



Filing Receipt

Received - 2022-10-31 01:50:25 PM
Control Number - 53385
ItemNumber - 804

**Ammper Power, LLC
Emergency Operations Plan
Executive Summary**

Executive Summary:

As a registered Retail Electric Provider (REP), Ammper Power, LLC ("Ammper") is required to develop, maintain, and utilize (when necessary) an Emergency Operations Plan (EOP), pursuant to the requirements set forth in the PUCT Rule § 25.53. Ammper has developed this plan to comply with the PUCT Rule, the applicable NERC Reliability Standards, as well as ensure a greater likelihood of continued operations during an emergency. Beginning in 2023, this plan must be updated annually by March 15 as required by Section 25.53(c)(3). At all times, the most recent approved copy of the Ammper Power Emergency Operations Plan must be available at the Ammper's main office for PUCT inspection.

For Ammper, the PUCT has ordered the following information be included and/or addressed in the Emergency Operations Plan:

- Approval and Implementation Section [25.53(d)(1)] (Page 3 of EOP)
- A Communication Plan [25.53(d)(2)] (Page 3 of EOP)
- A Plan for Maintenance of Pre-identified Supplies for Emergency Response [25.53(d)(3)] (Page 8 of EOP)
- A Plan that Addresses Staffing during Emergency Response -25.53(d)(4) (Page 6 of EOP)
- A Plan that Addresses how the REP Identifies Weather-Related Hazards, including Tornadoes, Hurricanes, Extreme Cold Weather, Extreme Hot Weather, Drought, and Flooding and the Process Used to Activate the EOP [25.53(d)(5)] (Pages 8-9 of EOP)
- List of primary and, if possible, backup emergency contacts [25.53(c)(4)(B)] (Page 9 of EOP)
- A Record of Distribution [25.53(c)(4)(A)] (Page 9 of EOP)
- Affidavit stating the following [25.53(c)(4)(C)(i-vi)] (Pages 7-10 of EOP):
 - Relevant operating personnel are familiar with and have received training on the applicable contents and execution of the EOP, and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency [25.53(c)(4)(C)(i)];
 - The EOP has been reviewed and approved by the appropriate executives [25.53(c)(4)(C)(ii)];
 - Drills have been conducted to the extent required by subsection (f) of the rule [25.53(c)(4)(C)(iii)];
 - The EOP or an appropriate summary has been distributed to local jurisdictions as needed [25.53(c)(4)(C)(iv)];
 - The entity maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident [25.53(c)(4)(C)(v)]; and
 - The entity's emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events have received the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System training [25.53(c)(4)(C)(vi)].
- **Annexes to be included in the EOP** - A Retail Electric Provider (REP) must include:

- A pandemic and epidemic annex [25.53(e)(3)(A)];
 - Annex F
- A hurricane annex that includes evacuation and re-entry procedures if facilities are located within a hurricane evacuation zone, as defined by TDEM [25.53(e)(3)(B)];
 - Annex L
- A cyber security annex [25.53(e)(3)(C)];
 - Annex-AP-EOP-001 Cyber Security
- A physical security incident annex [25.53(e)(3)(D)]; and
 - Annex-AP-EOP-001 Physical Security Plan
- Any additional annexes as needed or appropriate to the entity's particular circumstances
- Drills [25.53(f)]
 - Annex B

As a registered REP, it is Ammper's intent to fully comply with all requirements of the Public Utility Commission of Texas.

Record of Distribution:

<u>Title</u>	<u>Name</u>	<u>Date of Access to Training</u>	<u>Date of Training</u>
VP & General Manager	Juan Ignacio Romo García	09/26/2022	10/03/2022
Operations Manager jr.	Angel Gustavo Cedillo Jiménez	09/26/2022	10/03/2022
Operations Deputy Director	Erick Omar Morales Domínguez	09/26/2022	10/03/2022
Integral Management System Manager	Andrés Jesús Sánchez Rodríguez	09/26/2022	10/03/2022
IT Director	Néstor Francisco Flores Mendoza	09/26/2022	10/03/2022
Operations Director	Sergio Luna Quiroz	09/26/2022	10/03/2022

Emergency Operations Plan

Ammper Power, LLC

Version 1.0

Effective Date: October 1, 2022

This Emergency Operations Plan (AP-EOP-001) is developed to comply with PUCT Rule 25.53

Contents

Approval and Implementation	3
Communication Plan	3
Amnmp Power Emergency Operations Contact List.....	5
Amnmp Power Internal Emergency Operations Contact List.....	5
Definitions and Acronyms	6
Executive Summary	7
Staffing During Emergency Response	7
A hurricane annex	7
Affidavit	8
PUC Filing Requirements	9
Annual Review	10
Annual Drill	11
A cyber security annex	12
A physical security incident annex.....	12
A pandemic and epidemic annex.....	12

Approval and Implementation [25.53(d)(1)(A)]**Introduction:**

- This EOP is developed to help ensure Ammpower Power, LLC's ("Ammper") (REP Certificate No. 10310) continued operations, as a Retail Electric Provider ("REP"), in the event of emergency conditions, including, but not limited to pandemic(s) or severe weather. This plan includes the necessary elements, pursuant to PUCT Rule § 25.53.

The following individuals are responsible for maintaining the EOP and have the authority to change the EOP pursuant to § 25.107(d)(1)(B).

Name	Title	Date
Juan I. Romo	VP & General Manager	07/05/2022
Gustavo Cedillo	Assistant Manager, Operations	07/05/2022

- The revision control summary below lists the dates of each change made to the EOP since the initial EOP filing pursuant to paragraph (1) of this subsection [25.53(d)(12)(C)].

