacuation drills. The CRO is responsible for ensuring the Fire Department is notified, if necessary, and coordinating a response to the incident as well as directing the evacuation according to this plan. The Operations Manager or first available manager shall designate an Emergency Coordinator if the emergency requires personnel to evacuate. If a member of the plant management team is not readily available, the CRO shall assume control of the situation and designate the Emergency Coordinator.

F. The CRO is in charge and responsible for the entire facility until relieved by management and shall directly account for all operation and maintenance (O&M) personnel, contractors, and visitors on-site.

G. The Emergency Coordinator shall maintain radio communication with the CRO and keep a head count of all evacuated plant personal and contract personnel in order to report the status to the CRO. The Emergency Coordinator may be any qualified plant employee.

H. All personnel will be trained on their work areas regarding fire routes, exits, the location and use of emergency equipment, and understanding and following this plan. All personnel who have contractors or visitors at the facility shall ensure that they are familiar with this plan.

I. Two-way radios are the primary means of communication inside the plant. No group of plant personnel shall be allowed outside the administrative building without a radio.

J. Unless environmental conditions such as wind direction and/or location of the hazard prohibit, the primary muster location for a plant evacuation will be outside the automatic gate in an area that will not interfere with responding emergency vehicles.

10. EMERGENCY RESPONSE OVERVIEW

This procedure provides immediate action steps and guidance to be used in a variety of emergencies. It is impossible to provide the exact steps to be followed in all emergencies and emergencies can involve several types of problems at once (a fire with corresponding injuries and a release of hazardous materials for example). Also, the sequence of actions in this procedure may not be the best sequence given the specific situation of an emergency. Steps in this procedure should be performed in an order that fits each situation, relying on sound judgment from plant operators. For this reason, it is imperative that all personnel are familiar with this procedure and associated emergency response procedures.

The Emergency Response Event Log (Exhibit ERP-01D) should be utilized to document a timeline of events and actions taken during all plant emergencies.

Use the Emergency Response Call Record Form (Exhibit ERP-01E) to document all notifications made including all instructions given by parties contacted.

Reporting guidelines for injuries and near miss safety/environmental accidents is covered in SMP-14, Accident Reporting & Investigation.

4. HAZARDOUS WASTE OPERATIONS AND EMERGENCY RESPONSE (HAZWOPER)

A. CHEMICAL, OIL, AND HAZARDOUS MATERIALS SPILL RESPONSE PROCEDURE

NOTE

When working on or around the ammonia system, be alert as to the wind direction. At the first sign of ammonia odor, immediately try to determine where the release is coming from, then move crosswind and then upwind from the spill.

The following steps will be done **immediately** upon observation of ammonia, oil, or hazardous materials spills. This procedure is intended to be a concise list of the basic emergency response steps and must be used in conjunction with Hazardous Material Spill Background, Training and Follow-up section below.

1. **Assess specific hazards**. Refer to SDS for proper use of personnel protective equipment, hazards, and other cleanup instructions and other pertinent information.

NOTE

SDSs are maintained at the website below:

http://msdsmanagement.msdsonline.com/92a2f98a-0e59-4ba4-b8dd-7b45ad65d25d/ebinder/?nas=True

Employees can also access the SDS website by scanning the QR code located in the Red Emergency Response Binders located in the Control Room, Maintenance Shop, and Plant Management offices.

2. **Evacuate area**. If the chemical is hazardous, ensure that all personnel are evacuated from the area of the release. Assist any injured personnel out of the area to minimize the extent of the injury and to prevent further injury.

3. **Evacuate plant if necessary.** Evacuate the entire plant if it becomes necessary. Primary evacuation routes are shown on Exhibit ERP-01A. The Plant Manager or his designee may designate different evacuation routes at the time of the accident based on the type of accident, location of problem, location of personnel, wind direction, and any other information known at the time. Personnel may also be directed to go to a particular area of the plant to evacuate the area of the emergency if evacuation of the site is undesirable. Take note of wind direction when evacuating the plant. The normal exit through the West gate may be impeded and it may become necessary to evacuate through an alternate gate.

4. **Evaluate the need for a "shelter-in-place**". Additionally, if the emergency involves a toxic airborne release, the Plant Manager or his designee will evaluate the release and wind conditions and determine whether or not to evacuate plant

personnel or "shelter-in-place". Due to the uncertainty of wind direction and concentrations, it may be preferable to have all personnel in buildings remain there until the toxic cloud has dissipated. The shelter-in-place concept is preferable in the situation where a high concentration cloud of toxic gas passes a building containing people.

If the gas cloud is moving in the direction of the control room, shut down all air conditioning and ventilation systems. All personnel in the building should enter the control room area and all doors leading to this area should be closed.

5. **Stop the spill**. Take the necessary steps to mitigate the spill or chemical release (e.g., shut off pumps, close valves, discontinue loading/unloading operations, etc.) if it safe to do so. If at all possible, stop the spill at its source.

6. **Notify all personnel**. The CRO will **immediately** notify all personnel on-site by radio communication. CRO will use available manpower to assist communication to contractors as needed.

NOTE
The Plant Manager shall be notified as soon as possible, but this requirement should not interfere with proper physical responses to the emergency. REFER TO STEP 12 BELOW

7. **Assess spill control measures**. The Plant Manager (or his designee) will instruct plant personnel for further spill response measures. At any time, the Plant Manager determines that the spill or any measure needed to prevent, contain, control, or clean up the spill is beyond the ability of the facility's manpower and/or equipment, he shall immediately contact outside hazardous materials emergency responders and remediation contractors to help control/clean up the spill.

8. **Maintain plant security and communications.** The Plant Manager or his designee will maintain plant security and communications. Access shall be restricted so that only essential plant personnel and emergency personnel are admitted. In no case shall members of the press be admitted without the approval of the Plant Manager. The Plant Manager or his designee will handle all public relations, press releases, and outside inquiries.

9. **Keep the material on-site**. Make every reasonable effort to keep the spill on the plant property and away from navigable waters. In the event that the material has been released from the containment system, all necessary steps shall be taken to prevent it from entering storm sewers, public waters, or from escaping the facility property as long as it is safe to do so.

10. **Conduct spill control measures**. Build berms, place absorbent materials, plug storm drain inlets, culverts, and ditches to stop the flow of the spill. If necessary, plug culverts of streams and drainage ditches leaving the plant to stop the flow of the spill. Response to the spill can involve operating equipment remotely or

placing absorbents in the flow path if it can be done without placing employees in an unsafe condition.

11. **Document events and actions**. Document all events in detail as soon as possible in the Emergency Response Event Log (Exhibit ERP-01D).

12. **Report the Incident**. Follow up with the Plant Manager, Operations Manager, and EHS Manager to ensure all reporting requirements are met. Report all injuries in accordance with SMP-14, Accident Reporting & Investigation.

a. Notification

NOTE

When reporting releases, it is important to provide accurate, concise, and factual information. Do not exaggerate or speculate.

Upon observation of a release of a hazardous material, chemical, or oil, employees shall immediately contact the Plant Manager and provide him with information concerning the spill, such as:

(2) Employee name

(3) Location of spill

(4) Type and quantity of material spilled

(5) Actions and result of actions taken to mitigate the spill

(6) Circumstances that caused the spill

b. The Plant Manager, or his designee, will notify the necessary organizations and governmental agencies listed on the EMERGENCY NOTIFICATION CONTACT LISTS attachment. If necessary, the Plant Manager, or his designee may contact outside Hazardous Materials Emergency Response organizations, and/or hazardous waste clean-up contractors to assist in the remediation of the spill.

c. The Plant Manager or his designee will also notify corporate management and the Environmental Manager of all spills regardless of quantity and type as soon as practical.

d. The Plant Manager or his designee will provide the following information in the agency notification:

(1) The facility name, exact location, and phone number

(2) The source and cause of the spill

(3) The type (chemical name), volume of material released, and whether the material is classified as extremely hazardous

(4) The volume estimated that reached navigable waters

(5) The time, date, and duration of the spill

(6) The medium release went into (air, soil, water) and anticipated release movement

(7) The action taken and anticipated

(8) State whether evacuation is needed

(9) The weather conditions, if applicable

(10) Known health risks and required medical attention

(11) Names of other parties contacted

(12) Names of other parties to be contacted

e. Keep notifications factual and do not speculate. Keep a record of all notifications made including all instructions given by parties contacted using the Emergency Response Call Record Form shown on Exhibit ERP-01E. The records of notification shall be kept in the plant files for a period of 5 years.

