Tasks

Security Coordinators:

- Coordinating with local authorities to ensure CNP personnel access to storm damaged areas
- Coordinating and deploying contract guards and off-duty police officers
- Acting as a liaison with law enforcement or other governmental agencies
- Coordinating police escorts of crews and materials
- Handling promptly all incidents of a security nature
- Coordinating traffic control for morning and evening crew truck movements at staging sites

Security Technical Coordinators

- Coordinating toll road procedures with Harris County Toll Road Authority
- Maintaining, monitoring, and responding to information from electronic security systems

Security Billing Contractor Coordinators

- Keeping time for contract security resources
- Ensuring that CNP processes payments for security contract resources in a timely manner

Outputs

- Information on which foreign and mutual assistance vehicles will need access to toll roads (to HCTRA)
- Payments to contract security personnel

D.3.4.6 Staging Site Management Summary

Staging site management is responsible for setting up and managing bases of operations for major restoration efforts involving mutual assistance and contract crews.

Staffing

- One senior level manager per primary and secondary staging site, to set up and administer the site

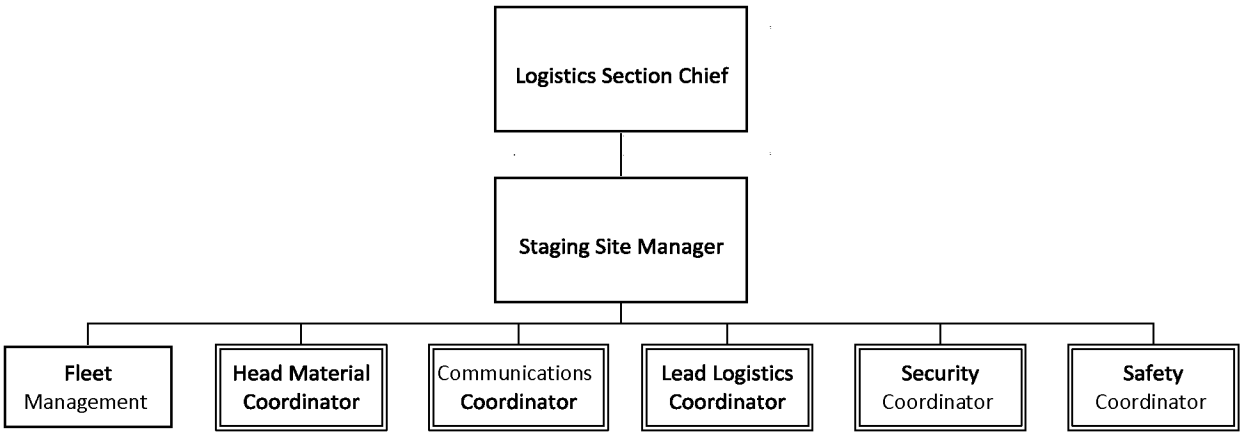
The secondary site managers will assist the primary site managers as needed

- Support personnel in order to provide Distribution Operations and their crews with basic services
- Security personnel: Responsible for:
  - Establishing a safe and secure area for the coming and going of all personnel and vehicles
  - Providing those crews with appropriate identification
  - Directing traffic, including hotel buses
  - Arranging for convenient parking of crew trucks
- Fleet personnel: Responsible for:
  - Locating the fuel skids in a safe and convenient location
  - Having all crew trucks fueled and ready for duty each day
  - Repairing and maintaining of internal fleet vehicles
  - Arranging for rentals if necessary
  - Putting external crews in touch with repair vendors
- Materials personnel: Responsible for:
  - Obtaining and stocking basic materials and supplies needed by the restoration crews
  - Providing tools

- Providing occasional hot shot delivery services to crews in the field

- Communications personnel: Responsible for establishing the communication network at the staging site, including telephone, internet service, and technical support.
- Staging Site Logistics personnel: Responsible for:
  - Providing sit down breakfast and dinner for all foreign crews and staging site support personnel
  - Providing carry out lunches
  - Taking care of crew laundry service and staging site cleanup services
  - Coordinating the service of portable restroom services

The following is the organizational structure of each site*:



Note: This is the structure for the Logistics branch only. Sites will also have Operations assigned to it and other support functions, such as Resource Check-in Coordinators.

Inputs

- Notice from Distribution Operations Branch Director about which sites need to be activated (the sizes of the staging sites that are activated determines the list of resource requirements)
- Kick-off pallets from the Special Material Release (from Supply Chain)

- Number and estimated arrival time of incoming crews (from Resource Acquisition group

Tasks

- Help with initial clearing of debris at staging sites
- Assist with coordination of staff that primarily are responsible for security, logistics, materials management, communications, fleet services, staging site resources, or facilities
- Set up flow patterns for traffic, including signage
- Establish parking
- Ensure the safety of the staging site
- Resolve issues that arise over the course of the restoration effort

Outputs

- Safe, functional staging site

D.3.5 Finance Section

D.3.5.1 Summary

The Finance Section is a critical part of ICS in complex incidents involving significant funding. The Section Chief tracks and reports to Incident Command the accrued cost as the incident progresses and may also be asked to provide forecasts to ensure operations are not negatively impacted. Some of the functions that fall within the scope of this Section are conducting overall cost analysis for the incident and maintaining typical operations such as accounts payable, and revenue billing. The Finance Section is responsible for:

- Minimizing financial risk and loss for CNP
- Tracking costs related to the event

- Reimbursing applicable parties per their existing agreements with CNP
- Helping to put together damage estimates for smaller events

Within the Finance Section, four primary Branches fulfill functional requirements:

- Reporting: provides cost analysis and forecasts to Incident Command
- Financial Services: continues typical operating functions such as accounts payable, remittance processing and revenue billing
- Insurance: administers all claims other than auto, general liability and excess liability
- Treasury: manages cash funding requirements

Although most groups in the Finance Section operate as normal, their activities are related to the Storm EOP. A brief summary of responsibilities are listed below.