Version	Approval Date	Effective Date	Revision Summary
1.0	10/01/2022	10/01/2022	Initial Emergency Operations Plan

EOP 1.0 was effective as of 10/01/2022. EOP Version 1.0 was approved on 10/01/2022 and supersedes all previous EOPs.

Communication Plan [25.43(d)(2)]

An entity that is a registered REP must describe the procedures during an emergency for communicating with:

- Public
 - Customer Communications
 - Customer communication procedures during an emergency will be overseen by Ammpower's Vice President & General Manager, Juan I. Romo. Prior to an impending emergency and through the method authorized in customer contracts, Ammpower will proactively contact customers who are on variable rate or indexed rate plans that could be financially impacted by the emergency, such as in the case of extreme hot or cold weather that will be reasonably expected to increase demand. Ammpower will advise customers of the potential impact to customers' bills and encourage curtailment of usage as appropriate to minimize charges. During an emergency, Ammpower will abide by the same methods of customer communication contemplated by customer contracts. If an alternate

method of emergency communication is established during an emergency, Ammper will contact customers via email. Ammper will proactively contact customers to set expectations for billing of charges incurred during the weather event, including any allowance for delayed payment.

- OPUC
 - Ammper will communicate status of the EOP, when in use, to the Office of Public Utility Counsel (“OPUC”) (see communication table)
- Media outlets
 - Ammper has identified a communication structure (press relations/spokesperson, internal and external communications) for responding to a local or global crisis. In a crisis Ammper will control the communication with the media, with only the appointed spokesperson, who has been trained for this purpose, and is authorized to speak to journalists.
- PUCT
 - Ammper will communicate status of the EOP, when in use, to the PUCT (see communication table)
- ERCOT
 - Ammper will communicate status of the EOP, when in use, to ERCOT (see communication table)
- Public
 - Communication with the public during an emergency will be overseen by Ammper’s Vice President & General Manager, Juan I. Romo, or his designee. Ammper will proactively communicate with the public as appropriate by strategically selecting the best medium for communication under particular circumstances, i.e., website postings, social media, and radio and television media, etc.
- Procedures for Handling Complaints during an Emergency
 - All customers will be provided and instructed to call a 24/7 hotline (855)-255-8609 to report any complaints. Customers will be able to leave a detailed voice message, which will be returned within 24 hours. The hotline will also be posted prominently on Ammper’s website and social media accounts.

Ammper Power Emergency Operations Contact List

EMERGENCY OPERATIONS CONTACT LIST (EXTERNAL)			
NAME	ENTITY	PHONE NUMBER	EMAIL
OPUC	OPUC		
PUCT	PUCT		
PUCT Infrastructure Staff			
ERCOT (Client Services Rep)	ERCOT		
Ammper Power Management	Ammper Power		

Ammper Power Internal Emergency Operations Contact List

INTERNAL AMMPER POWER EMERGENCY OPERATIONS CONTACT LIST			
NAME	ENTITY	PHONE NUMBER	EMAIL
ERCOT Operations Desk	Ammper Power		
Customer Care	Ammper Power		
Legal	Ammper Power		
Ammper Power Management	Ammper Power		

Definitions and Acronyms

TERM	ACRONYM	DEFINITION
<u>Annex</u>		A section of an emergency operations plan that addresses how an entity plans to respond in an emergency involving a specified type of hazard or threat.
<u>Drill</u>		An operations-based exercise that is a coordinated, supervised activity employed to test an entity's EOP or a portion of an entity's EOP. A drill may be used to develop or test new policies or procedures or to practice and maintain current skills.
<u>Electric Reliability Council of Texas</u>	ERCOT	Independent System Operator for approximately 90% of the state of Texas.
<u>Emergency</u>		A situation in which the known, potential consequences of a hazard or threat are sufficiently imminent and severe that an entity should take prompt action to prepare for and reduce the impact of harm that may result from the hazard or threat. The term includes an emergency declared by local, state, or federal government, or ERCOT or another reliability coordinator designated by the North American Electric Reliability Corporation and that is applicable to the entity.
<u>Entity</u>		An electric utility, transmission and distribution utility, PGC, municipally owned utility, electric cooperative, REP, or ERCOT.
<u>Hazard</u>		A natural, technological, or human-caused condition that is potentially dangerous or harmful to life, information, operations, the environment, or property, including a condition that is potentially harmful to the continuity of electric service.
<u>Public Utility Commission of Texas</u>	PUCT	The PUCT is the regulatory body for energy entities in the state of Texas.
<u>Qualified Scheduling Entity</u>	QSE	Submit bids and offers on behalf of resource entities (REs) or load serving entities (LSEs) such as retail electric providers (REPs).
<u>Retail Electric Provider</u>	REP	A Retail Electric Provider (REP) sells electric energy to retail customers in the areas of Texas where the sale of electricity is open to retail competition. A REP buys wholesale electricity, delivery service, and related services, prices electricity for customers, and seeks customers to buy electricity at retail.
<u>State Operations Center</u>	SOC	The SOC is operated by TDEM on a 24/7 basis and serves as the state warning point.
<u>Texas Department of Energy Management</u>	TDEM	coordinates the state emergency management program, which is intended to ensure the state and its local governments respond to and recover from emergencies and disasters and implement plans and programs to help prevent or lessen the impact of emergencies and disasters.
<u>Threat</u>		The intention and capability of an individual or organization to harm life, information, operations, the environment, or property, including harm to the continuity of electric service.

Executive Summary

As a registered REP, Ammper is required to develop, maintain, and utilize (when necessary) an Emergency Operations Plan pursuant to the requirements set forth in the PUCT Rule § 25.53. Ammper has developed this plan to comply with the PUCT Rule and, if required, any applicable NERC Reliability Standards, as well as ensure a greater likelihood of continued operations during an emergency. Beginning in 2023, this plan must be updated annually by March 15 as required by § 25.53(c)(3). At all times, the most recent approved copy of the Emergency Operations Plan must be available at Ammper Power's main office for PUCT inspection.

