Bianca Peregrino	902 S Loyola	Perryton, TX	79070		806-202-5064

Engineering Services Manager					
Joe Lane	[redacted]	Perryton, TX	79070		806-202-0305
Sean Roberts	[redacted]	Perryton, TX	79070		[redacted]
Michael McLaughlin	[redacted]	Booker, TX	79005		[redacted]
Justin Humphrey	[redacted]	Perryton, TX	79070		[redacted]
Ashtan Appelhans	[redacted]	Perryton, TX	79070		[redacted]
CFO					
Jennifer Roberts	[redacted]	Perryton, TX	79070		806228-0811
Angela Petersen	[redacted]	Perryton, TX	79070		[redacted]
Tiffany Constancio	[redacted]	Perryton, TX	79070		[redacted]
Ivette Cortez	[redacted]	Perryton, TX	79070		[redacted]
Brittany Yeary	[redacted]	Perryton, TX	79070		[redacted]
Engineering					
Jaime Pugh	[redacted]	Beaver, OK	73932		[redacted]
Marc Padgett	[redacted]	Perryton, TX	79070		[redacted]
Monte Eisenman	[redacted]	Perryton, TX	79070		[redacted]
Jimmie Burkhalter	[redacted]	Perryton, TX	79070		[redacted]
Russell Crain	[redacted]	Perryton, TX	79070		[redacted]
Custodial					
Rosario Bernal	[redacted]	Perryton, TX	79070		[redacted]

ANNEXES

Cooperative maintains the annexes designated below, which are attached and incorporated into the Plan:

Annex	Title	Included	Explanation, if not included
A	Load Shed	Yes	
B	Pandemic and Epidemic	Yes	
C	Wildfires	Yes	
D	Hurricanes	No	Not applicable. Cooperative service territory is not located near or within a hurricane evacuation zone, as defined by the Texas Division of Emergency Management.
E	Cybersecurity	Yes	
F	Physical Security	Yes	
G	TDU Requirements	No	Not Applicable. Cooperative is not a Transmission and Distribution Utility as defined in 16 TAC §25.5
H	Additional annexes	No	No additional annexes necessary
XXX	[Confidential Portions of ------]		

Southwest Power Pool ("SPP")

1. PROCEDURES FOR CONTROLLED SHEDDING OF LOAD

Southwestern Public Service's ("SPS") Transmission Operations Center receives Load Shed Instructions from SPP. SPS's Transmission Operations Center performs a calculation to allocate the load shed requirement for "North Plains Electric Cooperative" and communicates that instruction via voice communication.
Upon notification of curtailment and the target kW to be shed, NPEC personnel will begin opening feeder circuit breakers via SCADA (or via field personnel in the substation) as outlined in the cooperative's Emergency Load Curtailment Plan until the target kW is shed.
Once the target kW is shed, NPEC will notify SPS's Transmission Operations Center via voice communication that the allocated load has been shed.
Depending on the duration of the curtailment, it is planned to rotate load that has been shed among the substations and circuits on a one (1) hour basis. This is to spread the outages as evenly among the Members as possible and minimize the inconvenience associated with the outage.
All load shed Instructions will be executed as soon as possible and without delay.
The cooperative uses discretion in prioritization of selecting load shed feeders by giving highest priority to critical natural gas facilities to remain in service taking into consideration the guidance provided by PUCT (please refer to Appendix I), with other critical loads given lower priority to remain in service. Even though the cooperative plan attempts to prioritize critical natural gas facilities and other critical loads from manual load shed, designation as a critical natural gas facility or other critical load does not guarantee the uninterrupted supply of electricity.

1. PRIORITIES FOR RESTORING SHED LOAD TO SERVICE

Southwestern Public Service's Transmission Operations Center receives Instructions from SPP that load can be restored. SPS's Transmission Operations Center performs a calculation to allocate how much load can be restored for NPEC and communicates that Instruction via voice communication.

Upon notification of load restoration and the target kW to be restored, NPEC personnel will begin closing feeder circuit breakers via SCADA (or via field personnel in the substation) until the target kW is restored.

Once the target kW is restored, NPEC will notify SPS's Transmission Operations Center via voice communication the amount of load that has been restored.
If any critical natural gas facilities or other critical loads were curtailed, they will be given higher priority for service restoration.
In addition to the priorities concerning community health and safety, Cooperative will assign

crews to specific areas. Generally, the crews will concentrate on a given line section in order to restore power to as many members as possible. Restoration will be done systematically, with the best interest of all affected members in mind. However, one or more crews may be assigned to locations where special hazards exist or where especially critical loads require immediate attention. When not specifically assigned, these crews will be used to repair individual services

ANNEX B: PANDEMIC PREPARDNESS PLAN

Pandemic Continuity Plan

NORTH PLAINS ELECTRIC COOPERATIVE, INC.

NOVEMBER 1, 2014

Revised March 8, 2022
Approved March 17, 2022

The template was utilized to create the North Plains Electric Cooperative, Inc. Pandemic Continuity Plan with the permission of the San Francisco Department of Public Health. It is subject to copyright protection but is available for a Guide and Template. It was further stated that, if used, no entity should charge or receive fees. Also, the San Francisco Department of Public Health should be appropriately acknowledged.

Copyright 2008 San Francisco Department of Public Health

Approved: March/17/2022 Revision: ____/____/____

I INTRODUCTION

A. Purpose and Objectives

The primary purpose of the Pandemic Continuity Plan is for North Plains Electric Cooperative, Inc. (NPEC) to respond safely, effectively, and efficiently to a pandemic. Objectives during a pandemic outbreak are the following:

1. Reduce transmission of the pandemic virus strain among our employees, members, vendors and partners.
2. Minimize illness among employees and members.
3. Maintain essential operations and services.
4. Minimize social disruptions and the economic impact of a pandemic.

B. Supporting Plans

NPEC has an Emergency Operation Plan addressing emergency response and recovery. The Pandemic Continuity Plan will be implemented in conjunction with it.

C. Overview

a. Pandemic Overview

Severe pandemics represent one of the greatest potential threats to the public's health. Over time, people develop some degree of immunity to these viruses, and vaccines are developed annually to protect people from serious illness. Pandemic refers to a worldwide epidemic due to a new, dramatically different strain, to which there is no immunity. The new virus strain may spread rapidly from person to person and, if severe, may cause high levels of disease and death around the world

The worldwide public health and scientific community is concerned about the potential for a pandemic to arise. Although many officials believe it is inevitable that future pandemics will occur, just like with earthquakes, it is impossible to predict the exact timing of their arrival. It is difficult to predict the severity of the next pandemic and whether the pandemic virus strain will be treatable with existing medicines.

There are several characteristics that differentiate a pandemic from other public health emergencies. Unlike other natural disasters, where any disruption to business service provision is likely to be infrastructure-related, disruption to business operations in the event of a pandemic is anticipated to be human and material oriented. A pandemic has the potential to cause illness in a very large number of people, overwhelm the health care system, and jeopardize services by causing high levels of absenteeism in the workforce. Basic services, such as health care, law enforcement, fire, emergency response, communications, transportation, and utilities could be disrupted during a pandemic. Finally, the pandemic, unlike many other emergency events, could last many months and affect many areas

throughout the world simultaneously.

In a pandemic situation, the goal is to slow the spread of disease to prevent illness. The most effective strategy to accomplish this is through vaccination and boosters. However, it is likely that large quantities of effective vaccines will not be available for many months following the emergence of a new pandemic. Existing antiviral medications may also not be effective or available. Other disease control strategies such as social distancing, improved hygiene and respiratory etiquette, isolation, and quarantine may be used to control the spread of disease.

b. International Monitoring

The World Health Organization (WHO) and the United States Federal Government use a series of phases and stages of pandemic alert as a system for informing the world of the seriousness of the threat and of the need to launch progressively more intense preparedness and response activities.

WHO Phases		Federal Government Response Stages	
INTER-PANDEMIC PERIOD			
1	No new influenza virus subtypes have been detected in humans. An influenza virus subtype that has caused a human infection may be present in animals. If present in animals, the risk of human disease is considered to be low.	0	New domestic animal outbreak in at-risk country
2	No new influenza virus subtypes have been detected in humans. However, a circulating animal influenza subtype poses a substantial risk of human disease.		
PANDEMIC ALERT PERIOD			
3	Human infection(s) with a new subtype, but no human-to-human spread, or at most rare instances of spread to a close contact.	0	New domestic animal outbreak in at-risk country
		1	Suspected human outbreak overseas
4	Small cluster(s) with limited human-to-human transmission but spread is highly localized, suggesting that the virus is not well adapted to humans.	2	Confirmed human outbreak overseas
5	Larger cluster(s) but human-to-human spread still localized, suggesting that the virus is becoming increasingly better adapted to humans, but may not yet be fully transmissible (substantial pandemic risk).		
PANDEMIC PERIOD			
6	Pandemic phase: increased and sustained transmission in general population.	3	Widespread human outbreaks in multiple locations overseas
		4	First human case in North America
		5	Spread throughout United States
		6	Recovery and preparation for subsequent waves

II Activation & Notification

A. Activation

Some or all of the Pandemic Continuity Plan will be activated when one or more of the following criteria is met:

- WHO declares the pandemic is in Phase 6 (increased and sustained transmission in the general population)
- Essential services are impacted by a viral pandemic either due to employee absenteeism, lack of supplies, or other reasons.
- Employee absenteeism is at 40% or greater.
- Employee concern regarding personal safety from a pandemic virus exists.