D.3.5.2 Reporting Unit Summary

The Reporting Unit provides cost analysis and forecasts to Incident Command.

Staffing

- Reporting Unit branch director
- Liaisons

Inputs

Restoration:

Ad hoc reporting requests

Post-restoration:

- Requests for reporting

- Assumptions related to the regulatory recovery of storm costs (from Regulatory Reporting)

Tasks

Pre-storm:

- Send out information on how internal employees track time during a Storm EOP
- Setting up the cost collectors for an anticipated storm event

Restoration:

- Put together an estimate of what the storm will cost
- Coordinate with other Finance groups to gather the information needed for internal and external reporting, including:
  - Analysis of the impacts to revenues, operating expenses and capital
  - Timing and amount of regulatory recovery of storm costs
- Respond to requests for reports

Post-restoration:

- Coordinate with other Finance groups to gather the information needed for reports
- Respond to requests for reports
- In the event is serious enough that the Company service area is declared a federal disaster area, coordinate with the Tax department and Insurance to determine the amount of tax deduction

Outputs

Restoration:

- Estimate the amount that the storm will cost and the amount of regulatory recovery (to Investor Relations and Regulatory Reporting areas)
- Information on how to track costs

Post-restoration:

Financial reporting as required to support regulatory efforts (to Regulatory Reporting branch director)

D.3.5.3 Financial Services Summary

Accounts Payable ensures timely payment for goods and services rendered during restoration. Remittance Processing ensures the timely processing of checks. Payroll and Administration ensures timely payment to staff. Electric Revenue Billing determines the correct billing information to send to REPs on behalf of customers and calculates lost revenues

Financial Services does not have an official Storm EOP status. They will continue their normal activities during a Storm EOP. However, these activities are related to Storm EOP.

D.3.5.4 Insurance Risk Management Unit Summary

The Insurance Risk Management Unit is responsible for administering all claims other than auto, general liability, and excess liability.

Staffing

This group does not have an official Storm EOP status. They will continue their normal activities during a Storm EOP. However, these activities are related to a Storm EOP.

The staff includes 3 Corporate Insurance Coordinators and 1 administrative assistant.

The other Insurance staff are loaned to other branches during a Storm EOP, except the administrative assistant. The administrative assistant reports workers compensation claims through the One Call procedure.

Inputs

- Insurance claims information from daily status conference calls
- Injury information from Disability Management
- Workers compensation claim payments (from an outside vendor)

Tasks

- Notify property insurance brokers and adjusters if damage exceeds deductible
- Assist Environmental, Safety, Legal and Human Resources' representatives with submission of company incident reporting forms to meet insurance policy discovery and reporting time deadlines/restrictions.
- Gather preliminary facts and create reports for adjusters based on damage inspections of locations.
- Coordinate arrangements for adjusters to be at the damaged sites.
- Provide estimate of the property loss
- Assist affected business units, gather documentation to support an insurance claim.
- Manage claims through settlement.
- Process workers compensation claim payments on a weekly basis

Outputs

- Reports for executives as needed
- Deposit proceeds as directed by affected business unit
- Payments for workers compensation claims

- Information on lost time workers compensation claim payments (for Payroll salary continuation)

D.3.5.5 Treasury Summary

Shareholder Services: Serves as transfer agent, registrar and dividend paying agent for CNP common stock and administers CNP's Investor's Choice Plan. Long-term Finance: Long- Term Finance evaluates and implements financings, ensures that compliance reporting and other requirements in financing agreements are satisfied and administers trust relationships.

This branch does not have an official EOP status. They will continue their normal activities during EOP. However, these activities are related to EOP.

Tasks

Coordinate with the Director Operations for cash funding requirements prior to the storm. Per the CNP General Expense and Reimbursement policy, cash advances during an emergency other than EOP must be approved by the Business Unit President or functional area leader. Cash advances normally not available may be made available during an EOP situation when the card holder has established the cash feature of his or her OnePay card.

Section E: Annexes

Per 25.53. the following annexes are included in this section:

- Annex A – Weather Emergency Annex
- Annex B – Load Shed Annex
- Annex C – Pandemic and Epidemic Annex
- Annex D – Wildfire Annex
- Annex E – Hurricane Annex
- Annex F – Cyber Security Annex
- Annex G – Physical Security Incident Annex
- Annex H – Mobile Generation Annex

Annex A

Weather Emergency Annex

Hot Weather Emergency

PURPOSE

The purpose of the hot weather emergency annex is to provide a guide on preparing for and responding to extreme heat measures that could impact the CenterPoint Energy Houston Electric (CEHE) footprint.

SCOPE

There are two distinct responses that could cause an elevated response from CEHE during an extreme heat situation.

