

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 Astra Wind, LLC’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 Astra Wind, LLC as an entity with Low Impact BES Cyber Systems with Low Impact External Routable Connectivity (LERC) and Low Impact Electronic Access Point (LEAP) Cyber Assets. Astra Wind, LLC does not have any Medium or High Impact BES Cyber Systems.

| CIP-003 Standard Applicability | | | | | | | | | | | |
|--------------------------------|-------|------|-----|---------------|-------|------|-----|------------|------|------|--|
| High Impact | | | | Medium Impact | | | | Low Impact | | | |
| BCS | EACMS | PACS | PCA | BCS | EACMS | PACS | PCA | BCS | LEAP | LERC | |
| R2 | | | | | | | | ✓ | ✓ | ✓ | |

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 Astra Wind, LLC 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>

The following definitions help to understand the requirements of CIP-003 R2.

Low impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Low Impact Electronic Access Point (LEAP): A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

| | |
|---|---|
| RCP-NERC-CIP-003-ATT-A ASTRA WIND, LLC - HAPPY, TX | |
| Referencing Documents: NERC-RCP-CIP-003 R1.2 | Rev. 0 Revision Date: March 31, 2017 |

CYBER SECURITY POLICY

2. GENERAL

Astra Wind, LLC has developed this Cyber Security Policy to outline the Astra Wind, LLC’s commitment on protecting its Low Impact BES Cyber Systems. The intent is to ensure that all personnel are fully aware of their responsibilities and duties with regard to cyber security and protecting the Bulk Electric System.

This Cyber Security Policy addresses the security topics outlined in NERC CIP-003 R1.2. It further addresses the specific recommended security topics detailed in the CIP-003 Guidelines and Technical Basis section and CIP-003 – Attachment 1.

3. CYBER SECURITY AWARENESS (SECTION 1)

The details of Astra Wind, LLC’s Cyber Security Awareness program can be found in RCP-NERC-CIP-003-ATT-B. It is the policy of Astra Wind, LLC that all relevant personnel (relevant is defined as any employee, contractor, or vendor, who has a need for physical access to a Low Impact BES Cyber System), be subject to a Cyber Security Awareness program.

4. PHYSICAL SECURITY CONTROLS (SECTION 2)

The details of Astra Wind, LLC’s physical security controls can be found in the RCP-NERC-CIP-003-ATT-C.

Examples of acceptable methods of securing Low Impact BES Cyber System sites:

- Card Keys
- Biometrics
- Key Pads
- Locks
- Fences and gates that are in good condition

5. ELECTRONIC ACCESS CONTROLS (SECTION 3)

The details of Astra Wind, LLC’s electronic access controls can be found in RCP-NERC-CIP-003-ATT-D. It is the policy of Astra Wind, LLC that all Low Impact BES Cyber Systems facilities shall be protected by a LEAP, and restricted to only those employees, contractors, or vendors who have a need for access.

All LERCs (if any) for a Low Impact BES Cyber System facilities shall pass through a LEAP that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are confined to only those that are deemed necessary (e.g., IP addresses, ports, or services). (3.1)

Dial-up connectivity to a Low Impact BES Cyber System, per Cyber Asset capability shall be set to one of the following: (3.2)

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

| | |
|---|---|
| RCP-NERC-CIP-003-ATT-A ASTRA WIND, LLC - HAPPY, TX | |
| Referencing Documents: NERC-RCP-CIP-003 R1.2 | Rev. 0 Revision Date: March 31, 2017 |

CYBER SECURITY POLICY

- Incoming Dial-up Connectivity is to a dial back modem.
- A modem that must be remotely controlled by the control center or control room.
- The Cyber Asset has some form of access control.
- The low impact BES Cyber System has access control that includes the Dial-up devices.

6. CYBER SECURITY INCIDENT RESPONSE PLAN

The details of Astra Wind, LLC's Cyber Security Incident response plan can be found in RCP-NERC-CIP-003-ATT-E. The Cyber Security Incident response plan includes the following:

A. RECOGNITION AND NOTIFICATION OF CYBER SECURITY INCIDENTS

The Cyber Security Incident response plan is intended as a guide to understand how to recognize and respond to a cyber-security incident. The plan shall be used in all situations where there a security incident.

B. CYBER INCIDENT REPORTING OBLIGATION

Astra Wind, LLC shall ensure that all events determined to be Reportable Cyber Security Incidents are formally reported to the E-ISAC, unless prohibited by law. A process for this specific obligation shall be developed and included in Astra Wind, LLC's Cyber Security Incident response plan.

C. ROLES AND RESPONSIBILITIES

Roles and responsibilities for Cyber Security Incident response are documented in Appendix 1 of RCP-NERC-CIP-003-ATT-E.

D. TESTING OF THE RESPONSE PLAN

The response plan shall be tested once every 36 months and any changes shall be updated within 180 days of the change within RCP-NERC-CIP-003-ATT-E.

| | |
|---|---|
| RCP-NERC-CIP-003-ATT-A ASTRA WIND, LLC - HAPPY, TX | |
| Referencing Documents: NERC-RCP-CIP-003 R1.2 | Rev. 0 Revision Date: March 31, 2017 |

CYBER SECURITY POLICY

7. REVIEW

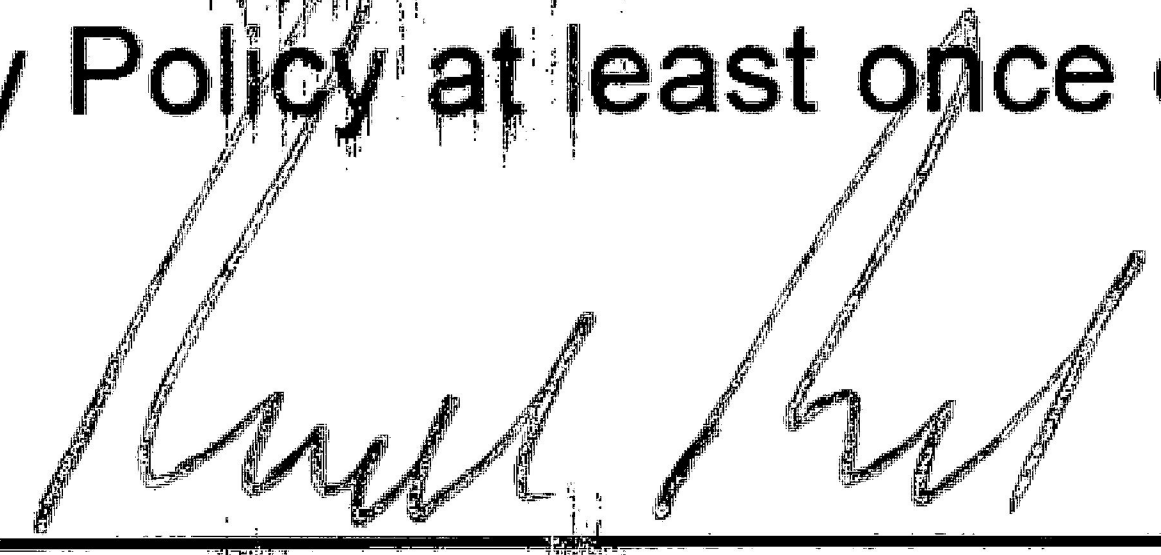
Astra Wind, LLC shall review and obtain CIP Senior Manager approval of this Cyber Security Policy document at least once every fifteen (15) calendar months.

8. POLICY RESPONSIBILITY


The Astra Wind, LLC CIP Senior Manager is the responsible person for this policy.

9. FIFTEEN (15) CALENDAR MONTH CIP SENIOR MANAGER APPROVAL

The CIP Senior Manager (as defined in RCP-NERC-CIP-ATT-H) shall review and approve the Cyber Security Policy at least once every fifteen (15) calendar months.



CIP Senior Manager
Rich Boone



Date

| | |
|---|---|
| RCP-NERC-CIP-003-ATT-A ASTRA WIND, LLC - HAPPY, TX | |
| Referencing Documents: NERC-RCP-CIP-003 R1.2 | Rev. 0 Revision Date: March 31, 2017 |

CYBER SECURITY POLICY

Latest Revision Approval: (Revision History)

Written By: NAES Corporation Date: March 31, 2017

Approved By: Walter Bukowski Date: March 31, 2017

| REVISION HISTORY LOG RCP-NERC-CIP-003-ATT-A | | | | |
|--|-------------------|--|----------------|----------------------|
| Rev. | Date | Description | By Initials | Approval Initials |
| D1 | 10/13/2015 | Revised to meet revision requirements. | DTB | AGB |
| 0 | March 31, 2017 | Updated template to Rev 0 for plant use. Astra Wind Implementation | MMT | RR |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |

RCP-NERC-CIP-003-ATT-C
ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
RCP-NERC-CIP-003 R2

Revision: 2
Revision Date: July 03, 2024

PHYSICAL SECURITY CONTROLS

1. INTRODUCTION.....2

 A. PURPOSE.....2

 B. SCOPE.....2

 C. DEFINED TERMS.....2

2. CONTROLLING PHYSICAL ACCESS2

 A. PHYSICAL ACCESS CONTROLS & MONITORING2

 B. PROCEDURES FOR GRANTING AND REVOKING PHYSICAL ACCESS.....3

3. INTERNAL CONTROLS/EVIDENCE4

4. REVIEWS AND UPDATES4

5. PROGRAM RESPONSIBILITY4

RCP-NERC-CIP-003-ATT-C ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
RCP-NERC-CIP-003 R2

Revision: 2
Revision Date: July 03, 2024

PHYSICAL SECURITY CONTROLS

1. INTRODUCTION

A. PURPOSE

This document defines Astra Wind, LLC's Physical Security Controls program. The purpose of this program is to ensure that Astra Wind, LLC's Low Impact BES Cyber Systems have adequate physical security controls.