13. All inquiries from the media and the public should be referred to the Plant Manager, or his designee. Under no circumstances shall any plant personnel provide information to media or the general public concerning the spill. Simply and politely refer all inquiries to the Plant Manager.

14. For plants with oil: Per 40 CFR 112.4, if a discharge of 1,000 gallons of oil escapes the containment systems and enters the navigable waters of the United States in a single spill event or a discharge of harmful quantities in two spill events within any twelve-month period occurs, the Plant Manager will submit notification in writing to the EPA Regional Administrator:

NOTE

An * denotes information included in the SPCC plan

(1) A complete copy of the SPCC plan

(2) Name, phone number, and address of the facility (*)

(3) Owner and operator name and address (*)

(4) Date and year of initial facility operation (*)

(5) Maximum storage capacity and average daily use (*)

(6) Description of the facility (*)

(7) Quantity and type of material spilled

(8) Cause(s) of the spill(s)

(9) Corrective actions

(10) Additional preventative measures

(11) Other pertinent information

15. The plant staff shall investigate each incident that resulted in, or could reasonably have resulted in, a release of hazardous materials. An incident investigation shall be initiated as promptly as possible, but not later than 24 hours following the incident.

The responsibilities of Quail Run Energy Center following a release include determining the origin of the incident, investigating the effectiveness of this procedure, and evaluating the potential need for modifications to this procedure and plant personal response. NAES will be responsible for the implementation and communication of any changes to this procedure following an accidental release of aqueous ammonia.

A summary shall be prepared at the conclusion of the investigation that includes at a minimum:

- Date of incident and investigation
- A description of the incident
- The factors that contributed to the incident
- Any recommendations resulting from the investigation

Quail Run Energy Center will promptly address and resolve the investigation findings and recommendations. Resolutions and corrective actions shall be documented. The findings shall be reviewed with all affected personnel whose job tasks are affected by the findings. Investigation summaries shall be retained for five years in the plant environmental files.

16. Spill Clean-up and Disposal Procedure

a. All residuals (recovered chemicals, contaminated clean up materials, and contaminated soil) resulting from spill remediation will be placed in

containers that have been inspected for use as such. If the spill residual has no reuse or salvage value, the spill residual will be properly disposed of off-site.

b. Clean up will be conducted to coordinate collection for isolation and disposal of contaminated products and materials, as appropriate. The following categories will be isolated and secured independently:

NOTE

These steps are necessary to reduce costs associated with clean up and disposal of contaminated materials.

(1) Recovered pure product for possible refining and reuse

(2) Contaminated PPE for separate disposal

(3) Oiled debris for separate disposal, i.e., wood products, beauty bark, etc.

(4) Contaminated soils for possible incineration or separate disposal

(5) Absorbent materials for incineration

c. Disposal of spilled material will meet all Federal and State regulations guiding the disposal of waste. Hazardous waste manifests will accompany containers of spill residues if the residue is determined by definitions of hazardous regulations to be hazardous. All required labeling and recordkeeping requirements will be followed.

d. Consult the SDS of the substance for cleanup procedures. Ensure all plant and contractor personnel assisting with the clean-up are aware of clean-up instructions and hazards listed on SDS's.

e. Refer to plant environmental instructions for further guidelines on the disposal of hazardous materials. Additionally, contact the Compliance Specialist.

B. HAZARDOUS MATERIAL SPILL BACKGROUND, TRAINING, AND FOLLOW-UP

This section provides details and information to be used in preparation for and response to emergencies involving hazardous materials incidents in compliance with OSHA Hazardous Waste Operations and Emergency Response Standard (29 CFR 1910.120). This section is also to be used in conjunction with the facility Spill Prevention, Control, and Countermeasure Plan (SPCC) if the spill involves an oil spill at the plant. The SPCC is required by EPA oil spill regulations 40 CFR 110 and 40 CFR 112. The SPCC is a document that describes the plant design features and administrative actions that prevent the discharge of oil and other hazardous materials to the environment. The SPCC is a spill prevention plan (that is, actions to be taken before the spill occurs), while this procedure is a spill response plan (that is, an action to be taken after the spill occurs).

An oil spill event, as defined in 40 CFR 112.2, is a discharge of oil into or upon the navigable waters of the United States or adjoining shorelines in harmful quantities.

Guidance pertaining to employee safety and training related to major hazardous materials releases and subsequent cleanup operations is contained in 29 CFR 1910.120, Hazardous Waste Operations and Emergency Response, referred to as HAZWOPER.

1. Overview of Hazardous Materials Releases

Hazardous Material

Any substance or mixture of substances defined as hazardous under OSHA, EPA, or DOT regulations, exposure to which results, or may result, in adverse effects to the health or safety of employees. (29 CFR 1910.120(a)(3)) Hazardous materials stored in quantities sufficient to require emergency response plans include: ammonia, fuel oil, sodium hydroxide, and sulfuric acid. One or all of the regulations listed above may classify other materials as hazardous, but the release of which is not likely to create health and safety hazards sufficient to result in an emergency (i.e., laboratory reagents).

Emergency Release of Hazardous Material

A Hazardous Materials Emergency is an occurrence that results, or is likely to result, in an uncontrolled release of a hazardous substance. A Hazardous Materials Emergency may cause high levels of exposure to toxic substances, is life or health threatening, presents a fire or explosion hazard, creates an oxygen deficient condition, or requires immediate attention because of danger.

The following chemicals and materials are on-site with the combination of characteristics and quantities which could, if released in an uncontrolled manner, require emergency response under the regulations specified by 29 CFR 1910.120. Some reportable quantities are listed above maximum quantities stored on site to account for emergencies.

On-Site Reportable Chemicals						
Chemical	**Reportable QTY Product in lbs.**	**EPA CAS #**	**Specific Gravity from SDS**	**Reportable QTY Product in Gallons**	**Max. Quantity on Site**	**Reporting Requirement**
Aqueous Ammonia-(19%) Ammonia Hydroxide	1,000 lbs.	1336216	0.9275	680 gallons	(2) 10,000 gallons	Immediate
Sodium Hypochlorite (12.5%)	900 lbs.	7681529	1.17	82 gallons	6,000 gallons	Immediate
Sulfuric Acid (93%)	1,005 lbs.	7664939	1.8	72 gallons	6,000 gallons (2) 350 gallons	Immediate
Oil	25 gallons	NA	NA	25 gallons	>64,000 gallons	As soon as possible but within 24-hours
Caustic (25%) Sodium Hydroxide	1,000 lbs.	1310732	1.270	378 gallons	350 gallons	Immediate
Cooling Tower Corrosion Inhibitor (10%) Phosphoric Acid (CL 5859)	49,610 lbs.	7664382	1.055	5,683 gallons	2,650 gallons	Immediate
Boiler Phosphate (5%) Sodium Hydroxide (BL 17942)	1,000 lbs.	1310732	1.270	1888 gallons	500 gallons	Immediate

Reportable quantities computed via NAES Release Reporting Calculator, EPA CAS# and specific gravity from SDS

On-Site Chemicals			
Chemical	**Quantity On-Site**	**Function**	**Location**
CT401	2,650 gallons	Bio-Penetrant/Surfactant	Cooling Tower
RL9005	350 gallons	RO membrane scale inhibitor	Water Treatment Building
CL206	350 gallons	RO Biocide	Water Treatment Building
BL124	350 gallons	RO chlorine scavenger	Water Treatment Building
BL17942	1000 gallons	Boiler phosphate treatment	Boiler Chemical Building
CL2212	35 gallons	Cooling water biocide	Oil/Chemical Storage Area
BL8100	100 gallons	Aux boiler treatment-Mixed chemical (Oxygen Scavenger, Descaler, and Inhibitor)	Oil/Chemical Storage Area
CL2632	250 gallons	Closed Cooling Tower Treatment	Oil/Chemical Storage Area
CL5859	350 gallons	Cooling Tower Inhibitor	Oil/Chemical Storage Area
CL240	55 gallons	Cooling water anti-foam	Oil/Chemical Storage Area
Ethylene Glycol	350 gallons	Closed Cooling Tower Loop	Oil/Chemical Storage Area
CL 2030	250 gallons	Evaporation Pond Biocide	Evaporation Ponds

An Incidental Release according to 29 CFR 1910, OSHA's Hazardous Waste Operations and Emergency (HAZWOPER) Standard, incidental hazardous substance releases can be absorbed, neutralized or otherwise controlled at the time of release by employees in the immediate release area or by maintenance personnel. Incidental Releases are defined as "one that does not cause a health or safety hazard to employees and does not need to be cleaned up immediately to prevent death or serious injury to employees."