For a REP like Ammper the PUCT has ordered the following information be included and/or addressed in the Emergency Operations Plan:

Staffing During Emergency Response

A plan that addresses staffing during emergency response. Ammper Power has identified appropriate staff and staffing levels to respond to emergency conditions in accordance with Annex C, including, but not limited to severe weather events, physical threats or physical damage, and cyber security events.

Additionally, those identified in Annex C are the operational and management staff that will remain on call or on stand-by for the duration of the emergency. This list may be dynamic and will be subject to change should conditions warrant it.

Evidence - Annex C should be completed to reflect a staffing plan for emergency events. Secondary evidence would consist of dated emails or documented evidence that staff was notified and understood their expectations during this event.

A hurricane annex that includes evacuation and re-entry procedures if facilities are located within a hurricane evacuation zone, as defined by TDEM;

In the event of a hurricane, the first priority is always the health and safety of Ammper personnel. Ammper's hurricane response process is listed below:

- Ensure all Ammper personnel and any potentially affected public personnel are not in danger.
- By using the evacuation routes in the link below, Ammper personnel must evacuate at a time recommended by local authorities.
- Ammper's facilities should be hardened, to the extent possible, against lasting damage from a hurricane. Some of these hardening details are listed below:
 - Ensure any loose material or equipment is secured, as applicable.
 - Ensure proper draining channels exist and are functional, as applicable.

Ammper Power facilities in [Region 1](#), as specified by TDEM, shall use the hurricane [evacuation routes](#) published by the Texas Department of Transportation.

Ammper Power facilities in [Region 2](#), as specified by TDEM, shall use the hurricane [evacuation routes](#) published by the Texas Department of Transportation.

Ammper Power facilities in [Region 3](#), as specified by TDEM, shall use the hurricane [evacuation routes](#) published by the Texas Department of Transportation.

Ammper Power facilities in [Region 4](#), as specified by TDEM, shall use the hurricane [evacuation routes](#) published by the Texas Department of Transportation.

Ammper Power facilities in [Region 5](#), as specified by TDEM, shall use the hurricane [evacuation routes](#) published by the Texas Department of Transportation.

Ammper Power facilities in [Region 6](#), as specified by TDEM, shall use the hurricane [evacuation routes](#) published by the Texas Department of Transportation.

Checklist(s) for Ammper Power personnel to address emergency events

Ammper shall use the checklist in Annex C to identify which personnel shall address events that arise during the emergency.

Evidence - Complete Annex C and document any actions taken to address any vulnerabilities found and addressed while completing the checklist.

Plan to Maintain Pre-Identified Supplies for Emergency Response

Ammper recognizes that in the event of an emergency, certain supplies are crucial to maintain its operational functions. To ensure Ammper's operations can continue during an emergency, Ammper has established the following plan to ensure pre-identified supplies are available:

Annually, Ammper will audit its office(s) to ensure that the pre-identified supplies below are available and functioning. If any necessary supplies are missing or not properly functioning, Ammper will immediately replace the supplies as necessary. Ammper will begin its supply audits by April 1 of 2023.

- Laptops, laptop chargers, backup batteries, wireless internet hotspots, first-aid kits, emergency non-perishable food supplies, bottled water, emergency blankets.

Plan to address how Ammpower identifies weather-related hazards:

Ammper has established the following plan for identifying the following weather-related hazards that will trigger activation of the EOP: Ammpower has subscribed to weather alerts and emergency alerts to identify when severe weather-related hazards are forecast or occurring. These severe weather-related hazards include tornados, hurricanes, extreme hot weather, extreme cold weather, droughts, and floods. The EOP will be activated in response to any of the aforementioned weather events at the discretion of Ammpower and any emergency response personnel.

Affidavit from an owner, partner, officer, manager, or other official with responsibility for Ammpower Power's operations affirming that all relevant Ammpower Power operating personnel are familiar with the contents of the emergency operations plan; and such personnel are committed to following the plan except to the extent deviations are appropriate under the circumstances during the course of an emergency.

Completed, executed, and notarized Annex A.

PUC Filing Requirements

Ammper Power must file an emergency operations plan (EOP) and executive summary pursuant with the PUCT submission and reporting requirements.

- An entity must file with the commission:
 - an executive summary that:
 - describes the contents and policies contained in the EOP;
 - includes a reference to specific sections and page numbers of the entity's EOP that correspond with the requirements of this rule;
 - includes the record of distribution required under paragraph (4)(A) of this subsection; and
 - contains the affidavit required under paragraph (4)(C) of this subsection; and
 - a complete copy of the EOP with all confidential portions removed.
- For an entity with operations within the ERCOT region, the entity must submit its unredacted EOP in its entirety to ERCOT.
- In accordance with the deadlines prescribed by paragraphs (1) and (3) of this subsection, an entity must file with the commission the following documents:
 - A record of distribution that contains the following information in table format:
 - titles and names of persons in the entity's organization receiving access to and training on the EOP; and

- dates of access to or training on the EOP, as appropriate.
- A list of primary and, if possible, backup emergency contacts for the entity, including identification of specific individuals who can immediately address urgent requests and questions from the commission during an emergency.
- An affidavit from the entity's highest-ranking representative, official, or officer with binding authority over the entity affirming the following:
 - relevant operating personnel are familiar with and have received training on the applicable contents and execution of the EOP, and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency;
 - the EOP has been reviewed and approved by the appropriate executives;
 - drills have been conducted to the extent required by subsection (f) of this section;
 - the EOP or an appropriate summary has been distributed to local jurisdictions as needed;
 - the entity maintains a business continuity plan for responding to epidemics or pandemics, addressing return-to-normal operations after disruptions caused by the event; and
 - the entity's emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events have received appropriate training.