B. SCOPE

CIP-003 R2 applies to Astra Wind, LLC as an entity with Low Impact BES Cyber Systems. Astra Wind, LLC does not have any Medium or High Impact BES Cyber Systems. Astra Wind, LLC 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-003-7, 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 Astra Wind, LLC 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

Astra Wind, LLC has defined a number of operational and procedural controls to restrict physical access to the Astra Wind, LLC'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

Astra Wind, LLC has implemented and documented the following physical access controls for its Low Impact BES Cyber Systems:

1. Fences with locking gates around the Operations & Maintenance Building and substation. The gates are open during normal business hours when personnel are onsite. The gates are closed outside of normal business hours.
2. Keyed doors e.g. power house buildings, computer rooms
3. Enclosed computer room with locks (physical keys control access to the rooms). The site manager possesses and maintains access to the key.

Astra Wind, LLC has implemented and documented one or more of the following physical access monitoring devices for its Low Impact BES Cyber Systems.

RCP-NERC-CIP-003-ATT-C

ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
RCP-NERC-CIP-003 R2

Revision: 2
Revision Date: July 03, 2024

PHYSICAL SECURITY CONTROLS

4. Monitored surveillance cameras (currently being installed).
5. Monitored alarms (currently being installed)
6. Human Observation

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 Facility Manager based on need. Astra Wind, LLC shall retain evidence that access is controlled per this procedure. Access is controlled via a key log. The Facility Manager maintains the key log.

Identified Roles Requiring Access:

1. Systems support personnel - ensure that BES Cyber Systems are set up and working correctly.
2. Plant management staff including engineers - supervise plant employees.
3. Technicians - ensure proper operation and maintenance of the facility.
4. Asset Managers (Owner Representatives) - ensure assets are maintained to the asset owner's satisfaction and ensure proper operation and management decisions.
5. Project Managers - ensure that the plant staff are maintaining the asset per contract requirements.
6. Plant Admin Staff - ensure plant communications and business continuity.

Temporary Access

Other positions as dictated by plant needs may include:

1. Delivery Personnel / Contractors – plant personnel 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.
2. Visitors – plant personnel 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 control room or administration building to sign in and out on the visitors' log. The visitors' log will document each visitor's name, 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.

| | |
|---|---|
| RCP-NERC-CIP-003-ATT-C ASTRA WIND, LLC - HAPPY, TX | |
| Referencing Documents: RCP-NERC-CIP-003 R2 | Revision: 2 Revision Date: July 03, 2024 |

PHYSICAL SECURITY CONTROLS

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:

1. Change of padlock combination
3. Revoking access to the physical key
4. Removing electronic access in electronic access control or other firewall devices.

3. INTERNAL CONTROLS/EVIDENCE

Astra Wind, LLC has implemented the following, additional physical security controls:

Quarterly reviews and documentation to validate business need, and employee status of:

- Keyed entry point lists
- Physical Key and Inventory that contains identification of assigned personnel and key number

Other routine reviews or controls:

- Inspections of the security fence or other physical controls
- Test of alarm notifications (door held open, door forced open, unauthorized access attempts) (currently being installed).

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 Astra Wind, LLC's CIP Senior Manager or delegate is the responsible person for this program and shall approve revisions.

RCP-NERC-CIP-003-ATT-C
ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
RCP-NERC-CIP-003 R2

Revision: 2
Revision Date: July 03, 2024

PHYSICAL SECURITY CONTROLS

Latest Revision Approval: (Revision History)

Written By: NAES Corp

Date: 2/15/2019

Approved By: Rich L. Rohde

Date: 7/3/2024

| REVISION HISTORY LOG RCP-NERC-CIP-003-ATT-C | | | | |
|--|------------|---------------------------|----------------|----------------------|
| Rev. | Date | Description | By Initials | Approval Initials |
| 0 | 3/31/2017 | Updated Template to Rev 0 | MMT | RLR |
| 1 | 12/31/2019 | Updated for CIP Vers 7 | MMT | RLR |
| 2 | 07/03/2024 | Updated access protocols | SS | RLR |
| 3 | | | | |

RCP-NERC-CIP-003-ATT-K ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
NERC-CIP-003 R2, Attachment 1, Section 5

Revision: 1
Revision Date: December 31, 2019

Transient Cyber Asset & Removable Media Authorization Record

| | | |
|--|---|--|
| TC Asset/RM Owner: <input type="checkbox"/> Astra Wind, LLC/Astra Wind, LLC <input type="checkbox"/> Vendor Name: _____ | | |
| TC Asset/RM Identifier: | Date: | TCA or RM Record #: |
| Date Range of Intended Use: | Start Date: | End Date: |
| TCA or RM Type or Group: <input type="checkbox"/> Laptop <input type="checkbox"/> Flash Media <input type="checkbox"/> Portable Hard Drive <input type="checkbox"/> Test Equipment <input type="checkbox"/> Other: _____ | Purpose: <input type="checkbox"/> Data Transfer <input type="checkbox"/> Vulnerability Assessment <input type="checkbox"/> Maintenance <input type="checkbox"/> Trouble shooting <input type="checkbox"/> Other: _____ | BES Cyber System: List: _____ _____ |
| Describe process to be used to allow for automatic installation of security patches, anti-virus signature updates, and policy updates. Third party vendors or contractors may submit an attestation indicating their company's policy for Transient Cyber Assets used by field engineers to comply with NERC CIP requirements to mitigate the introduction of malicious code into an entity's cyber systems. | | |
| Malware Protection Malware Application used? Update Version Level? | Describe malware update process | |
| Application Whitelisting | Describe process used | |
| System Hardening | Describe process to harden the asset | |

RCP-NERC-CIP-003-ATT-K
ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
NERC-CIP-003 R2, Attachment 1, Section 5

Revision: 1
Revision Date: December 31, 2019

Other processes used to mitigate the introduction of malicious code:

Indicate enabled bridged network functionality, if applicable: (I.e. wireless, Bluetooth, IRD...)

TCA Authorization Date:

TCA Revocation Date:

Signature

Signature

X _____
Astra Wind, LLC Representative

X _____
Vendor Representative

Additional Comments/Notes:

RCP-NERC-CIP-003-ATT-K
ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
NERC-CIP-003 R2, Attachment 1, Section 5

Revision: 1
Revision Date: December 31, 2019

Latest Revision Approval: (Revision History)

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

Approved By: Rich L. Rohde Date: December 31, 2019

| REVISION HISTORY LOG RCP-NERC-CIP-003-ATT-K | | | | |
|--|------------|---------------------------|----------------|----------------------|
| Rev. | Date | Description | By Initials | Approval Initials |
| 0 | 3/31/2017 | Updated Template to Rev 0 | MMT | RLR |
| 1 | 12/31/2019 | Updated for CIP Vers 7 | MMT | RLR |
| 2 | | | | |
| 3 | | | | |

RCP-NERC-CIP-003-ATT-L
ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
NERC-CIP-003 R1.2.6

Revision: 1
Revision Date: December 31, 2019

CIP EXCEPTIONAL CIRCUMSTANCES PROCEDURE

| | |
|---|----------|
| 1. INTRODUCTION..... | 2 |
| A. PURPOSE..... | 2 |
| B. SCOPE..... | 2 |
| C. DEFINITIONS AND DEFINED TERMS | 2 |
| 2. CIP EXCEPTIONAL CIRCUMSTANCES PROCESS | 2 |
| A. IDENTIFYING AN EXCEPTIONAL CIRCUMSTANCE..... | 2 |
| B. DECLARATION OF A CIP EXCEPTIONAL CIRCUMSTANCE..... | 3 |
| C. DOCUMENTING A CIP EXCEPTIONAL CIRCUMSTANCE | 3 |
| D. APPLICABLE REQUIREMENTS | 3 |
| E. REVIEWING A CIP EXCEPTIONAL CIRCUMSTANCE | 3 |
| 3. PROCEDURE RESPONSIBILITY | 3 |

RCP-NERC-CIP-003-ATT-L ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
NERC-CIP-003 R1.2.6

Revision: 1
Revision Date: December 31, 2019

1. INTRODUCTION

A. PURPOSE

This document describes the process followed at Astra Wind, LLC to request, review, approve, and track CIP Exceptional Circumstances.

B. SCOPE

CIP-003 R1.2.6 applies to Astra Wind, LLC as an entity with Low Impact BES Cyber Systems. Astra Wind, LLC 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 Astra Wind, LLC-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.”

| | |
|---|---|
| RCP-NERC-CIP-003-ATT-L ASTRA WIND, LLC - HAPPY, TX | |
| Referencing Documents: NERC-CIP-003 R1.2.6 | Revision: 1 Revision Date: December 31, 2019 |

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

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 Department Manager/Director affected by the exception and the designated CIP Senior Manager or delegate.
3. Acceptance of the exception results is verified in periodic reviews by Astra Wind, LLC until the exception is removed or retired.

3. PROCEDURE RESPONSIBILITY

The Astra Wind, LLC CIP Senior Manager is responsible for this Procedure.

