10. Any violation notices issued during the time frame approved by Commissioner's Court should be sent to Corporate Security via fax or email within five days of the invoice date stated on the notice. Corporate Security will then send the notice to HCTRA for dismissal.

Factors CNP Uses to Determine EOP Phases

Factor	Description
Hurricane Risk Indicator (HRI) goes positive for the report location.	A negative HRI for a location denotes no hurricane threat has been identified through the coming week. When StormGeo identifies a location as "Positive" for a hurricane risk, in addition to putting that notice atop the TropicsWatch web page, they will also notify CNP's EOP Coordinator by phone and by email.
Worst Case Scenario (WCS) for 39 mph winds reaching the report location	StormGeo's Worst Case Scenario (WCS) parameter lets CNP know the approximate earliest arrival times of 25, 39, 58, 74, and 100 mph winds at defined report locations if an active storm were to quickly travel straight to that location. CNP's WCS activation parameter will be based on the 39 mph wind. Assumptions: The storm movement is directly toward our location Assumes a forward speed equal to the maximum forecasted forward speed over the time period prior to the storm's ETA at our location Intensity is set to the projected maximum sustained winds possible during the time period from the current position until it reaches our location Wind field size is set to the maximum projected in any one quadrant of the storm prior to reaching our location
The Probability of 58 mph Wind Impacting (PWI) the report location.	StormGeo's "Probability of Wind Impact" displays the probability of a location receiving a certain threshold of wind. Wind probabilities will be calculated for wind speeds of 25 mph, 39 mph, 58 mph, 74 mph and 100 mph. CNP's PWI activation parameter will be based on the 58 mph wind.
The Forecasted Time of Arrival (FTA) of 39 mph winds reaching the report location	As the certainty of impact to the Company's service area becomes definite, the forecast changes from Worst Case Scenario to Forecasted Time of Arrival (FTA). Again, EOP activation parameter will be based on the 39 mph wind.

Factor	Description
Sustained Winds fall below 39 mph	As the storm begins to move out of the Company's service areas, StormGeo will forecast when wind speeds for each report location are scheduled to fall below 39mph.

Activation Phase Descriptions

The following table describes fourteen phase points for which CNP has designated specific storm preparation activity. This table describes the parameters required to determine when each of these phase points has been or will be achieved. These phases are based on When StormGeo identifies a location as "Positive" for a hurricane risk. A notification of this risk will be made by adding a notice atop the TropicsWatch web page and communicating with CNP's EOP Coordinator by phone and by email.

Phase	Description
1 - Hurricane risk indicator is positive	**Notification to executives** The EOP Coordination Team communicates potential storm threat to executives. Keep executives clearly informed of developing storm conditions and obtain concurrence to begin employee communications.
2 - The worst case scenario for 39 mph winds reaching this location is < 120 hours and the probability of 58 mph winds impacting this location is > 8%	**Communication to employees** The Public/Employee Information Officer (P/EIO) sends out company-wide communications to employees to tell them to prepare home and family for a storm, know their EOP assignment, etc. The P/EIO also keeps employees clearly informed of developing storm conditions. **Functional managers verify and report EOP readiness** Make an early ID of shortfalls and take corrective actions as necessary (roster, supplies, personnel, facilities, ice machines, telecommunications, generators, etc.). **Branch directors leaders initiate communication with EOP-assigned employees** Keep EOP assigned employees clearly informed of developing storm conditions and notify them to begin preparations for manning their EOP assignments. Confirm information for EOP team members.

Phase	Description
3 - The worst case scenario for 39 mph winds reaching this location is < 96 hours and the probability of 58 mph winds impacting this location is > 15%	**RTO implements storm updates using email and text messaging systems** RTO commences tracking of storm and periodically communicates position of storm to CNP personnel using the email and text messaging systems. The purpose of this action is to keep CNP personnel updated as to direction/intensity of storm.
4 - The worst case scenario for 39 mph winds reaching this location is < 72 hours and the probability of 58 mph winds impacting this location is > 20%	**Incident Commander declares EOP activation** The Incident Commander makes recommendations for this action based on latest updates from StormGeo. **The Resource Acquisition group contacts Regional Mutual Assistance Groups (RMAG's) as needed to set up mutual assistance conference calls.** CNP is a member of the S.E.E., the Midwest, and the Texas RMAG's. Contact these groups as needed to initiate Mutual Assistance Conference Calls. Following is their contact information: S.E.E. – Contact any S.E.E. staff member at 404-233-1188 and let them know you wish to hold a conference call for storm response. Refer to the S.E.E. Mutual Assistance Procedures and Guidelines, Section 9.3, for additional information. Midwest – CNP may contact EON-US (Shenita Gazaway 502-627-3925 or David Guy 502-627-4104) to request that a Midwest conference call be set up. Texas – CNP may refer to the Texas Mutual Assistance Conference Call Guidelines. CNP may send an e-mail to each member on the roster announcing a conference call, and provide a 1-800 conference call number with password. **Logistics section makes lodging arrangements** This action is taken in preparation to accommodate CNP personnel that are storm riders and first responders that must evacuate according to the Harris County Office of Emergency Management. These activities continue as more zip codes are evacuated. The Lead Hotel Coordinator should book hotel space based as CNP head count determined. **P/EIO implements communications plan/activate storm hotline**