Incidental Release Response

Incidental releases can be controlled, contained, and cleaned up by employees in the immediate area. No outside or special assistance is required. Nuisance spills and minor releases which do not require immediate attention (due to lack of danger to employees) would be considered within the normal activities and training of the

employee. No additional or special training is required to properly deal with an incidental release.

Incidental releases, for the purposes of operator training and response activities pertaining to the unintended release of hazardous materials on-site, may be approached, controlled, stopped, absorbed, neutralized, and cleaned up as long as plant personnel do not endanger themselves, others, or the environment in the process.

Personnel will carry out system operations at a safe distance to minimize the severity of the release. Remote control of valves and pumps will be employed as available to minimize the necessity of approaching the point of origin of an incidental release. Personnel will employ PPE, as needed and for which they are trained, to minimize potential for contact with the released materials. Clean up and hazardous material disposal techniques, as outlined in on-going training, will be followed to ensure safe and efficient return to normal operations. These actions implement the training conducted as part of normal system operations.

Disposal guidelines outlined below should be followed. Recording and reporting of the release should be made promptly as described in the Notification section below. As incidental releases often do not leave the plant, no outside notification may be necessary. The Plant Manager, or his designee shall review the situation and notification requirements to determine what outside organizations are required to be notified. As a minimum, the Plant Manager shall always be notified of every spill or release regardless of size or material with the exception of raw and potable water. Refer to the preceding table for Reportable Quantities for Extremely Hazardous Substances that are stored on-site. Proper decontamination of equipment and PPE shall be implemented after the cleanup is completed.

Emergency Response

A hazardous materials emergency response is any response effort by employees from outside the immediate release area or by other designated responders (i.e., mutual aid groups, local fire departments, etc.) to an occurrence which results, or is likely to result, in an uncontrolled release, which may cause high levels of exposure to toxic substances, or which poses danger to employees requiring immediate attention (29 CFR 1910.120(a)(3)). While a release resulting in an emergency is highly unlikely, Quail Run Energy Center employees will be trained and prepared to carry out appropriate responsibilities. No Quail Run Energy Center employee shall attempt to perform actions for which they have not been prepared, through training and/or experience, or for which they are not properly equipped. On-site and off-site training will be conducted both initially and on a continuing basis, as necessary, to ensure that personnel have the knowledge and experience to make a reasonable determination of the dangers when faced with a release situation.

For planning purposes the only credible scenario, which could result in an **uncontrolled** release requiring HAZWOPER response, would be the highly

improbable situation in which a chemical storage tank ruptured or rupture of a line with isolation impossible, with a simultaneous rupture of secondary containment and/or control system(s) failure.

2. Resource Allocation

The Plant Manager has the authority to commit resources and funds for any spill remediation activity. He may delegate duties to other Quail Run Energy Center employees to expedite spill containment, clean-up, and disposal. In the event of a major spill or release, the Plant Manager will be in charge of the handling and cleanup of the toxic material. This person would either be from the licensed spill remediation company or a government agency (i.e., Ammonia supplier or other chemical supplier, Fire Department, or commercial response organization). The Plant Manager or his designee would remain in charge of the overall plant operation and coordination of spill response activities.

In the event that the Plant Manager or his designee is not available, the Operations Manager in consultation with corporate management personnel shall assume the responsibility for supervision of any spill response activities.

3. Emergency Response Training

Training shall be based on the duties and functions to be performed by each employee. Documentation of such training, including program agendas (with a copy of any outlines, PowerPoints, or handouts) and training rosters shall be maintained.

Facility response personnel are given instruction in emergency procedures related to a release of a hazardous substance or any hazardous chemical. Topics of instruction include emergency equipment (proper use, inspection and maintenance procedures), emergency systems (such as alarms/communications, key cut off systems for automatic feed systems), response procedures for fires, explosions, and spills (including spills to groundwater), and the organizational responsibilities of response personnel under the Incident Command System.

<u>Hazwoper Awareness Level</u>

First responders at the awareness level are individuals who are likely to witness or discover a hazardous substance release and who have been trained to initiate an emergency response sequence by notifying the proper authorities of the release. They would take no further action beyond notifying the authorities of the release. First responders at the awareness level shall have sufficient training or have had sufficient experience to objectively demonstrate competency in the following areas:

a. An understanding of what hazardous substances are, and the risks associated with them in an incident

b. An understanding of the potential outcomes associated with an emergency created when hazardous substances are present
c. The ability to recognize the presence of hazardous substances in an emergency
d. An understanding of the role of the first responder awareness individual in the employer's emergency response plan, including site security and control and DOT's Emergency Response Guidebook
e. The ability to realize the need for additional resources, and to make the appropriate notifications to the communications center

Hazwoper Operations Level

First responders at the operations level are individuals who respond to releases or potential releases of hazardous substances as part of the initial response to the site for the purpose of protecting nearby persons, property, or the environment from the effects of the release. They are trained to respond in a defensive fashion without trying to stop the release. Their function is to contain the spill from a safe distance, keep it from spreading, and prevent exposures. First responders at the operational level shall have received at least eight hours of training or have had sufficient experience to objectively demonstrate competency in the following areas in addition to those listed for the awareness level:

a. Knowledge of the basic hazard and risk assessment techniques
b. Knowledge of how to select and use proper PPE provided to the first responder operational level
c. An understanding of basic hazardous materials terms
d. Knowledge of how to perform basic control, containment and/or confinement within the capabilities of the resources and PPE available within their unit
e. Knowledge of how to implement basic decontamination procedures
f. An understanding of the relevant standard operating and termination procedures

Hazwoper Technician Level

All Quail Run plant operations personnel are trained at the Hazwoper technician level through the completion of a 24-hour training course meeting the OSHA Hazwoper training requirements of 29 CFR 1910.120 (q)(6)(iii). First responders at the technician level demonstrate competency in the following:

a. Approach the point of release to plug, patch or otherwise stop the release.
b. Perform advanced control, containment, and/or confinement operations within the capabilities of the resources and personal protective equipment with the plant.
c. Understand and implement decontamination procedures
d. Understand termination procedures
e. Understand basic chemical and toxicological terminology and behavior

5. FIRE RESPONSE PROCEDURE

B. In the event of any fire, immediately report the fire to the Control Room Operator (CRO) via plant radio, cell phone, or other means. The report to the CRO shall include the following:

1. Your name
2. Nature of event – "Fire"
3. Location of the fire
4. Severity of the fire
5. Your planned action (ex. - evacuate or use fire extinguisher)

C. If the fire is in the incipient stage (see NOTE) and you have been properly trained, respond using the appropriate fire response equipment (fire extinguisher, etc.).

NOTE:

INCIPIENT FIRES - INFERS A FIRE THAT HAS JUST BEGUN AND IS OF SUCH SIZE THAT POOR VISIBILITY, SMOKE INHALATION, AND HIGH TEMPERATURES HAVE NOT REACHED THE DEGREE TO REQUIRE THE USE OF BREATHING APPARATUS.

-INTERIOR STRUCTURAL FIRES - ARE FIRES OF THE TYPE WHERE IT IS NECESSARY TO WEAR BREATHING APPARATUS IN ORDER TO BE ADEQUATELY PROTECTED.