RCP-NERC-CIP-003-ATT-L
ASTRA WIND, LLC - HAPPY, TX

Referencing Documents:
NERC-CIP-003 R1.2.6

Revision: 1
Revision Date: December 31, 2019

Latest Revision Approval: (Revision History)

Written By: NAES Corporation

Date: 2/15/2019

Approved By: Rich L. Rohde

Date: December 31, 2019

| REVISION HISTORY LOG RCP NERC 003-ATT-L | | | | |
|--|------------|---------------------------|----------------|----------------------|
| Rev. | Date | Description | By Initials | Approval Initials |
| 0 | 3/31/2017 | Updated Template to Rev 0 | MMT | RLR |
| 1 | 12/31/2019 | Updated for CIP Vers 7 | MMT | RLR |
| 2 | | | | |
| 3 | | | | |

Astra Wind
Emergency Operations Plan (EOP)
(Per 16 TAC Sect. 25.53)

Attachment I



BUSINESS CONTINUITY PLAN

| | |
|------------------|------------|
| Document Version | 1.2 |
| Date | 04/01/2025 |

| Document Properties | |
|---------------------|-------------------|
| Property | Description |
| Circulation | Internal Use Only |
| Classification | Confidential |
| Document Owner | VP Operations |

| Revision History | | | |
|------------------|------------|------------------------|-------------|
| Version | Date | Description of Changes | Revised by |
| 1.0 | 09/29/2020 | Finalized | Chris Sweet |
| 1.1 | 10/20/2021 | Annual Review | Chris Sweet |
| 1.2 | 04/01/2025 | Minor Edits | Rich Rohde |

September 2020

Contents

| | |
|---|-----------|
| EXECUTIVE OVERVIEW | 5 |
| 1. INTRODUCTION | 6 |
| Overview | 6 |
| Plan Scope & Applicability | 6 |
| Plan Objectives | 6 |
| Plan Assumptions | 6 |
| 2. RISK ASSESSMENT | 8 |
| 3. CRITICAL BUSINESS FUNCTIONS | 10 |
| Overview | 11 |
| 4. PLAN ACTIVATION PROCEDURES..... | 15 |
| Plan Activation During Normal Business Hours..... | 15 |
| Plan Activation Outside Normal Business Hours..... | 15 |
| Actions upon Activation | 15 |
| 5. INTERNAL COMMUNICATION PROCEDURES..... | 16 |
| Staff accountability for a facility evacuation | 16 |
| 6. ALTERNATE FACILITIES..... | 17 |
| 7. ORDERS OF SUCCESSION AND DELEGATIONS OF AUTHORITY | 18 |
| 7.1 OVERVIEW..... | 18 |
| 7.2 ORDERS OF SUCCESSION..... | 18 |
| 7.3 DELEGATIONS OF AUTHORITY..... | 18 |
| 8. PLAN DEACTIVATION | 19 |
| 8.1 OVERVIEW | 19 |
| 8.2 CRITERIA FOR PLAN DEACTIVATION..... | 20 |
| 8.3 RESUMPTION PROCEDURES..... | 20 |
| 9. EMPLOYEE CONTACT LIST..... | 22 |
| Table 8 | 22 |
| 10. VENDOR CONTACT LIST..... | 24 |
| 11. FAMILY EMERGENCY PLAN..... | 27 |
| 11.1 Basic Disaster Supplies Kit | 27 |
| 11.2 Additional Emergency Supplies | 27 |

| | |
|---|-----------|
| 12. TRAINING..... | 28 |
| 13. ANNUAL PLAN AUDIT | 28 |
| 14. INSURANCE CONSIDERATIONS | 29 |
| OWNERSHIP AND REVIEW | 30 |
| CONTACT INFORMATION | 30 |

EXECUTIVE OVERVIEW

This plan includes an overview of continuity operations, outlines the approach for supporting an organization's critical business functions, and defines the roles and responsibilities of staff. It also outlines the orders of succession, notification procedures and communication methods, plan activation and deactivation protocols, provisions for alternate work locations, and the plan for maintaining and restoring access to vital records.

This document establishes procedures and processes to maintain operational continuity for businesses based on three types of disruptions that could occur individually or in any combination:

- Loss of access to parts of or the entire facility (e.g., following a fire, sudden storm, or flooding).
- Loss of services due to a reduction in workforce (e.g., during pandemic Covid-19).
- Loss of services due to equipment or systems failure (e.g., information technology (IT) systems failure, electrical grid failure).

1. INTRODUCTION

Overview

The Business Continuity of Operations (BCOP) planning ensures businesses can continue or immediately resume performing their organization's critical business functions, which are the functions that support the organization's mission, comply with legal requirements, and support life-safety, under all circumstances. This includes natural, technological, and man-made incidents, as well as incidents that result in loss of access to parts of or an entire facility or loss of service due to equipment or systems failure. The benefit of BCOP planning includes the ability to anticipate response actions following a myriad of incidents, improve the businesses performance of its critical business functions, and ensure timely recovery.

Plan Scope & Applicability

The scope of this plan covers active WindHQ Operations sites. The plan is applicable once the safety of employees, customers, and guests has been verified and if a facility is or will become inaccessible. It can be active during normal business hours and after hours, with and without warning.

Plan Objectives

The WindHQ Operations Business Continuity Plan objective is to facilitate the resumption of critical operations, functions, and technology in a timely and organized manner to ensure a viable and stable organization. In doing this it is critical to ensure the safety and well-being of employees, customers, and guests.

The primary objectives of the plan are to:

- Maintain Critical Business Functions
- Ensure that employees have safe access to facility.
- Protect vital records.
- Ensure that records are accessible under all conditions.

Plan Assumptions

The following assumptions were used while creating this plan:

- An event has occurred that affects normal business operations.
- There is limited or no access to the affected facility.

- Documents and equipment within the facility are inaccessible.
- Qualified personnel are available to continue operations.

2. RISK ASSESSMENT

The following table reflects hazard probability assumptions.

Table 1. 2017 Hazard Mitigation Analysis

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
|-----------------------------------|---|---|--|---|--|
| Flooding | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Hurricane Tropical Storms | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Thunderstorm Lightning Hail | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Tornado | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Winter Storms Ice Storms | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| High Winds | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Wildfire | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
|------------|---|---|--|---|--|
| Landslide | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Earthquake | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |

Table 1.1 WindHQ Hazard Mitigation Analysis

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
|---|---|---|--|---|--|
| Loss of Power (Utility) | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Loss of employees (Pandemic or illness) | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Loss of equipment (Electrical failure) | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Loss of Equipment (Mechanical failure) | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Loss of Equipment IT | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
|----------------------|---|---|--|---|---|
| Cyber Attack | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low |
| Fire | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Injury or accident | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low |
| Environmental Hazard | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low |
| Security Threat | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Bio-Hazard | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low |
| Reputational Threat | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Low |
| | | | | | <input type="checkbox"/> |

3. CRITICAL BUSINESS FUNCTIONS

Overview

WindHQ owns and operates the Astra Wind Farm. Astra is connected to ERCOT's transmission system. Astra is a registered PGC with ERCOT and provides renewable (wind) energy to the ERCOT transmission system.

Tables 3 - 3.2 provide a list of the WindHQ critical business functions. This includes the main business process, a list of the responsible staff, trusted vendors, vital records, and the permissible downtime.

Table 3. Critical Business Function

| WindHQ Critical Business Function | | | | |
|--|---------------------------|--|---|-----------------------|
| Critical Business Function 1: Maintain the wind farm in operating condition and maximize wind generation availability. | | | | |
| Business Process to Complete: Maintain the wind farm in operating condition and maximize wind generation availability. | | | | |
| Supporting Elements | | | | |
| Supporting Activities (describe) | Lead POC | Vendors and External Contacts | Vital Records | Max Allowed Down Time |
| | Alternate | | | Criticality |
| Maintain Electrical infrastructure | Electrical Manager | Cooke Power Services, David Evans and associates, GE O&M | Emergency & methods of procedures for restoring the wind farm critical systems, wiring diagrams, one-line drawings, equipment operating manuals | 0 time / 0 Days |
| | Senior Electrical Manager | | | Critical |
| Maintain Security infrastructure | Site Captain | Verkada, | Post orders, hard key logs, badge records, camera logs, room access reports | 0 / 0 |
| | Security Manager | | | High |
| Implications if not Conducted: Interruption and/or loss of any of the above systems would interrupt the customers' critical operations causing downtime and potential lease service level agreement (SLA) violations. The competitive benchmark for operating a wind farm is based on providing continuous dependable up time, equipment cooling and site security. Calendar Dependent: This function is continuous and always occurring. | | | | |
| Required Resources: Staff, equipment, supplies, Information Technology, and other resources. | | | | |
| Facilities: Standard office space that can accommodate up to 15 people at any time. Traditional office equipment and space for phones, computers, scanners, printers, etc., with network access to Internet, radio, and other telecommunications services. | | | | |

Supporting Partners: Cooke Power Systems, David Evans and Associates,

Vital Records: Methods of procedures for restoring the wind farm critical systems, wiring diagrams, one-line drawings, equipment operating manuals, operating IT infrastructure including ALC and other ancillary support information.

Table 3.1 Critical Business Function

| WindHQ Critical Business Function | | | | |
|---|---|-------------------------------|--|-----------------------|
| Critical Business Function 2: Maintain staffing to support the Wind farms in operating condition per the lease requirements. | | | | |
| Business Process to Complete: Maintain a robust human resources operations plan and roster to supplement the wind farm’s staffing as needed in a crisis. Critical staffing matrix must include competent electrical, mechanical, and security support teams trained in the intricacies of operating the wind farm. | | | | |
| Supporting Elements | | | | |
| Supporting Activities (describe) | Lead POC | Vendors and External Contacts | Vital Records | Max Allowed Down Time |
| | Alternate | | | Criticality |
| Maintain operations staffing to address wind farm operations functions | VP of Operations | GE O&M, Cooke Power Services | Contractual agreements for on-site staffing | 168 hours / 7 Days |
| | Senior Electrical and Mechanical Managers | | | High |
| Maintain Security staffing | Site Captain | Verkada, Firehawk | Contractual agreements for security surveillance systems; central station monitoring | 48 hours / 2 day |
| | Security Manager | | | High |
| Implications if not Conducted: major interruptions and/or loss of staffing can be covered with management teams and contractual support staffing from other local operating wind farms. Prolonged interruptions to staffing would likely result in incomplete service orders, site access disruptions and deferred maintenance program implementation | | | | |
| Calendar Dependent: This function is continuous and always occurring. | | | | |
| Required Resources: Staffing | | | | |

Facilities: Standard office space that can accommodate up to 15 people at any time. Traditional office equipment and space for phones, computers, scanners, printers, etc., with network access to Internet, radio, and other telecommunications services.

Supporting Partners: Cooke Power Systems, David Evans, and Associates,

Vital Records: Contractual staffing agreements for site support.