Only authorized staff may direct the activation/deactivation of the Pandemic Continuity Plan. Staff authorized to activate the plan include:

- Executive Vice President & General Manager
- CFO
- Board of Directors

B. Notification

The following groups will be notified when the plan has been activated:

- Board of Directors
- Employees
- Members
- Vendors

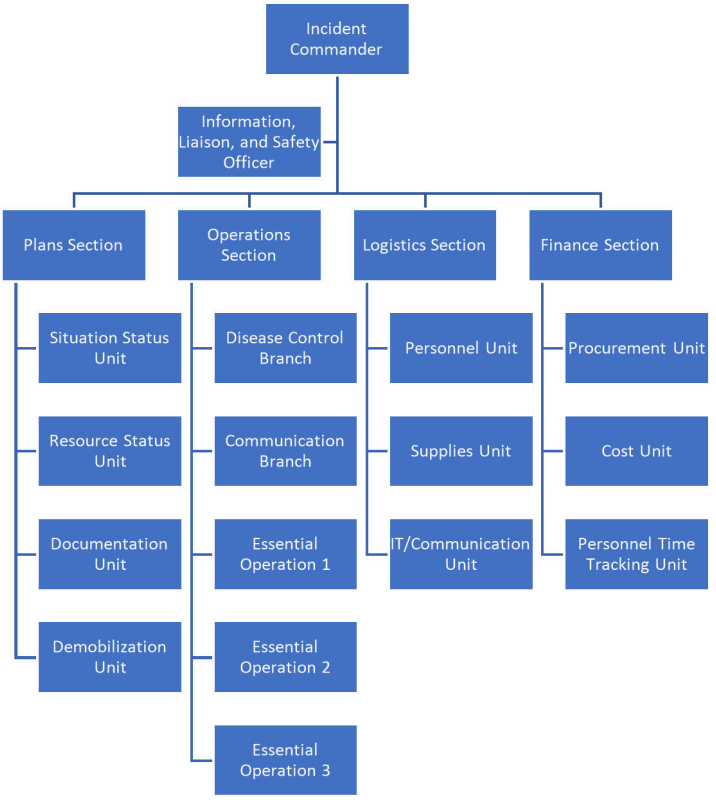
III AUTHORITY

A. Response Organizational Structure

The following organizational structure can be used to manage the response. This structure is based on the [daily operating organizational structure, the Incident Command Structure, or other emergency response structure]. Some or all of the organizational chart will be activated for the response. Modifications can be made to the structure throughout the response as needed.

Note
The Incident Command Structure (ICS) is one method for managing an emergency response. In the United States it is used by national and local governments and has also been adopted by many businesses. To learn more about ICS see: http://training.fema.gov/

Pandemic Continuity Organizational Response Structure



B. Overall Management of Response

When the Pandemic Continuity Plan has been activated, overall management of the response is delegated to the Incident Commander, who presently is the CFO. Their primary responsibilities include:

- Oversight for implementation of the plan and company operations
- Expenditure approval consistent with established organizational procedure
- Allocation of personnel and non-personnel resources
- Policy decision making authority

The individuals that hold the following positions at NPEC are eligible to assume overall management of the response.

4. Primary Executive V.P. & General Manager
5. Backup Safety Coordinator
6. Backup Engineering Services Manager
7. Backup Operations Manager
8. Backup Engineer
9. Backup Engineering & Operations Supervisor

The designated individual retains all assigned obligations, duties, and responsibilities until officially relieved by an individual higher on the list. If a designated individual is unavailable, authority will pass to the next individual on the list. "Unavailable" is defined as:

- The designated person is incapable of carrying out the assigned duties by reason of death, disability, or distance from the facility.
- The designated person is unable to be contacted within 24 hours.
- The designated person has already been assigned to other emergency activities.

IV SITUATION ANALYSIS

A. Mission

To inform the response, a situation analysis will be conducted regularly (daily or as needed) to identify up-to-date information, new guidance, and assess the impact of the pandemic on the business, partners, and community. This information will be shared with response leaders to inform decisions and with employees to ensure that they have accurate and up-to-date information.

B. Implementation

a. Pandemic Status

The scope and spread (e.g., number of cases) of pandemic viruses in the community will be monitored. Key sources for reliable information include:

- Texas Department of Safety & Health Services www.dshs.state.us
- Centers for Disease Control and Prevention www.cdc.gov
- World Health Organization www.who.int

Newspapers and other popular sources of information will be monitored in order to address misinformation and emerging public concerns.

b. Disease control safety recommendations

Local safety recommendations and requirements issued by the Texas Department of Safety & Health Services will be collected. These may include recommendations specific to individuals, workplaces, healthcare facilities, and/or other sites. Disease control safety recommendations may address personal protective equipment (e.g., masks), social distancing measures (e.g., closure of schools, closure of large events), escalation of healthy habits (e.g., hand washing), and other strategies to reduce the transmission of a pandemic virus.

These recommendations will be shared and adopted by the individuals responsible for implementing disease control in the workplace. Sources for local NPEC disease control safety recommendations include:

- Official government press releases
- Official government press conferences
- Website: www.dshs.state.us
- Area Hospital guidance
- Radio stations:

KEYE 1400 AM
KXDJ 98.3 AM

c. Community impact

The impact on the general public, members, and community will be assessed to provide situational awareness and inform operations.

d. Demand changes

Member demand for NPEC's services/electricity may increase or decrease due to the pandemic situation. Changes in demand will be assessed. Additionally, recommendations on modifications that can be made to the types of services provided and/or the way they are provided, to increase demand and instill member confidence will be made.

e. Input changes

Vendors or partners that routinely provide services or material to NPEC may be impacted by the pandemic. Vendor ability to maintain services or provide products, and how or if this will impact operations, will be assessed.

Contact information for vendors is located in the Emergency Operation Plan.

Vendors with whom NPEC does not routinely work, but may be able to supply needed goods and/or services during an emergency, will also be assessed.

f. Operational capabilities

Routine and essential operations may be affected by the pandemic situation due to staff absenteeism, regulatory agency modifications, or other impacts. NPEC's ability to maintain the following activities with the available human and material resources will be assessed:

ESSENTIAL OPERATIONS

- Maintain office presence & continuity in person and remotely
- Maintain engineering group availability
- Maintain operations group & ability to respond to outages
- Retain ability to dispatch inhouse or through CRC.
- Maintain ability to stock material& fuel supply

Suspended standard daily operations

- Employees reporting to office to fulfill workday responsibilities

- In person safety meetings and employee meetings
- Lobby closed to members and public in general
- Vendor visits suspended

g. Financial analysis

An update on the business' financial performance will be conducted regularly. This information will be used to inform decisions about resource allocation.

C. Management and Staffing

Situation analysis activities will be managed by the CFO and the Executive Vice President & General Manager. Positions required to perform operations include:

Situation Analysis Staffing Positions

Job Title	Task Overview	Critical Skills Required	Number of Employees
Situation Status Leader	Oversee the collection, analysis, and sharing of information.	Management and HR	3
Situation Analyst	Collect, synthesize, and share situational information.	Cooperative Business Knowledge	7
Financial Analyst	Collect, synthesize, and share financial information.	RUS Accounting	2

V COMMUNICATION

A. Mission

During a pandemic there may be a high level of fear and anxiety. Rumors and misinformation will fuel those emotions. [Insert name of business] realizes that in order to sustain employee, member, and vendor confidence and morale, information sharing will be critical. NPEC will strive to provide clear, consistent, relevant, truthful, and timely information to the following audiences:

- **Employees**
- **Members**
- **Product and service vendors**
- **Public**
- **Government**

B. Implementation

All content will be disseminated by one coordinated working group to ensure that messages are consistent, complete, and effectively reaching all audiences. However, various individuals may assist in developing messages. All outgoing content will first be approved by:

- CFO or their designee

a. Content

a.1. Employee Communication

Sustaining employee confidence and morale for many months will be challenging. **NPEC** is committed to maintaining a two-way line of communication and providing regular (e.g., daily, bi-weekly, weekly) updates to all employees.

Prior to the pandemic, employees were provided with information about the continuity of operations plan, pandemic facts, healthy habits to use everyday and during a pandemic, and where to get information during an emergency.

During a pandemic, key topics for inclusion in employee updates will include:

- Status of the pandemic
- Status of operations and response
- How routine updates and urgent communications will be disseminated (e.g., telephone information line, posted flyer, e-mail)
- Disease control measures utilized in the workplace
- Policy changes
- Job reassignments
- Absentee reporting process

- Other applicable information as needed

a.2. Vendor Communication

NPEC is committed to providing regular updates and ongoing dialogue with vendors and other partners regarding operations, service/product needs, and emergency response activities. Key topics include:

- Changes in supply and service needs
- Disease control requirements they must adhere to at the work site
- Status of operations and response
- How routine updates and urgent communications will be disseminated (e.g., telephone information line, posted flyer, e-mail)
- Updated contact information

a.3. Member and Public Communication

To ensure that members and the general public are aware of services/electricity and adopted disease control safety standards, key messages will include:

- Operating hours
- Updated contact information
- Disease control safety standards being implemented at the business
- How updates will be disseminated

b. Information Dissemination

Information will be disseminated to audiences throughout the pandemic using the modes of communication described below. Multiple strategies will be used to create redundancy and ensure that intended recipients receive messages.

- **Telephone Systems.** Internal agency information line [insert telephone number], external public information line, mass voicemail message, call center/phone bank, call-down tree
- **Electronic Systems*.** Mass e-mail message, website posting [www.npec.org], intranet posting, on-line chat
- **Hard copy*.** Mailing, interoffice mail, mass faxes, notice board postings, pay check mailing
- **In person.** Meeting, presentation.
- **Media- TV, Radio, Newspaper.** Press releases
- **Social Media**

* Information may be packaged in the form of letters, memos, fact sheets, brochures, newsletters, etc.

Urgent updates

The primary method(s) for disseminating urgent communications will be:

Employees. Email, Text, Personally
Members. Mailing, Website posting, Social Media
Vendors. Email , Telephone
Public. Media, Print, Social Media

Routine updates

The primary method(s) for disseminating routine emergency related updates will be:

Employees. Email, In-Person communications
Members. Mailing, Website posting, Social Media
Vendors. Email , Telephone
Public. Media, Social Media

VI COMMUNICABLE DISEASE CONTROL

A. Mission

Safeguarding the health of employees, members, vendors, and the public during a pandemic is a key objective for NPEC. A combination of communicable disease control measures, including heightened hygiene practices, social distancing, and protective equipment and supplies will be utilized to slow the spread of disease.