If the fire is an interior structural fire or has progressed to a life-threatening event, immediately evacuate the area and notify the Control Room.

D. The CRO shall evaluate the situation to decide if evacuation of all personnel or outside emergency response service (Fire Department) is necessary.

E. In the event that the fire is beyond the incipient stage and requires outside emergency response, the manager or designee (notifier) shall contact outside personnel like fire, medical, and rescue services (911) and announce the need for plant evacuation over the radio.

F. Onsite emergency Personnel shall isolate and power down the energized system or systems from a remote location as needed to safely allow responding fire fighters to extinguish interior structure fires. Quail Run management personnel or CRO will direct emergency Personnel to the location of the interior structure fire.

G. The manager or designee will appoint a fire pump operator. The fire pump operator checks the electric and diesel fire pump when the fire alarm sounds. If the fire pump is safely accessible, this person starts the pump (if it has not started automatically) and keeps it operating until instructed to shut it off.

H. To facilitate a quick response, the manager will designate a liaison to meet the Fire Response Service at the main entrance gate.

I. Evacuation Area: One area on-site has been designated as a primary muster area. The primary muster area is to be posted as such with appropriate signage. The following area has been identified as the primary muster area (Exhibit ERP-01A):

1. Main Entrance Gate Area – Evacuation Area

In the event that environmental conditions or the hazard location prohibit the use of the primary muster area, site personnel will be directed to an alternate muster area designated in the Emergency Response Plan and directed by the CRO via 2-way radio.

Upon hearing the fire evacuation order, all personnel shall evacuate to the primary evacuation area.

J. The CRO shall dispatch a designee with the site sign-in rosters for employees and contractors to the muster area to account for all plant and contract personnel.

K. Following the event, the manager in charge will designate a salvage team. The salvage team gets the facility back in operation as soon as possible after an emergency. (multi-craft team)

L. Safety drills shall be conducted at a minimum on an annual basis. All occupants at the facility shall participate in the fire drill unless their participation could create an operational upset. Evacuation orders shall be given verbally by the CRO over the plant radios.

6. MEDICAL EMERGENCIES

B. All injuries must be reported to your supervisor, no matter how small. First Aid/CPR trained personnel will be called to respond to minor first aid injuries. If applicable, the injured person may be taken to plant's approved health care facility and/or local emergency room for further evaluation.

C. If someone is seriously hurt, notify the CRO of the location of the injured person, nature of the injury, and any other important information related to the incident scene (ex. down power line next to injured person, chemical drum spill, etc.).

D. The CRO will dial 911 to alert emergency crews. An individual will be designated to meet emergency crews at the main entrance gate.

E. The CRO will make a radio announcement for all available First Aid/CPR trained personnel to report to the incident site. The First Aid/CPR trained personnel will administer first aid and any other measures within their training until the emergency crews arrive at the scene.

F. If the situation warrants the rescue of an unconscious or immobile person from a confined space or an elevated surface, the CRO will be instructed to dial 911 and shall explain to emergency personnel the type, location, and hazards of the confined space. Again, an individual will be designated to meet the emergency crews at the appropriate entrance to expedite the response.

NOTE

For emergencies that involve an immobile or unconscious person in a confined space, entry shall not be made unless personnel are trained and the proper procedures are followed. See the Confined Space and Enclosed Space Entry (SMP-07).

7. EARTHQUAKES, TORNADOS, AND SEVERE WEATHER EMERGENCIES

A. Quail Run's Severe Weather procedure is located in PEP-007 and contains guidance for High Winds, Thunderstorms, Tornadoes, Earthquakes, and Hot and Cold Weather Emergencies. It also addresses severe weather staffing and emergency supplies in the event of extreme weather events.

B. Severe weather staffing is addressed as follows. To ensure the appropriate personnel are on hand to help the facility additional off-shift operations personnel will be utilized as necessary to prepare and respond to severe weather events. Maintenance department assigns 1 mechanical-maintenance technician and instrumentation-control-electrical (IC&E) technician on call at all times on a weekly rotational basis. A secondary person is assigned as backup in the event the primary person for that week cannot be reached. Operations has a shift schedule and will call out off-shift personnel as needed to supplement the onsite team.

C. Changes in the weather associated with fast-moving severe storm fronts give little or no warning. Tornados develop from powerful thunderstorms. They are incredibly violent local storms that extend to the ground with winds that can reach 300 mph. In the event of impending severe weather, plant personnel will monitor the local emergency weather broadcast. The safety of on-site personnel and the integrity of plant equipment will be the first concern.

During severe thunderstorms, caution should be used during outside activities. If thunderstorms are in the immediate area of the plant, outside activities should be curtailed as much as possible. Personnel shall avoid being the highest elevation on any structure. The safety of plant personnel shall be the prime concern and reasonable judgment shall be used.

D. Quail Run maintains 2 tornado shelters between the Admin Building and Water treatment building – each with a capacity of 20 people standing.

E. Proceed to PEP-007 for actions to take in a Severe weather event including Hot and Cold Weather Emergencies..

8. THREATS TO THE FACILITY - BOMB THREATS, CYBERSECURITY, AND SABATOGE

A. RECOGNITION

Understanding when threat to the facility is taking place or is about to take place is the first step towards preventing the subsequent injury and damage that can ultimately result. These tools are available as Appendices to this procedure and are described below:

1. EXHIBIT ERP-01B - Actions for Suspected Sabotage Events (including cyber events) contains a list and description of potential events as well as immediate actions to be taken in case of those types of events.

2. EXHIBIT ERP-01C – Bomb Threat Checklist contains a checklist to be used when a bomb threat is received over the phone. This will help the receiver of the call obtain as much information as possible to help find the source.

3. EXHIBIT ERP-01D – Suspected Bomb/Sabotage Device Safety Precautions contains a list of precautions to be taken around unidentified packages, bombs, and suspected Sabotage devices.

The Plant Manager and all plant personnel and visitors shall maintain and enforce a strict site security policy to try and avoid any potential Sabotage events.

B. RESPONSE

Although many threats turn out to be hoaxes, it is very important to not dismiss the possibility of injury and damage and treat every situation seriously. When a bomb threat or discovery of a suspected Sabotage event is discovered, remember to not panic, remain calm, and follow the steps below:

1. For any abnormal events that could potentially be acts of Sabotage, refer to EXHIBIT ERP-01B – Actions for Suspected Sabotage Events and Threats (Including Cybersecurity).

2. When a call is received regarding a bomb threat or other act of Sabotage, refer to EXHIBIT ERP-01C – Bomb Threat Checklist while keeping the following items in mind:

   a. Engage the caller in as much conversation as possible and complete the checklist as the call progresses. If you are at a phone with caller ID, note the phone number of the caller.

   b. Keep the caller on the line as long as possible. Ask the caller to repeat the message even if you fully understood the message the first time. This will stall or cause a delay and allow the operator more time to react properly and involve the necessary personnel.

c. If the caller does not give a location of the device, Sabotage method, or a time for the event, attempt to attain this information.

d. Inform the caller that the building is occupied and that such an event (explosion or equipment destruction) would result in serious injury or death to innocent people.

e. Be aware of the caller's voice and any background noises that may assist in identifying the location of the call. Record your findings on the checklist.

f. Attempt to have the caller speak to a designated member of management.

g. Do not hang up until the conversation ends and the caller hangs up.

3. Maintain security and communications. The Plant Manager (or designee) shall maintain plant security by restricting access so that only essential plant personnel and emergency personnel are admitted. The telephones should be manned if there are enough people on-site. Two-way radio communication should be kept free to be used as needed. In no case shall members of the press be admitted without the approval of the Owner Representative. The Owner Representative or his designee will handle all public relations, press releases, and outside inquiries.

4. Quickly search the plant area for suspicious, unusual, or foreign items (suspected bombs/Sabotage devices), and report any findings, but do not touch, move, jar, disturb, or cover any suspicious items found. Observe the safety precautions listed in EXHIBIT ERP-01D. When police arrive, assist as necessary with a more detailed search of the plant.