Table 3.2 Critical Business Function

| WindHQ Critical Business Function | | | | |
|---|------------------|--|---|-----------------------|
| Critical Business Function 3: Maintain continued operations for service to onsite direct connected data center. | | | | |
| Business Process to Complete: Wind farms are expensive to construct. Damaged equipment is expensive to replace and the associated lead time to replace is | | | | |
| Supporting Elements | | | | |
| Supporting Activities (describe) | Lead POC | Vendors and External Contacts | Vital Records | Max Allowed Down Time |
| | Alternate | | | Criticality |
| Maintain financial flexibility to account for critical component replacement | VP of Operations | GE (Full-Service O&M provider, Cooke Power Systems | Contractual agreements for on-site staffing | 168 hours / 7 Days |
| | CFO | | | High |
| Implications if not Conducted: Critical component failure could lead to wind farm downtime and service levels interruptions. Prudent financial soundness includes paying vendors in a timely manner and partnering with and selecting equipment from reputable organizations with a proven track record. Bankrupt equipment manufacturers have no leverage for continued site support. | | | | |
| Calendar Dependent: This function is continuous and always occurring. | | | | |
| Required Resources: Existing financial resources and debt facilities | | | | |
| Facilities: This function can be completed remotely with occasional visits to the wind farm | | | | |
| Supporting Partners: Cooke Power Systems, David Evans and Associates, | | | | |
| Vital Records: Contractual agreements for financial site support. | | | | |

4. PLAN ACTIVATION PROCEDURES

The Vice President of Operations (VP Ops) or his designee initiates the implementation of the Business Continuity Plan.

Plan Activation During Normal Business Hours

If it is determined that the facility cannot be re-inhabited, the VP Ops or his designer will inform personnel on next steps. Employees may be instructed to go home to await further instructions or to activate the Business Continuity Plan and move to the alternate site. Further communications, such as instructions on where and when to report for work will utilize the communication procedures detailed in Sections 5 and 9.

Plan Activation Outside Normal Business Hours

If an event occurs outside normal business hours that renders a facility uninhabitable, the VP Ops or designee will activate the Business Continuity Plan using the communication procedures detailed in Section 5 and 9.

Actions upon Activation

Upon activation of the Business Continuity Plan, the VP Ops or designee will be responsible for notifying the alternate site, if appropriate, of their impending arrival.

5. INTERNAL COMMUNICATION PROCEDURES

Staff accountability for a facility evacuation

Once employees, customers, and guests have evacuated personnel should remain at the primary assembly point and await further instructions.

Once at the assembly point accountability must be performed by the security team at the site:

- Initiate headcount and make note of missing and/or injured employees, customers, and guests; and
- Report missing and/or injured employees to the VP Ops or his designee. This information should be shared with emergency first responders on scene.

The VP Ops or its designee should determine the best methods for disseminating communications to staff. See Section 9, Employee Contact List.

Table 4

| Employee Communication Methods | |
|--------------------------------|---|
| 1 | <i>Staff work email, list located <u>company</u> Human Relations management software-Paylocity.</i> |
| 2 | <i>Staff work mobile phones, list located in Section 9 and is available on the 365-outlook email server</i> |

6. ALTERNATE FACILITIES

None

6.1 Telework as an Alternate Site

Teleworking is an arrangement between an employee and the employee's supervisor that allows the employee to work at home or other non-traditional location. Telework is not always an option for all business types, though it should be utilized when available. Astra wind uses Telework routinely for maintaining availability. GE O&M monitors the wind farm remotely 24/7.

7. ORDERS OF SUCCESSION AND DELEGATIONS OF AUTHORITY

7.1 OVERVIEW

Orders of succession are prepared to provide clarity of senior leadership roles if individuals in these roles, whether they be decision-making or management roles, are unavailable. A delegation of authorities provide successors with legal authorization to act on behalf of critical positions within the organization for specific purposes and duties.

7.2 ORDERS OF SUCCESSION

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

7.3 DELEGATIONS OF AUTHORITY

Delegations of authority are the legal authorization to act on behalf of critical positions within the organization for specific purposes and duties. To ensure a rapid response to any situation requiring the activation of a Business Continuity Plan employees who serve in key senior leader positions must develop and maintain pre-delegated authorities for policy determinations and decisions, as needed. The delegations of authority should include what type of authority is being delegated, such as signatory or credit card authorization for purchasing, and limitations of the delegated authority. All duties of each senior leader are delegated to the position in the orders of succession when the incumbent cannot fulfil that authority for any reason, including but not limited to:

- Absence
- Illness
- Leave
- Death
- Termination

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

Table 6. Delegation of Authority

| Position to be Succeeded | Successors | Delegated Authorities | Activation and Termination Triggers |
|--------------------------|---------------------------------------|--|--|
| VP Operations | Successor 1 Director of Operations | Delegated authorities or all duties as assigned by VP of Operations | <u>Activate:</u> Incapacitated, unavailable, or selective decision <u>Terminate:</u> Return of VP Operations |
| | Successor 2 Director of IT | Delegated authorities or all duties as assigned by VP of Real Estate | <u>Activate:</u> Incapacitated or unavailable <u>Terminate:</u> Return of VP of Real Estate |
| | Successor 3 Director of EHS | Delegated authorities or all duties as assigned Director of IT | <u>Activate:</u> Incapacitated or unavailable <u>Terminate:</u> Return of Director of IT |

8. PLAN DEACTIVATION

8.1 OVERVIEW

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

8.2 CRITERIA FOR PLAN DEACTIVATION

The VP of Operations or his designee will determine, based on input from first responders, staff responsible and other entities when it is safe and when the organization is prepared to restore or transfer critical business functions to a facility for long term usage.

Critical business functions must be restored in priority sequence based upon the classification and criticality of the function. The following elements are typically completed prior to plan deactivation.

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

8.3 RESUMPTION PROCEDURES

Each potential business operating risk as outlined in Table 1.1 is shown below with a bridge solution and required resource which staff members will need to identify need to be active participants in this process.

Table 7. Business Function Resumption/Plan Deactivation

| # | Function | Bridge Solution | Required Resources |
|---|---|---|--|
| 1 | Loss of Power (Utility) | Emergency diesel generators operate until power is successfully restored. | Power provided by Oncor Energy shall be confirmed to be satisfactory by the critical team. |
| 2 | Loss of employees (Pandemic or illness) | Remote operation of the wind farm(s) is possible for a lengthy duration but is not preferred | . We have ten plus staff to leverage to fulfill the staffing needs |
| 3 | Loss of equipment (Electrical failure) | spare parts are in inventory to address equipment failures | Vendor resources are dependent on the system that fails, availability of spare parts and timeliness of the repair. |
| 4 | Loss of Equipment IT | Some redundant IT is available and remote resetting, programming, and troubleshooting can be completed. | IT malfunctions require user interface for remote resetting, troubleshooting, or programming. Occupancy by IT staff is most likely required in certain cases |

| # | Function | Bridge Solution | Required Resources |
|----|----------------------|---|--|
| 5 | Cyber Attack | Certified third party malware and virus protections systems are deployed internally and on critical systems. Firewalls secure the network. | External vendor resources may need to be engaged for extreme or complex cases |
| 6 | Fire | Buildings include fire alarm systems. | |
| 7 | Injury or accident | Buildings are equipped with first aid supplies and AEDs. Staff are trained in CPR, first aid and AED use. We contact 911 for emergencies beyond first aid | We rely on local emergency and first responder resources in cases where injuries or accidents require treatment beyond first aid |
| 8 | Environmental Hazard | Buildings are equipped with spill supplies and leak detection equipment. Staff are trained in the elements of spill response and emergency notifications | We rely on local emergency and first responder resources in cases of larger spills. We have agreements in place to address the clean-up of hazmat |
| 9 | Security Threat | Buildings are equipped with CCTV and badge readers. Security enrollment requires Govt ID verification | We rely on local police resources in cases of theft, property damage or vandalism or workplace violence. Securitas is the primary security vendor administering badge enrollment |
| 10 | Loss of Equipment IT | Buildings are carrier neutral environments. We have dedicated resources to provide internet and wireless cell coverage | Internal systems are locally maintained. Vendor resources may need to be engaged for extreme or complex cases |
| 11 | Bio-Hazard | Buildings are equipped with limited pandemic supplies and remote ventilation shut down capabilities | We rely on local emergency and first responder resources in cases of larger events. We have agreements in place to address the clean-up of bio hazards in facilities |
| 12 | Reputational Threat | Procedures in place to address employee engagement with media. Legal counsel is available | The threat is somewhat undefined at this stage. Need to define and strengthen assets in this area. |

9. EMPLOYEE CONTACT LIST

Table 8

| Employee Name | Title / Responsibility | Home / Cell Number | Personal Email Address |
|-----------------|---------------------------------|--------------------|-------------------------|
| Bob Rosenberger | VP OPS | (202) 679-0819 | Bob@WindHQ.com |
| Brian Zemcik | VP Development | (202) 603-9738 | Bzemcik@WindHQ.com |
| Keith Harney | COO | (202) 408-0005 | KH@WindHQ.com |
| Michelle Melito | VP HR | (202) 934-4104 | michelle@WindHQ.com |
| Rebecca Palmer | HR Manager | (202) 368-1699 | Rpalmer@WindHQ.com |
| David McKeegan | Senior Director of EHS | (571) 866-6489 | Dmckeegan@WindHQ.com |
| Patrick Quinn | VP Real Estate | (202) 702-0596 | Pq@WindHQ.com |
| Dan Molloy | VP DCIT | (202) 768-5899 | Dmolloy@WindHQ.com |
| Matt Hartle | Director of IT | (540) 538-7285 | Mhartle@WindHQ.com |
| John Shea | Security Manager | (202) 255-8557 | Jshea@WindHQ.com |
| Chris Sweet | Director of EHS | (571) 266-9809 | Csweet@WindHQ.com |
| Robert Strachan | Director Electrical Engineering | (202) 304-7801 | Rstrachan@WindHQ.com |
| Chris Jones | Director Mechanical Engineering | (540) 287-8079 | Cjones@WindHQ.com |
| Tad Hartsell | Electrical Manager | (703) 929-1235 | Thartsell@WindHQ.com |
| Dave Tayman | Mechanical Manager | (571) 296-4950 | Dtayman@WindHQ.com |
| Kevin Ford | Assistant Mech Manager | (202) 704-8702 | Kford@WindHQ.com |
| Mehrdad Nemazee | Senior Property Manager | (202) 438-7345 | Mnemazee@WindHQ.com |
| Daniel McClure | Assistant Elec. Manager | (571) 714-6827 | dmccclure@WindHQ.com |
| Matthew Adamson | Physical Security Engineer | (571) 512-8343 | madamson@WindHQ.com |
| Leighton Le | Site Security Captain | (703) 217-2941 | leightonle@WindHQ.com |
| William White | Electrical Foreman | (202) 285-2824 | Willaimwhite@WindHQ.com |
| Issael Guardado | Facilities Assistant | (571) 420-8250 | iguardado@WindHQ.com |