B. Implementation

Communicable disease control refers to strategies that can be used to reduce the transmission and acquisition of contagious diseases. Contagious diseases spread in different ways. Viruses are spread through either:

- Breathing in respiratory particles (usually not visible to the human eye) that are expelled from the respiratory tract during coughing, sneezing, or talking. These particles travel short distances (up to 6 feet) and may remain suspended in the air for short amounts of time depending on the size of the particle, temperature, humidity and other conditions.
- Contact with contaminated respiratory droplets or secretions (e.g., touching a surface that has recently been contaminated with respiratory droplets or secretions followed by touching the nose, eyes, or mouth).

There are various strategies that can be used to reduce the transmission of the virus. Preliminary recommendations for a severe pandemic are included.

a. Disease Control Supplies

For employees to practice disease control recommendations properly, the following supplies should be regularly available:

- Soap (at all hand-washing sinks)
- Tissues
- Hand sanitizer (minimum 60% alcohol content)
- Office cleaning and disinfecting supplies (see details in table, Disinfecting Solutions)
- Paper towels
- Trash bags
- Personal protective equipment (See Section VI, B, b)

A stockpile of these supplies are stored in the north closet near the Willie room.

b. Personal Protective Equipment

Use of personal protective equipment during a severe pandemic may be recommended by NPEC. NPEC will ensure that face masks are available. Recommended equipment may include:

- **Face masks.** The general public may be asked to wear face masks when in public settings, including workplace settings. Face masks are loose-fitting, disposable masks that cover the nose and mouth, and have ear loops or ties for a secure fit. These include products labeled as surgical, dental, medical procedure, isolation, and laser masks. Facemasks are designed to prevent the wearer from spreading germs found in respiratory droplets, to others. They are not designed to protect the wearer from breathing in very small particles. When supplies are available, facemasks should be used once and then thrown away in the trash, especially if they become moist.
- **Gloves.** Frequent hand washing will be recommended. If adequate hand washing occurs, it is not necessary to wear gloves for routine activities. However, gloves are recommended for cleaning with disinfectant. Gloves come in many types that are suitable in different situations. In general, gloves must be liquid-proof and should fit comfortably.

c. Disinfect Surfaces

During a pandemic, thorough workplace disinfection measures will be required to minimize the transmission through surfaces.

Simple cleaning with a damp cloth may not kill or remove viruses, therefore disinfection is required for this purpose. Viruses are readily killed by disinfectants. Any of the following solutions can be used to disinfect surfaces:

DISINFECTING SOLUTIONS

Disinfectants	Recommended Use	Precautions
EPA-Approved Disinfectant* Product should be labeled as a disinfectant and have an EPA registration number	Use to disinfect only after cleaning the surface first. Follow directions on label for proper dilution and contact time.	Follow precautions on label.
Sodium Hypochlorite (Bleach) 1 part bleach to 100 parts of water, or 1:100 dilution. Usually achieved by 2 1/2 tablespoons bleach into 1 gallon of water.	Use to disinfect only after cleaning the surface first. Allow a contact timeLeave solution on the surface for at least 10 minutes.	• Use in well-ventilated areas. • Avoid inhalation • Wear gloves while using bleach solution. • Do not mix with strong acids or ammonium based products to avoid release of noxious fumes. • Corrosive to metals and certain materials.
Alcohol Isopropyl alcohol 70% (rubbing alcohol), or Ethyl alcohol 60%	Use to disinfect only after cleaning the surface first. Make sure the surface becomes wet or damp with the alcohol and then dries completely.	• Flammable and toxic. Used in well ventilated areas. • Avoid inhalation. • Keep away from heat sources, electrical equipment, flames, and hot surfaces. • Dry completely- this usually takes about 10 minutes

** Look for the EPA (U.S. Environmental Protection Agency) registration number on disinfectant products. This indicates that the product has met efficacy and safety standards.*

c.1. Items to disinfect

Surfaces that are frequently touched by hands should be cleaned and disinfected often, at least daily. When a person with suspected virus is identified and has left the workplace, their work area, along with any other known places they have been, should be cleaned and disinfected.

Surfaces to disinfect include commonly touched surfaces like doorknobs, water-cooler taps, telephones, and other items that are touched by various people throughout the day. Non-essential items (e.g., magazines/newspapers) from common areas will be removed.

c.2. Steps to disinfect

The person cleaning and disinfecting should follow these steps:

5. Wash hands with soap and water, or use hand sanitizer if not visibly dirty
6. Put on a face mask
7. Put on gloves
8. Clean surfaces if they appear dirty
9. Apply disinfectant in the appropriate dilution and leave on for at least the minimum contact time

10. Disinfect all surfaces detailed above
11. Remove gloves
12. Remove mask
13. Wash hands with soap and water, or use hand sanitizer if not visibly dirty

d. Heightened Hygiene Practices

Request that employees escalate their use of healthy habits to limit the spread of disease. Disseminate reminders throughout the work site. Key messages include:

- Wash your hands often with soap or use hand sanitizer.
- Avoid touching eyes, nose, and mouth with un-washed hands.
- Cover your cough and sneeze.
- Stay home when sick. Depending on virus, symptoms include:
    - Fever
    - Chills, shivering
    - Muscle aches
    - Sore throat
    - Dry cough
    - Headache
    - Fatigue (extreme tiredness)
    - Loss of taste or smell
- Avoid close contact (6 feet or less) with others including skin-to-skin contact..
- All persons in the workplace should wear a mask or covering over the mouth and nose when in the same room as another person.
- Clean and disinfect commonly used surfaces.
- Minimize close contact with sick persons.

Additional hygiene practices may be recommended depending on the situation and characteristics of the pandemic virus.

e. Social Distancing

Social distancing refers to a disease control strategy that includes limiting or altering the frequency and closeness of people in order to reduce the spread of contagious diseases from one person to another. Some social distancing strategies include restricting events that congregate people (e.g., concerts), utilizing physical barriers (e.g., glass divider) to restrict the sharing of air when face-to-face contact is required, modifications to social behavior (e.g., no hand shaking), and creating distance between work spaces that are greater than the virus' movement. During a pandemic people may be advised to stay at least 6 feet apart (this recommendation may be altered by the health department during a pandemic event).

NPEC has the ability to utilize the following social distancing strategies to reduce close contact among individuals.

e.1. Telecommuting

Whenever possible, NPEC will encourage employees to work from home. This reduces the risk of disease transmission to all employees by minimizing the number of persons in the work setting

e.2. Videoconferences

Face to face meetings will be discouraged. Videoconferences can be held multiple party groups.

e.3. Staggered work shifts

The work shifts of all employees/work units can be spread over the workday or can be modified to a flexible schedule of extended hours in fewer days.

e.4. Face-to-face barriers

Some of NPEC's services are provided in a face-to-face setting (individuals are less than 6 feet apart). To reduce the possibility of transmission, alterations may be made to reduce face-to-face contact in the work setting (e.g., services provided by telephone instead of in-person, glass barriers set-up between individuals). The types of services and number of employees who have regular face-to-face contact with members, and modification that can be made to reduce contact, are listed below:

Services requiring face-to-face contact (under 6 feet)	**Number of employees performing service**	**Modifications that can be made to eliminate/reduce face-to-face contact**
Cashier/ Reception	Up to 5	Mask, Clear Barrier
Member Service Rep	2	Mask
Staking Tech	2	Outdoors using 6 feet rule

When it is not possible to eliminate face-to-face contact under 6 feet, face masks should be worn by both employees and members.

e.5. Distance between work sites

Create distance (at least 6 feet) between employees who must work in the same room. Room layouts that allow for 6 feet of distance between work stations are preferred.

Employees will be encouraged not to congregate in communal spaces – break rooms.

f. Restrict workplace entry of people with symptoms

During a pandemic, asking individuals with described symptoms to stay out of the work setting may limit the spread of disease. When the plan is activated, the following steps will be taken to limit entry of people with symptoms:

2. Post notices at all workplace/facility entry points advising staff and visitors not to enter if they have symptoms. The signs may say:

"To help limit the spread of infection, it is important that you do not come inside this facility if you feel feverish, have a cough, have body aches, or have a sore throat. We may ask you to leave this facility in order to protect our employees and visitors from getting infected. Your cooperation is appreciated."

3. Provide hand sanitizer at the entrance of the facility. Instruct everyone entering and leaving the facility to clean their hands.

4. Advise employees to call the designated staff if they become ill at home or work.

g. Ventilation

At present there are no special pandemic heating, ventilation, and air conditioning (HVAC) systems recommendations outside of a healthcare setting. HVAC systems should receive regular maintenance checks according to standards and building codes. In specific rooms where there is a potentially infected person, the ventilation should be increased as much as possible (e.g. by opening windows).

h. Manage employees who become ill

In order to reduce the transmission of disease, it is important that individuals who are sick, with pandemic virus or other contagious illnesses, stay out of the work setting. Individuals with flu-like symptoms may be asked to stay home for a specific time period, referred to as home isolation, until they are no longer contagious. The isolation period (or period when individuals are contagious and should stay away from others) could be as long as 1 to 2 weeks after symptoms develop.

h.1. Employees who become ill at work

If an employee begins to feel sick while at work, it will be important to follow key steps to reduce the transmission of disease to others. Advise employees that if a person feels ill, or if someone observes that another person is exhibiting flu like symptoms at work, they are to immediately contact their supervisor and then leave.

C. Management and Staffing

Disease control activities will be managed by all staff employees. Staffing will be completed by supervisors available.

VII PERSONNEL

A. Mission

During a severe pandemic, worker absenteeism (20 – 50% in excess of standard absenteeism rates) may occur at all personnel levels due to illness, family member illness, death, unmet childcare needs (e.g., children may be dismissed from school), and "worried well" (otherwise healthy people who avoid the workplace for fear of exposure). Additionally, NPEC will likely recommend that individuals who are experiencing flu-like symptoms stay at home or away from others until they are no longer contagious (this is known as the isolation period).

NPEC is committed to safely maintaining essential operations and supporting personnel during the emergency. Personnel may be re-assigned and provided with just-in-time training to ensure that essential operations can be performed. Personnel absenteeism will be tracked, non-punitive personnel policies will be activated, and employees who report sick will be supported.