5. If a suspicious item or bomb is located during the search, do the following:

   a. Isolate and DO NOT TOUCH OR DISTURB the item.

   b. Make notes of the location, appearance, colors, wires, etc.

   c. Contact the civil authorities and management in person.

   d. Do not use two-way radios or intercoms.

NOTE

At any time during these actions, the Plant Manager or on shift CRO can order the shutdown of equipment and evacuation if, in his judgment, there are strong indications of an immediate serious threat to the plant and/or its personnel.

6. If the plant is evacuated at any point, do not return until after the police have declared the site safe.

7. Upon completion of the threat, the management team shall assemble to critique the handling of the situation. Any recommendations for improvement must be incorporated into the policy and re-training conducted with the necessary personnel.

C. COMMUNICATION

1. Report the event to the police as soon as possible. Provide the police with the following information:

   a. Your name
   b. Your location and phone number
   c. A detailed account of the event
   d. If the event is a threat received (via phone or other method), report the following:
      (1) Name of the initial recipient
      (2) Name of any employee threatened by the caller
      (3) Normal work location of any threatened employee
      (4) Time the bomb is supposed to explode/Sabotage event is to occur
      (5) Exact location of the bomb or Sabotage device
      (6) Outside appearance or description of the bomb or device

2. Ensure that plant operating personnel are aware of the sabotage event on your facility and any sabotage event that would affect larger portions of the Interconnection.

3. When the police arrive at the site, the Plant Manager (or designee) shall brief the police as to:

   a. Location of any emergency control valves or switches,

   b. Plant overall security status, and

   c. Any other information regarding the nature of the threat or event.

NOTE

Have all written records or notes of the threat available utilizing the event log and EXHIBIT ERP-01C Checklist at the end of this procedure.

4. Appropriate assistance should be requested from the police including site protection and personnel protection during an evacuation.

5. As soon as the threat has been at least tentatively identified and controlled, notify the Plant Manager, the Owners Representative, and the NAES Headquarters Operations Director. Applicable telephone numbers are listed below for quick access.

Table 1. Emergency Organizational Telephone Numbers for Threat Control

Name	Title	Contact Telephone Number	Fax Number
Andy Duncan	Plant Manager		
Rob Simmerman	SR. Operations Director		
Rob Watson	Owners Representative		

D. REPORTING

1. The following events are reportable to the DOE and NERC ERO. If either of these conditions occur, contact the contact the Plant Manager and NERC Compliance manager to ensure proper DOE and NERC reporting complete. Refer to procedure RCP-NERC-EOP-004-ATT-A-Event Response Guidelines- in conjunction with this procedure.

   a. For damage or destruction of the facility that results from actual or suspected intentional human action
   b. physical threat to the facility that could degrade the normal operation of the facility

NOTE:

NAES NERC procedure RCP-EOP-004-ATT-A contains reporting guidelines for reporting damage or destruction of the Facility that results from actual or suspected intentional human action as well as any physical threats to the Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Please refer to RCP-NERC-EOP-004-ATT-A for NERC Event Reporting guidelines for these instances.

   c. For response to cybersecurity events, contact the Plant Manager and the NERC Compliance Manager. Refer to RCP-NERC-CIP-003-ATT-E-Cybersecurity incident response plan. This procedure contains steps to identify, assess, and respond to Cybersecurity incidents. The NERC Compliance Manager should assist with this procedure and notification steps.

   d. Upon completion of the threat, the management team shall assemble to critique the handling of the situation. Any recommendations for improvement must be incorporated into the policy and re-training conducted with the necessary personnel.

9. GAS PIPELINE EMERGENCIES

A. Leaks

A leak or gas detected inside or near a building must be given immediate attention to protect the general public and property. A secondary, but important, consideration is to prevent the loss of gas service.

B. Fire and explosives

Emergency precautions must be taken after explosions and during major fires to protect system facilities and to insure that the presence of gas will not create additional problems for firefighting and damage control personnel.

C. Abnormal pressure conditions

OVERPRESSURE OF SYSTEM

When pressures exceeding the maximum allowed operating pressures of components on a system are experienced, action must be taken to eliminate conditions that might endanger life or property.

UNDER-PRESSURE OF SYSTEM

When pressures less than those required to operate equipment safely are experienced, specific steps must be taken to ensure that an increase to normal operating pressure will not endanger life or property.

Refer to Quail Run/Exel Pipeline Services - Natural Gas Pipeline O&M Procedures/Emergency Procedures for additional information.

10. TRAINING

B. All plant employees shall receive training on emergency response procedures on an annual basis.

C. All newly hired employees shall receive this training during orientation.

D. Contract employees must receive this training as integrated into the contractor orientation and training.

> **NOTE**
>
> In addition to the training, the appropriate number of radios shall be determined and issued to the Contractor Supervisor/Foreman.

E. All plant employees training must include at a minimum the following:

1. Familiarization with this plan
2. Any Hazmat Training that may be applicable
3. The use of any firefighting equipment available
4. Any special items or needs that may rise

F. All contract employees training must include the following:

1. A general overview of this plan
2. Any special items or needs that may arise during the course of their stay on-site

G. A written record must be maintained of all plant employees and contract employees who have received the training.

DOCUMENT HISTORY

Revision 2	Date 03/08/2013
Writer	Mike Gallaher
Reviewer(s)	Mike Gallaher QREC Environmental Specialist
Approver(s)	Philip Neal, QREC Operations Manager
Reason Written	Replace Environmental Specialist contact information.

Revision 3	Date 9/16/2013
Writer	Mike Gallaher
Reviewer(s)	Philip Neal
Approver(s)	Philip Neal
Reason for Change	1) EMS action item to incorporate EN-EP-109 by reference for required chemical release reporting form for Exelon reportable and non-reportable release/spill incidents. 2) Include clarity regarding incipient and structural fires and emergency response to fires.

Revision 4	Date 12/16/2013
Writer	Philip Neal
Reviewer(s)	Bob Valvo
Approver(s)	Jeff Klier
Reason for Change	1) Include clarity regarding incipient and structural fires and emergency response to fires. Pg. 17 sections D through G and K

Revision 5	Date 8/2/2016
Writer	Philip Neal
Reviewer(s)	Scott Garner
Approver(s)	Earl Shoemake
Reason for Change	NAES and site procedure update reference. Exelon reference removal and written to be site specific.

Revision 6	Date 8/6/2018
Writer	Eleonora Witzky
Reviewer(s)	
Approver(s)	
Reason for Change	Wording changes noted as part of annual review

	Revision 7	**Date 1/4/2019**
Writer	Westley Curtis	
Reviewer(s)	Steve Reinhart	
Approver(s)	Steve Reinhart	
Reason for Change	Wording changes, reportable quantity/chemical chart additions, gas pipeline emergencies and contacts added	

	Revision 8	**Date 6/16/2020**
Writer	Scott Garner	
Reviewer(s)	Andy Duncan	
Approver(s)	Andy Duncan	
Reason for Change	Chemical list update from Nalco to Chemtreat	

	Revision 9	**Date 2/25/2021**
Writer	Linda Talbot	
Reviewer(s)	Andy Duncan	
Approver(s)	Andy Duncan	
Reason for Change	Updated the Emergency Notification Contact List to Include Asset Manager Jack Breen	

	Revision 10	**Date 3/29/2021**
Writer	Linda Talbot	
Reviewer(s)	Andy Duncan	
Approver(s)	Andy Duncan	
Reason for Change	Updated the Plant Evacuation Layout Figure Page 30	

	Revision 11	**Date 3/29/2021**
Writer	Linda Talbot	
Reviewer(s)	Andy Duncan	
Approver(s)	Andy Duncan	
Reason for Change	Updated the Emergency Notification contact list to include our new asset manager Dan Rorabaugh and old asset manager Jack Breen was removed.	