133

Phase	Description
	Finance submits a request for cash to Treasury
	Logistics section secures food beginning 48 hours after the landfall
	Operations section secures enough food to feed personnel at all EOP operating sites until the caterers have had a chance to arrive and set up.
	Operations evacuates service centers in storm surge areas
	Operations will conduct Galveston and Baytown Service Center evacuations in conjunction with evacuation plans for Harris and Galveston counties. Baytown Service Center will evacuate to Humble Service Center. Galveston Service Center will evacuate to South Houston Service Center.
	Logistics tops off CNP fuel tanks and secure additional fuel and fuel tanks
	Logistics coordinates fuel deliveries to top off underground fuel storage tanks and facility backup generator fuel tanks.
	They also secure temporary fuel tanks and fuel products for service centers, offsite parking and staging sites.
	Telecom executes cell relay/DCE extensions to maximum days
	Grid & Market Operations sends communications to Texas market regarding possibility of interruptions regarding meter data
	Operations assesses the operability of production IG devices
	Telecom considers securing satellite telephone rentals
	Telecom Services will evaluate need of rental satellite telephones for the staging site supervisors.
	Telecom considers securing portable voice radio rentals
	Telecom Services will evaluate need of rental of portable voice radios to supplement CNP's normal inventory.
5 - The worst case scenario for 39 mph winds reaching this location is < 66 hours and the probability of 58 mph winds impacting this location is > 25%	**Incident commander conducts conference call** Potential topics to cover: • actual or expected storm category • storm condition • trouble level of the event

134

Phase	Description
	• type of event
	• damage projection
	• time of impact
	• duration of event
	• EOP timeline status
	• plan for recovery
	• level of preparedness
	• communications
	Logistics alerts material and logistics suppliers
	The Logistics sections provide these suppliers with advance notice to begin making their preparations to supply CNP with storm restoration materials. They alert suppliers of the coming need for tents, trash, cars, food, laundry, etc. They also alert materials suppliers for poles, transformers, wire, insulators, hardware etc.
	Logistics begins relocation of storm stock
	The Logistics section delivers the remaining EOP material and bedding to service centers in advance of evacuations.
	Logistics analyzes EOP inventory levels
	In preparation for the Special Material Release presentation to the section chiefs, the Logistics section will prepare to make preliminary recommendation for purchase quantities based on current inventory levels and storm strength projections. Logistics will continually monitor and evaluate material requirement needs for the Special Material Release as the storm approaches in preparation for the final Special Material Release recommendation at 6 hours prior to landfall.
	Logistics alerts staging site owners
	Staging site supervisors make preliminary contact with the staging site owners to notify them of our possible intent to activate our contracts with them.
	Resource Acquisition participates in the RMAG Conference Call
	The Resource Acquisition group participates in a conference call for each RMAG that calls were set up with. The purpose of these calls is to determine the number of first wave line and tree trimming

Phase	Description
	resources that are available from these RMAG's. Mutual Assistance utilities can provide line crews, damage assessors, material handlers, and staging site management teams, along with various other personnel.
6 - The worst case scenario for 39 mph winds reaching this location is < 60 hours and the probability of 58 mph winds impacting this location is > 25%	**Conduct operations conference call** Branch directors, SADs, and service center operations conduct conference call to determine preparation progress. **Section chiefs assess Special Material Release** Purchasing presents results of assessment to section chiefs and recommends Special Material Release quantities, values, and timing. **Section chiefs assess preparation** Section chiefs update command staff in a face-to-face meeting. The main objective is to provide an update on preparation progress.
7 - The worst case scenario for 39 mph winds reaching this location is < 54 hours and the probability of 58 mph winds impacting this location is > 25%	**Activate the Incident Command Center** CNP will: • Ensure all systems and equipment at the Incident Command Center are functioning properly • Obtain supplies as needed; set up rooms as planned • Set up computers, telephones, Satellite TV access • Test communications • Ensure that the Incident Command Center phone number rings at that location. **The Public/Employee Information Officer issues employee communication regarding employee evacuation of storm surge area.** **Resource Acquisition group participates in RMAG Conference Call #2** The purpose of this call is to further refine the available resource numbers. **Test radio communications at Evaluation Centers** Telecom visits each evaluation center and tests its radio for operational performance.
8 - The worst case scenario for 39 mph winds reaching this location is < 48 hours and	**Logistics updates logistics and material suppliers**

136

Phase	Description
the probability of 58 mph winds impacting this location is > 30%	The Logistics section provides these suppliers with updated information to assist them in their preparations to supply CNP storm requirements. **Logistics updates staging site owners** Staging site supervisors make update calls to staging site owners. They verify the availability of facilities previously agreed upon. **Resource Unit pre-positions local tree and line contractors** The Resource Unit allocates all local contractor resources to the service centers in accordance with the plan, to enable contractors to provide immediate response for priority service work. **Fleet Services branch secures rental vehicles** The Fleet Services group within the Fleet Services branch secures rental vehicles to meet EOP storm needs. Based on severity of storm, Fleet will contact potential users of rental vehicles to determine pre- and post-storm needs, and make arrangements to obtain needed vehicles.
9 - The forecasted time of arrival for 39mph winds for this location is < 36 hours and the probability of 58 mph wind impacting this location is > 50%	**Conduct operations conference call** Distribution Operations branch managers, SADs, and service center operations conduct a conference call to determine progress of preparation. **Logistics section activates logistics (suppliers, caterers, etc.)** At the direction of Operations, the Logistics section engages logistics suppliers to execute CNP EOP logistics plan. **Logistics prepares for employee refueling (if necessary)** The Fleet Services group within the Logistics section sets up employees for access to the automated fueling system. Distribute instructions and recording forms in case of fuel system by-pass and temporary fuel tanks. **The PEIO/management communicates with employees regarding EOP show up time** **Logistics activates staging sites as required at the direction of Operations** Logistics begins activating staging sites. They continue to update staging site owners if we will use or not use their facility.