Annual Review

An entity must continuously maintain its EOP. Beginning in 2023, an entity must annually update information included in its EOP no later than March 15 under the following circumstances:

- An entity that in the previous calendar year made a change to its EOP that materially affects how the entity would respond to an emergency must:
 - file with the commission an executive summary that:
 - describes the changes to the contents or policies contained in the EOP;
 - includes an updated reference to specific sections and page numbers of the entity's EOP that correspond with the requirements of this rule;
 - includes the record of distribution required under paragraph (4)(A) of this subsection; and
 - contains the affidavit required under paragraph (4)(C) of this section;
 - file with the commission a complete, revised copy of the EOP with all confidential portions removed; and
 - submit to ERCOT its revised unredacted EOP in its entirety if the entity operates within the ERCOT power region.
- An entity that in the previous calendar year did not make a change to its EOP that materially affects how the entity would respond to an emergency must file with the commission:

- a pleading that documents any changes to the list of emergency contacts as provided under paragraph (4)(B) of this subsection;
- an attestation from the entity's highest-ranking representative, official, or officer with binding authority over the entity stating the entity did not make a change to its EOP that materially affects how the entity would respond to an emergency; and
- the affidavit described under paragraph (4)(C) of this subsection.

Annual Drill

An entity must conduct or participate in at least one drill each calendar year to test its EOP. Following an annual drill, the entity must assess the effectiveness of its emergency response and revise its EOP as needed. If the entity operates in a hurricane evacuation zone as defined by TDEM, at least one of the annual drills must include a test of its hurricane annex. An entity conducting an annual drill must, at least 30 days prior to the date of at least one drill each calendar year, notify commission staff, using the method and form prescribed by commission staff on the commission's website, and the appropriate TDEM District Coordinators, by email or other written form, of the date, time, and location of the drill. An entity that has activated its EOP in response to an emergency is not required, under this subsection, to conduct or participate in a drill in the calendar year in which the EOP was activated.

By applying the Emergency Operations Drill Instructions and completing Annex B, Ammper's Emergency Operations Plan shall be tested each year, no later than December 1st, and includes a review section, to identify and correct any vulnerabilities in the Emergency Operations Plan. Ammper's Emergency Operations Drill Procedure has a section dedicated to any applicable facility that is located within a defined hurricane evacuation zone.

Evidence - Emergency Operations Drill documentation, instructions, Annex B, attendance/participation records with dates and names.

As a registered REP, Ammper shall provide ERCOT with any updated versions of their EOP by **June 1** for any updates made between November 1 and April 30, and by **December 1** for any updates made between May 1 through October 31. Ammper shall submit all updated plans electronically. Annex I is the attestation ERCOT requires for notification, along with the EOP.

Evidence - Electronic copy or screenshot of successful submittal to ERCOT (Annex I and complete plan, should there be any updates).

A cyber security annex;

- The Ammper Power Cyber Security Incident Response Policy (Annex J) contains this information.

A physical security incident annex;

This section contains reporting for physical threats to any Ammper facility, as well as actual damage to or destruction of any Ammper facility.

Please see Annex G - Ammper Power Physical Security Plan (CIP-003)

A pandemic and epidemic annex;

Ammper's existing pandemic/epidemic plan for business continuity is listed in Annex F.

ATTACHMENT B - EMERGENCY OPERATIONS DRILL
Section 2.2.1

[illegible]