- Load Shed as directed by ERCOT
- Widespread outages due to heat related transformer outages (also known as a Transformer Tsunami)

RESPONSE – Load Shed

- CEHE's Real Time Operations (RTO) utilizes and maintains a response plan for Load Shed that is directed and coordinated by ERCOT. The RTO Team will utilized the Emergency Operation Plan (EOP) as necessary to support this response.
- For additional information regarding the load shed plan, please reference (Annex B)

RESPONSE – Equipment Failure

- Distribution Operations maintains a Storm Response Organization to respond to localized weather events. It is the responsibility of the Incident Commander (IC) on duty to monitor the situation and determine if the Response Plan within Distribution Operations should be activated.
- Upon activation, the Incident Command structure will be based on the roles identified in the Storm Response Plan. The IC and support team will make determinations on staffing, resources and materials as necessary.
- In the event of a significant shortfall of materials, staffing, or other issues the IC has the discretion to activate the EOP at Level 1 to provide additional support and garner additional awareness from leadership.
- For additional information, please reference the CEHE Storm Response Plan.

Cold Weather Emergency

Proactive Weatherization

- CEHE designs its transmission circuits to conform with the latest edition of the NESC, which is the industry standard for ice and wind design for coastal and inland areas. The Company's practice for designing all new transmission lines is to utilize Grade B loading requirements. Grade B applies the highest geographically applicable NESC values for wind and ice loading as well as the highest safety overload factors. CEHE also incorporates anti-cascade design features in its transmission lines.
- CEHE designs its substations to conform with the latest version of the NESC wind maps. The Company's practice for new substations and equipment is to utilize 2 wind zones:140-mph (Coastal) and 120-mph (Non-Coastal), which meets or exceeds the NESC wind load based on the substation's location.
- CEHE's equipment specifications and acceptance testing standards include the use of ANSI/IEEE standards, which specify temperature ranges for service conditions covering a wide temperature range. The temperature ranges vary based on type of equipment from -4°F or -22°F to 104°F or 131°F. CEHE equipment specifications specify -22°F for all major substation equipment.
- CEHE installs heaters in substation transformer and breaker control cabinets.
- CEHE's substation control cubicles are climate controlled.
- CEHE utilizes antifreeze for cooling its station service backup generation equipment, and the equipment is oriented in a manner that avoids water and ice buildup on components which could inhibit operation.
- CEHE utilizes station service voltage transformers (SSVTs) in new substation installations, which have been retrofitted to key transmission substations where the station service feed is provided by local distribution providers.
- CEHE installs weep holes in substation buses to avoid water and ice buildup.

Transmission Routine Maintenance

- CEHE has a comprehensive transmission line inspection and rehabilitation program based on a 5-year cycle to ensure that the integrity of existing transmission structures and wires is maintained. Twenty percent of the transmission system is ground inspected and maintainedeach year. Any line component identified that will likely cause a failure or a circuit outage within a critically short period of time is promptly addressed.

Substation Routine Maintenance

- CEHE performs periodic station checks on applicable equipment to verify pressures and levels for Sulfur Hexafluoride (SF6), oil, nitrogen levels, transformer and breaker cabinet heaters, alarms, and supporting circuitry. Station checks are scheduled

monthly for 345kV and select 138kV substations. Station checks for the remaining substations are scheduled every 2 months.

- CEHE performs additional substation equipment and protection system maintenance according to manufacturer recommendations or in accordance with NERC maintenance interval requirements, generally whichever is more frequent.

Distribution Routine Maintenance

- CEHE has a comprehensive distribution wood pole inspection and rehabilitation program based on a 10-year cycle to ensure that the integrity of existing wood pole structures is maintained. Ten percent of the transmission system is ground inspected and maintained each year. Any line component identified that will likely cause a failure or a circuit outage within a critically short period of time is promptly addressed.

Anti-galloping

- Additionally, beginning in 2015 and continuing into 2022, CEHE has completed system hardening projects to retrofit portions of 69 kV and 138 kV transmission circuits with anti-galloping devices to avoid damage from icing conditions.

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.

Annex B

Load Shed Annex

Load Shed Annex

Procedure for controlled shedding of load

Pursuant to the ERCOT Protocols, the Company coordinates with ERCOT during an Energy Emergency Alert (EEA) event. Real-Time Operations Dispatchers coordinate electric grid activities with ERCOT System Operators using ERCOT Protocols and Operating Guides as well as in-house procedures. CNP is required to implement ERCOT-directives to maintain grid reliability.

In accordance with NERC Standard TOP-001-5 R1, without direction from ERCOT, the Company has the flexibility to curtail load by a variety of means, which include implementing the following measures, as time permits:

1. Curtailing all non-essential load within Company facilities;
2. Reducing distribution circuit voltage to achieve load reduction; and
3. Appealing through the media that all customers voluntarily reduce load.

After implementing the above measures, if circumstances require that load be reduced further, the Company will initiate its manual load shedding programs. This is accomplished by shedding distribution circuits as necessary to maintain system frequency, while rotating the outages of distribution circuits. Circuits are divided into four categories called “blocks”. The blocks consider the following: Emergency Load Reduction Schedule (ELRS), NERC standards, and ERCOT Protocols and Operating Guides. In the event that the manual load shedding program does not correct the emergency conditions, automatic under-frequency programs will be activated at the following specific frequency levels: 59.3 Hz, 58.9 Hz and 58.5 Hz. Load assigned to the block for each frequency will in turn be curtailed.

Priorities for restoring shed load to service

Load manually shed as a result of an ERCOT declared EEA load shed event will be rotated and restored based on the order of the distribution feeders for each block as defined in the ELRS.