137

Phase	Description
	Section chiefs assess Special Material Release Purchasing presents updated recommendations for the Special Material Release based on evolving storm and material availability data.
10 - The forecasted time of arrival for 39 mph winds for this location is < 30 hours and the probability of 58 mph winds impacting this location is > 60%	Incident Commander and Section chiefs conduct conference call Potential topics to cover: • actual or expected storm category • storm condition • trouble level of the event • type of event • damage projection • time of impact • duration of event • EOP timeline status • plan for recovery • progress of preparedness • communications Operations sends select crews and staff home The Operations section releases crews to prepare their homes for storm. They rotate crews, sending half the first 4 hours and the second half the next 4 hours.
11 - The forecasted time of arrival of 39 mph winds for this location is < 24 hours and the probability of 58 mph winds impacting this location is > 60%	**Operations restricts Galveston and/or Baytown access** Once Harris and Galveston Counties have been evacuated and restrictions put in place by government entities, CNP service area management representing the service areas in the perspective counties identifies and follows the process for re-entering restricted areas. **Resource Acquisition participates in the RMAG Resource Division Conference Call**

Phase	Description
	The call will be necessary if more than one utility is impacted by the Storm event. The impacted utilities will divide the available resources based on the expected outage counts and amount of damage.
	Resource Acquisition initiates efforts to secure additional resources outside of S.E.E., Texas and Midwest RMAGs
	This effort should be initiated if additional resources are still required after exhausting the available resources of the three RMAG's we are members of. The Resource Acquisition group arranges additional conference calls with RMAG's that are more distant from our area but could still provide resources if necessary.
12 - The forecasted time of arrival of 39 mph winds for this location is < 18 hours	**Operations suspends normal operations**
	The Operations section notifies day crews to start when safe, then begin work the next day, working from 5 am to 9 pm.
	Operations puts night crews and critical operations personnel in place
	Operations rolls trouble shooters and third-shift employees, with a support employee, to the night shift (5 pm to 9 am) to ride out the storm and continue to work that shift throughout the restoration.
	Incident Commanders conducts leadership conference call
	Potential topics to cover:
	• actual or expected storm category
	• storm condition
	• trouble level of the event
	• type of event
	• damage projection
	• time of impact
	• duration of event
	• EOP timeline status
	• plan for recovery
	• progress of preparedness
	• communications

139

Phase	Description
13 - The forecasted time of arrival of 39 mph winds for this location is < 6 hours	**Section chiefs assess Special Material Release and approve placement of order** The Supply Chain group presents final recommendations for the Special Material Release based on evolving storm and material availability data. **Supply Chain notifies vendors of Special Material Release** The Supply Chain group places the Special Material Release approved by section chiefs.
14 - Sustained winds fall below 39 mph	**Operations branch directors conduct operations conference call** The Operations branch directors, SAD's, and service center operations conduct conference call to determine impact to their facility, equipment and ability to operate. They also report any initial damage assessment. Activate helicopters The Operations section chief communicates with Transmission, Substations, and Distribution regarding the need for helicopters and the number needed by each group. Establish landing sites, number of passengers flying, and estimated duration (number of days/hours). Activated when wind is on our shore. **Resource Acquisition participates in RMAG Conference Call #3** Resource Acquisition updates the Resource Request from previous conference calls. They also determine assigned resources, and request additional resources outside of S.E.E. if needed. **Update the employee storm hotline** Public/Employee Information Officer updates information and instructions on the employee storm hotline. Resource Acquisition continues to maintain contact with responding resources and keep them updated as they travel to our territory. **Logistics sets up staging sites** The Staging Site Managers within Logistics report on the progress of staging site setup to the Logistics Section Chief. The Logistics Section Chief will provide updates to Operations as needed. **Security director activates security and traffic control**

Phase	Description
	The director of Security, in the Logistics sections, works with local authorities to provide access for CNP personnel conducting restoration activities to storm-damaged areas.
	The director also provides security and traffic control for service centers and staging sites.
	Incident Commander and Section chiefs conduct conference call
	This is the first scheduled Incident Commander/Section chief update after landfall. The call may cover updated versions of the topics mentioned previously.
	Logistics
	Based on the latest resource count, the Hotel Coordinator will begin contacting hotels and reserving rooms for incoming mutual assistance and contract crews. These activities will continue throughout the duration of the incident.

D. Command Centers

Upon activation of the EOP, the Company establishes evaluation centers. Assigned personnel at these evaluation centers act as data collection points for a variety of information such as specific system statuses, conditions, and restoration schedules. They also help CNP track progress for the following tasks:

- Coordination of logistical support and the assignment of manpower to support restoration priorities.
- Communication with outside utilities for assistance, arrival and departure schedules, and other coordination as needed.
- Information collected by these evaluation centers is relayed, compiled and displayed at the Incident Command Center.

Incident Command Center

The Incident Commander (IC) is responsible for establishing and operating the Incident Command Center located at the Greenspoint Annex – Room 1550. If necessary, a backup evaluation center will be stood up at the Bellaire Service Center Auditorium. Personnel will be assigned as necessary to make contacts with outside utilities using mutual assistance processes and the applicable agreements, posting

141

information as provided by other evaluation centers, and supporting other resource needs. Staffing requirements for the Incident Command Center will be based on a 24-hour operational period and will be staffed in 12 or 16-hour shifts as the Incident Commander deems appropriate based on the needs of the response efforts.

Access to the Incident Command Center is limited to assigned duty employees, command staff, and appropriate Company officers.

Activation of the Incident Command Center

At the discretion of the Incident Commander, storm riders must report to the Incident Command Center when specified by the IC. Advanced authorization may be appropriate when fully staffing the center if, in the judgment of leadership, it is necessary to avoid later unsafe road conditions and other possible hazards such as dangerous wind speeds.