	VULNERABILITIES AND ISSUES IDENTIFIED & CORRECTIVE ACTIONS
1.	<p>The following are the vulnerabilities identified during the assessment:</p> <ul style="list-style-type: none"> Weak Password Policy: The current password policy requires passwords to be at least 8 characters long, containing uppercase letters, lowercase letters, numbers, and special characters. However, it does not enforce a minimum age or complexity score, leading to weak passwords being used. Lack of Multi-Factor Authentication (MFA): MFA is not implemented for all users, particularly for administrative accounts, increasing the risk of unauthorized access. Outdated Software: Several critical applications and operating systems are outdated, leaving known vulnerabilities unpatched. Insecure Configuration: Default configurations for several services were found to be insecure, allowing for potential exploitation. Data Backup Vulnerability: Backups are performed regularly, but there is no encryption for backup data, and recovery procedures are not fully tested. User Privilege Management: Excessive privileges are assigned to some users, and there is no regular review of user roles and permissions. Insufficient Logging and Monitoring: Critical system events are not logged, and there is no real-time monitoring for suspicious activity. Physical Security Gaps: Physical access controls to server rooms are basic, and there is no strict policy regarding device usage in sensitive areas. Third-Party Vendor Risk: No formal process exists to assess the security posture of third-party vendors who have access to internal systems. Disaster Recovery Plan (DRP) Outdated: The DRP has not been updated in over two years and lacks specific runbooks for various disaster scenarios. Security Awareness Training Lacking: Employees receive minimal training on security best practices, making them susceptible to social engineering attacks. Insider Threat Mitigation Weak: There are no effective measures in place to detect or prevent insider threats, such as data exfiltration by employees. Cloud Security Misconfigurations: Cloud storage buckets are publicly accessible due to misconfigurations, exposing sensitive data. API Security Weaknesses: Many APIs lack proper authentication and authorization mechanisms, posing a risk to integrated services. Mobile Device Management (MDM) Inadequate: Mobile devices used by staff are not managed centrally, increasing the risk of data loss if lost or stolen. Supply Chain Vulnerabilities: Dependencies on external libraries and services are not monitored for updates or security issues. Incident Response Process Unclear: Roles and responsibilities during an incident response are not clearly defined, leading to confusion. Compliance Gaps: The organization does not perform regular audits to ensure compliance with relevant standards like ISO 27001 or GDPR. Wireless Network Security Weak: Wi-Fi networks use WPA2-Personal instead of enterprise-grade WPA3, which is less secure. BIOS/Firmware Updates Neglected: BIOS and firmware updates are often overlooked, leaving hardware-level vulnerabilities unaddressed. Email Security Measures Basic: Only basic spam filtering is in place, with no advanced email security solutions like DMARC or SPF enforcement. IoT Device Integration Risks: IoT devices connected to the network are not secured, potentially acting as entry points for attackers. Vendor Access Controls Missing: Vendors who need access to systems do not undergo background checks or have limited, time-bound access. Configuration Drift Not Monitored: Changes to system configurations are not tracked, leading to drift from the baseline state. Service Availability Concerns: Redundancy for critical services is limited, increasing the risk of downtime. Open Source Software (OSS) Licenses Ignored: OSS licenses are not reviewed for legal or security implications. Network Segmentation Poor: Different departments share the same network segment, increasing the blast radius of an attack. Endpoint Protection Signature-Based Only: Endpoint protection relies solely on signature-based detection, missing zero-day exploits. Business Continuity Planning (BCP) Limited: BCP focuses only on IT recovery and does not consider broader business operations. Security Toolset Outdated: Existing security tools are old versions, possibly missing newer threat signatures and features. Penetration Testing Frequency Low: Penetration tests are conducted annually, which may not catch new vulnerabilities that emerge. Account Lockout Policies Inconsistent: Some accounts have strict lockout policies, while others do not, creating inconsistent security across the environment. SSL/TLS Certificate Management Manual: Managing SSL certificates manually increases the risk of expired certificates going unnoticed. Database Security Weak: Database servers have default settings, and sensitive data is not encrypted at rest. Containerization Security Oversight: Containers used for application deployment are not scanned for vulnerabilities. Zero Trust Architecture Not Implemented: The organization follows a perimeter-based security model instead of Zero Trust principles. Security Metrics Not Tracked: Key performance indicators (KPIs) for security are not tracked to measure improvement over time. External Attack Surface Unknown: A comprehensive inventory of the organization's external attack surface is missing. Insider Activity Monitoring Absent: There is no monitoring for unusual behavior or data access patterns by internal users. Secure Development Lifecycle (SDLC) Not Enforced: Developers do not follow mandatory security checks before deploying code. Threat Intelligence Feeds Not Utilized: The organization does not leverage external threat intelligence feeds for proactive defense. Incident Escalation Path Unclear: The path for escalating incidents to management or external responders is unclear. Security Roles and Responsibilities Undefined: Specific security roles like Security Analyst, Incident Responder, etc., are not formally defined. Legacy System Decommission Delayed: Legacy systems that are no longer supported are kept running, introducing unnecessary risk. Supply Chain Transparency Low: Lack of visibility into the supply chain makes it difficult to identify risks from upstream providers. AI/ML Model Security Unaddressed: If AI/ML models are used, their security and integrity are not verified. Cryptocurrency Wallet Security Weak: Any cryptocurrency wallets held by the organization are not stored securely. Blockchain Data Integrity Not Verified: If blockchain technology is used, data integrity verification processes are missing. Quantum Computing Preparedness Zero: No plans exist for mitigating risks posed by future quantum computing breakthroughs. Biometric Authentication Rollout Slow: Biometric authentication, which offers stronger security than passwords, is not widely adopted. Geographical Distribution of Assets Not Considered: Assets located in different geographical regions are not protected against localized disasters. Legal and Regulatory Requirements Not Fully Met: Certain industry-specific regulations might not be fully adhered to. Security Culture Not Strongly Embedded: Security is seen as an IT department responsibility rather than a shared organizational culture. Emergency Contact List Outdated: The contact list for emergency response teams is outdated and inaccessible. Disaster Communication Plan Missing: A clear communication plan for disasters is missing, hindering coordination during crises. Insurance Coverage Gaps: Cyber insurance coverage might be insufficient to cover potential losses from a major breach. Reputation Management Strategy Lacking: A strategy to manage the organization's reputation in case of a public security incident is lacking. Stakeholder Engagement Minimal: Regular engagement with stakeholders to understand their security needs and concerns is minimal. Competitive Advantage Through Security Not Leveraged: Security is not leveraged as a competitive advantage through certifications or transparent reporting. Future-Proofing Investments Low: Investments in emerging security technologies are low, putting the organization at risk of obsolescence. Global Incidents Response Capability Limited: The organization's ability to respond to global incidents quickly and effectively is limited. Supply Chain Resilience Not Assessed: The resilience of the supply chain in the face of disruptions is not assessed. Ethical Hacking Program Not Formalized: An ethical hacking program is not formalized to proactively find weaknesses. Security Research Community Engagement Low: Engagement with the security research community for knowledge sharing is low. Public Disclosure Policy Unclear: A clear policy on how and when to disclose security incidents to the public is unclear. Board Level Security Oversight Weak: The board of directors does not have strong oversight on security matters. Executive Buy-In for Security Initiatives Limited: Getting executive buy-in for large-scale security initiatives is challenging. Security as a Service (SecaaS) Adoption Slow: Adopting SecaaS models for faster deployment of security solutions is slow. Automated Compliance Checks Not Implemented: Automated checks for compliance with standards are not implemented. Security Skills Gap Significant: There is a significant gap in specialized security skills among the workforce. Talent Acquisition Focus on General