B. Implementation

a. Pandemic Policies

A flexible work policy should include instructions for notifying your workers' compensation carrier that there are employees who are working from home and the days they are doing so. There is no home inspection requirement, because the Occupation Safety and Health Administration (OSHA) has already issued a directive stating so (OSHA Directive Number: CPL 2-0.125). Discuss details with your legal representative.
Standard operating policies and practices may need to change during a pandemic. The following policies may be activated as part of the pandemic response. The decision to activate the following policies will be made by the CFO & General Manager. Employees will immediately be notified of policy changes.

a.1. Employee Leave

The following emergency leave policies address employee absences due to personal illness, family member illness, trauma, isolation, quarantine, and/or school dismissal.

Board Policy #5 covers this section.

a.2. Flexible Work

Working from home and flexible work hour (e.g. staggered shifts, extended shifts) policies may be activated or enhanced to allow for social distancing. These include:

- Staggering schedule for crews that work in the field
- Isolating crew members in separate vehicles to and from the worksite
- Restrict free movement within office area and warehouse area
- Adhere as much as possible to the 6 feet rule in all work zones
- Move field employees to an extended work day
- Provide office employees that can work from hoe that opportunity when necessary

a.3. Travel Policies

During a pandemic response the travel policies will be assessed and determined based on severity of

outbreak and conditions at that time.

b. Track staff

Because absenteeism may be erratic for many weeks, NPEC will track present and absent staff and forecast future staff absenteeism. Key information to collect includes, name of individual, position title, department/unit routinely assigned to, key skills, anticipated return date, and reason for absence (if provided).

b.1. Employees who report sick

A telephone number will be provided for employees to call if they feel ill and/or need to report sick. The following protocol will be followed:

PROTOCOL FOR EMPLOYEES WHO REPORT ILL

1. Speak with the individual by phone.
2. Check if the employee has any flu-like symptoms.

   - Fever (higher than 100.4°F / 38°C)
   - Chills
   - Muscle aches
   - Headache
   - Fatigue (extreme tiredness)
   - Cough
   - Sore throat
   - Loss of smell and/or taste

   If the employee does not have any of these symptoms and has not been in contact with someone with the virus, they are unlikely to have the virus and should be reassured and advised to call again later or to seek medical attention if they are still concerned. If the employee has flu-like symptoms, they should be treated as a "suspect case."
3. If the employee is at work, provide them with a face mask and instruct them to put the mask on immediately. (This is to help protect other staff.)
4. Instruct the employee to leave work.
5. Advise the employee on how long to stay away from work.
6. Have the employee's work station cleaned and disinfected.
7. Advise supervisor of employee absence.
8. Communicate with the employee during his/her absence from work via telephone or e-mail.
9. Encourage employees to return to work once they have recovered and the isolation period has ended.

c. Re-assign staff

If staff shortages impede the ability to perform essential operations, cross-trained employees from other operational areas, may have added responsibility. Supervisors will be responsible for collecting information on workplace needs and assigning staff to priority activities.

Approved: March/17/2022 Revision: ____/____/____

VIII INFORMATION AND TECHNOLOGY SYSTEMS

A. Mission

During a pandemic, it will be critical that information and technology systems are in working order and able to support standard and/or new communication needs.

B. Implementation

a. Information Technology (IT) Systems

Telecommuting. Some employees may be asked to work from home and telecommute during a pandemic. IT systems will be monitored to ensure that staff can access and share files and communicate through e-mail.

Websites. The NPEC website and intranet may need to be updated with up-to-date information for the employees, members, vendors, and the public. This information will be provided by the IT Specialist or Communications Specialist.

Data Back-up. Routine data backup procedures will be maintained throughout the pandemic.

b. Communication Systems

Teleconferencing. In order to reduce close contact between people, telephone conversations and videoconferencing may be utilized in lieu of meetings. video conference are now a regular occurrence and TEAMS and Zoom work extremely well for this meeting method.

C. Management and Staffing

IT and communication activities will be managed by the IT Specialist and IT consultant.

IX DEMOBILIZATION

A. Mission

Following the pandemic, it will be necessary to demobilize and coordinate a smooth transition from emergency response activities to standard (or modified standard) daily operating procedures and evaluate the response.

B. Implementation

a. Deactivation

NPEC will assess the impact of the pandemic on operations, personnel, members, partners, and vendors. Recovery from the pandemic can begin when it is determined that adequate personnel, supplies, resources, and systems exist to manage all or the majority of standard daily operating activities. The CFO and General Manager must approve deactivation and the transition plan.

b. Transition Plan

If the decision is made to deactivate, a transition timeframe and plan with the following details will be developed:

- Staff assignments (if some staff are still out)
- How and when employees should exit their response positions and resume their routine positions.
- Policy changes
- Modifications that should be made to standard operating practices (e.g., new services to add, continued disease control practices)
- Hours of operation
- Contact information for business and staff
- Method to collect documentation from the response.
- Community recovery needs and ways to provide assistance

c. Notifications

When the CFO and General Manager have approved demobilization of the response, the following audiences will be notified and provided with instructions on how to transition to standard operating activities.

d. Evaluation

Conduct an internal evaluation of NPEC's pandemic response. Gather documentation from the response

and feedback from all stakeholders and incorporate into an after-action report and corrective action plan. Update the Pandemic Continuity Plan and other emergency response plans as appropriate.

APPENDIX

Brainstorming Questions for Developing Pandemic Policies

Employees Who Become Ill

1. The following is guidance that during a pandemic, employees with flu-like symptoms should stay home from work. If the organization chooses to follow this guidance:
    - Will a doctor's note be required? What if that is not feasible?
    - Will employees be required to take sick or vacation days?
    - What if employees have used up all their sick and vacation days?
    - Will sick employees who are required to stay home be compensated if they do not have any sick or vacation time? Will they be dismissed?

2. Will there be a special policy on returning to work after illness with an influenza/Covid-like illness? The San Francisco Department of Public Health may request that individuals with flu-like symptoms stay in home isolation for a certain number of days (e.g. up to 1 or 2 weeks) until they are better and no longer contagious.
    - Some employees may try to hide their symptoms because they do not want to use personal leave or take a leave of absence. How will you encourage people with symptoms to stay home?
    - Some employees may feel well enough to work before the isolation period is over and may not want to use their personal leave, may not have any personal leave, and/or may be concerned about loss of wages.

3. What will be the protocol for employees who become ill at work?

4. If an employee believes he/she was infected while on the job, what Workers' Comp is available? Can papers be processed if it is not possible to get a doctor's note?

Employees Who are Quarantined

15. If employees are quarantined, will they be required to use sick or vacation time during the period they are asked to stay home?
    - What if they do not have any sick or vacation days?
    - Will employees who are quarantined be compensated if they do not have any sick or vacation time?

2. Are there any provisions for employees to work while staying at home (without using personal leave) when they are in quarantine (e.g. telecommuting)? Or when they are recovering from illness?

Employees Who Do Not Report to Work

1. How will you deal with employees who stay home to care for ill family members?
    - Will they be required to take vacation or sick leave?
    - What if they have used up all their vacation and sick leave?

    - Will healthy employees who choose to stay home to care for someone be compensated if they do not have any personal leave time?

16. If public or private schools, adult daycare centers, or other care organizations are closed and employees must stay home to care for family members, will they be asked to use personal leave time?
    - What if they have none? Will they be compensated? Will they be dismissed?

17. How will you respond to employees who are too afraid to come to work because they think a co-worker or a client will infect them?
    - Will healthy employees who choose to stay home due to safety concerns be compensated if they do not have any sick or vacation time? Will they be dismissed?

18. What if an employee believes they have not been given the proper personal protective equipment (e.g., masks) to keep them from becoming infected and refuses to come to work?

19. What if the stockpile of personal protective equipment runs out? How will you cope with employees who do not want to work without it?

Flexible work

1. Are there policies that allow for flexible worksites (e.g. telecommuting) and flexible work hours (e.g. staggered shifts, extended shifts)?

2. Is there a policy on how "non-essential workers" can be re-assigned for other "essential" duties in other departments?

3. Will policies for "essential workers" differ from those for "non-essential workers"?

4. Will individuals who are more at risk (e.g. immuno-compromised) for severe illness or death from the virus have special assignments in non-direct contact areas that are different from workers who are not considered high risk groups?

Health care at work

1. Will workers have access to medical and mental health service?

ANNEX C – WILDFIRE MITIGATION PLAN

Purpose

- The intent of this plan is to outline the wildfire mitigation efforts of Cooperative related to its overhead electrical distribution lines and associated equipment throughout its service territory.

Plan

- Cooperative operations personnel will monitor weather conditions, county emergency management alerts and applicable state agency advisories regarding drought conditions and Red Flag warnings. Such sources include:

  Texas A&M Forest (www.texaswildfirerisk.com)
  Texas Forest Service (fire index ratings)
  USFS fire danger class
  NWS Red Flag warnings

- When conditions warrant (or when relevant advisories are issued), Cooperative will require a visual inspection of any line in its service territory that has been de-energized by protective relaying prior to re-energizing.

NPEC performs maintenance on transmission, substations and distribution lines

- System hardening using shorter spans, more stringent pole replacement criteria, using permanent squeeze on connectors at all service devices and retirement or disconnection of idle lines is included in the current procedures.
- Distribution poles are inspected using sound & bore technique on a 10-year rotation.
- Transmission poles are inspected, shaved from groundline to 18 inches below surface, treated and wrapped every 10 years.
- Line maintenance is performed based on contractor visual pole inspections and employee line patrols.
- Line conductor has been changed when found to be brittle and breaking often.
- Tree pruning performed annually on rotational basis. Limbs and leaves found in proximity of conductor are pruned as soon as possible.
- Cooperative exploring use of fire retardant fabrics and chemicals.

ANNEX D – HURRICANES

Not applicable. Cooperative service territory is not located near or within a hurricane evacuation zone, as defined by the Texas Division of Emergency Management.