Operation of the Incident Command Center

Initial activation of the Incident Command Center will be for the purpose of assessing the status of preparation by departments. The Incident Commander is responsible for scheduling and communicating the requirement for periodic conference calls to assess the status of preparation by the various departments. As the event approaches and crosses CNP's service area, personnel at the Incident Command Center will collect data on system conditions and customer outages initially from EC/DC. In order to ensure a continuing, accurate and consistent flow of information into the Incident Command Center, communications will be established only through the following points for reports issued by the Incident Command Center:

- Real Time Operations (RTO) at Addicks Operations Center (AOC)
- The Distribution Evaluation (DVAL) Center at Greenspoint Service Center
- The Underground Evaluation Center at Harrisburg Service Center
- The Transmission and Substation Evaluation Center at EC/DC

Distribution Evaluation Center

The Director of Distribution Operations will be responsible for establishing a Distribution Evaluation Center in the Greenspoint Service Center, 2nd Floor. The Operations Branch Director will staff and assign personnel as appropriate to the Distribution Evaluation Center to ensure:

- Accurate and comprehensive assessment and evaluation of system conditions
- Initiation of corrective measures
- Effective organization of restoration activities
- Efficient prioritization of all resources

142

- Written summaries regarding available information will be prepared and provided to the Incident Commander, command staff and section chiefs in accordance with the ICS Planning Process

To facilitate tracking system status and restoration progress, information will be maintained on a master system map in the Distribution Evaluation Center room. Personnel to maintain this map will be provided according to the staffing list. Contingent on availability of the supporting systems, Situational Awareness will be used to track restoration progress and prioritization of restoration.

Official reports shall be available by approximately 9:00 am daily. This schedule allows for releasing the most accurate information. The status of restoration assessment and progress shall be communicated to the Incident Command Center via the scheduled periodic conference calls. Staffing requirements will be based on 16-hour shifts with adjustments as deemed necessary by the Incident Commander. Access to the evaluation centers shall be limited to assigned duty employees, interface personnel, and appropriate Company officers.

Activation of the Distribution Evaluation Center

The Distribution Evaluation Center shall be activated to assess and direct restoration activities and will be accomplished in coordination with the Incident Command.

Upon activation of the Incident Command, a report of readiness to the Incident Command Center will be required. The decision to staff the evaluation center prior to storm impact should be made based on projected accessibility after the event passes. In most cases, assessment of damage cannot begin until:143

- Daylight hours have arrived
- Flooding has receded
- Field personnel or helicopters can be safely sent into the impacted area

Operation of the Distribution Evaluation Center

The Distribution Evaluation Center is responsible for providing accurate and consistent information on a timely basis concerning the extent of damage to the distribution facilities, the plans to restore service, and the progress being made in executing that plan in their respective service centers and staging sites. CNP will need to use re-dedicated manpower or crews from

neighboring utilities or contractors. In order to achieve timely restoration, Resource Acquisition reports that information to Incident Command as soon as the information is available

Underground Evaluation Center

The Major Underground Manager will be responsible for establishing an evaluation center at the Harrisburg Service Center. The Major Underground Manager will staff and assign personnel as appropriate to the Harrisburg Service Center in order to assure accurate and comprehensive assessment and evaluation of system conditions, initiation of corrective measures, effective organization of restoration activities, and efficient prioritization of all resources. The Major Underground Evaluation Center reports up through the Distribution Operations Branch Director.

Transmission and Substation Evaluation Centers

The Transmission / Substation Branch Director, or their designee, will be responsible for establishing the Transmission and Substation Evaluation Centers at EC/DC. Personnel will be assigned as necessary to ensure:

• Accurate and comprehensive assessment and evaluation of system conditions

• Initiation of corrective measures

• Effective organization of restoration activities

• Efficient prioritization of all resources

Status of restoration assessment and progress shall be communicated to Incident Command per the update schedule determine by the Incident Commander. Staffing requirements will be based on 16-hour shifts as deemed appropriate by the Incident Commander and with adjustments as conditions warrant. Access to these evaluation centers shall be limited to assigned duty employees, interface personnel, and appropriate Company officers and staff.

Activation of the Transmission and Substation Evaluation Centers.

Activation of the Incident Command will require a report of readiness from each evaluation center to the Incident Command Center, though staffing may not be necessary. The decision to staff the evaluation centers will be made based on accessibility both before and after the event passes. Preemptive steps may be taken to avoid or minimize system damage. In most cases, assessment of damage cannot begin until daylight hours and field personnel or helicopters can

144

be safely sent into the impacted area. Once the evaluation centers are fully staffed, a report will be made to Incident Command.

Operation of the Transmission and Substation Evaluation Centers

The Transmission and Substation Evaluation Centers are responsible for providing accurate and consistent information to the other evaluation centers on a timely basis. The Transmission and Substation Evaluation Centers will provide this information as the event develops and passes through the area, and will concern:

- Transmission network conditions
- The extent of damage to Transmission and Substation facilities
- The projected restoration of service plan
- The progress being made in executing that plan
- The need for and the ability to use re-dedicated manpower or crews from neighboring utilities to achieve timely restoration

Logistics Command Center

The Managers of Supply Chain, Procurement and Logistics are responsible for establishing the Distribution Material Evaluation Center at South Houston Materials Management, Building A. The Distribution Material Evaluation Center may relocate, as appropriate, to another CNP office facility. This location will be selected based on storm damage proximity and available office space. Alternate locations include the Cypress, Sugarland, and Spring Branch Service Centers. Personnel will be assigned as necessary to ensure that distribution material issues are resolved quickly and support the overall restoration effort. Details as to staffing, activation, operation, and communications are contained in the departmental plan for Logistics.

Annex F

Cyber Security Annex

CYBER SECURITY ANNEX

1. INTRODUCTION

Cyber incidents are not unlike operational incidents. When a user or operation identifies or believes a cyber incident is occurring or has occurred, their first responsibility is to initiate actions, procedures, and/or practices to stabilize any impact to business or operational systems which may jeopardize employee or public safety, or may result in material consequences to employee or customer information, or will result in interruption of business continuity. It is incumbent upon the user to initiate the procedures outlined in the Cyber Incident Response Plan ("CIRP") immediately upon the initial incident detection.