IT Skills: Recruitment focus is more on general IT skills than specialized security talent. Retention Strategies for Security Experts Lacking: Retention strategies for top security experts are lacking. Knowledge Transfer Mechanism Absent: A formal mechanism for transferring knowledge between team members is absent. Mentorship Program Not Established: A mentorship program to guide junior staff by experienced professionals is not established. Cross-Functional Collaboration Encouraged: Encouraging collaboration between different functional areas to address security holistically is encouraged. Regular Cross-Team Exercises Conducted: Regular exercises involving multiple teams to simulate complex incidents are conducted. Documentation Standardized: All security-related documentation follows a standardized template and format. Version Control Used for Configs: Version control systems are used to manage configuration files and scripts. Immutable Infrastructure Principles Applied: Principles of immutable infrastructure are applied where feasible. Infrastructure as Code (IaC) Practices Followed: IaC practices are followed for consistent and repeatable deployments. Secrets Management Solution Deployed: A dedicated secrets management solution is deployed to handle credentials and keys. CI/CD Pipeline Securely Configured: CI/CD pipelines are securely configured to prevent unauthorized changes. Deployment Frequency Monitored: Deployment frequency is monitored to ensure stability and quick rollback capabilities. Rollback Procedures Well Defined: Clear and well-defined rollback procedures are in place for failed deployments. Performance Testing Integrated: Performance testing is integrated into the development lifecycle to catch bottlenecks early. Load Balancing Effectively Utilized: Load balancing is effectively utilized to distribute traffic and prevent overload. Scalability Plans Documented: Scalability plans are documented for handling increased demand or traffic spikes. Resource Allocation Flexible: Resource allocation is flexible enough to scale up or down based on requirements. Budgeting Transparent: Budgeting for IT resources is transparent and aligned with strategic goals. ROI Calculation for Tech Investments: ROI calculation is attempted for major tech investments to justify costs. Vendor Negotiation Skills Strong: Strong negotiation skills are used when dealing with vendors to get better terms. Contract Review Thorough: Contracts with vendors are thoroughly reviewed before signing. SLA Agreements Strictly Enforced: SLA agreements with vendors are strictly enforced to ensure service quality. Exit Strategies Planned: Exit strategies are planned for key vendors to avoid dependency and ensure continuity. Internal Audit Function Active: Internal audit function is active and provides regular reviews and recommendations. External Audit Partnerships Established: Partnerships with external audit firms are established for periodic assessments. Audit Findings Promptly Addressed: Audit findings are promptly addressed with corrective actions. Transparency in Reporting Maintained: Transparency is maintained in reporting financial and operational metrics. Stakeholder Meetings Regular: Regular meetings are held with stakeholders to discuss progress and challenges. Communication Channels Open: Open communication channels are available for feedback and suggestions. Feedback Loop Effective: An effective feedback loop is in place to learn from mistakes and improve processes. Change Management Process Robust: A robust change management process ensures controlled and documented changes. Risk Register Actively Maintained: A risk register is actively maintained to track and mitigate potential risks. Risk Assessment Methodology Consistent: A consistent methodology is used for assessing risks across the organization. Risk Tolerance Levels Clearly Defined: Risk tolerance levels are clearly defined and communicated throughout the organization. Contingency Plans Tested: Contingency plans are regularly tested to ensure they work as intended. Business Impact Analysis (BIA) Conducted: BIA is conducted to understand the impact of various types of disruptions. Recovery Time Objectives (RTO) Set: RTOs are set for critical business functions to guide recovery efforts. Recovery Point Objectives (RPO) Set: RPOs are set to determine acceptable data loss during recovery. Disaster Drill Scheduled Annually: Disaster drills are scheduled annually to test the overall disaster recovery plan. Post-Drill Debriefs Conducted: Post-drill debriefs are conducted to analyze what went well and what needs improvement. Lessons Learned Incorporated: Lessons learned from drills and incidents are incorporated into future planning. Continuous Improvement Mindset Cultivated: A mindset of continuous improvement is cultivated across all teams. Innovation Encouraged: Innovation is encouraged to find new ways to solve problems and improve efficiency. Pilot Programs Used Before Full Scale: Pilot programs are used to test new initiatives before full-scale implementation. Small Wins Celebrated: Small wins are celebrated to motivate the team and show progress. Recognition Program Implemented: A recognition program is implemented to reward exceptional performance. Employee Wellness Programs Offered: Employee wellness programs are offered to support mental and physical health. Diversity and Inclusion Efforts Continued: Diversity and inclusion efforts are continued to foster a inclusive workplace. Sustainability Goals Aligned: Sustainability goals are aligned with the organization's overall mission and vision. Green IT Initiatives Implemented: Green IT initiatives are implemented to reduce environmental impact. Carbon Footprint Calculated: Carbon footprint is calculated to measure the organization's environmental impact. Renewable Energy Sources Explored: Renewable energy sources are explored for powering operations. Waste Reduction Programs Initiated: Waste reduction programs are initiated to minimize environmental waste. Water Conservation Measures Taken: Water conservation measures are taken in offices and facilities. Energy Efficiency Audits Conducted: Energy efficiency audits are conducted to identify areas for improvement. Smart Building Technologies Adopted: Smart building technologies are adopted to optimize resource usage. Community Engagement Activities Participated: Participation in community engagement activities to give back. Philanthropic Contributions Made: Philanthropic contributions are made to support social causes. Supplier Ethics Guidelines Enforced: Supplier ethics guidelines are enforced to ensure responsible sourcing. Human Rights Policies Adhered To: Human rights policies are adhered to in all business operations. Anti-Corruption Measures Strengthened: Anti-corruption measures are strengthened to maintain integrity. Whistleblower Protection Mechanisms In Place: Whistleblower protection mechanisms are in place to encourage reporting. Code of Ethics Widely Promoted: Code of ethics is widely promoted and understood by all employees. Leadership Commitment Visible: Leadership commitment to ethical values is visible through actions. Regular Ethics Training Provided: Regular ethics training is provided to reinforce values. Transparent Decision Making Process: A transparent decision-making process is followed for major decisions. Stakeholder Input Sought Regularly: Stakeholder input is sought regularly to inform decision making. Clear Lines of Accountability Established: Clear lines of accountability are established for all roles. Empowerment of Employees Encouraged: Empowerment of employees is encouraged to take ownership of their work. Collaborative Work Environment Fostered: A collaborative work environment is fostered for better teamwork. Open Office Spaces Preferred: Open office spaces are preferred to facilitate interaction and idea exchange. Virtual Meeting Options Available: Virtual meeting options are available for flexibility and cost savings. Flexible Working Hours Offered: Flexible working hours are offered to accommodate different lifestyles. Remote Work Policies Clearly Defined: Remote work policies are clearly defined and consistently applied. Hybrid Work Models Explored: Hybrid work models are explored to balance office and remote work. Office Ergonomics Checked Regularly: Office ergonomics are checked regularly to prevent injuries. Healthy Snacks Provided: Healthy snacks are provided to boost morale and productivity. Gym Memberships Subsidized: Gym memberships are subsidized to promote employee fitness. Mental Health Support Offered: Mental health support is offered through counseling services. Financial Wellness Programs Introduced: Financial wellness programs are introduced to help employees manage finances. Life Events Assistance Provided: Assistance is provided for life events like marriage, childbirth, etc. Employee Assistance Program (EAP) Utilized: EAP is utilized to provide confidential support for employees. Regular Check-ins with Managers: Regular check-ins are held between managers and team members. One-on-One Sessions Encouraged: One-on-one sessions are encouraged for career guidance and feedback. Peer-to-Peer Mentoring Program Started: A peer-to-peer mentoring program is started to facilitate learning. Career Development Paths Identified: Career development paths are identified for each role. Skills Gap Analysis Conducted: Skills