Hazardous conditions, such as downed power lines, are the highest priority. Because the objective is to restore service to as many customers as possible, restoration of transmission circuits, substations, and distribution feeder mains are begun simultaneously. The distribution restoration proceeds in the following order:

1. primary feeder lines;
2. primary fused laterals;
3. transformers;
4. secondaries; and

5. service drops.

Inspection of and repairs to the feeder circuits are prioritized, so that service to large blocks of customers can be restored as soon as possible. Crews are directed that they must sweep the circuit (i.e. repair ALL damage related to that circuit: circuit, fuses, transformers and service drops) before moving on to the next circuit. After this, the restoration effort is guided by information provided by the Company's Outage Management System (OMS). The information printed on each trouble order includes the name of the device determined to be out of service as well as the number of customers affected. After a device is determined to be out of service, the Company stops printing further orders unless a hazardous condition is reported. Trouble orders from OMS are dispatched to the crews in the affected area in the following order:

1. line-fuse vicinities;
2. transformer vicinities; and
3. single order lights out.

The crews then schedule repairs on the basis of the critical nature of the customers and the location and number of customers affected. This system allows for an orderly and prompt response in restoration of the Company's delivery system.

Procedure for maintaining an accurate registry of critical load customers

Critical loads are defined by the PUC as "loads for which electric service is considered crucial for the protection or maintenance of public safety; including but not limited to hospitals, police stations, fire stations, critical water and wastewater facilities and customers with special in-house life-sustaining equipment."

The Company maintains a registry of critical load customers, which includes two lists: a list of critical load public safety customers, critical load industrial customers, and critical natural gas facilities and a list of chronic condition residential customers and critical care residential customers. The list of critical load public safety customers, critical load industrial customers, and critical natural gas facilities is managed by the Company's Distribution Accounts group, and the list for chronic condition residential customers and critical care residential customers is managed by the Company's Revenue Protection. The registry of critical load customers is an electronic database located in a secured area within the Company's corporate information technology architecture. The registry is updated as necessary but, at a minimum, annually.

The registry of critical load is updated as customers are approved through the application process. Approved Critical natural gas facilities are tracked for awareness during load shed and restoration planning. To ensure that the critical load registry is accurate, the Company's

personnel interact with various local government and area representatives to review and validate the information.

The critical load registry is used to develop circuit prioritization. When a critical load customer is initially added to the registry, the Company circuit serving that critical load is included in that critical load customer's record. Within the critical load registry, reports can be extracted by circuit, and this information is then utilized in an annual circuit prioritization process. In addition, both the Company's Outage Management System and the Geographic Information System depict critical load accounts. The Company assists critical load customers by restoring power after an unplanned outage in a systematic way that takes critical loads into account.

Critical Load, Critical Care Residential and Chronic Condition Residential customers are notified when they are approved to be in the Registry of Critical Load Customers. Critical Care Residential and Chronic Condition Residential customers receive notification by mail reminding them to reapply for inclusion in the Registry of Critical Load Customers. Since a load shed event is an emergency order from ERCOT based on a shortfall of electricity being generated, electric utilities, including CEHE, do not have the information to be able to notify individual customers if they may lose power, when they may lose power or how long the load shed event may last. However, we will work to keep our customers informed about the situation through local media outlets, social media, and direct communications.

Customer Service conducts formal training on aspects of serving Critical Load Customers for all Customer Service Representatives. Operations and Engineering personnel are trained to refer customers inquiring about acquiring Critical Load, Critical Care Residential, or Chronic Condition Residential customer status to their Retail Electric Provider and the electric portion of the CNP website.

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.

Annex C

Pandemic and Epidemic Annex

Pandemic and Epidemic Annex

Introduction

CNP, like many other businesses and governmental entities, has developed over the years a variety of business continuity plan in response to uncontrollable events and natural disasters. One area of increasing concern has been the possible need to conduct operations over a number of weeks or months with a substantially reduced workforce and without the ability to call or rely on outside contractor assistance. This more recent requirement has been based on the realization that a world-wide infectious disease or a pandemic could strike unexpectedly.

CNP, drawing from a wide variety of authoritative governmental and scientific sources, as well as its own experience in responding to natural disasters affecting its service area, has developed detailed plans in preparation of a possible pandemic. The response activities can apply to other similar catastrophes that might cause large scale workforce absenteeism.

Objectives

CNP's interest is in preparedness, not panic. It is recognized that a knowledgeable, confident and healthy workforce will represent a key factor in the success of our response plan activities. CNP has three main objectives for the Pandemic Preparedness Plan:

1. Educate employees on how to be personally prepared for a potential infectious epidemic. Employees should understand their roles and responsibilities in support of the company's response activities and continue to have the opportunity to work in a safe and healthy environment.
2. Respond in an appropriate manner to any such threat and attempt to limit the spread of infection, thereby protecting our workforce as much as possible. The plan will identify critical corporate and infrastructure energy delivery functions and devise methodologies for continuing such tasks without undue interruption.
3. Maintain essential services to the community and protect the enterprise and safety of our customers through coordinated efforts with various governmental authorities represented in our area and business footprint.

Key elements

Since we live and work in a highly mobile, global economy, an outbreak of a pandemic infectious disease may provide little lead time before operations are affected. CNP will continue to encourage education of its employees, customers and other business partners as to how they can prepare for such an epidemic.