Cyber Security programs at CNP are enforced through Information Technology ("IT") Security policies and procedures that identify:

- Authorized and unauthorized actions within CNP on technology systems.

- Assigned organizational responsibilities.

- Acceptable levels of risk.

When CNP's IT Security policies and procedures are violated, a cyber incident may have occurred. To detect, respond, and manage violations, incident response policies and procedures should be in place to minimize risk as well as facilitate recovery from a violation.

1.1. Purpose

The purpose of CNP's CIRP is to provide a structured, systematic incident response process for all company information technology systems, including third party services and/or systems to: identify, escalate, and respond to Information Security incidents. The CIRP is intended to:

- Assist CNP and third-party personnel to quickly and efficiently recover from different levels of Information Security Incidents (as defined in Section 1.4).

- Define the business, Information Technology, and/or control systems incident process and step-by-step guidelines creating a consistent, repeatable incident response process.

- Mitigate and/or minimize the loss or theft of information or disruption of critical infrastructure.

- Provide consistent documentation of activities related to actions taken during incidents.

- Synthesize knowledge and experience into preventative security measures.

- Reduce overall exposure for CNP.

- Decrease the total time to reach incident resolution by initiating an effective and efficient response to Information Security Incidents.

147

- Provide for business understanding and participation in the Information Technology Incidents response and incident management processes in order to establish a more effective strategy and response to future Information Security Incidents.

1.2. Scope

The standards and guidelines contained in this document define CNP's CIRP that applies to:

- The fundamental information actions and tasks needed for Information Technology personnel to provide incident response services to CNP's control system and/or related I.T. systems.

- All CNP business groups, divisions and subsidiaries and their employees, contractors, vendors and business partners.

- All computer systems, computing devices, control systems, and networks connected to the CNP network.

- Incident notifications that are automated (i.e. – system notification) or manual (i.e. – employee notification, external party notification).

1.3. Issuing Authority

I.T. Director Corp Cyber Security, Corporate I.T. Cyber Security

1.4. Use of this Document

This document is designed to provide both the procedures and the essential tools (such as quick reference guides and checklists) for managing an Information Security Incident.

1.5. Maintaining this Document

This document will be subject to both planned reviews and continuous improvement activities.
The document will be reviewed annually and approved by the Issuing Authority (Section 1.3).
The CIRP will be reviewed during the follow-up meeting to every Information Security Incident initiation. Suggested improvements to the plan or to this document will be documented, sent to the Issuing Authority for approval and communicated to the individuals who have responsibilities within the process.

1.6. Training

It is essential training on the CIRP be performed regularly. All the key groups and roles described in the CIRP need both initial detailed training and periodic (at least annual) review training. Developing the training materials and conducting the training will be the responsibility of the Corporate I.T. Security Risk & Compliance group.

148

1.7. Process Improvement

In order to remain relevant and useful, this incident response plan needs to be continually improved. This is accomplished by enhancing the process documents with input from the lessons-learned sessions, conformance with industry standards and compliance with regulatory requirements. While this is a continuous process, it should occur at least annually.

2. SECURITY INCIDENT RESPONSE CAPABILITIES

2.1. Need for a Cyber Incident Response Plan

Cyber incident response is an organized approach to address and manage activities during and after an Information Security Incident. The goal of the CIRP is to handle the situation in an organized and effective manner, limit damage to the organization and reduce recovery time and cost. This CIRP provides guidelines on what constitutes an Information Security Incident and a process that must be followed when an Information Security Incident occurs.

2.2. Incident Preparation

To quickly respond to Information Security Incidents that could adversely affect the CNP environment, this CIRP should be followed to reduce the damage and minimize risk to the organization. The CIRT members should represent Subject Matter Experts ("SME") needed to help resolve the issue. Employees should be trained on how to respond to any suspicious activity.

2.3. Cyber Incident Response Team ("CIRT")

The CIRT is activated by the Director Corp Cyber Security or his/her designee.

The CIRT role is to provide a quick, organized and effective response to Information Security Incidents.

The CIRT's mission is to minimize serious loss of information, information assets and customer confidence by providing an immediate, effective and informed response to any event involving CNP's information systems, networks or control systems.

The CIRT is authorized to take appropriate steps necessary to mitigate and resolve a security incident. The team is responsible for investigating suspected intrusion attempts and loss of company information and assets in a timely manner. Additionally, the CIRT is responsible for reporting findings to management and to the appropriate authorities, as necessary.

Upon notification of an Information Security Incident requiring response, CIRT members must reprioritize their daily responsibilities to respond to the Information Security Incident and must have the appropriate level of authority to make decisions regarding risk and security measures.

2.4. Roles and Responsibilities

To efficiently and effectively respond to an Information Security Incident, the groups responsible for investigating, containing, remediating and returning the systems back to normal are outlined below with their roles and responsibilities during an Information Security Incident.

For each incident a contact list with assigned parties will be maintained.

2.5. Unavailability of Personnel

Unavailability of critical personnel can arise at any time, because Paid Time Off ("PTO"), illness, accidents and unforeseen events are inevitable. To avoid a single point of failure, backup arrangements for personnel should be made in advance. Members of the CIRT should not be allowed to have the same day off. The lack of critical personnel may arise during the time just before and after business hours. During that time most of the critical team members may be commuting to or from home. They may be reachable but may have a difficult time performing specific actions. This can be avoided by having team members "stagger" their business hours.

For these reasons, each Business Unit must prepare and maintain a list of primary and secondary contacts and provide the list to the Director of Corp Cyber Security on a monthly basis.