	Revision 12	**Date 10/22/2021**
Writer	Linda Talbot	
Reviewer(s)	Andy Duncan	
Approver(s)	Andy Duncan	
Reason for Change	Updated On-Site Reportable Chemical Table. Changes made to Table: ▪ Added Chem Treat Numbers to Cooling Tower Corrosion Inhibitor and Boiler Phosphate. • Changed the volume on site for the Sodium Hypochlorite tank from 5,000 gallons to 6,000 gallons. • Added note regarding usage of Caustic (25%) Sodium Hydroxide	

	• Updated reportable QTY Produce in lbs. for Sodium Hypochlorite (12.5%) to 800 lbs. from 100 lbs. Updated On-Site Chemical Table: • Deleted BL 1772 and added BL 17942 due to change in chemical number used. • Changed on site quantity for CL2632 from 350 gallons to 250 gallons • Changed on site quantity for CL240 from 20 gallons to 55 gallons • Added note regarding chemical mixture utilized to before outage only. Updated locations of SDS availability: • Deleted availability of SDS in binder in control room • Added SDS electronic storage website • Added that SDS location QR code can be found in red emergency response binders. Emergency response binders are located in the control room, maintenance department, and within each managers office Updated Contact Phone Number for Spill Response Contractor Safety Kleen from 888-375-5376 to 877-333-4244 Added Note Box to clarify the level of training required to respond and help with spill clean-up activities.

Revision 13	**Date 04/06/2022**
Writer	Edward Nielsen / Linda Talbot
Reviewer(s)	Andy Duncan
Approver(s)	Andy Duncan
Reason for Change	Minor editing to HAZWOPER response. • Consolidated notification steps from follow up section into immediate action steps to ensure timely response. • Minor administrative changes Edited Hazwoper response to include chemical response. Edited Earthquakes, Tornados, and Severe weather emergencies section • moved actions to PEP-007 Severe Weather Plan to support TAC 25.53 requirements and avoid duplicate procedures. Edited Bomb threats, Sabotage, Physical Damage to facility, and Cybersecurity events section • added reference to procedure to applicable NERC procedures CIP-003 and EOP-004 attachments to ensure proper notifications complete. • Minor sequence changes to incorporate NERC requirements

Revision 14	**Date 03/08/2023**
Writer	Edward Nielsen / Linda Talbot
Reviewer(s)	Andy Duncan
Approver(s)	Andy Duncan
Reason for Change	Annual Review. Moved cold and hot weather emergency response to PEP-007 Severe Weather Emergencies. Additional administrative corrections made.

EXHIBIT ERP-01A

PLANT EVACUATION LAYOUT

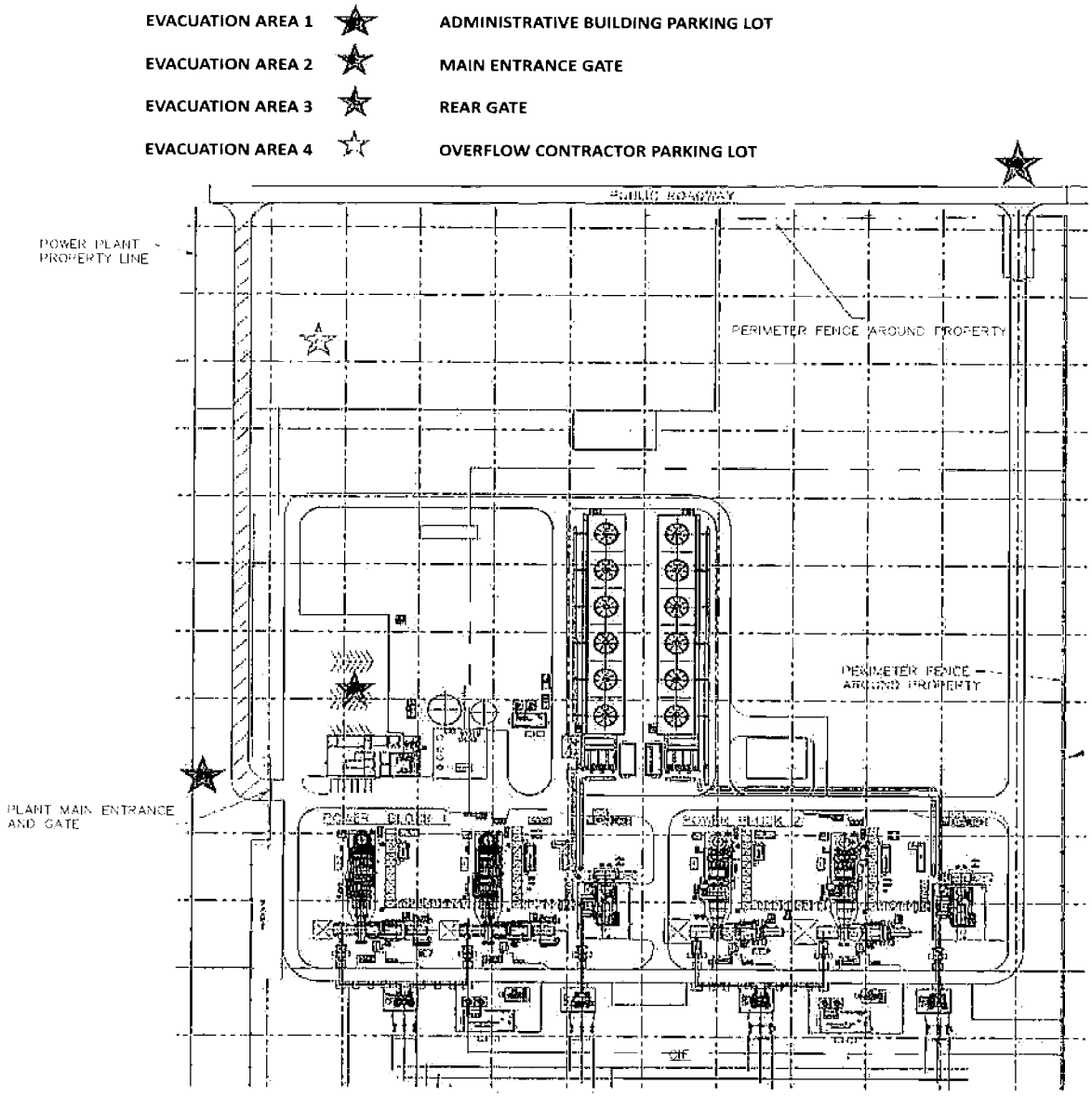

EXHIBIT ERP-01B Actions for Suspected Sabotage Events and Threats (Including Cybersecurity)

All personnel should pay close attention to the events described in the table below. For all situations, perform the following actions along with the supplementary actions and then refer back to Section 4:

1. **Immediately contact the Plant Manager (or designee in his/her absence).**
2. **Ensure that all on duty personnel are alerted to the possibility of a sabotage event.**
3. **Document as many details about the situation as possible. Note times, events, and descriptions as applicable to the situation.**
4. **If appropriate, notify law enforcement and parties of the interconnection as applicable.**
5. **Physical and Cybersecurity events require actions per NERC standards. Contact NERC Compliance Manager for assistance**

Event	Event Definition	Supplementary Actions
Abnormal Behavior of Personnel	Persons with disgruntled, violent, or threatening behavior. Persons with a history of health or financial problems or any other reason that may cause odd behavior.	• Stay calm and don't aggravate the situation • If they are receptive, try to calm the person down. Explain that you wish to help.
Unfamiliar/Unescorted Visitors	Anyone who is on-site without permission and without an escort	• Provide escort to a secure area of the facility • Gather information as to the purpose of their visit
Unexplained Packages or Shipments	Any delivery with questionable labeling or from an unknown shipping company. Any package of suspicious origins that cannot be identified.	• DO NOT DISTURB THE OBJECT • Refer to Exhibit ERP-01D - Suspected Bomb/Sabotage Device Safety Precautions
Abandoned Vehicles	Vehicles on-site or near the facility that are not recognized and have no purpose being there	• Inquire as to the owner of the vehicle • Record a description of the vehicle and its license plate number
Abnormal Observations	Observation of any suspicious persons taking pictures and/or notes around the facility.	• Attempt to identify the person and their intent • Take note of identifying details about the person and their method of transportation.