Employees:

A high priority will be to protect our workforce from the threat of illness by:

- Emphasizing a clean and healthy working environment,
- Coordinating our activities with federal, state and local public health authorities to assist in providing vaccinations and other medications to the extent that they are available, and
- Stressing the need for the sick or those potentially exposed/impacted to remain away from the workplace.

An important weapon against the spread of infectious disease is the isolation of personnel where practical and the use of temporary "physical distancing". Families should stockpile necessary provisions to be self-sufficient within their homes. However, during a pandemic event some sheltering in place may be required for a lengthy period of time, perhaps weeks, since travel and daily shopping may be limited. In addition, schools and day care will likely be closed during community outbreaks, placing an additional need for food, water and other essentials within the home. While ensuring that families are reasonably secure and protected, CNP employees will also need to focus on supporting the business services upon which our communities heavily rely.

Managers:

Each manager and supervisor should develop and maintain business process alternatives and business continuance plans with the expectation that a significant portion of their staff may be unavailable or away from usual work locations. In order for this to be an effective and sustainable plan during an actual infectious outbreak, it will be essential to retain the active participation of all available employees and contract personnel regardless of their normal job duties or work locations.

Crises Response Plan Team (CRPT) Notification

1. The Corporate Response Plan is the Company's strategic resource on how to respond to various types of incidents and crises. The CRP is designed to ensure that resources and other support are provided to the business following an incident.

2. If an incident shows potential for escalation, it is recommended you notify the CRPT immediately.

3. To report incidents and contact CRPT during an incident, please utilize the Corporate Response Telephone and Mailbox.
4. The CRPT consists of the following personnel:

Function	CRP Description
Finance	Finance Officer
Legal	Legal Officer
CCR	Corporate Communications Officer
Safety	Safety Officer
Gas Operations	Gas Operations Officer
Electric Operations	Electric Operations Officer
IT	IT Officer
HR	HR Officer
Regulatory	Regulatory Officer
ERM	Head of ERM
Security	Head of Corporate Security
Customer	Customer Officer
ERM Analyst	ERM Analyst
Emergency Operations	EOP Coordinator

Critical company functions

Unlike the disasters contemplated by some of the company's other business continuity plan, a pandemic does not significantly damage or destroy company facilities or directly affect service to customers. Well into the outbreak, it is expected that our electric utility facilities and gas utility facilities will be operating normally. Should such a disaster affect our service territories, it is not about the equipment itself, but rather the skilled workers that operate that equipment and the multitude of support personnel that constitute CNP.

Further, it will not only be important to maintain service to critical institutions such as hospitals, fire and police stations and government health organizations, but to our customers in general who may have increased needs of critical infrastructure entities. CNP's Pandemic Preparedness Plan Team, in conjunction with others within our organization, is charged with maintaining a current list of important company functions, and ensuring that detailed response plans are in place to continue operations with a reduced workforce. The following work type levels are utilized by this plan to describe those important business, service and support activities.

Level 1 – Business activities that must continue uninterrupted, even in the face of significant workforce absenteeism, in order to maintain appropriate service delivery levels, public safety and corporate financial integrity. Work activities that fall into this critical category may have to be modified so that any absenteeism experienced will not:

- cause disruptions to service according to current emergency plan restoration priorities or
- impact functions that maintain public or private safety.

Level 2 – Business activities that could be delayed for as much as a week without serious business or service consequences. This delay should not:

- jeopardize the supply chain and inventory levels,
- seriously impact company infrastructure, including
  - voice, data and information systems
  - inter-company billings
  - transportation systems
  - payroll processing
- place the company in a serious adverse position relative to contracts, laws or regulations or
- materially impact the financial stability and/or cash flow of the company.

Level 3 – Non-critical business functions that could be delayed indefinitely and rescheduled based on available workforce. Personnel associated with activities in this category could be redeployed as needed to perform Level 1 or Level 2 type work.

Strategies

The strategies outlined below are generally based on a pandemic threat like those monitored by the World Health Organization (WHO). WHO uses phased alerts to inform world health authorities and governments of the changing status of influenza pandemic threats as well as other health-related public threats.

Interpandemic period

Phase 1: No new virus subtypes have been detected in humans. A virus subtype that has caused human infection may be present in animals. If present in animals, the risk of human infection or disease is considered to be low.

Phase 2: No new virus subtypes have been detected in humans. However, a circulating animal virus subtype poses a substantial risk of human disease.

Pandemic alert period

Phase 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. Table B within the Appendix details the actions CNP will take at this phase of a Pandemic event.

Phase 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.

Phase 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

Phase 6: Pandemic: New virus is spreading rapidly within human populations around a significant portion of the globe causing serious health concerns. It should be noted that a pandemic may affect countries, as well as populations within a county, to varying degrees during any of these alert phases as the infectious disease spreads.

Recovery Period

Once the pandemic wave has passed, CNP will begin recovery of its workforce and develop schedules for completing work that may have been temporarily delayed. The possibility for additional infectious waves must also be considered; therefore, recovery activities should be prioritized as to importance.

Generally, an important activity during the Interpandemic period is the review of key areas, functions and personnel that are vital to a sustained delivery infrastructure and corporate financial integrity. During Pandemic Alert period, CNP will be focused on employee education, departmental contingency planning, workplace health and safety, and response activity practice. Beginning with Pandemic period, CNP may need to limit employee business travel and discourage other nonessential outside travel. The timing of these and other response activities will be based on information from various authoritative sources such as the Centers for Disease Control (CDC), as well as management's assessment of the nature of specific pandemic threats.