2.6 Inner Organization Communications

In the event of a Priority Level 3 (Severity Level 2) Escalation or the Suspected Breach of Confidential Information, Initiate Contact with the following groups.

2.6.1 Legal Department/Data Privacy Office

Legal/the Data Privacy Office shall be notified immediately upon first indication of an Information Security Incident as well as when there is a material likelihood that confidential information has been affected by the Information Security Incident. If necessary, the Data Privacy Office will activate the Privacy Incident Response Plan. Consulting with legal counsel allows for guidance, direction, and ensures attorney-client privilege is appropriately attached

2.6.2 Corporate Response Plan Team

First Notify the Corporate Response Plan Team at Escalation to Priority Level 3 (Severity Level 2) in order to activate the Corporate Response Plan at the proper stage.

2.6.3   Technology Systems Control Center (TSCC)
First Notify TSCC at Escalation to Priority Level 3 (Severity Level 2) in order to activate the TSCC Incident Coordinator.

2.6.4   Corporate Communications
First Notify Corporate Communications at Escalation to Priority Level 3 (Severity Level 2)

2.6.5   Physical Security Team
First Notify Physical Security Team at Escalation to Priority Level 3 (Severity Level 2)

3. INCIDENT RESPONSE PROCEDURE
There are defined actions for the operational aspects of cyber incident response. Considerations should be given to specific incident-handling procedures and described in detail. The internal procedures are intended to facilitate the appropriate assessment of an Information Security Incident and provide required resources for incident response based on the priority rating of the incident.

The CenterPoint Energy Incident Response Framework is composed of the five (5) steps to handle Information Security Incidents in a consistent manner: Detect, Notify, Analyze, Recover, and Follow-Up.

4. COMMUNICATION
Timely, relevant and authentic communication during an incident is critical to the resolution of the incident. The procedure outlined below is based on the Corporate Response Plan and must be observed for the duration of the CIRP. For further explanation, please reference the Corporate Response Plan.

5. INCIDENT RESPONSE PLAN TESTING
This CIRP should be tested periodically to ensure employees involved are aware of CNP environment. The I.T. Corporate Technology Security Director is responsible for planning and initiating the testing.

As referenced previously, the Company utilizes three emergency activation levels, designed to ensure sufficient resources are available to effectively respond to any type of event impacting CEHE's service territory. The alert levels may be activated, based on need, during a variety of

151

event types. Please see Section A: Overview for additional details regarding the Company's response to emergency events.

Annex G

Physical Security Incident Annex

CENTERPOINT ENERGY HOUSTON ELECTRIC

CenterPoint Energy

EMERGENCY OPERATIONS PLAN (EOP)

Physical Security Incident Annex

Scope

This annex addresses company facilities and assets including; office buildings, service centers, vehicles, equipment, materials, and supplies, as well as company employees and contractors on company property or while performing work on behalf of CNP.

For CNP facilities or assets subject to federal security requirements such as North American Electric Reliability Corporation (NERC), Transportation Security Administration (TSA) Pipeline Security Guidelines, Department of Homeland Security (DHS) 6 CFR 27 Chemical Facility Anti-Terrorism Standards (CFATS) or 49 CFR 193 LNG, the applicable federal rules / requirements are primary, and the CNP security guidelines and requirements are supplementary.

This document is considered supplementary and secondary to the CNP Physical Security Policy.

Section 1: Security Program Structure

100 Use of This Document

A. This document will be issued electronically and made available on the Corporate Security page of CNP Today Intranet for access by employees and contractors.

B. Mandatory items are indicated by the words "shall", "will", or "must". Recommended items or practices are indicated by the word "should".

101 Security Information Governance Council (SIGC) Responsibilities
The Security Governance Council (SIGC) is responsible for helping to develop and maintain security policies, coordinate compliance with the policies, and assist individual business units and functional groups with mitigating potential security risks.

102 Physical Security Policy
Corporate Security has published a Physical Security Policy which is a controlling and overarching policy above this manual. This manual is secondary and supplementary to the Physical Security Policy available in the Policies section of CNP Today.

154

CENTERPOINT ENERGY HOUSTON ELECTRIC

⌖ **CenterPoint**
Energy

EMERGENCY OPERATIONS PLAN (EOP)

103   Security Operations Center (SOC)

The Security Operations Center (SOC) is a 24/7 operation center, which provides dispatch and security support to all CNP properties, employees, contractors, and other stakeholders. As the primary point of contact for security issues and incidents that occur at CNP properties, SOC Operators play a key role in both operational security and facility safety. Using various technical security systems and monitoring software, the SOC is responsible for the detection, triage, and alerting of routine and critical security incidents. The SOC assists with the escalation and incident management of critical security incidents.

104   Security Incident Reporting

The immediate reporting of security incidents to the Corporate Security Department is required and is very important to help ensure a prompt Company response and the implementation of effective mitigation solutions.

WHAT TO REPORT

- Crimes - thefts, threats, assaults, etc.
- Security related incidents - fires, cut fences, trespassers, card reader doors propped open, improper security procedures being followed, etc.
- Suspicious and unusual incidents - persons photographing Company facilities, unknown packages left unattended, aircraft low fly-overs of critical facilities, unusual calls to obtain Company information, etc.

COST OF LOSS

Business units should report an estimated cost of loss when the incident is originally reported. The actual cost of loss will be reported after all costs of loss and repair have been completed and calculated.

Cost of loss is defined as the total cost to replace the loss of an asset. As an example, cost of loss for the theft of equipment would include the replacement cost, plus the estimated cost of labor involved in obtaining the replacement equipment. In the event of a copper theft the cost of loss would be the cost of replacement material, employee

CENTERPOINT ENERGY HOUSTON ELECTRIC

⊖ *CenterPoint*
Energy

EMERGENCY OPERATIONS PLAN (EOP)

labor, and any contractor costs. Cost of loss can be a determining factor in deciding the appropriate security mitigation actions.