ANNEX E – CYBERSECURITY
Incident Reporting and Response Plan

1 PURPOSE

The purpose of this Incident Reporting and Response Plan is to provide a process for North Plains Electric Cooperative's (NPEC) formal, focused, and coordinated approach to responding to security events categorized as either cyber security or physical security incidents.
This Incident Reporting and Response Plan ensures that incidents are responded to in a systematic approach that is consistent with NPEC's overall objectives and strategies. The plan ensures communication efforts to appropriate federal agencies, law enforcement agencies, members, and the media are defined, focused, and controlled. The plan will also ensure consistent incident handling and response and provides for future development and refinement of security controls.

2 SCOPE

The Incident Reporting and Response Plan (IRRP) is applicable to all personnel who have been identified to have direct or indirect assigned duties for the cooperative. North Plains Electric Cooperative, Inc. maintains physical and cyber security best practices internally. These best practices are based on the NIST Cybersecurity Framework.

3 GOALS

NPEC works to promote resilience and enhance cyber security capabilities and works to convey current information on emerging cyber threats and initiatives, including critical infrastructure protection efforts, and realistic practices for improving operational resilience. The information technology specialist (Incident Response Manager) will keep cooperative members and staff informed while maintaining a working partnership among the various cooperative functional groups on matters of cyber security.
Short Term Goals:

- Identify gaps in cyber management practices and recommend process improvements.
- Reinforce cyber security best practices and examine resilience concepts and objectives.
- Discuss and practice processes to maintain and repeatedly carry out protection and sustainment activities for critical assets and services.
- Share information with GSEC functional groups related to cyber security policies, initiatives, and capabilities.
- Leverage Security Information and Event Management (SIEM) to increase incident detection time.

Long Term Goals:

- Address gaps in cyber management practices and implement process improvements.
- Document a process to maintain and repeatedly carry out protection and sustainment activities for critical assets and services.
- Enhance cyber incident response and business continuity capabilities.
- Increase the cybersecurity maturity and resilience of the cooperative and its employees.

4 ROLES AND RESPONSIBILITIES

This Incident Reporting and Response Plan must be followed by all directors, personnel,

including all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of NPEC.
Below are details about the roles and responsibilities of each member of NPEC to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.
Appendix A lists the name of the person who currently holds each role/position and it lists the below responsibilities again.

4.1 Incident Response Manager

The Incident Response Manager (IRM) is responsible for:

- Making sure that the Security Incident Reporting and Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Reporting and Response Plan is **current, reviewed and tested at least once each year.**
- Making sure that **staff with Security Incident Reporting Response Plan responsibilities are properly trained at least once each year.**
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Reporting and Response Plan when needed.
- Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.
- Devise and delegate ad hoc roles as required by the incident.
- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead (if applicable) of an incident when they receive a security incident report from staff.
- Investigating and documenting each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.

4.2 Communications Manager

The Communications Manager is responsible for:

- Writing and sending internal and external communications about the incident.
- Updates business continuity or incident status to the public/media when authorized.
- Collect and compile member responses or concerns from the customer support lead.
- Follow up with members concerns on an as needed basis when authorized by the general manager.

4.3 Customer Support Lead

The customer support lead is responsible for:

- Taking and passing on, to the communications lead, concerns from phone calls and emails from members.
- Answering questions with authorized statements as dictated by the general manager.
- Taking and passing on, to the IRM, member-sourced details concerning the incident when reported through a CSR desk.

4.4 Subject Matter Expert

The Subject Matter Expert is responsible for:

- Responding to the IRM with answers to technical questions.
- Suggesting and implementing fixes
- Providing context and updates to the IRM.
- Contacting additional subject matter experts as needed and authorized by the IRM.
- Aiding the root cause analyst with the aftermath analysis and reporting.

4.5 Social Media Lead

The Social Media Lead is responsible for:

- Communicating about the incident on social media channels as directed by the general manager.
- Sharing real-time member feedback with the general manager.

4.6 Scribe

The Scribe is responsible for:

- Recording key information about the incident and its response effort.
    - Maintain a detailed log with times, dates, names, and actions taken. This log will be in chronological order.

4.7 Legal Liaison

The Legal Liaison is responsible for:

- Relaying the scope of the incident to the cooperative's legal team when necessary.
- Gather any reports, logs, and evidence from the IRM as requested by the cooperatives legal team.
- Gather any invoices, reports, logs, and evidence from the IRM to file claims for insurance as needed.

4.8 Root Cause Analyst

The Root Cause Analyst is responsible for:

- Going beyond the incident's resolution to identify the root cause.
- Identifying and changes that need to be made to avoid the same issue in the future
- Coordinating, running, and recording an incident post-mortem.
- Logging and tracking remediation efforts.

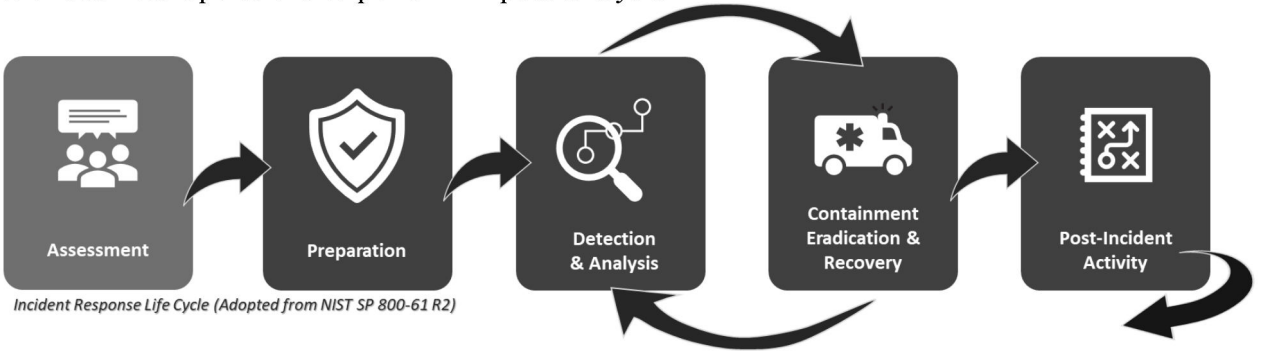
4.9 All Staff Members

All Staff Members are responsible for:

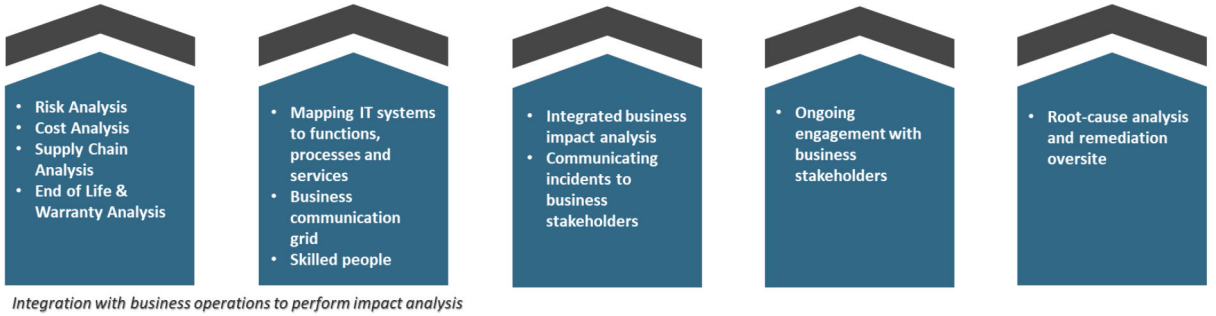
- Making sure they understand how to identify and report a suspected or actual security incident.
- Follow any and all instructions given by any member of the Security Incident Response Team (SIRT) as it pertains to the incident.

5 INCIDENT RESPONSE LIFE CYCLE

This Incident Response Plan is designed to provide a cooperative-wide, systematic business approach to the Incident Response Life Cycle. The Incident Response Life Cycle is paralleled with business operations to perform impact analysis.



Incident Response Life Cycle (Adopted from NIST SP 800-61 R2)



Integration with business operations to perform impact analysis

5.1 Life Cycle Objectives and Processes

5.1.1 Assessment

Establish an approach to analyze business impact and risk. Perform a risk analysis cooperative wide and understand what assets and resources must be protected. Determine operational and financial risks that could impact business operations in the event of a security incident. Regularly review supply chain risk and vulnerability management assessments.

5.1.2 Preparation

Establish an approach to incident handling that includes development of policy and procedures. Review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Security Incident Response Team (SIRT).

5.1.3 Detection and Analysis

Analyze detection devices and reports from people to identify and classify the activity and begin handling the evidence. Monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

5.1.4 Containment

Ensure the impact of the incident does not increase. Perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.

5.1.5 Eradication

Determine the cause and remove it. Remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

5.1.6 Recovery

Restore the system to its original state and validate the clean system. bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.

5.1.7 Post-Incident Activity

Develop follow-up reports, identify lessons learned, and update procedures as necessary. No later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved. In some instances, documentation may be needed for compliance requirements.

5.2 Integration of Business Operations

Develop a risk register which includes the systems and processes necessary to continue business operations and the impacts of each in the event systems are not available. The risk register should also include a list of contacts. The integration of business operations will assist incident handlers and stakeholders with identifying potential risks and associated services along the incident response life cycle. The risk register and contact lists should be kept as a hard copy for reference when systems are not available.

6 INCIDENT SCORING AND IMPACT RATING

The cooperative uses a weighted arithmetic mean to produce a score from zero to 10. This score drives the incident triage and escalation processes and assists in determining the

prioritization of limited incident response resources and the necessary level of support for each incident.

(Current Functional Impact * 40%) + (Potential Functional Impact * 25%) + (Informational Impact * 10%) + (System Criticality *20%) + (Recoverability Timeframe * 5%) = The Incident Score

The five factors are assigned values between 0 and 10 based on value assigned the individual severity rating for each of the factors as described in this plan using the formula above.

The purpose of weighting the factors is to provide a repeatable formula that is heavily biased by the actual impact of the incident but also considers potential impacts to the cooperative if the incident were not contained. Guide appropriate actions with sufficient urgency to prevent a minor or moderate incident from escalating into an emergency.

7 **Incident Categorization**

7.1 CAT 1 UNAUTHORIZED ACCESS

Physical

2. Could the incident impact the reliability of the bulk power system?
3. Was there intentional damage to security systems that protect the physical perimeter.
4. Was sensitive information lost or removed without authorization. Was social engineering involved?