| | | | |
|------------------|------------------------------|----------------|---------------------------|
| John Merrick | Electrical Manager | (202) 580-5027 | jmerrick@WindHQ.com |
| Robert Bruce | Mechanical Manager | (571) 230-3862 | rbruce@WindHQ.com |
| Keisa Reid | Property Manager | (571) 919-0967 | kreid@WindHQ.com |
| Jonathan Waldron | Senior EHS Manager | (571) 461-8649 | jwaldron@WindHQ.com |
| Ben Hartsell | Assistant Elec. Manager | (571) 719-0238 | bhartsell@WindHQ.com |
| Dan Dowd | Assistant Mech. Manager | (571) 340-0889 | Danieldowd@WindHQ.com |
| Shane Hibner | Electrical Foreman | (571) 719-0593 | shanehibner@WindHQ.com |
| Ricardo Vela | Facilities Assistant | (202) 823-1023 | rvela@WindHQ.com |
| Kim Snyder | Site Security Captain | (571) 317-4681 | KimberlySnyder@WindHQ.com |
| Mohammad Ali | Audit and Compliance Manager | (571) 919-5576 | mali@WindHQ.com |

10. VENDOR CONTACT LIST

Table 9. Vendor Contacts

| Vendor | Resource/Service | Contact Information |
|-------------------------------|---|---|
| Ingersoll Rand | Air Compressor | Ingersoll Rand Richmond, VA 804-214-7054 |
| TRANE | Chiller | Boland Services 240-306-3000 |
| ESI | Day Tank, fuel oil cleaner, diesel fuel | ESI 703-263-7600 |
| Ferguson Enterprises Inc. | Domestic Hot Water Circulation | Ferguson Enterprises Inc. 703-375-5800 |
| Stancor | Elevator sump pump | Elcon Enterprises Inc. 301-586-9300 |
| Greenheck | Exhaust fans | C.G. Wood Company Inc. 240-241-5300 |
| Alban CAT | Engine Generator | |
| Tanks Direct | Fuel pump | Tanks Direct 800-865-5555 |
| Advantage Controls | Glycol Feeder | Advantage Controls 918-686-6211 |
| Munters | Humidifier | Munters 978-330-6960 |
| Miratec | Muffler | Jim McDonald 215-407-9001 |
| AAON | Roof Top Air Handling Units | Havtech 301-206-9225 |
| DAIKIN | Roof Top Air Handling Units | Havtech 301-206-9225 |
| Tanks Direct (Highland Tanks) | Underground Fuel Tank, Thermal Storage Tank | Tanks Direct 800-865-5555 |
| INDEECO | Unit Heater | Boland Services 240-306-3000 |
| Nailor | VAV Terminal | Metropolitan Equipment Group, Inc. 804-744-4774 |
| Bell & Gossett | | Cummins-Wagner 301-490-9007 |
| Harmsco | | Chemtreat Inc. 804-935-2000 |
| Stulz | CRAC & CRAH | Stulz 888-529-1266 |

| Vendor | Resource/Service | Contact Information |
|--------------------------|---|--|
| Square D | Bus Plugs, busway | 1-844-362-6387 |
| Cooper Power Systems | Transformer | |
| Eaton | Panels, Breakers | 1-262-524-2379 |
| SAI | EDP, CDP, Switchboards | 1-847-688-9013 |
| ASCO | Load Bank, ATS | 1-216-573-7600 |
| Schneider Electric | MV Gear & UPS | 1-844-362-6387 |
| PDI | | 1-804-737-9880 |
| Bussman | | 1-800-386-1911 |
| SENS | Battery charger | 1702-826-0819 |
| Seimens | Switchgear | https://new.siemens.com/us/en/company/about/contact-us.html |
| PDS | UNIT SUBSTATION TRANSFORMERS | 1-803-259-6003 |
| Dominion Virginia Energy | Utility power | Dominic J. Minor Key Account Manager Dominic.j.minor@dominionenergy.com 866-366-4357 |
| Verizon | Cell and internet service | www.verizon.com |
| Zayo | Internet service | 866-364-6033 |
| Fiberlight | Internet service | 844-509-0775 |
| Myriad | IT equipment | 866-725-1025 |
| Amazon | IT equipment | www.amazon.com |
| Clean Harbors | Waste disposal & emergency spill response | Kevin Malone 301-466-1570 or 800-645-8265 |
| Grainger | Supplies | www.grainger.com |

| Vendor | Resource/Service | Contact Information |
|-----------------|--|---|
| Cintas & Stat | First aid and safety, pandemic disinfectants | Julie Hanigan 301-802-8661 (Stat) Gary Eversole 703-819-0599 (Cintas) |
| Staples | Office Supplies | www.staples.com |
| Clean Solutions | Housekeeping | Boris Barrios (703) 975-9683 |
| Poole and Kent | Operations contractor | Mike Everitt (443) 717 0189 or meveritt@emcor.com |
| Securitas | Site Security | Justin Boudville (571) 220-4669 |

11. FAMILY EMERGENCY PLAN

Employees must also prepare in advance for what to do in an emergency and should develop a Family Support Plan to increase personnel and family preparedness. To develop your Family Support Plan, use the templates available at www.ready.gov. this site includes a ‘Get Ready Now’ pamphlet, which explains the importance of planning and provides a template that you and your family can use to develop your specific plan. The following list is gathered from <https://www.ready.gov/build-a-kit>.

11.1 Basic Disaster Supplies Kit

To assemble your kit, store items in airtight plastic bags and put your entire disaster supplies kit in one or two easy-to-carry containers such as plastic bins or a duffel bag.

A basic emergency supply kit could include the following recommended items:

- Water - one gallon of water per person per day for at least three days, for drinking and sanitation
- Food - at least a three-day supply of non-perishable food
- Battery-powered or hand crank radio and a NOAA Weather Radio with tone alert
- Flashlight
- First aid kit
- Extra batteries
- Whistle to signal for help
- Dust mask to help filter contaminated air and plastic sheeting and duct tape to shelter-in-place
- Moist towelettes, garbage bags and plastic ties for personal sanitation
- Wrench or pliers to turn off utilities
- Manual can opener for food
- Local maps
- Cell phone with chargers and a backup battery
- Download the Recommended Supplies List (PDF)

11.2 Additional Emergency Supplies

Consider adding the following items to your emergency supply kit based on your individual needs:

- Prescription medications
- Non-prescription medications such as pain relievers, anti-diarrhea medication, antacids or laxatives.
- Glasses and contact lens solution.
- Infant formula, bottles, diapers, wipes, diaper rash cream

- Pet food and extra water for your pet
- Cash or traveler's checks.
- Important family documents such as copies of insurance policies, identification and bank account records saved electronically or in a waterproof, portable container.
- Sleeping bag or warm blanket for each person
- Complete change of clothing appropriate for your climate and sturdy shoes
- Household chlorine bleach and medicine dropper to disinfect water.
- Fire extinguisher
- Matches in a waterproof container.
- Feminine supplies and personal hygiene items
- Mess kits, paper cups, plates, paper towels and plastic utensils.
- Paper and pencil
- Books, games, puzzles, or other activities for children

12. TRAINING

WindHQ employees will be thoroughly trained in emergency evacuation and restoration procedures. Specifically,

- All employees will review disaster preparation and emergency action plan procedures.
- Annual training will involve one or more of the following drills:
 - Walkthrough drills: The business continuity planning team, department heads and site teams will perform their emergency response functions.
 - Functional drills: These drills will evaluate specific functions such as medical response, emergency notifications, warning and communication procedures and equipment. Facility shutdown procedures will be evaluated, reviewed, and modified as needed. Personnel are asked to evaluate the systems and identify problem areas.
 - Evacuation drills: Personnel will walk the evacuation route to a designated area where procedures are evaluated for accounting for all personnel.
 - Full-scale exercise: A real-life emergency is simulated as close as possible. These exercises involve company emergency response personnel, employees and management, and community response organizations.

13. ANNUAL PLAN AUDIT

A formal audit of the business continuity plan will be conducted annually and should be evaluated and modified after each training exercise, emergency, changes in personnel responsibilities, changes in facility layout or design and changes in policies or procedures. Personnel will be briefed every time changes or modifications have been made to the plan.

14. INSURANCE CONSIDERATIONS

Contact our insurance agent or broker to discuss our business insurance coverage and needs.

OWNERSHIP AND REVIEW

The VP of Operations owns this standard.

This standard shall be reviewed on an annual basis.