HOW TO REPORT

In case of a fire or life-threatening emergency, immediately call 911, and then notify your supervisor and Corporate Security.

CORPORATE SECURITY RESPONSE TO INCIDENTS

Corporate Security will notify local law enforcement agencies for response to all suspected or actual criminal incidents. As appropriate, Corporate Security will notify state or federal security or law enforcement agencies (FBI, DHS, State Police, etc.)

Section 2: Protection of People and Assets

201   Suspicious Persons and Activities

A.   All employees should be aware of their work surroundings and report any and all suspicious persons or activities the employee may observe.

B.   Suspicious persons or activities could include:

1.   Unknown persons or vehicles in the work area.

2.   Transients.

3.   An employee in an area they do not belong.

4.   Persons loitering near company property or work areas.

C.   Indicators of suspicious surveillance of the company:

1.   Demeanor of the individuals (Do they avoid eye contact?)

2.   Do they appear interested in something that is not there or that would not normally hold long periods of interest?

3.   Do they appear to be taking measurements with their feet/stride, vehicle (driving a pattern), or using a range finder?

156

CENTERPOINT ENERGY HOUSTON ELECTRIC

CenterPoint Energy

EMERGENCY OPERATIONS PLAN (EOP)

4. Attempts to gain sensitive information about security measures or personnel, entry points, peak days, and hours of operation, and access controls such as alarms or locks.

5. Observations of security procedures or staffing positions.

6. Discreet or unusually suspicious use of cameras or video recorders, sketching or note taking, particularly of or about sensitive areas or restricted access points.

7. Unusual or suspicious interest in speaking with building maintenance personnel.

8. Observations of or questions about facility security measures, to include barriers, restricted areas, cameras, and intrusion detection systems.

9. Observations or questions about facility air conditioning, heating, or ventilation systems.

10. Attempted or unauthorized access to rooftops or other potentially sensitive areas.

D. What may constitute suspicious activity to one person may not be suspicious to another person. A good gauge for distinguishing suspicious persons or activities is if your intuition or instinct tells you something is wrong, it probably is wrong. By recognizing and reporting suspicious activity we may prevent a loss or crime from occurring and help to better ensure the safety of employees and company assets.

1. Should you observe suspicious persons or activities report it immediately to:

   − Your supervisor.

   − Corporate Security.

2. Call 911 immediately if a crime is occurring or the situation appears dangerous or threatening.

202 Sabotage

Sabotage is the deliberate destruction of property, equipment, controls, or communication with the intent of causing:

- Interruptions to critical operations
- System Failure
- Disruption of the bulk electric system or gas distribution system

Events caused by theft and vandalism are not considered sabotage.

157

CENTERPOINT ENERGY HOUSTON ELECTRIC

⊖ *CenterPoint*
Energy

EMERGENCY OPERATIONS PLAN (EOP)

A. The key to protecting CNP facilities from sabotage is to be conscious of activities in or around our facilities. Early detection and recognition of potential and actual sabotage events are critical. Sabotage may be the work of terrorists, hostile individuals, or disgruntled employees. Sabotage events can be cyber, physical, and/or operational and may include events like:

- Terrorist threats or attacks.

- Discovery of explosives.

- Extensive damage to our electrical, gas distribution, gathering, and distribution facilities and equipment.

- Suspicious packages in/around our facilities and equipment.

- Apparent forced entry.

- Intelligence gathering attempts; unauthorized people requesting information about items such as operations, software, and telecommunications, etc.

- Unauthorized physical surveillance, including photography.

- Other suspicious events.

B. Employees who observe an act, event, unusual conduct, unusual inquiry, any questionable or suspicious activity involving company physical and/or cyber facilities, assets, or personnel should consider such activity a potential threat.

C. Employees should be avoid "confirmation bias" to explain their observations – in other words, developing a "good reason" why something may have occurred. Some examples are, "That person is just really curious so is asking lots of questions" OR "There's damage to this equipment but it was probably just kids messing around."

D. It is the responsibility of all company employees to report suspicious activities by notifying their supervisor and the Corporate Security Department as soon as possible. If an immediate risk of damage, injury, or sabotage is present, employees should call 911 immediately.

203   Trespassers

A. Trespassers are not permitted on company property.

B. If trespassers are found upon company property, take the following actions.

CENTERPOINT ENERGY HOUSTON ELECTRIC

CenterPoint Energy

EMERGENCY OPERATIONS PLAN (EOP)

1. If your facility has a security officer, notify the security officer immediately so the person(s) can be removed.

2. If no security officer is at your facility, then notify your supervisor or building management.

3. If you feel safe to do so, advise the loiterer or trespasser that you represent the company property and that they need to leave immediately. If the person fails to leave, call the police.

4. When the police arrive they will ask you if you want to trespass the person. You will have to tell the police officer that the person is not welcome, is trespassing and that you want them to leave. If the person persists and refuses to leave after being given this notice then they will be subject to arrest by the police for trespassing.

Section 3: Physical Security Support to EOP for Non-Security Related Activations

301 Staging Site Security

Corporate Security coordinates staffing assignments for security guards and off-duty law enforcement to secure crew staging sites. Corporate Security also oversees the work of security coordinators assigned to staging sites.

302 Crew Security

Corporate Security coordinates the assignment of off duty law enforcement and/or security guards, as requested by business unit leadership.

As referenced previously, the Company utilizes three emergency activation levels, designed to ensure sufficient resources are available to effectively respond to any type of event impacting CEHE's service territory. The alert levels may be activated, based on need, during a variety of event types. Please see Section A: Overview for additional details regarding the Company's response to emergency events.