Cyber

2. Could the incident impact the cooperative? Was social engineering involved? Was sensitive information copied, transmitted, viewed, stolen or used by an unauthorized individual?
3. Was this an attempt to compromise the cooperative either electronically or physically? (*report within 1 hour*)

7.2 CAT 2 DENIAL OF SERVICE

1. Was malicious software or data modification discovered on a cyber asset or assets that may impact the reliability of the system or greater bulk power system?
2. Was social engineering involved?
3. If yes to any of these questions report to E-ISAC within the listed timeframe

7.3 CAT 3 MALICIOUS CODE

2. Was malicious software or data modification discovered on a cyber asset or assets that may impact the reliability of the cooperative?
3. Was social engineering involved?

7.4 CAT 4 IMPROPER USAGE

2. Was social engineering involved?
3. Did an unauthorized employee access confidential or restricted resources?

7.5 CAT 5 SCANS/PROBES/ATTEMPTED ACCESS/SURVEILLANCE/THREATS

Physical

2. Was this an attempt to compromise the cooperative either electronically or physically?
3. Was suspicious photo taking observed?
4. Were suspicious surveillance activities observed?
5. Was a suspicious fly over observed?
6. Was a threat communicated where the threatened action has the potential to damage or compromise facility or personnel?
7. Were explosives discovered at or near a facility?
8. Were there suspected or actual attacks against generation, transmission, or company-owned or operated communication facilities, cyber assets, or personnel?

7.6 CAT 6 INVESTIGATION

2. Could the incident impact the reliability of the cooperative?
3. Is there targeted, focused, or repetitive attempted access to cyber assets (such as critical cyber assets) whose impairment could impact bulk power system reliability?
4. Was social engineering involved?
5. Was a threat communicated where the threatened action has the potential to damage or compromise facility or personnel?
6. Was this an attempt to compromise the system or greater bulk power system either electronically or physically?

8 INCIDENT REPORTING GUIDELINES

8.1 Reporting Forms (Internal)

Appendix D for the NPEC's Reporting form

- This form will be filled out and filed for every cyber security incident.

8.2 Reporting Agency Forms (External)

8.2.1 Department of Energy (DoE)

Required Respondents (taken from the DoE website)

Electric utilities that operate as Control Area Operators and/or Reliability Authorities as well as other electric utilities, as appropriate, are required to file the form. The form is a mandatory filing whenever an electrical incident or disturbance is sufficiently large enough to cross the reporting thresholds. Reporting coverage for the Form DOE-417 includes all 50 States, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and the U.S. Trust Territories.

Electric Disturbance Events (DOE-417)

Online Form: https://www.oe.netl.doe.gov/OE417/

Downloadable PDF Form: https://www.oe.netl.doe.gov/docs/OE417_Form_05312024.pdf

Offline Reporting: If you are unable to submit online or by fax, forms may be e-mailed to doehqeoc@hq.doe.gov, or call and report the information to the following telephone number:

(202) 586-8100.

8.2.2 Electricity Information Sharing and Analysis Center (E-ISAC)

The Electricity Information Sharing and Analysis Center (E-ISAC) provides cooperative an option to add a physical or cyber bulletin posting for information sharing purposes. An account must be created and approved for sharing information. Information shared may include details about a security incident attack and the Indicators of Compromise (IoC) to assist other cooperatives with mitigation of similar attacks.

E-ISAC website login: https://www.eisac.com

8.3 What to Include in your Incident Report

The following format is a guide. While internal reporting must be complete, some external reports may need to omit certain pieces of information to retain confidentiality. External reporting should be reviewed by managers, senior leadership, and sometimes legal counsel. The following must be determined for each incident:

- Incident Type
- Names of system(s) involved (spell out each acronym used at its first use
- If the system has failed over to an available backup system
- Categorization of system(s) involved
- Type of data involved (Confidential or Restricted Information)
- Functional use of systems involved
- Identified or suspected cause of incident
- Identified or suspected impact of incident
- What dangers or effects on the facility or facility personnel safety may be caused by the event?
- If the incident has the potential to spread across other networks or even outside to partners or customers
- Investigation, containment, and remediation steps taken
- Incident detection/identification method
- Parties involved (include descriptive titles and names if required for remediation)
- Date and timeframe of occurrence(s)
- If the reported incident is real or a false positive
- What stage the incident is in—beginning, in process, or has already occurred
- What organizations will be affected and who should be part of the response.

If applicable, provide:

- Host-based indicators, Network indicators, and Email characteristics
- Security controls that blocked and/or detected the activity
- Date/time the activity was blocked and/or detected
- Host operating systems
- Name of malicious logic
- How did the exploit occur, and can it happen again? In what timeframe?
- What type of attacker tools if any were placed onto the system?
- Actions taken by affected system

- Network activity observed (including IPs and URLs connections made or attempted, associated ports)
- Type of unauthorized access attempted or obtained (including capabilities associated with that type of access)
- Attack vector

For incidents involving privacy or PII, also include:

- The number of individuals
- The number of records
- The number of data points or source of compromise

9 COMMUNICATIONS

9.1 Internal Reporting Chain

The cooperative's Internal Reporting Chain during an incident is based on the severity rating. If a member of the reporting chain is unavailable, their designated delegate will be contacted. If both the primary and their delegate cannot be contacted, the next person in the chain will be notified. All members of the chain must select a delegate.

Severity	Reporting Guidance
Insignificant	Reporting is not necessary
Low	The Incident Response Manager will notify any department head affected by the incident.
Medium	The Incident Response Manager will notify the General Manager.
High	The Incident Response Manager will notify the General Manager who then decides whether or not to notify the Board of Directors. The IRM also informs other departments that have a need to know. At this severity level, the IRM will establish a Virtual channel for incident handling activities understanding that Confidential or Restricted Information is not stored or shared via the channel.
Extreme	The Incident Response Manager will notify the General Manager who then will notify the Board of Directors. The IRM also informs other departments that have a need to know. At this severity level, the IRM will establish a Virtual channel for incident handling activities understanding that Confidential or Restricted Information is not stored or shared via the channel.

9.2 External Reporting Chain

Name	Email	Phone
DoE	https://www.oe.netl.doe.gov/OE417/ FAX Form DOE-417 to (202) 586-8485	(202) 586-8100

	Email Form DOE-417 to doehqeoc@hq.doe.gov	
E-ISAC	operations@eisac.com	404-446-9780 #2
NCCIC (includes ICS-CERT and US-CERT)	central@cisa.gov Online form: https://us-cert.cisa.gov/forms/report	1-888-282-0870
ICS-CERT	soc@us-cert.gov online form: https://us-cert.cisa.gov/forms/report	1-888-282-0870
US-CERT	soc@us-cert.gov online form: https://us-cert.cisa.gov/forms/report	1-888-282-0870
Department of Homeland Security, Cyber Security Regional Contact	Chad Adams CISARegion6@hq.dhs.gov	1-888-282-0870

9.3 Key Vendor Contacts

- Milsoft: 1-800-344-5647
- Partner: 706-354-1833
- NISC: 7-866-999-6472
- Aclara: 1-800-892-9008
- Survalent: 1-855-402-2600
- CRC: 1-800-892-1578
- GSEC SOC: 806-420-5345 (GSEC Cyber Security Operations Center)
- Wayne Brockwell: 806-681-2400

9.4 Media Communications

Only employees authorized by the General Manager and his or her designee are permitted to speak to, give statements to, or participate in interviews with members of the news media as an official representative of the Cooperative.

By default, employees are not authorized by the General Manager to communicate with the news media as an official representative of the Cooperative and should refer any news media enquiries to an authorized employee.

9.5 Impaired Communications

The cooperative will identify another means to establish communications in the event that

communications are disrupted. The cooperative will utilize cell phones, networks, the internet, etc.

10 FORENSICS

The cooperative, when deemed necessary to investigate possible criminal activity, will provide forensic services and it is not intended for law enforcement or to be court admissible. If it is determined that forensics be conducted, the cooperative shall require a dedicated evidence storage and analysis facilities with physical access limited to authorized forensics personnel, mobile evidence gathering tools required to establish chain of custody; to collect and label evidence at incident sites; and to securely package and transport the collected evidence. The cooperative shall: Develop, maintain, and follow a Standard Operating Procedure (SOP) for computer forensics collection and analysis follow the cooperative disclosure and privacy guidance and maintain a chain of custody of evidence. In the event that law enforcement services are required, the Incident Response Lead makes initial contact with senior leadership, legal and law enforcement organizations to establish evidentiary chain of custody. The Incident Response Lead will coordinate with appropriate law enforcement organizations. If necessary, the cooperative or the Incident Response Lead may package and ship equipment to a designated computer forensic processing facility. If it is determined that the source of the suspected criminal activity is external to the cooperative, the appropriate law enforcement organization will be notified immediately by the Incident Response Lead, or if necessary, by other organizations who will inform the cooperative at the earliest time possible.

11 TESTING AND PLAN CHANGES

The Incident Reporting and Response Plan will be reviewed and tested at least once every 24 calendar months for updates and improvements. NPEC reserves the right to modify or amend this policy at any time, with or without prior notice. No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, lessons learned, or the absence of any lessons learned will be documented. The Incident Reporting and Response Plan will be updated and distributed to those individuals with a documented role and responsibility in the IRRP via email based on any documented lessons learned associated with the plan. If roles and responsibilities change or if there is a technology change that impacts NPEC's ability to execute the plan, the Incident Reporting and Response Plan will be updated and each person with a defined role and responsibility in the IRRP will be notified via email.

12 TRAINING REQUIREMENTS FOR INCIDENT RESPONSE TEAMS

Training requirements for the incident handlers includes:

- Intrusion Detection System training
- Security Information and Event Management training (if applicable)
- Ticketing/Reporting system
- Additional security monitoring and reporting tools as necessary
- Regular review of the Incident Response and Reporting Plan
- Cybersecurity Framework for all areas of the Cooperative
- Communications applications (Teams, etc.)
- Practice with locating and filling out External Agency reports (DoE, E-ISAC, etc.)