Communication

Accurate, timely and objective communication with all CNP stakeholders has been identified as a key element to the effectiveness on the Preparedness Plan.

Coordination with employees at all levels of the organization, as well as contractors, suppliers, customers, regulatory agencies, news media and the public may prove critical to the level of success we have as a company and community leaders in quickly responding to a pandemic should it occur. Described below is an outline of some of the communication strategies that will be employed in our preparedness efforts.

Communication plan

- Maintain effective communications with all stakeholders
- Coordinate activities with federal, state and local authorities
- Sustain a knowledgeable and confident workforce
- Respond appropriately as threats materialize to protect and reassure our employees

Employees

CNP's employees are our most valuable assets and will continue to be given careful attention in preparation for a potential pandemic. The company will endeavor to maintain a healthy and safe work environment, as well as emphasize the vital role and responsibility of the employee in CNP's response activities should a highly infectious disease affect our service territory. This requires an understanding of the issues by all involved, communication of our Preparedness Plan, discussion with the employees about their roles and responsibilities and rehearsing response activities as appropriate for each work group to sustain confidence in the effectiveness of the plans.

Therefore, several types of employee communication will be used as appropriate to the audience and situation.

Individual preparation

- Brief email messages about the issues and their national and local importance.
- Listings of useful web sites for self-exploration and education.
- Web access to CNP's Pandemic Preparedness Plan
- Executive updates at employee meetings and/or through electronic messages to provide current information and respond to questions.
- Emails and posters encouraging seasonal flu vaccination and vaccination to address new viruses for all family members, personal hygiene and social etiquette.

- Education and preparation storyboards for computer-based employee education.
- Special reports and voice mail broadcast messages as necessary

Departmental Preparation

- Presentation planning material for staff and safety meetings.
- Custom communication for first responder personnel as needed.
- Instructional material for telecommuting and teleconferencing from home.
- Website and Pandemic Hotline with current information and work instructions.

Other stakeholders

CNP will continue to coordinate its pandemic preparedness plans with its outside stakeholders, including suppliers, contractors, federal, state and local governments and emergency management offices, and regulatory agencies, to clarify roles and responsibilities, verify current contact information and assess and revise response strategies and activities as appropriate.

Training:

The Pandemic Preparedness Plan Team will meet annually to discuss necessary updates to the plan. A corporate communication will be sent to CNP managers annually to educate on the purpose of the plan and to encourage their employees to prepare for such a threat.

Educational resources will be available and accessible to all employees on the CNP Today Pandemic page.

Educational resources

CNP's Pandemic Preparedness Plan is based on a foundation of employee knowledge and understanding of the issues, as well as their dedication and support in executing response activities both at home and work. In that regard, employees should occasionally check for and familiarize themselves with current information on CNP's intranet website.

The following additional websites also provide excellent background information on pandemics, personal and family preparation and current news articles:

- Centers for Disease Control
  http://www.cdc.gov/
- World Health Organization
  http://www.who.int/topics/influenza/en/

- University of Minnesota's Center for Infectious Disease
  http://www.cidrap.umn.edu/cidrap/content/influenza/panflu/index.html
- American Red Cross
  www.redcross.org/news/ds/panflu

Conclusion

CNP will routinely review and update this preparedness plan so that response activity strategies can remain current and effective. The success of the company's response activities, if and when they are needed, will not only be dependent on full employee participation in the review and understanding of these plans, but their practice as well.

Annex D

Wildfire Annex

Wildfire Mitigation Efforts

The Company performs periodic maintenance including clearing trees away from the conductors and equipment on approximately 1,600 circuits. This proactive maintenance takes place on a cyclical basis. For 35kV voltage and some selected 12kV circuits, maintenance is performed about every three years while the remaining 12kV circuits are maintained on a five-year basis. Unplanned tree clearing maintenance may be performed at other times based on locations identified by area operations personnel or as reported by customers.

A proactive hazard tree inspection program is performed along the main feeder portions of circuits in areas with tree species that traditionally experience higher mortality rates. Other circuit feeders may be included during times of drought or infestations.

Periodic transmission circuit and Right-of-Way (ROW) tree clearing maintenance is performed on a five-year cycle basis with the facilities inspections performed the quarter following the vegetation work. CEHE performs an annual inspection of the whole transmission system to identify hazardous trees or other vegetation issues that need immediate attention. Additional inspections may be performed in selected areas as warranted by conditions or situations conducive to increased tree mortality or risk exposure.

Additionally, when advance notice of a hazardous fire conditions are issued by the local Fire Marshal that could involve transmission ROWs and facilities, mowers are dispatched to reduce brush within the ROWs along with herbicide contractors to apply fire retardants to the bases of the Company's towers and structures to mitigate or reduce potential fire damage.

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.

Annex E

Hurricane Annex

HURRICANE ANNEX

A. Introduction

This annex provides a framework for the activation of the EOP for both a system-wide and partial system hurricane response. Hurricane events that may cause disruption to the area's electric service are varied and unpredictable as to severity and portion of the system affected.

In order to activate the plan, clear communication must be provided to all personnel involved in the planning, response and recovery phases supporting the restoration of electric service.