Event	Event Definition	Supplementary Actions
Equipment Misuse/Abuse	Unauthorized changes to equipment that affect functionality or deliberate efforts to damage or destroy equipment.	• Coordinate with the Plant Manager and the Control Room to place the facility in a safe condition if the affected equipment cannot be isolated from the system. • Determine the extent of which the equipment was misused/abused
Attempted Intrusion (Physical)	A detected effort to gain unauthorized access of a person or a device through the physical perimeter but without obvious success.	• Inform all personnel of the event and conduct a search of the area for anything or anyone that appears to be suspicious. • Secure all sensitive plant areas through any available means
Attempted Intrusion (Cyber)	A detected effort to gain unauthorized ingress or egress through the electronic perimeter or into an electronic perimeter device but without obvious success.	• Record all activity that led you to determine the event was an attempted intrusion • Using an alternate means of communications (e.g., cell phone), contact appropriate entities listed on Exhibit ERP-01F – Emergency Notifications Contact List • Refer to RCP-NERC-CIP-003 ATT E – Cybersecurity Incident Response Plan
Cyber and/or Communication Disruptions	Failure, degradation of functionality, or unauthorized access or use of facilities used for the exchange of voice or data.	• Record details of any suspicious events that led up to the disruption • Using an alternate means of communications (e.g., cell phone), contact appropriate entities listed on Exhibit ERP-01F – Emergency Notification Contact List • Refer to RCP-NERC-CIP-003 ATT E – Cybersecurity Incident Response Plan
Information Theft and/or Loss of Sensitive Plant Information	Unauthorized removal or loss of sensitive information.	• Record details about the theft including the last time you saw or used the data or documentation in question • Contact appropriate entities listed on Exhibit ERP-01F – Emergency Notification Contact List • Refer to RCP-NERC-CIP-003 ATT E – Cybersecurity Incident Response Plan
Unauthorized Modification of Software or Data	Unauthorized addition or modification of software or data associated with the proper operation of cyber assets.	• Record details regarding the modification • Ensure any affected systems are in a safe condition and close the affected programs. • Contact appropriate entities listed on Exhibit ERP-01F – Emergency Notification Contact List • Refer to RCP-NERC-CIP-003 ATT E – Cybersecurity Incident Response Plan

Event	Event Definition	Supplementary Actions
Multiple breaker operations in your switchyard and adjacent Transmission Owners switchyard	Multi-Site/Area Sabotage	◦ Inform operating personnel • Have operating personnel informed others in the Interconnection. • Call FBI ◦ Contact appropriate entities listed on Exhibit ERP-01F – Emergency Notification Contact List • Refer to RCP-NERC-EOP-004-ATT A Event Response Guidelines
Cyber systems for parties in the interconnection start showing equipment operation that has not physically occurred.	Multi-Site/Area Sabotage	• Inform operating personnel • Have operating personnel informed others in the Interconnection. ◦ Call FBI ◦ Contact appropriate entities listed on Exhibit ERP-01F – Emergency Notification Contact List • Refer to CIP policies and procedures. RCP-NERC-CIP-003 ATT E – Cybersecurity Incident Response Plan
Any Damage / destruction to the facility observed from actual or suspected intentional human action.	Damage to Facility	◦ Inform Operating Personnel and Operations Manager ◦ Investigate using cameras and walkdowns if safe to do so for cause of damage ◦ Contact appropriate entities listed on Exhibit ERP-01F – Emergency Notification Contact List • Refer to RCP-NERC-EOP-004-ATT A Event Response Guidelines – this includes event reporting guidance to DOE and NERC
Physical threats to the Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility	Potential Damage to Facility	• Inform Operating Personnel and Operations Manager • Contact appropriate entities listed on Exhibit ERP-01F – Emergency Notification Contact List • Refer to RCP-NERC-EOP-004-ATT A Event Response Guidelines – this includes event reporting guidance to DOE and NERC

EXHIBIT ERP-01C Bomb Threat Checklist

Instructions: Have someone else call police (911) and keep caller on the line. Listen; do not interrupt the caller except to ask:

1. When will it go off?_____
2. Where is it planted?_____
3. What floor is it on?_____
4. What kind of bomb is it?_____
5. What does it look like?_____
6. Why are you doing this?_____
7. Who are you?_____
8. Where are you?_____

Call received by:_____ Time of Call_____

Date_____ Time of Hang-up_____

Description of Caller: ☐ Male ☐ Female ☐ Adult ☐ Juvenile _____ App. Age

Voice Characteristics		Speech		Language	
☐ Loud	☐ Soft	☐ Fast	☐ Slow	☐ Excellent	☐ Good
☐ High Pitch	☐ Deep	☐ Distinct	☐ Distorted	☐ Fair	☐ Poor
☐ Pleasant	☐ Raspy	☐ Stutter	☐ Nasal	☐ Four	☐ Other
☐ Intoxicated		☐ Slurred	☐ Precise	Use of Certain Words or Phases:	
☐ Other		☐ Other			
Accent		**Manner**		**Background Noises**	
☐ Local	☐ Not Local	☐ Calm	☐ Angry	☐ Office	☐ Street
☐ Foreign	☐ Regional	☐ Rational	☐ Irrational	☐ Machines	☐ Traffic
☐ Race	☐ Other	☐ Coherent	☐ Incoherent	☐ Factory	☐ Airplanes
Explain:		☐ Deliberate	☐ Emotional	☐ Machines	☐ Trains
		☐ Righteous	☐ Laughing	☐ Bedlam	☐ Voices
		Is voice familiar? Sounds like _____		☐ Animals	☐ Music
				☐ Quiet	☐ Party
				☐ Mixed	☐ Atmosphere

Action to take immediately after call:

1. Notify plant management.
2. Notify Owner's Representative.
3. Notify NAES Headquarters' Management.
4 Refer to RCP-NERC-EOP-004-ATT-A for NERC related reporting
5. Forward a copy of this to parties above ASAP.
6. Write exact statement or caller below:

_____

_____

EXHIBIT – ERP-01D Suspected Bomb/Sabotage Device Safety Precautions

The safety precautions below are designed to acquaint you with dangers inherent in the search, discovery, and handling of "suspected bombs" or "Suspected Sabotage Devices".

While some of the following safety precautions may seem elementary, do not dismiss them as unimportant nor take them for granted, because adequate knowledge of these precautionary provisions may save your life or the lives of other plant operators and visitors.

1. Do not touch a suspected object.
2. Do not shake, shock, or jar a suspected Bomb/Device.

WARNING

The presence of nearby equipment/storage tanks that could present secondary hazards in the event of explosion or other sabotage event.

3. Do not use radio equipment near the Bomb/Device to transmit messages.
4. Do not move light switches.
5. Do not smoke.
6. Do not accept the contents of any container as bona fide, simply because it was delivered by routine means.
7. Do not accept container markings and/or appearance as sole evidence of their contents' identification and legitimacy.
8. Do not cover a suspected bomb/device.
9. Do not carry a suspected bomb/device.
10. Do not assume that a suspected bomb/device is of a specific (high explosive or incendiary) type.
11. Do not open any suspicious container or object.
12. Do not cut a string, cord, or wire on a suspicious container or object.
13. Do not cut or remove the wrapper on a suspicious object or container.
14. Do not unscrew the cover, move the latch or hook on the cover, or raise or remove the cover of a suspicious container.
15. Do not change the position of a suspicious container or object.
16. Do not place a suspicious container or object into water.

EXHIBIT ERP-01D

EMERGENCY RESPONSE EVENT LOG

Emergency Description:_____

_____

_____

Date and Time of Emergency:_____

Note: Log all events associated with the emergency chronologically. Keep logs factual and concise.