13 ROAD MAP FOR MATURING THE INCIDENT RESPONSE CAPABILITY

The cooperative will follow the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), to define their roadmap for maturity in Incident Reporting and Response Planning.

Appendix A – ASSIGNED ROLES

Role	Name(s)
Incident Response Manager/Root Cause Analyst	IT Specialist (Rusty Pickett)
Communications Manager/Social Media Lead	Member Services (Bianca Peregrino)
Customer Support Lead	CSR (Ivette Cortez)
Subject Matter Expert	IT Consultant (Wayne Brockwell)
Scribe	Work Order Clerk (Tiffany Constancio)
Legal Liaison Lead	CFO (Jennifer Roberts)
All Staff	Every Employee of NPEC

4.1 Incident Response Manager

The Incident Response Manager (IRM) is responsible for:

- Making sure that the Security Incident Reporting and Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Reporting and Response Plan is current, reviewed and tested at least once each year.
- Making sure that staff with Security Incident Reporting Response Plan responsibilities are properly trained at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Reporting and Response Plan when needed.
- Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.
- Devise and delegate ad hoc roles as required by the incident.
- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating and documenting each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.

- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.

4.2 Communications Manager

The Communications Manager is responsible for:

- Writing and sending internal and external communications about the incident.
- Updates business continuity or incident status to public/media when authorized.
- Collect and compile member responses or concerns from the customer support lead.
- Follow up with members concerns on an as needed basis when authorized by the general manager.

4.3 Customer Support Lead

The customer support lead is responsible for:

- Taking and passing on, to the communications lead, concerns from phone calls and emails from members.
- Answering questions with authorized statements as dictated by the general manager.
- Taking and passing on, to the IRM, member-sourced details concerning the incident when reported through the CSR desk.

4.4 Subject Matter Expert

The Subject Matter Expert is responsible for:

- Responding to the IRM with answers to technical questions.
- Suggesting and implementing fixes
- Providing context and updates to the IRM.
- Contacting additional subject matter experts as needed and authorized by the IRM.
- Aiding the root cause analyst with the aftermath analysis and reporting.

4.5 Social Media Lead

The Social Media Lead is responsible for:

- Communicating about the incident on social media channels as directed by the general manager.
- Sharing real-time member feedback with the general manager.

4.6 Scribe

The Scribe is responsible for:

- Recording key information about the incident and its response effort.
    - Maintain a detailed log with times, dates, names, and actions taken. This log will be in chronological order.

4.7 Legal Liaison

The Legal Liaison is responsible for:

- Relaying the scope of the incident to the cooperative's legal team when necessary.
- Gather any reports, logs, and evidence from the IRM as requested by the cooperatives legal team.
- Gather any invoices, reports, logs, and evidence from the IRM to file claims for insurance as needed.

4.8 Root Cause Analyst

The Root Cause Analyst is responsible for:

- Going beyond the incident's resolution to identify the root cause.
- Identifying and changes that need to be made to avoid the same issue in the future
- Coordinating, running, and recording an incident post-mortem.
- Logging and tracking remediation efforts.

4.9 All Staff Members

All Staff Members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Follow any and all instructions given by any member of the Security Incident Response Team (SIRT) as it pertains to the incident.

Response

Responding to security incidents can take several forms. Incident response actions may include triaging alerts from your endpoint security tools to determine which threats are real and/or the priority in which to address security incidents. Incident response activities can also include containing and neutralizing the threat(s)—isolating, shutting down, or otherwise "disconnecting" infected systems from your network to prevent the spread of the cyber attack. Additionally, incident response operations include eliminating the threat (malicious files, hidden backdoors, and artifacts) which led to the security incident.

- Immediately contain systems, networks, data stores and devices to minimize the breadth of the incident and isolate it from causing wide-spread damage. **(Incident Response Manager)**
- Determine if any sensitive data has been stolen or corrupted and, if so, what the potential risk might be to your business. **(Incident Response Manager)**
- Eradicate infected files and, if necessary, replace hardware. **(Incident Response Manager)**
- Keep a comprehensive log of the incident and response, including the time, data, location and extent of damage from the attack. Was it internal, external, a system alert, or one of the methods described previously? Who discovered it, and how was the incident reported? List all the sources and times that the incident has passed through. At which stage did the security team get involved? **(Scribe)**
- Preserve all the artifacts and details of the breach for further analysis of origin, impact, and intentions. **(Incident Response Manager)**
- Prepare and release public statements as soon as possible, describe as accurately as possible the nature of the breach, root causes, the extent of the attack, steps toward remediation, and an outline of future updates. **(Communications Manager)**
- Update any firewalls and network security to capture evidence that can be used later for forensics. **(Incident Response Manager)**
- Engage the legal team and examine compliance and risks to see if the incident impacts any regulations. **(Legal Liaison Lead)**
- Contact law enforcement if applicable since the incident may also impact other organizations. Additional intelligence on the incident may help eradicate, identify the scope, or assist with attribution. **(Incident Response Manager)**

Post-incident activities (Recovery and Follow-up actions) include eradication of the security risk, reviewing and reporting on what happened, updating your threat intelligence with new information about what's good and what's bad, updating your IR plan with lessons learned from the security incident, and certifying then re-certifying your environment is in fact clear of the threat(s) via a post-incident cybersecurity compromise assessment or security and IT risk assessment.

Recovery

(Incident Response Manager)

- Eradicate the security risk to ensure the attacker cannot regain access. This includes patching systems, closing network access, and resetting passwords of compromised accounts.
- During the eradication step, create a root cause identification to help determine the attack path used so that security controls can be improved to prevent similar attacks in the future.
- Perform an enterprise-wide vulnerability analysis to determine whether any other vulnerabilities may exist.
- Restore the systems to pre-incident state. Check for data loss and verify that systems integrity, availability, and confidentiality has been regained and that the business is back to normal operations.
- Continue to gather logs, memory dumps, audits, network traffic statistics and disk images. Without proper evidence gathering, digital forensics is limited so a follow-up investigation will not occur.

Follow-Up

(Incident Response Manager)

- Complete an incident response report and include all areas of the business that were affected by the incident.
- Determine whether management was satisfied with the response and whether the organization needs to invest further in people, training or technology to help improve its security posture.
- Share lessons learned. What went well, what didn't and how can procedures be improved in the future?
- Review, test and update the cybersecurity incident response plan on a regular basis, perhaps annually if possible.
- Conduct a compromise assessment or other security scans on a regular basis to ensure the health of systems, networks and devices.
- Update incident response plans after a department restructure or other major transition.
- Keep all stakeholders informed about the latest trends and new types of data breaches that are happening. Promote the message that "security is everyone's job."

Ransomware Attack Response Checklist

Step 1: Disconnect Everything

- ☐ Unplug computer from network
- ☐ Turn off any wireless functionality; Wi-Fi, Bluetooth, NFC

Step 2: Determine the Scope of the Infection, Check the Following for Signs of Encryption

- ☐ Mapped or shared drives
- ☐ Mapped or shared folders from other computers
- ☐ Network storage devices of any kind
- ☐ External Hard Drives
- ☐ USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- ☐ Cloud-based storage: DropBox, Google Drive, OneDrive etc.

Step 3: Determine Ransomware Strain

- ☐ What strain/type of ransomware? For example: CyrptoWall, Teslacrypt etc.

Step 4: Determine Response

Ransomware response should be determined by a response team, senior leadership, and legal counsel at a minimum. In many cases, law enforcement may provide addition insight or suggestions. You may also want to call in a ransomware response team to assist with restoration.

Response 1: Restore your Files from Backup

1. Locate your backups
   a. Ensure all files you need are there
   b. Verify integrity of backups (i.e., media not reading or corrupted files)
   c. Check for Shadow Copies if possible (may not be an option on newer ransomware)
   d. Check for any previous versions of files that may be restored on cloud storage e.g., DropBox, GoogleDrive, OneDrive
2. Remove the ransomware from your infected system
3. Restore your files from backups
4. Determine infection vector and handle

Response 2: Try to Decrypt

1. Determine strain and version of the ransomware if possible
2. Locate a decryptor, there may not be one for newer strains; If successful, continue to next steps…
3. Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)
4. Decrypt files
5. Determine the infection vector and handle

Response 3: Do Nothing (Lose Files)

1. Remove the ransomware

2. Backup your encrypted files for possible future decryption (optional)

Response 4: Negotiate and/or Pay the Ransom

1. If possible, you may attempt to negotiate a lower ransom and/or longer payment period
2. Determine acceptable payment methods for the strain of ransomware: Bitcoin, Cash Card etc.
3. Obtain payment, likely Bitcoin:
   a. Locate an exchange you wish to purchase a Bitcoin through (time is of the essence)
   b. Set up account/wallet and purchase the Bitcoin
4. Re-connect your encrypted computer to the internet
5. Install the TOR browser (optional)
6. Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been setup for this specific ransom case
7. Pay the ransom: Transfer the Bitcoin to the ransom wallet
8. Ensure all devices that have encrypted files are connected to your computer
9. File decryption should begin within 24 hours, but often within just a few hours
10. Determine infection vector and handle

Step 5: Protecting yourself in the Future

- ☐ Implement Ransomware Prevention Checklist to prevent future attacks

Ransomware Prevention Checklist

First Line of Defense: End Users

- ☐ Implement effective security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.
- ☐ Conduct simulated phishing attacks to inoculate users against current threats.
- ☐ Require multi-factor authentication for all end user accounts, regular and administrative

Second line of Defense: Software

- ☐ Ensure you have and are using a firewall.
- ☐ Implement antispam and/or anti-phishing. This can be done with software or through dedicated hardware.
- ☐ Ensure everyone in your organization is using top notch up-to-date antivirus software, or more advanced endpoint protection products like whitelisting and/or real-time executable blocking.
- ☐ Implement software restriction policies on your network to prevent unauthorized applications from running. (optional)
- ☐ Implement a highly disciplined patch procedure that updates any and all applications that have vulnerabilities.

Third Line of Defense: Backups

- ☐ Implement a backup solution: Software based, hardware based, or both.
- ☐ Ensure all possible data you need to access or save is backed up, including mobile/USB storage.
- ☐ Ensure your data is safe, redundant and easily accessible once backed up.