CONTACT INFORMATION

Rich Rohde

VP Operations

509-688-3476

rrohde@windhq.com

DOCUMENT RACI

| | | |
|--------------------|---|--|
| Responsible | Assigned to do the work | Site Managers Director of operations |
| Accountable | Final decision, ultimately answerable | Director of Operations |
| Consulted | Consulted BEFORE an action or decision is taken (proactive) | Executive Management |
| Informed | Informed AFTER a decision or action has been taken (reactive) | Named Participants in this document. Other parties affected by the change |

Astra Wind
Emergency Operations Plan (EOP)
(Per 16 TAC Sect. 25.53)

Attachment J



BUSINESS CONTINUITY PLAN

| | |
|------------------|------------|
| Document Version | 1.2 |
| Date | 04/01/2025 |

| Document Properties | |
|---------------------|-------------------|
| Property | Description |
| Circulation | Internal Use Only |
| Classification | Confidential |
| Document Owner | VP Operations |

| Revision History | | | |
|------------------|------------|------------------------|-------------|
| Version | Date | Description of Changes | Revised by |
| 1.0 | 09/29/2020 | Finalized | Chris Sweet |
| 1.1 | 10/20/2021 | Annual Review | Chris Sweet |
| 1.2 | 04/01/2025 | Minor Edits | Rich Rohde |

September 2020

Contents

| | |
|---|-----------|
| EXECUTIVE OVERVIEW | 5 |
| 1. INTRODUCTION | 6 |
| Overview | 6 |
| Plan Scope & Applicability | 6 |
| Plan Objectives | 6 |
| Plan Assumptions | 6 |
| 2. RISK ASSESSMENT | 8 |
| 3. CRITICAL BUSINESS FUNCTIONS | 10 |
| Overview | 11 |
| 4. PLAN ACTIVATION PROCEDURES..... | 15 |
| Plan Activation During Normal Business Hours..... | 15 |
| Plan Activation Outside Normal Business Hours..... | 15 |
| Actions upon Activation | 15 |
| 5. INTERNAL COMMUNICATION PROCEDURES..... | 16 |
| Staff accountability for a facility evacuation | 16 |
| 6. ALTERNATE FACILITIES..... | 17 |
| 7. ORDERS OF SUCCESSION AND DELEGATIONS OF AUTHORITY | 18 |
| 7.1 OVERVIEW..... | 18 |
| 7.2 ORDERS OF SUCCESSION..... | 18 |
| 7.3 DELEGATIONS OF AUTHORITY..... | 18 |
| 8. PLAN DEACTIVATION | 19 |
| 8.1 OVERVIEW | 19 |
| 8.2 CRITERIA FOR PLAN DEACTIVATION..... | 20 |
| 8.3 RESUMPTION PROCEDURES..... | 20 |
| 9. EMPLOYEE CONTACT LIST..... | 22 |
| Table 8 | 22 |
| 10. VENDOR CONTACT LIST..... | 24 |
| 11. FAMILY EMERGENCY PLAN..... | 27 |
| 11.1 Basic Disaster Supplies Kit | 27 |
| 11.2 Additional Emergency Supplies | 27 |

| | |
|--|-----------|
| 12. TRAINING..... | 28 |
| 13. ANNUAL PLAN AUDIT | 28 |
| 14. INSURANCE CONSIDERATIONS..... | 29 |
| OWNERSHIP AND REVIEW | 30 |
| CONTACT INFORMATION | 30 |

EXECUTIVE OVERVIEW

This plan includes an overview of continuity operations, outlines the approach for supporting an organization's critical business functions, and defines the roles and responsibilities of staff. It also outlines the orders of succession, notification procedures and communication methods, plan activation and deactivation protocols, provisions for alternate work locations, and the plan for maintaining and restoring access to vital records.

This document establishes procedures and processes to maintain operational continuity for businesses based on three types of disruptions that could occur individually or in any combination:

- Loss of access to parts of or the entire facility (e.g., following a fire, sudden storm, or flooding).
- Loss of services due to a reduction in workforce (e.g., during pandemic Covid-19).
- Loss of services due to equipment or systems failure (e.g., information technology (IT) systems failure, electrical grid failure).

1. INTRODUCTION

Overview

The Business Continuity of Operations (BCOP) planning ensures businesses can continue or immediately resume performing their organization's critical business functions, which are the functions that support the organization's mission, comply with legal requirements, and support life-safety, under all circumstances. This includes natural, technological, and man-made incidents, as well as incidents that result in loss of access to parts of or an entire facility or loss of service due to equipment or systems failure. The benefit of BCOP planning includes the ability to anticipate response actions following a myriad of incidents, improve the businesses performance of its critical business functions, and ensure timely recovery.

Plan Scope & Applicability

The scope of this plan covers active WindHQ Operations sites. The plan is applicable once the safety of employees, customers, and guests has been verified and if a facility is or will become inaccessible. It can be active during normal business hours and after hours, with and without warning.

Plan Objectives

The WindHQ Operations Business Continuity Plan objective is to facilitate the resumption of critical operations, functions, and technology in a timely and organized manner to ensure a viable and stable organization. In doing this it is critical to ensure the safety and well-being of employees, customers, and guests.

The primary objectives of the plan are to:

- Maintain Critical Business Functions
- Ensure that employees have safe access to facility.
- Protect vital records.
- Ensure that records are accessible under all conditions.

Plan Assumptions

The following assumptions were used while creating this plan:

- An event has occurred that affects normal business operations.
- There is limited or no access to the affected facility.

- Documents and equipment within the facility are inaccessible.
- Qualified personnel are available to continue operations.

2. RISK ASSESSMENT

The following table reflects hazard probability assumptions.

Table 1. 2017 Hazard Mitigation Analysis

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
|-----------------------------------|---|---|--|---|--|
| Flooding | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Hurricane Tropical Storms | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Thunderstorm Lightning Hail | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Tornado | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Winter Storms Ice Storms | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| High Winds | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Wildfire | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
|------------|--|--|---|---|---|
| Landslide | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Earthquake | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |

Table 1.1 WindHQ Hazard Mitigation Analysis

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
|---|--|--|---|---|---|
| Loss of Power (Utility) | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Loss of employees (Pandemic or illness) | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Loss of equipment (Electrical failure) | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Loss of Equipment (Mechanical failure) | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Loss of Equipment IT | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
|----------------------|---|---|--|---|---|
| Cyber Attack | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low |
| Fire | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Injury or accident | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low |
| Environmental Hazard | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low |
| Security Threat | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low |
| Bio-Hazard | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low |
| Reputational Threat | 4. Highly Likely 3. Likely 2. Possible 1. Unlikely | 4. Catastrophic 3. Critical 2. Limited 1. Negligible | 4. Minimal 3. 6 - 2 hrs. 2. 12-24 hrs. 1. 24+ hrs | 4. 12+ hrs 3. 6-12 hrs. 2. 3 – 6 hrs 1. < 3 hrs. | <input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Low |
| | | | | | <input type="checkbox"/> |

3. CRITICAL BUSINESS FUNCTIONS

Overview

WindHQ owns and operates the Astra Wind Farm. Astra is connected to ERCOT's transmission system. Astra is a registered PGC with ERCOT and provides renewable (wind) energy to the ERCOT transmission system.

Tables 3 - 3.2 provide a list of the WindHQ critical business functions. This includes the main business process, a list of the responsible staff, trusted vendors, vital records, and the permissible downtime.

Table 3. Critical Business Function

| WindHQ Critical Business Function | | | | |
|--|---------------------------|--|---|-----------------------|
| Critical Business Function 1: Maintain the wind farm in operating condition and maximize wind generation availability. | | | | |
| Business Process to Complete: Maintain the wind farm in operating condition and maximize wind generation availability. | | | | |
| Supporting Elements | | | | |
| Supporting Activities (describe) | Lead POC | Vendors and External Contacts | Vital Records | Max Allowed Down Time |
| | Alternate | | | Criticality |
| Maintain Electrical infrastructure | Electrical Manager | Cooke Power Services, David Evans and associates, GE O&M | Emergency & methods of procedures for restoring the wind farm critical systems, wiring diagrams, one-line drawings, equipment operating manuals | 0 time / 0 Days |
| | Senior Electrical Manager | | | Critical |
| Maintain Security infrastructure | Site Captain | Verkada, | Post orders, hard key logs, badge records, camera logs, room access reports | 0 / 0 |
| | Security Manager | | | High |
| Implications if not Conducted: Interruption and/or loss of any of the above systems would interrupt the customers' critical operations causing downtime and potential lease service level agreement (SLA) violations. The competitive benchmark for operating a wind farm is based on providing continuous dependable up time, equipment cooling and site security. Calendar Dependent: This function is continuous and always occurring. | | | | |
| Required Resources: Staff, equipment, supplies, Information Technology, and other resources. | | | | |
| Facilities: Standard office space that can accommodate up to 15 people at any time. Traditional office equipment and space for phones, computers, scanners, printers, etc., with network access to Internet, radio, and other telecommunications services. | | | | |

Supporting Partners: Cooke Power Systems, David Evans and Associates,

Vital Records: Methods of procedures for restoring the wind farm critical systems, wiring diagrams, one-line drawings, equipment operating manuals, operating IT infrastructure including ALC and other ancillary support information.

Table 3.1 Critical Business Function

| WindHQ Critical Business Function | | | | |
|--|---|-------------------------------------|--|-----------------------------|
| Critical Business Function 2: Maintain staffing to support the Wind farms in operating condition per the lease requirements. | | | | |
| Business Process to Complete: Maintain a robust human resources operations plan and roster to supplement the wind farm’s staffing as needed in a crisis. Critical staffing matrix must include competent electrical, mechanical, and security support teams trained in the intricacies of operating the wind farm. | | | | |
| Supporting Elements | | | | |
| Supporting Activities (describe) | Lead POC | Vendors and External Contacts | Vital Records | Max Allowed Down Time |
| | Alternate | | | Criticality |
| Maintain operations staffing to address wind farm operations functions | VP of Operations | GE O&M, Cooke Power Services | Contractual agreements for on-site staffing | 168 hours / 7 Days |
| | Senior Electrical and Mechanical Managers | | | High |
| Maintain Security staffing | Site Captain | Verkada, Firehawk | Contractual agreements for security surveillance systems; central station monitoring | 48 hours / 2 day |
| | Security Manager | | | High |
| <u>Implications if not Conducted:</u> major interruptions and/or loss of staffing can be covered with management teams and contractual support staffing from other local operating wind farms. Prolonged interruptions to staffing would likely result in incomplete service orders, site access disruptions and deferred maintenance program implementation | | | | |
| <u>Calendar Dependent:</u> This function is continuous and always occurring. | | | | |
| <u>Required Resources:</u> Staffing | | | | |

Facilities: Standard office space that can accommodate up to 15 people at any time. Traditional office equipment and space for phones, computers, scanners, printers, etc., with network access to Internet, radio, and other telecommunications services.