CENTERPOINT ENERGY HOUSTON ELECTRIC

CenterPoint Energy

EMERGENCY OPERATIONS PLAN (EOP)

Annex H

Mobile Generation/Long Lead Time Facilities Annex

Confidential - FOR OFFICIAL USE ONLY

CENTERPOINT ENERGY HOUSTON ELECTRIC

⊖ *CenterPoint*
   Energy

EMERGENCY OPERATIONS PLAN (EOP)

Temporary Mobile Generation ~~Annex~~

As a result of amendments to PURA in the 2021 Texas Legislative session, TDUs may lease and operate facilities for temporary emergency electric energy to aid in restoration for distribution level customers during "a widespread power outage" (defined as an event that results in a loss of electric power that (A) affects a significant number of distribution customers of a transmission and distribution utility and (B) has lasted or is expected to last for at least eight hours, and is a risk to public safety) in which load shed has been ordered or the TDU's distribution facilities are not being fully served by the bulk power system under normal operations.[1]

In accordance with applicable statutes,[2] CEHE has entered into a lease agreement with a mobile generation provider to secure emergency back-up generation capacity, with the lease agreement ending on June 30, 2029. This lease agreement also extended the lease term for certain temporary mobile generation units that CEHE had previously leased under a short-term lease agreement. CEHE has leased up to approximately 500 MW of temporary mobile generation units, with actual output depending on ambient and other operating conditions. CEHE has the following temporary mobile generation units to deploy, if necessary:

- Up to fifteen (15) mobile gas turbine generator sets capable of providing approximately 30 MW or more of power each depending on ambient and other operating conditions.

- Up to five (5) mobile gas turbine generator sets capable of providing approximately 5 MW or more of power each depending on ambient and other operating conditions.

- Appropriate support resources within prescribed times to transport and operate the equipment.

- CEHE expects to be able to operate the equipment until either the deactivation of the EOP or until affected customers are eligible to receive service (i.e. the statutory requirements are no longer met). Depending upon storm severity, this could range from 1-6+ weeks.

---

[1] Public Utility Regulatory Act, Tex. Util. Code §§ 39.918 ("PURA")
[2] *Id.*

CENTERPOINT ENERGY HOUSTON ELECTRIC

CenterPoint Energy

EMERGENCY OPERATIONS PLAN (EOP)

Finally, based on system needs, and in coordination with appropriate government officials and regulators, CEHE will determine the potential location(s) where the back-up mobile generation facilities will be best utilized, to the extent possible based on actual conditions of a particular event. These determinations will be based on good utility practice, system conditions, and the circumstances and customer needs during each individual EOP event.[3] Some back-up mobile generation facilities listed above have been pre-positioned at certain locations in CEHE's service area. Under the long-term lease agreement, the mobile generation provider must provide transportation and assembly services if mobile generation facilities need to be relocated. CEHE will coordinate with the mobile generation provider in the event that the pre-positioned mobile generation facilities need to be relocated to other locations in CEHE's service area during an EOP event as operating conditions, road conditions, and other safety considerations permit.

CEHE's operation of back-up mobile generation facilities during an EOP event is not a guarantee against fluctuations, irregularities, or interruptions in delivery service. CEHE's operation of back-up mobile generation facilities is subject to the provisions in CEHE's PUCT-approved tariff, including, but not limited to, provisions related to quality of delivery service, emergencies and necessary interruptions, limitation of warranties, and limits on liability.

As referenced previously, the Company utilizes three emergency activation levels, designed to ensure sufficient resources are available to effectively respond to any type of event impacting CEHE's service territory. The alert levels may be activated, based on need, during a variety of event types. Please see Section A: Overview for additional details regarding the Company's response to emergency events.

---

[3] PURA §§ 39.918 (g)

CENTERPOINT ENERGY HOUSTON ELECTRIC

EMERGENCY OPERATIONS PLAN (EOP)

Long Lead Time Facilities

The Texas legislature amended the Public Utility Regulatory Act, adding § 39.918 Utility Facilities for Power Restoration After Widespread Power Outage. As a part of this statutory revision subsection (b)(2) addressed the need for transmission and distribution utilities ("TDUs") to have long-lead time facilities.

The statute authorizes TDUs to take proactive measures to ensure they have the facilities necessary to aid in restoring service to customers following a widespread power outage, which is defined in the statute as an event that results in a loss of electric power that affects a significant number of TDU distribution customers and has lasted or is expected to last for at least eight hours and is a risk to public safety. Subsection (b)(2) specifically permits a TDU to "procure, own, and operate...transmission and distribution facilities that have a lead time of at least six months and would aid in restoring power to the utility's distribution customers following a widespread power outage." The statute further excludes from long-lead time facilities electric energy storage equipment or facilities under Chapter 35 of the Utilities Code. Subsection (h) states the "commission shall permit" a TDU that "procures, owns and operates facilities under Subsection (b)(2) to recover the reasonable and necessary costs of procuring, owning, and operating the facilities, using the rate of return" from the TDU's last base rate proceeding. Based on the statute, long-lead time facilities are those that take at least six months to acquire and would be used to restore power after a widespread outage.

The Company interpreted Sec. 39.918(a) to apply to any widespread power outages resulting from several natural or man-made causes, including, but not limited to: tornados, hurricanes, microbursts, flooding, extreme heat/cold, fire events, or an intentional attack on the electric grid e.g., terrorist events, cyber-attacks. Given this statutory language, the Company undertook an evaluation to identify the facilities that are critical to restoring electric service following widespread power outages with a lead time of at least six months.

As a result of this regulation, the Company has added a specific long lead time facility (LLTF) designation for qualifying material items. Materials items are reviewed monthly to validate the long lead time and widespread power outage criteria are met. When both criteria are met, the material item is determined to be a qualifying LLTF material item and are designated as such.

163