[illegible]

ATTACHMENT C - EMERGENCY STAFFING SCHEDULE
Section 2.1.1.6

[illegible]

Pandemic & Epidemic Business Continuity Plan

Ammper Power, LLC

Version 1.0

Effective Date: 10/01/2022

Contents

EXECUTIVE SUMMARY & APPROVAL.....	3
INTRODUCTION.....	4
Epidemic and Pandemic Procedure.....	4
CRITICAL BUSINESS FUNCTIONS.....	7
PLAN ACTIVATION PROCEDURES	10
PLAN DEACTIVATION.....	12
Employee Contact List:	14
Review and Approval	16

EXECUTIVE SUMMARY**Introduction:**

After evaluating recent responses to pandemics and epidemics, Ammper Power, LLC ("Ammper") has developed this Pandemic Response Plan (PRP) to address business continuity challenges presented by pandemics or epidemics. This PRP provides a framework, guidance, and details operations to support Ammper's efforts to continue and/or rapidly restore critical business functions in the event of a disruption to normal operations. This plan includes an overview of continuity operations, outlines the approach for supporting Ammper's critical business functions, and defines the roles and responsibilities of staff. It also outlines the orders of succession, notification procedures, communication methods, plan activation and deactivation protocols, provisions for alternate work locations, and the plan for maintaining and restoring access to vital records.

This plan establishes procedures and processes to maintain operational continuity for businesses based on the loss of services due to a reduction in workforce (e.g., during pandemic Covid-19).

The following individuals are responsible for maintaining, implementing, and revising the PRP.

Name	Title	Permission(s)
Juan I. Romo	VP & General Manager	Approval
Gustavo Cedillo	Assistant Manager, Operations	Edits, updates, maintenance

- The revision control summary below lists the dates of each change made to the EOP since the initial EOP adoption.

Version	Approval Date	Effective Date	Revision Summary
1.0	09/26/2022	10/01/2022	Initial Pandemic and Epidemic Response Plan

As of 10/01/2022, EOP Version 1.0, approved on 10/01/2022, and supersedes all previous PRPs.

INTRODUCTION

Overview:

Continuity of Operations planning ensures Ammper is able to maintain or quickly resume performing critical business functions, which are the functions that support the organization's mission, comply with legal requirements, and support safety under all contemplated circumstances, to the extent possible. The benefit of this planning includes the ability to anticipate response actions following a pandemic or epidemic, improve the performance of its operations facilities, and ensure timely recovery.

Plan Scope & Applicability:

The Ammper PRP is applicable once the safety of employees, customers, and guests has been verified. It can be active during normal business hours and after hours, with and without warning.

Plan Objectives:

The objective of the Ammper PRP is to facilitate the resumption of critical operations and functions in a timely and organized manner to ensure a viable and stable organization. The primary objectives of the plan are to:

- Maintain Critical Business Functions during the pandemic or epidemic
- Adjust business functions to address staffing issues and safety
- Ensure employees are able to safely perform work remotely, where applicable and appropriate
- Protect vital records

Plan Assumptions:

The following assumptions were used while creating this plan:

- An event has occurred that affects normal business operations.
- Access to Ammper facilities may be limited.
- Qualified personnel are available to continue operations.

Epidemic and Pandemic Procedure

Affected Employee

1. Notify immediately to the Organizational Development Manager (ODM), Office Manager (OM), and/or Integrated Management System Manager (IMSM).
2. Leave the facilities and seek medical attention or isolate if it is not possible to leave facilities.