Electric Operations leadership, or authorized designees, shall have the following responsibilities:

- Activating the EOP when a system-wide storm emergency situation exists or a threat is imminent
- Directing all operations once the EOP is activated
- Keeping the President and Chief Executive Officer of CNP informed of system conditions, activities, and progress towards restoration of electric power under the EOP

B. Pre-Storm Preparation

Hurricane Drill

To promote familiarity with the EOP, a general hurricane drill exercise is outlined below. When possible, this exercise coincides with the State Hurricane exercises to provide increased realism. Mock hurricane advisories are communicated similar to those given by the local National Weather Service (NWS) during an actual storm. These notifications are designed to test tracking and activation procedures. These advisories are given regularly during the exercise. Minor disruption of some regular employee activities is anticipated but there are no line crews engaged.

The primary objectives are:

- Testing the communications involved with activation of the Emergency Operations Plan;
- Testing employee information systems:
    - Corporate email
    - Corporate employee hotline
- Evaluating pre-season preparations;
- Verifying knowledge of specific EOP duty assignments;

- Activating the Incident Command Center in the Greenspoint Annex ;
- Activating the Distribution, Transmission and Substation, and the Energy Control Evaluation Centers;
- Utilizing recommendations from previous exercises and events to test and practice Storm EOP procedures;
- Evaluating implementation of Incident Command processes and procedures;
- Simulating media and regulatory reports; and
- Simulating damage assessments and restoration schedules between evaluation centers, and posting them in a test version of Outage Tracker.

If the annual Company functional exercise coincides with the State of Texas hurricane exercise and the City of Houston and/or the Harris County Office of Homeland Security and Emergency Management have activated their Emergency Operations Centers, then the Company will also test communication techniques with those entities.

EOP Storm Roster

The Employee Storm Roster (ESR) is a web-based application that has been developed in house in SAP to help:

- Manage Storm EOP assignments for Company personnel
- Manage and track mutual assistance and contract personnel
- Manage lodging facilities required during a storm event

A process is in place to manage the assignment of personnel as employees are hired, transferred or leave the Company. Employees are encouraged to log into ESR at any time to update and review their EOP-related information as needed. Employees can access ESR by clicking on the "Employee Storm Roster" button on the Company's internal website.

Hurricane Vacation Policy

During Hurricane Season (June 1st through November 30th), when an EOP event is declared, no vacation requests will be approved for Operations staff in CEHE and Houston Gas who serve in Storm Rider and First Responder roles, including critical support functions. Furthermore, vacations already scheduled during the restoration period may be cancelled by management, and no new vacation requests will be authorized.

If a non-operations employee has a planned vacation, but an EOP event is declared prior to the start of that vacation, the employee is expected to talk to his or her EOP leader and direct supervisor. The EOP leader and the employee's direct supervisor have the discretion to allow the employee to take the vacation as planned or deny the time off based on the criticality of his or her EOP role.

If an employee is already on vacation and out of town at the time the Company declares a storm EOP event, the employee is not expected to immediately return to fill his/her EOP role. Upon returning from vacation the employee is expected to immediately report for EOP duty in the designated role. If the vacationing employee is in town, he or she is expected to return to work immediately to fulfill his or her EOP assignment, and any unused vacation may be rescheduled after the Company returns to normal operations.

If the employee is denied the time away from work and suffers financial loss directly associated with the vacation, such as airline tickets, hotel/condo rental, tour or cruise expenses, he or she shall submit a request for reimbursement to the Company's designated Human Resource Manager, within 10 days after being relieved of EOP duties. The request will be reviewed by management and a decision made within 30 days after the final day of the EOP event.

Employee Responsibilities

If the Company activates the EOP because of a threat to the continuation of electric service to our customers, employees may be called upon to change job assignments prior to and/or during service restoration. There will be a plan for employees to be released for final storm preparation prior to a Storm EOP event and lodging planned for "First Responders" with established criteria will be communicated by local management.

Business continuity during an EOP is critical. All employees, whether in their normal job or an EOP assignment, are essential to successful service restoration. The Company values the role each employee plays in serving the needs of our community. Employees are expected to:

• Understand their roles and responsibilities.

• Understand that the primary reporting relationship during the EOP is to the assigned EOP Leader. Daily assignments during EOP will be determined by the EOP Leader and employees may be asked to take on different assignments as needs change during the service restoration process.

• Participate in the annual EOP Drill, training, and other planning activities as required.

• Make the necessary personal pre-storm preparations to be ready and available to perform the EOP assignment.

• Establish storm plans with their families in advance to ensure employees are prepared to report as directed and to fully execute their assignments during EOP.

• Maintain a hard copy of important phone numbers, including EOP contacts, immediate supervisor, CNP Storm Mailbox (which provides general information during EOP) and the HR Hotline (which provides employee assistance).

• Be aware that employees in "Day 1" assignments will not be allowed to leave the greater Houston area once EOP is declared (72 hours or less until storm landfall).

• Make their management aware of any special needs that may impact their ability to report to duty for EOP assignments, in advance of EOP activation.

• Understand that employees are ultimately responsible for their own personal safety and that of their families and take appropriate actions to ensure a safe and timely execution of their roles and responsibilities in the EOP.

• Maintain current contact information in Employee Service Roster (ESR) and ensure their EOP Leader and immediate supervisor have the most current information.

• Notify immediate supervisor and EOP Leader throughout the year and during EOP assignment, if necessary, of any change in personal needs or responsibilities that may affect their ability to fulfill their EOP assignment. Examples could include: change in residence, phone numbers, or fitness for duty.

• Establish and maintain contact with immediate supervisor and EOP Leader in the event of EOP activation and throughout the active period.