EXHIBIT ERP-01E

EMERGENCY RESPONSE CALL RECORD FORM

Emergency Description: _____

_____

Date and Time of Emergency: _____

Time	Company/Agency Notified	Name of Contact	Name of Notified

Description of Correspondence:

_____

_____

_____

Time	Company/Agency Notified	Name of Contact	Name of Notified

Description of Correspondence:

_____

_____

_____

Time	Company/Agency Notified	Name of Contact	Name of Notified

Description of Correspondence:

_____

_____

_____

EXHIBIT ERP-01F

EMERGENCY NOTIFICATION CONTACT LISTS

Person/Organization	Primary Phone Number	Secondary Phone Number
Plant Manager Primary Emergency Coordinator Andy Duncan	(432) 272-8572	
Operations Manager Secondary Emergency Coordinator Scott Garner	(432) 272-8514	(432) 352-3615 (Cell)
Maintenance Manager (Response to Material/Equipment Issues) Pablo Chaves	(432) 272-8515	
EHS Manager (Environmental, Health, Safety Issues) Linda Talbot	(432) 272-8578	
Plant Engineer / NERC Compliance (Physical and Cybersecurity Incidents) Edward Nielsen	(432) 272-8530	
Operations Director Corporate Contact Rob Simmerman		
Asset Manager Rob Watson		
City of Odessa Police / Fire Department	911	(432) 333-3641 (Dispatcher) for non-emergencies
Law Enforcement: Ector County	911	Ector County Sheriff: 432-335-3050 for non-emergencies
Hospital: Medical Center Hospital	(432) 640-6587	
Ambulance/EMS:	911	
Ector County Emergency Management Coordinator (Assistance coordinating resources when 911 not suitable)	(432) 257-0502	

ENVIRONMENTAL AGENCIES EMERGENCY NOTIFICATION LIST

Person/Organization	Telephone Number
National Response Center (NRC)	(800) 424-8802
Local TCEQ Field Office (Midland)	(432) 570-1359
Texas Emergency Management Agency (24-hour)	(800) 832-8224
Ector County Emergency Planning Committee	(432) 335-4654 Spill Phone (911)

EXHIBIT ERP-01F - EMERGENCY NOTIFICATION CONTACT LISTS (Continued)

OIL SPILL RESPONSE CONTRACTORS' NOTIFICATION LIST

Contractor	Phone Numbers	Response Time	Contractor Responsibility
Safety Kleen	877-333-4244	< 2 hours	Spill Response, containment, and cleanup

GAS PIPELINE NOTIFICATION LIST

Contractor	Phone Numbers	Response Time	Contractor Responsibility
Richard Partin Exel Pipeline	602-376-8972/480-883-8512	As soon as possible	Identification/isolation as needed
Robert Eubank Exel Pipeline	432-202-1391	<2-Hours	Identification/isolation as needed
Oneok (Gas Supplier)	800-562-5879	<2-Hours	Personnel Notification
Enterprise (Gas Supplier)	800-644-4773	<2-Hours	Personnel Notification

Annual Drill Notification

Contact	Phone Numbers / Contact Info	Notes
PUC	eopdrillnotice@puc.texas.gov	Required 30 days in advance
TDEM	https://www.tdem.texas.gov/regions/region-4 O:(432) 498-2175 C:(432) 416-0063	Verify contact on website. Notify 30 days in advance for at least 1 drill annually.

QuailRun POWER

Training Record

Topic: Annual EOP Training

Work Group: Quail Run | Instructor: Linda Talbot

Date: March 3, 2023 -March 10, 2023

Present

Patterson, John	Mechanical Maint. Tech	3/8/23	Michael Hudgins	Control Room Operator	3/7/23
Bell, Randy	System Technician	3/8/23	Burns, Yesenia	Plant Administrator	3/8/23
Baze, Derrick	Auxiliary Plant Operator	3-8-23	Runa, Stan	IC&E Technician	N/A
	Auxiliary Plant Operator		Rick Leon	IC&E Technician	3/8/23
Pate, Cliff	Lead Control Room Operator	3-4-23	Torres, Ramon	Auxiliary Plant Operator	
Santa, Mark	Control Room Operator	3-5-23	Mooney, James	Auxiliary Plant Operator	3-4-23
Breazeale, Kenneth	Mechanical Maint. Tech	3/8/23	Garner, Scott	Operations Manager	3/8/23
Juan Carrillo	Auxiliary Plant Operator		Procter, Wade	Control Room Operator	3-4-23
Jaime Rendon	Auxiliary Plant Operator	3/5/23	Chaves, Pablo	Maintenance Manager	3/8/2023
Brian Austin	Auxiliary Plant Operator	3/5/23	Duncan, Andy	Plant Manager	3/8/23
Hooks, Kelby	Control Room Operator	3-4-23	Galvan, Cruz	Auxiliary Plant Operator	3/5/23
Linda Talbot	EHS Manager	3-6-23	Benbow, Jeffrey	IC&E Technician	3/8/23
Valdez, Jorge	Mechanical Maint. Tech	3-8-23	Nielsen, Ed	Plant Engineer	3/6/2023

unredacted Form
submitted to PUC
at emc@puc.texas.gov

Emergency Contact Information Update

Background

16 Texas Administrative Code §25.53(e) and §26.51(b)(4) require electric market entities and telecommunications utilities to provide emergency contact information to the Commission. In addition, should this information change, these entities must provide the updated information to the Commission within 30 days. This information may be sent to the Commission using either mail or email at the addresses below: (Please complete this form in its entirety)

Public Utility Commission of Texas
Attention: Emergency Management Coordinator
1701 Congress Ave., PO Box 13326
Austin, TX 78711-3326
emc@puc.texas.gov – Subject line: "Emergency Contact Information"

Entity Information

Entity Name: QUAIL RUN ENERGY PARTNERS LP	**Certificate or Registration #:** 20169	
Texas Address: 2950 E. INTERSTATE 20		
City: ODESSA	**ZIP:** TX	**Customer Service Phone #:** 432-272-8572

Emergency Contact Information

Primary Emergency Contact:		
Name:	**Title:** Plant Manager	
Address: 2950 E. Insterstate 20		
City: Odessa	**State:** TX	**ZIP:** 79766
Email:		
Office Phone:	**Cell Phone:**	**Fax:**

Secondary Emergency Contact:			
Name:		**Title:** Operations Manager	
Address: 2950 E. Interstate 20			
City: Odessa		**State:** TX	**ZIP:** 79766
Email:			
Office Phone:	**Cell Phone:**	**Fax:**	
Tertiary Emergency Contact:			
Name:		**Title:** Asset Manager	
Address:			
City:		**State:**	**ZIP:**
Email:			
Office Phone:	**Cell Phone:**	**Fax:**	

PEP- 002-APPENDIX-A AFFIDAVIT

Affidavit per TAC 25.53 (c) (4) (C)

AFFIDAVIT OF MADE IN SUPPORT OF Quail Run Energy Center Partners, LP

POWER GENERATING COMPANY COMPLIANCE FILING PURSUANT TO P.U.C. SUBSTANTIVE RULE § 25.53

1. I am Rob Waton/Asset Manager (name/title) I am responsible for supervising operations at Quail Run Energy Center and accordingly, I am familiar with the facts attested to herein.
2. All operating personnel at Quail Run Energy Center are familiar with and have received training on the contents of Quail Run Energy Center's Emergency Operating Procedures. Trained operating personnel are instructed to follow the applicable portions of the EOP except the extent deviations are appropriate as a result of the circumstances during the course of an emergency
3. All procedures are reviewed and approved by the appropriate manager responsible for the scope of the corresponding procedure.
3. For the year 2022, the EOP was activated due to a cold weather OCN issued by ERCOT. Therefore per TAC 25.53 2.D.3, a drill was not required since the EOP was activated.
4. Quail Run Energy Center's Emergency Operating Procedures currently do not require to be distributed to any local jurisdictions.
5. Quail Run Energy Partners, LP maintains a business continuity plan that addresses returning to normal operation after disruptions caused by an incident.
6. Site management personnel at Quail Run Energy Center have completed National Incident Management System training.

Rob Watson

Digitally signed by: Rob Watson
DN: CN = Rob Watson O = Electric Reliability Council of Texas, Inc. OU = EmployeeID - 09232020RWATSON, MP - QUAIL RUN ENERGY PARTNERS LP (RE), DUNS Number - 788151350, ERCOT Enterprise, 09232020RWATSON, 788151350
Date: 2023.03.13 15:04:45 -04'00'

(signature / date)

Quail Run Energy Partners, LP
2950 E Interstate 20
Odessa, Tx 79766

(Company / Address)