Supporting Partners: Cooke Power Systems, David Evans, and Associates,

Vital Records: Contractual staffing agreements for site support.

Table 3.2 Critical Business Function

| WindHQ Critical Business Function | | | | |
|---|------------------|--|---|-----------------------|
| Critical Business Function 3: Maintain continued operations for service to onsite direct connected data center. | | | | |
| Business Process to Complete: Wind farms are expensive to construct. Damaged equipment is expensive to replace and the associated lead time to replace is | | | | |
| Supporting Elements | | | | |
| Supporting Activities (describe) | Lead POC | Vendors and External Contacts | Vital Records | Max Allowed Down Time |
| | Alternate | | | Criticality |
| Maintain financial flexibility to account for critical component replacement | VP of Operations | GE (Full-Service O&M provider, Cooke Power Systems | Contractual agreements for on-site staffing | 168 hours / 7 Days |
| | CFO | | | High |
| Implications if not Conducted: Critical component failure could lead to wind farm downtime and service levels interruptions. Prudent financial soundness includes paying vendors in a timely manner and partnering with and selecting equipment from reputable organizations with a proven track record. Bankrupt equipment manufacturers have no leverage for continued site support. | | | | |
| Calendar Dependent: This function is continuous and always occurring. | | | | |
| Required Resources: Existing financial resources and debt facilities | | | | |
| Facilities: This function can be completed remotely with occasional visits to the wind farm | | | | |
| Supporting Partners: Cooke Power Systems, David Evans and Associates, | | | | |
| Vital Records: Contractual agreements for financial site support. | | | | |

4. PLAN ACTIVATION PROCEDURES

The Vice President of Operations (VP Ops) or his designee initiates the implementation of the Business Continuity Plan.

Plan Activation During Normal Business Hours

If it is determined that the facility cannot be re-inhabited, the VP Ops or his designer will inform personnel on next steps. Employees may be instructed to go home to await further instructions or to activate the Business Continuity Plan and move to the alternate site. Further communications, such as instructions on where and when to report for work will utilize the communication procedures detailed in Sections 5 and 9.

Plan Activation Outside Normal Business Hours

If an event occurs outside normal business hours that renders a facility uninhabitable, the VP Ops or designee will activate the Business Continuity Plan using the communication procedures detailed in Section 5 and 9.

Actions upon Activation

Upon activation of the Business Continuity Plan, the VP Ops or designee will be responsible for notifying the alternate site, if appropriate, of their impending arrival.

5. INTERNAL COMMUNICATION PROCEDURES

Staff accountability for a facility evacuation

Once employees, customers, and guests have evacuated personnel should remain at the primary assembly point and await further instructions.

Once at the assembly point accountability must be performed by the security team at the site:

- Initiate headcount and make note of missing and/or injured employees, customers, and guests; and
- Report missing and/or injured employees to the VP Ops or his designee. This information should be shared with emergency first responders on scene.

The VP Ops or its designee should determine the best methods for disseminating communications to staff. See Section 9, Employee Contact List.

Table 4

| Employee Communication Methods | |
|--------------------------------|---|
| 1 | <i>Staff work email, list located <u>company</u> Human Relations management software-Paylocity.</i> |
| 2 | <i>Staff work mobile phones, list located in Section 9 and is available on the 365-outlook email server</i> |

6. ALTERNATE FACILITIES

None

6.1 Telework as an Alternate Site

Teleworking is an arrangement between an employee and the employee's supervisor that allows the employee to work at home or other non-traditional location. Telework is not always an option for all business types, though it should be utilized when available. Astra wind uses Telework routinely for maintaining availability. GE O&M monitors the wind farm remotely 24/7.

7. ORDERS OF SUCCESSION AND DELEGATIONS OF AUTHORITY

7.1 OVERVIEW

Orders of succession are prepared to provide clarity of senior leadership roles if individuals in these roles, whether they be decision-making or management roles, are unavailable. A delegation of authorities provide successors with legal authorization to act on behalf of critical positions within the organization for specific purposes and duties.

7.2 ORDERS OF SUCCESSION

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

7.3 DELEGATIONS OF AUTHORITY

Delegations of authority are the legal authorization to act on behalf of critical positions within the organization for specific purposes and duties. To ensure a rapid response to any situation requiring the activation of a Business Continuity Plan employees who serve in key senior leader positions must develop and maintain pre-delegated authorities for policy determinations and decisions, as needed. The delegations of authority should include what type of authority is being delegated, such as signatory or credit card authorization for purchasing, and limitations of the delegated authority. All duties of each senior leader are delegated to the position in the orders of succession when the incumbent cannot fulfil that authority for any reason, including but not limited to:

- Absence
- Illness
- Leave
- Death
- Termination

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

Table 6. Delegation of Authority

| Position to be Succeeded | Successors | Delegated Authorities | Activation and Termination Triggers |
|--------------------------|---------------------------------------|--|--|
| VP Operations | Successor 1 Director of Operations | Delegated authorities or all duties as assigned by VP of Operations | <u>Activate:</u> Incapacitated, unavailable, or selective decision <u>Terminate:</u> Return of VP Operations |
| | Successor 2 Director of IT | Delegated authorities or all duties as assigned by VP of Real Estate | <u>Activate:</u> Incapacitated or unavailable <u>Terminate:</u> Return of VP of Real Estate |
| | Successor 3 Director of EHS | Delegated authorities or all duties as assigned Director of IT | <u>Activate:</u> Incapacitated or unavailable <u>Terminate:</u> Return of Director of IT |

8. PLAN DEACTIVATION

8.1 OVERVIEW

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

8.2 CRITERIA FOR PLAN DEACTIVATION

The VP of Operations or his designee will determine, based on input from first responders, staff responsible and other entities when it is safe and when the organization is prepared to restore or transfer critical business functions to a facility for long term usage.

Critical business functions must be restored in priority sequence based upon the classification and criticality of the function. The following elements are typically completed prior to plan deactivation.

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

8.3 RESUMPTION PROCEDURES

Each potential business operating risk as outlined in Table 1.1 is shown below with a bridge solution and required resource which staff members will need to identify need to be active participants in this process.

Table 7. Business Function Resumption/Plan Deactivation

| # | Function | Bridge Solution | Required Resources |
|---|---|---|--|
| 1 | Loss of Power (Utility) | Emergency diesel generators operate until power is successfully restored. | Power provided by Oncor Energy shall be confirmed to be satisfactory by the critical team. |
| 2 | Loss of employees (Pandemic or illness) | Remote operation of the wind farm(s) is possible for a lengthy duration but is not preferred | . We have ten plus staff to leverage to fulfill the staffing needs |
| 3 | Loss of equipment (Electrical failure) | spare parts are in inventory to address equipment failures | Vendor resources are dependent on the system that fails, availability of spare parts and timeliness of the repair. |
| 4 | Loss of Equipment IT | Some redundant IT is available and remote resetting, programming, and troubleshooting can be completed. | IT malfunctions require user interface for remote resetting, troubleshooting, or programming. Occupancy by IT staff is most likely required in certain cases |

| # | Function | Bridge Solution | Required Resources |
|----|----------------------|---|--|
| 5 | Cyber Attack | Certified third party malware and virus protections systems are deployed internally and on critical systems. Firewalls secure the network. | External vendor resources may need to be engaged for extreme or complex cases |
| 6 | Fire | Buildings include fire alarm systems. | |
| 7 | Injury or accident | Buildings are equipped with first aid supplies and AEDs. Staff are trained in CPR, first aid and AED use. We contact 911 for emergencies beyond first aid | We rely on local emergency and first responder resources in cases where injuries or accidents require treatment beyond first aid |
| 8 | Environmental Hazard | Buildings are equipped with spill supplies and leak detection equipment. Staff are trained in the elements of spill response and emergency notifications | We rely on local emergency and first responder resources in cases of larger spills. We have agreements in place to address the clean-up of hazmat |
| 9 | Security Threat | Buildings are equipped with CCTV and badge readers. Security enrollment requires Govt ID verification | We rely on local police resources in cases of theft, property damage or vandalism or workplace violence. Securitas is the primary security vendor administering badge enrollment |
| 10 | Loss of Equipment IT | Buildings are carrier neutral environments. We have dedicated resources to provide internet and wireless cell coverage | Internal systems are locally maintained. Vendor resources may need to be engaged for extreme or complex cases |
| 11 | Bio-Hazard | Buildings are equipped with limited pandemic supplies and remote ventilation shut down capabilities | We rely on local emergency and first responder resources in cases of larger events. We have agreements in place to address the clean-up of bio hazards in facilities |
| 12 | Reputational Threat | Procedures in place to address employee engagement with media. Legal counsel is available | The threat is somewhat undefined at this stage. Need to define and strengthen assets in this area. |