- ☐ Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups.

NPEC Cyber Security Incident Response Report Form

INCIDENT IDENTIFICATION INFORMATION	
Date and Time of Notification:	
Incident Detector's Information:	
Name:	Date and Time Detected:
Title:	Location:
Phone/Contact Info:	System or Application:

INCIDENT SUMMARY

Type of Incident Detected:

☐ Denial of Service ☐ Malicious Code ☐ Unauthorized Use
☐ Unauthorized Access ☐ Unplanned Downtime ☐ Other

Description of Incident:

Names and Contact Information of Others Involved:

INCIDENT NOTIFICATION – OTHERS

☐ Cooperative Leadership ☐ System or Application Owner ☐ System or Application Vendor
☐ Security Incident Response Team ☐ Public/Media ☐ Legal Counsel
☐ Administration ☐ Social Media
☐ Other:

ACTIONS

Identification Measures (Incident Verified, Assessed, Options Evaluated):

Containment Measures:

Evidence Collected (Systems Logs, etc.):

Eradication Measures:

Recovery Measures:

Other Mitigation Actions:

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.

ANNEX F – PHYSICAL SECURITY INCIDENT

1. PURPOSE

This document provides Cooperative personnel with the tools necessary to understand and identify a possible or actual local physical security event at Cooperative's facilities and immediately report suspicious activity or actual malicious destruction of any of their facilities. It addresses how personnel interact with each other and other entities to provide timely information and situational awareness.

In order to recognize a physical security event, one must understand what a physical security event is. For this procedure, the following definitions will be utilized:

Sabotage is defined as a deliberate action designed to disrupt or destroy any facilities, including, but not limited to, elements of the Bulk Electric System (BES). It can also be a deliberate action at weakening or destroying infrastructure through subversion.

Vandalism is defined as the malicious and deliberate defacement or destruction of property.

Criminal Mischief is defined as any damage, defacing, alteration, or destruction of tangible property with criminal intent.

Vandalism and Criminal Mischief can, and often do, go hand in hand with each other.

2. DEFINITION

This document provides Cooperative personnel with the tools necessary to understand and identify a possible or actual local physical security event at Cooperative's facilities and immediately report suspicious activity or actual malicious destruction of any of their facilities. It addresses how personnel interact with each other and other entities to provide timely information and situational awareness.

3. RECOGNITION

All Cooperative personnel are responsible for following the reporting procedures in this section for any event that involves:

- Damage or destruction of facilities that results from actual or suspected intentional human action.
- Physical threats to Cooperative's personnel.
- Physical threats to a facility that have the potential to degrade the normal operation.
- Suspicious device or activity at a facility.
- Theft that has the potential to degrade operation

Determining what is truly Sabotage from Vandalism or Criminal Mischief can be a daunting task. The key to determining physical security is intent. If the intent is to disrupt or disable the BES, then the event would be considered Sabotage. Most events experienced by Cooperative are simply mischievous people or those with criminal intent. Below is a list of events that may possibly occur on Cooperative's system and the determination of the event status:

Sabotage Event	Criminal Mischief/Vandalism Event
Unbolting transmission tower legs (deliberate	*A farmer who cuts a pole down due to*

act to cause harm to the electric system and electric operations)	*blocking access to his fields (intent is access property not disrupt electric operations)*
Coordinated destruction of wooden structures (deliberate and coordinated attack to cause harm to the electric system and electric operations)	*Entry into a substation to steal copper conductor (intent is theft by taking, not disruption of electric operations)*
Shooting transmission facilities intending to cause destruction and electrical disturbances (typically multiple insulator strings along a stretch of line)	*Isolated shooting of a transmission line insulator (intent is criminal (destruction of property), not disruption of electric operations)*
Breaking and entering into a substation to destroy equipment (intent is to disrupt electric operations and cause harm to the BES and electric operations)	*Motor vehicle accident (consequence of action may be harm to the BES or electric operations; however, the intent was not to cause disruption)*
Driving a motor vehicle through a substation fence (substations are typically away from road rights of ways indicating an intentional action)	*Graffiti on equipment (while this indicates entry into station, the intent was not disruption and no physical damage was done to facilities)*
Deliberate cyber attack or cyber intrusion with intent to disrupt or take down SCADA network that could have a material impact on the BES	*Deliberate cyber intrusion with the intent of stealing personally identifiable information for the purposes of stealing Cooperative's personnel' identities for monetary gain*

Suspicious Activity, Objects, or Persons	
Threats to disrupt or damage Cooperative's electric system or other infrastructure	*Threats to injure Cooperative's personnel*
Intentional injury to Cooperative's personnel	*Unauthorized attempts to access Cooperative's facilities, such as a substation*
Unauthorized individuals present on Cooperative's property who exhibit suspicious behavior	*Unauthorized photography of Cooperative's facilities*
Unauthorized access or attempted access to the Cooperative's computer systems through physical or cyber intrusion	*Unknown persons loitering in the vicinity of Cooperative's facilities for extended periods of time*
Individuals, without proper identification or escort, and /or having unusual dress, appearance, or accents	*Unknown person calling Cooperative's facilities to ascertain security, personnel or procedural information*
Unknown persons who attempt to gain information about Cooperative's facilities by walking up to personnel or their families and engaging them in a conversation	*Theft of facility vehicles, personnel identification, uniforms or operating procedures*

4. REPORTING POSSIBLE OR ACTUAL PHYSICAL SECURITY INCIDENT (COOPERATIVE FIRST RESPONDER)

The Cooperative employee who discovers a possible or actual physical security event (First Responder) should take the following actions upon discovery if the Cooperative employee's safety is not at risk:

Actions Upon Discovery of a Possible or Actual Physical security Event (First Responder)
1. Make sure the scene is safe for you and the public. Make the scene safe if possible.
2. Stay calm and quickly report to your Manager.
3. Make a clear and accurate report to your Manager. Provide your name and contact information.
4. Describe the possible or actual physical security act. Be as specific as possible.
5. Remain in contact with your Manager until released. Additional information may be requested.
6. Record any information about your surroundings including vehicles, people, or abnormal odors.
7. Remain available for further questions from law enforcement.

If your personal safety is at risk, retreat to a safe area and contact your Manager as soon as possible. Notify law enforcement and emergency services for response to the scene. Keep the public away from the danger and evacuate area as necessary.

5. REPORTING POSSIBLE OR ACTUAL PHYSICAL SECURITY (MANAGER)

Once a possible or actual physical security event has been reported, the Manager shall inform all operating personnel of the possible or actual event. The Cooperative shall as soon as possible notify their Transmission Operator of the event and details. The Cooperative should provide the following information:

Information to Provide to Transmission Operator (see Appendix B for Physical Security Incident Information Form)
1. Geographic area and county affected/impacted.
2. Date and time incident began.
3. Date and time incident ended.

4. Did the incident originate at your Cooperative?
5. Amount of demand involved (estimated).
6. Number of member-consumers affected.
7. Physical or cyber attack.
8. Equipment involved in the event.
9. Description of events.
10. Station or line identifiers.

6. Roles

Cooperative serve as First Responders for this procedure and must never ignore a suspected or actual act of physical security or suspicious person, object or activity that could threaten the Cooperative's facilities, personnel or operations. In addition, the Cooperative provides key information to their Transmission Operator to allow for timely and accurate reporting of possible or confirmed physical security events or subversive activities.

7. Training

Cooperative shall review and perform training on this procedure at least annually.

ATTACHMENT A

Physical Security Incident Information Form

Cooperative: _____ **Facility:** _____

1. Date and time of incident: _____

2. Location of incident (e.g. county, city, line and station identifiers): _____

3. Type of incident (e.g. physical, cyber): _____

4. System parameters before the incident (Voltage, Frequency, Flows, Lines, Substations, etc.)

_____

5. System parameters after the incident: _____

6. Network configuration before the incident _____

7. Relay indications observed and performance of protection: _____

8. Damage to equipment: _____

9. Supplies interrupted and duration, if applicable: _____

10. Amount of electric service lost (demand/member-consumers), if applicable: _____

11. Estimate of time to return to service: _____

12. Cause of incident (if known): _____

13. Any other relevant information including notifications [and remedial action taken]: _

_____

_____

14. Recommendations for future improvement/repeat incident: _____

_____

Time:	
Date:	Signature and Designation of the Distribution Cooperative Person(s) Reporting the Incident

Approved: March/17/2022 Revision: ____/____/____

ANNEX G: REQUIREMENTS FOR TRANSMISSION AND DISTRIBUTION UTILITIES

Not Applicable. Cooperative is not a Transmission and Distribution Utility as defined under 16 TAC §25.5.

ANNEX: H- ADDITIONAL ANNEXES

(INSERT ANY ADDITIONAL ANNEXES IF ANY)

FEMA Enabling Legislation
STAFFORD ACT, Public Law 93-288, known as:
The Robert T. Stafford Disaster Relief and Emergency Assistance Act, Title 42 U.S.C. # 5121, as revised Sept 1, 1999.

The Stafford Act authorizes the President (FEMA per Executive Order 12673) to provide financial and other forms of assistance to State and local governments, certain Private Non-Profit organizations, and individuals following Presidential-declared major disasters and emergencies. **Electric Cooperatives are eligible under the Private Non-profit status.**

APPLICANT ELIGIBILITY
To be eligible for FEMA reimbursement, ALL must be eligible, the applicant, the facility, the work and the cost.

REIMBURSEMENT
FEMA reimbursement is 75% of the eligible work. Additional Presidential Declarations may raise this amount in extensive damage and hardship conditions. **Co-ops should treat all FEMA and State funds as a loan until the Co-op has proven, after the fact, that the money was all properly spent on eligible work. Co-ops MUST properly document all work and expenses.**

LOCAL CONTACT
Texas Emergency Management will assist Co-ops with their FEMA claims. **TEM should be kept appraised of a Co-op's progress, especially when it becomes apparent that the project may over-run either the quantities measured in the PW or the costs.** Cooperatives should cultivate an open and cooperative relationship with TEM. TEM normally sends a liaison reservist to accompany the FEMA Project Officer. Most are knowledgeable and can help the process.