• Recognize EOP assignments will require working extended hours with shifts ranging from 10 to 16 hours per day, seven days a week. Some assignments require long periods of exposure to all weather conditions, walking several miles a day, standing for hours, or taking vehicles off road.

• Recognize that failure to report to duty as scheduled or failure to fully execute the EOP assignment may subject employees to disciplinary action, up to and including termination of employment.

C. INITIAL STORM ACTIVATION

Basis of activation

The Company determines when it activates the EOP and response activities based on StormGeo data on the anticipated intensity of the event. The StormGeo program issues trigger reports every six hours leading up to the event. These reports help determine the appropriate course of action. The Company uses the following phases to guide the actions to be taken but the Incident Commander has the authority to deviate from these guidelines:

Trigger parameter	Phase
Response Plan Activator (RPA) is positive *	1
The Worst Case Scenario (WCS) for 39 mph winds reaching this location is < 120 hours and the probability of 58 mph Wind Impacting (PWI) this location is > 8%	2
The WCS for 39 mph winds reaching this location is < 96 hours and the PWI of 58 mph at this location is > 15%	3
The WCS for 39 mph winds reaching this location is < 72 hours and the PWI of 58 mph at this location is > 20%	4
The WCS for 39 mph winds reaching this location is < 66 hours and the PWI of 58 mph at this location is > 25%	5
The WCS for 39 mph winds reaching this location is < 60 hours and the PWI of 58 mph at this location is > 25%	6
The WCS for 39 mph winds reaching this location is < 54 hours and the PWI of 58 mph at this location is > 25%	7
The WCS for 39 mph winds reaching this location is < 48 hours and the PWI of 58 mph at this location is > 30%	8
The FTA for 39 mph winds reaching this location is < 36 hours and the PWI of 58 mph at this location is > 50%	9

Activation Alerts

The Company has a three level alert system for weather and system conditions which are used in operations and are not exclusive to a hurricane , storm, weather related or other event. These three EOP levels are designed to ensure sufficient resources are available to effectively respond to any type of event impacting CEHE's service territory. The Company is beginning to implement three activation levels in 2021.

The following is a summary of the alert levels that may be activated, based on the needs, during a specific type of event:

EOP Level 1:

- Short duration or low impact event affecting the entire CEHE service territory
- Severe impacts to only a specific area of the CEHE service territory
- Additional support roles may be needed

EOP Level 2:

- Medium duration and impact event
- Severe impacts to multiple areas of the CEHE service territory
- Additional support roles needed

EOP Level 3:

- High duration and impact event
- Severe impacts to all or nearly all areas of the CEHE service territory
- All support roles needed unless otherwise notified
- Individual department emergency plans and/or business continuity plans initiated as needed, and Corporate Response Plan activated as appropriate

Regardless of the EOP level declared, employees must be prepared to respond. Employees should connect with their supervisor and know their EOP role if any level of EOP is declared. If necessary and called upon, management is encouraged to release their employees from their normal responsibilities to assist in the EOP response. Since emergency events can change quickly, employees should be prepared to escalate response is necessary. Employees who have an electric storm assignment that requires participation in both response activities, and any drills will be contacted by their EOP storm response leader and provided with EOP instructions on where to report. For those who do not currently have a role, the EOP team will make assignments after determining where assistance is most needed.

Evacuation and Re-Entry Procedures

In the event of a storm, the Galveston and Baytown Service Centers evacuate in conjunction with activation of the evacuation plans of Harris and Galveston Counties. The Galveston Service Center evacuates to the South Houston Service Center, and the Baytown Service Center evacuates to the Humble Service Center. All CNP personnel that live in evacuation zones and that also have Day 1 or Day 2 EOP Storm assignments will be offered lodging by the Company, so that they can be readily available for duty immediately after a storm. The Company has worked with local emergency officials and the State of Texas Phased Re-entry Plan to obtain written permissions and to facilitate/expedite the movement of restoration resources into evacuated areas for the purpose of restoring power.

Toll Road Procedures

A key route utilized to access portions of the Company's service area is the Harris County Toll Road system. The following procedures have been put in place to address usage:

The Security Branch Director will contact the Harris County Toll Road Authority (HCTRA) to obtain approval from Harris County Commissioners Court for a specific start and end time that restoration vehicles can utilize the toll roads "toll" free. Providing license plate information is imperative to this process.

In the event of a storm:

1. Fleet will send a list of the license plate information for any rental vehicles to Corporate Security as soon as possible.
2. Fleet will send a list of the license plate information for Houston-area fleet vehicles and trailers.
3. Service Area Managers will provide a list of the license plate information for any EOP responders needing access to the toll roads and submit it to the Security Branch.
4. Check-in Support at the staging sites will gather CNP personnel license plate information and submit it to Corporate Security.
5. During check-in of mutual assistance crews at staging sites:
6. Check-in Support will verify any license plate information provided on the rosters and attach CNP decals near the back license plate (such as on the bumper below license plate or on the tailgate above license plate) on each non-CNP vehicle.
7. If license plate information is not provided, Check-in Support will record license plate numbers and the state issued for mutual assistance vehicles and trailers.
8. Site administrators will send these lists to the Security Branch via fax or email.
9. The Security branch will send the license plate information to HCTRA for entry into their system to automate the "No Fine" process.

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**

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

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**

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.

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

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

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

- 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

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.

- 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.

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

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

Annex G

Physical Security Incident Annex

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.

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

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?

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.

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.

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.

Annex H

Mobile Generation Annex

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.*

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)