9. EMPLOYEE CONTACT LIST

Table 8

| Employee Name | Title / Responsibility | Home / Cell Number | Personal Email Address |
|-----------------|---------------------------------|--------------------|-------------------------|
| Bob Rosenberger | VP OPS | (202) 679-0819 | Bob@WindHQ.com |
| Brian Zemcik | VP Development | (202) 603-9738 | Bzemcik@WindHQ.com |
| Keith Harney | COO | (202) 408-0005 | KH@WindHQ.com |
| Michelle Melito | VP HR | (202) 934-4104 | michelle@WindHQ.com |
| Rebecca Palmer | HR Manager | (202) 368-1699 | Rpalmer@WindHQ.com |
| David McKeegan | Senior Director of EHS | (571) 866-6489 | Dmckeegan@WindHQ.com |
| Patrick Quinn | VP Real Estate | (202) 702-0596 | Pq@WindHQ.com |
| Dan Molloy | VP DCIT | (202) 768-5899 | Dmolloy@WindHQ.com |
| Matt Hartle | Director of IT | (540) 538-7285 | Mhartle@WindHQ.com |
| John Shea | Security Manager | (202) 255-8557 | Jshea@WindHQ.com |
| Chris Sweet | Director of EHS | (571) 266-9809 | Csweet@WindHQ.com |
| Robert Strachan | Director Electrical Engineering | (202) 304-7801 | Rstrachan@WindHQ.com |
| Chris Jones | Director Mechanical Engineering | (540) 287-8079 | Cjones@WindHQ.com |
| Tad Hartsell | Electrical Manager | (703) 929-1235 | Thartsell@WindHQ.com |
| Dave Tayman | Mechanical Manager | (571) 296-4950 | Dtayman@WindHQ.com |
| Kevin Ford | Assistant Mech Manager | (202) 704-8702 | Kford@WindHQ.com |
| Mehrdad Nemazee | Senior Property Manager | (202) 438-7345 | Mnemazee@WindHQ.com |
| Daniel McClure | Assistant Elec. Manager | (571) 714-6827 | dmccclure@WindHQ.com |
| Matthew Adamson | Physical Security Engineer | (571) 512-8343 | madamson@WindHQ.com |
| Leighton Le | Site Security Captain | (703) 217-2941 | leightonle@WindHQ.com |
| William White | Electrical Foreman | (202) 285-2824 | Willaimwhite@WindHQ.com |
| Issael Guardado | Facilities Assistant | (571) 420-8250 | iguardado@WindHQ.com |

| | | | |
|------------------|------------------------------|----------------|---------------------------|
| John Merrick | Electrical Manager | (202) 580-5027 | jmerrick@WindHQ.com |
| Robert Bruce | Mechanical Manager | (571) 230-3862 | rbruce@WindHQ.com |
| Keisa Reid | Property Manager | (571) 919-0967 | kreid@WindHQ.com |
| Jonathan Waldron | Senior EHS Manager | (571) 461-8649 | jwaldron@WindHQ.com |
| Ben Hartsell | Assistant Elec. Manager | (571) 719-0238 | bhartsell@WindHQ.com |
| Dan Dowd | Assistant Mech. Manager | (571) 340-0889 | Danieldowd@WindHQ.com |
| Shane Hibner | Electrical Foreman | (571) 719-0593 | shanehibner@WindHQ.com |
| Ricardo Vela | Facilities Assistant | (202) 823-1023 | rvela@WindHQ.com |
| Kim Snyder | Site Security Captain | (571) 317-4681 | KimberlySnyder@WindHQ.com |
| Mohammad Ali | Audit and Compliance Manager | (571) 919-5576 | mali@WindHQ.com |

10. VENDOR CONTACT LIST

Table 9. Vendor Contacts

| Vendor | Resource/Service | Contact Information |
|-------------------------------|---|---|
| Ingersoll Rand | Air Compressor | Ingersoll Rand Richmond, VA 804-214-7054 |
| TRANE | Chiller | Boland Services 240-306-3000 |
| ESI | Day Tank, fuel oil cleaner, diesel fuel | ESI 703-263-7600 |
| Ferguson Enterprises Inc. | Domestic Hot Water Circulation | Ferguson Enterprises Inc. 703-375-5800 |
| Stancor | Elevator sump pump | Elcon Enterprises Inc. 301-586-9300 |
| Greenheck | Exhaust fans | C.G. Wood Company Inc. 240-241-5300 |
| Alban CAT | Engine Generator | |
| Tanks Direct | Fuel pump | Tanks Direct 800-865-5555 |
| Advantage Controls | Glycol Feeder | Advantage Controls 918-686-6211 |
| Munters | Humidifier | Munters 978-330-6960 |
| Miratec | Muffler | Jim McDonald 215-407-9001 |
| AAON | Roof Top Air Handling Units | Havtech 301-206-9225 |
| DAIKIN | Roof Top Air Handling Units | Havtech 301-206-9225 |
| Tanks Direct (Highland Tanks) | Underground Fuel Tank, Thermal Storage Tank | Tanks Direct 800-865-5555 |
| INDEECO | Unit Heater | Boland Services 240-306-3000 |
| Nailor | VAV Terminal | Metropolitan Equipment Group, Inc. 804-744-4774 |
| Bell & Gossett | | Cummins-Wagner 301-490-9007 |
| Harmsco | | Chemtreat Inc. 804-935-2000 |
| Stulz | CRAC & CRAH | Stulz 888-529-1266 |

| Vendor | Resource/Service | Contact Information |
|--------------------------|---|--|
| Square D | Bus Plugs, busway | 1-844-362-6387 |
| Cooper Power Systems | Transformer | |
| Eaton | Panels, Breakers | 1-262-524-2379 |
| SAI | EDP, CDP, Switchboards | 1-847-688-9013 |
| ASCO | Load Bank, ATS | 1-216-573-7600 |
| Schneider Electric | MV Gear & UPS | 1-844-362-6387 |
| PDI | | 1-804-737-9880 |
| Bussman | | 1-800-386-1911 |
| SENS | Battery charger | 1702-826-0819 |
| Seimens | Switchgear | https://new.siemens.com/us/en/company/about/contact-us.html |
| PDS | UNIT SUBSTATION TRANSFORMERS | 1-803-259-6003 |
| Dominion Virginia Energy | Utility power | Dominic J. Minor Key Account Manager Dominic.j.minor@dominionenergy.com 866-366-4357 |
| Verizon | Cell and internet service | www.verizon.com |
| Zayo | Internet service | 866-364-6033 |
| Fiberlight | Internet service | 844-509-0775 |
| Myriad | IT equipment | 866-725-1025 |
| Amazon | IT equipment | www.amazon.com |
| Clean Harbors | Waste disposal & emergency spill response | Kevin Malone 301-466-1570 or 800-645-8265 |
| Grainger | Supplies | www.grainger.com |

| Vendor | Resource/Service | Contact Information |
|-----------------|--|---|
| Cintas & Stat | First aid and safety, pandemic disinfectants | Julie Hanigan 301-802-8661 (Stat) Gary Eversole 703-819-0599 (Cintas) |
| Staples | Office Supplies | www.staples.com |
| Clean Solutions | Housekeeping | Boris Barrios (703) 975-9683 |
| Poole and Kent | Operations contractor | Mike Everitt (443) 717 0189 or meveritt@emcor.com |
| Securitas | Site Security | Justin Boudville (571) 220-4669 |

11. FAMILY EMERGENCY PLAN

Employees must also prepare in advance for what to do in an emergency and should develop a Family Support Plan to increase personnel and family preparedness. To develop your Family Support Plan, use the templates available at www.ready.gov. this site includes a ‘Get Ready Now’ pamphlet, which explains the importance of planning and provides a template that you and your family can use to develop your specific plan. The following list is gathered from <https://www.ready.gov/build-a-kit>.

11.1 Basic Disaster Supplies Kit

To assemble your kit, store items in airtight plastic bags and put your entire disaster supplies kit in one or two easy-to-carry containers such as plastic bins or a duffel bag.

A basic emergency supply kit could include the following recommended items:

- Water - one gallon of water per person per day for at least three days, for drinking and sanitation
- Food - at least a three-day supply of non-perishable food
- Battery-powered or hand crank radio and a NOAA Weather Radio with tone alert
- Flashlight
- First aid kit
- Extra batteries
- Whistle to signal for help
- Dust mask to help filter contaminated air and plastic sheeting and duct tape to shelter-in-place
- Moist towelettes, garbage bags and plastic ties for personal sanitation
- Wrench or pliers to turn off utilities
- Manual can opener for food
- Local maps
- Cell phone with chargers and a backup battery
- Download the Recommended Supplies List (PDF)

11.2 Additional Emergency Supplies

Consider adding the following items to your emergency supply kit based on your individual needs:

- Prescription medications
- Non-prescription medications such as pain relievers, anti-diarrhea medication, antacids or laxatives.
- Glasses and contact lens solution.
- Infant formula, bottles, diapers, wipes, diaper rash cream

- Pet food and extra water for your pet
- Cash or traveler's checks.
- Important family documents such as copies of insurance policies, identification and bank account records saved electronically or in a waterproof, portable container.
- Sleeping bag or warm blanket for each person
- Complete change of clothing appropriate for your climate and sturdy shoes
- Household chlorine bleach and medicine dropper to disinfect water.
- Fire extinguisher
- Matches in a waterproof container.
- Feminine supplies and personal hygiene items
- Mess kits, paper cups, plates, paper towels and plastic utensils.
- Paper and pencil
- Books, games, puzzles, or other activities for children

12. TRAINING

WindHQ employees will be thoroughly trained in emergency evacuation and restoration procedures. Specifically,

- All employees will review disaster preparation and emergency action plan procedures.
- Annual training will involve one or more of the following drills:
 - Walkthrough drills: The business continuity planning team, department heads and site teams will perform their emergency response functions.
 - Functional drills: These drills will evaluate specific functions such as medical response, emergency notifications, warning and communication procedures and equipment. Facility shutdown procedures will be evaluated, reviewed, and modified as needed. Personnel are asked to evaluate the systems and identify problem areas.
 - Evacuation drills: Personnel will walk the evacuation route to a designated area where procedures are evaluated for accounting for all personnel.
 - Full-scale exercise: A real-life emergency is simulated as close as possible. These exercises involve company emergency response personnel, employees and management, and community response organizations.

13. ANNUAL PLAN AUDIT

A formal audit of the business continuity plan will be conducted annually and should be evaluated and modified after each training exercise, emergency, changes in personnel responsibilities, changes in facility layout or design and changes in policies or procedures. Personnel will be briefed every time changes or modifications have been made to the plan.

14. INSURANCE CONSIDERATIONS

Contact our insurance agent or broker to discuss our business insurance coverage and needs.

OWNERSHIP AND REVIEW

The VP of Operations owns this standard.

This standard shall be reviewed on an annual basis.

CONTACT INFORMATION

Rich Rohde

VP Operations

509-688-3476

rrohde@windhq.com

DOCUMENT RACI

| | | |
|--------------------|---|--|
| Responsible | Assigned to do the work | Site Managers Director of operations |
| Accountable | Final decision, ultimately answerable | Director of Operations |
| Consulted | Consulted BEFORE an action or decision is taken (proactive) | Executive Management |
| Informed | Informed AFTER a decision or action has been taken (reactive) | Named Participants in this document. Other parties affected by the change |