Control Room Operator

1. Notify immediately the Control Room Head and OMD that a control room operator may have a contagious disease
2. Get instructions on how to isolate and where to go. It may be necessary to go to the hospital or another place where is safe to isolate

3. Notify all employees, if possible, with whom the affected employee has had contact
4. Prohibit any visitors to any contaminated area until it has been disinfected

Plan Management

1. Notify all employees who may be at risk of getting infected, e.g., those who had contact or shared equipment or areas with the affected employee.
2. Provide frequent updates (as necessary), regarding the pandemic situation and events in company.
3. Distribute information regarding symptoms, protective measures, and how to control and prevent the disease.
4. Contact health authorities to determine whether it is an active case within the country or an isolated event.
5. Implement communications, procedures, as necessary regarding how to prevent and detect the contagious disease and what to do.
6. To all Staff:
 - a. Minimize staff levels to only critical personnel necessary to maintain Ammper's operations
 - b. Implement customized shift arrangements (split shifts and/or segregated work locations).
 - c. Implement home office and remote operations and support as needed.
 - d. Suspend in-person group meetings and use instead Microsoft Teams and other corporate communication mediums.
 - e. Restrict use of common areas to the capacity recommended by health professionals, e.g., 50% of total capacity to ensure sufficient social distance to avoid disease transmission.
 - f. If recommended by health professionals, register symptoms of all visitors and employees
 - g. Suspend all non-critical planned maintenance activities and drills.
 - h. Purchase supplies in greater quantities to reduce supply runs, when applicable.
 - i. Require contractors to utilize protocols to reduce disease transmission and share with them internal procedures if a visit to facilities or meetings are needed.
 - j. Review access control to restricted areas to allow only the necessary persons.
 - k. Reduce in-person authorizations and encourage written authorizations and permits e.g., by email or other electronic communication mediums).
 - l. Place disinfection gel or spray and sanitization products in facilities and provide to personnel in shared areas
 - m. Sanitize workplace and devices at start and end of each shift, mainly those who are shared. Use gloves for cleaning activities and any required Personal Protective Equipment ("PPE").
 - n. Avoid sharing work tools and computer devices
7. Isolation measures
 - a. Avoid travel when it is not strictly necessary (travels must be informed to ODM).
 - b. Lockdown control room entrance door.
 - c. Visitors will not be allowed to enter operational control room(s).
 - d. Consider alternative transportations methods to avoid crowded places and peak times.
 - e. If needed, each person will bag their own trash and dispose exiting the facility.
8. Supplies
 - a. Double or triple inventory levels of mandatory PPE, e.g., masks, sanitizer, etc.
 - b. Ensure enough supply of water and food.

- c. Determine the need to purchase extra operational supplies (e.g., Diesel).
9. Communications
 - a. All communications will be performed using methods to limit or avoid contact.
 - b. All meetings must be remote, when possible, consider using Microsoft Teams, Zoom or cellphones
10. External Resource Options

Consider changes in:

 - a. Accounting – process payables, spending limits, reporting periods and format
 - b. Communication – internal/external communication, VPN
 - c. Digital – Laptops, connectivity, information security.
 - d. Human Resources – assist with staffing needs.
 - e. Legal – Terms and conditions, guidelines
 - f. Internal Control -physical entry control

Mitigation plan

Implement additional hygiene measures, consider isolation measures for internal employees, limit access to control rooms to only essential personnel, immediately report any sign of illness.

Ammper's facilities and its restricted areas are controlled against unauthorized access as described below:

Access	Entry Control	Necessary People	Description
Head Office	Building Access Control	8 Directors	Visitors must register at the front desk to get access to the organization's offices
Data Center	Building Access Control + Access Control System	None	Key card access control to authorized personnel
Operation rooms	Building Access Control + Access Control System	4 Control Room Operators	Key card access control to authorized personnel
Archive	Building Access Control + Access Control System	None	Key card access control to authorized personnel
PPE warehouse	Building Access Control + Key	None	Key card access control to authorized personnel

General Response plan

1. Any employee that finds themselves ill or notices someone with contagious symptoms, must notify the ODM of the event.
2. The ODM must communicate immediately with appropriate human resource staff and if necessary and proper external personnel with whom the infected person had contact and notify local authorities if applicable.

3. Preventive measures and constant communication regarding the disease will be communicated to all staff by the ODM and other authorized persons.
4. Once the facilities are under control and there are no potential threats, workers will be notified to return to normal operations.

CRITICAL BUSINESS FUNCTIONS

Overview:

Critical business functions are those functions and critical activities that Ammpower Power must maintain when there has been a disruption to normal operations, to sustain the mission of the organization, comply with legal requirements and support safety. The following sample bullets should be used to define business practices and operations during such periods:

- Function - Enter the specific function that may need to be resumed.
- Business Process to Complete - Write a high-level description of the function process. Include any specific forms or systems that may be needed. Supporting Activities
- Supporting activities - Those tasks performed to achieve a critical business function and should be described.
- Lead Point of Contact (POC) and Alternate - Identify and include contact information, if necessary, for staff POCs for each supporting activity.
- Vendors and External Contacts - Identify and include contact information, if necessary, for vendor POCs for each supporting activity.
- Vital Records - Vital Records are those records a business needs to sustain the mission of the organization and comply with legal requirements. Vital records must be stored in multiple places in multiple formats. The identification, protection, and ready availability of vital records needed to support essential functions are critical components of a successful PRP.
- Maximum Allowed Downtime - Identify the amount of time your business could afford for the function to be down before it could cause irreparable harm. Consider using the following units:
 - Less than 24 hours
 - 1 day to 1 week
 - 1 to 2 weeks
 - 2 to 4 weeks
 - 30 days or greater
- Criticality - Enter High, Medium, or Low depending on how critical the function is to the operations of your business. Following are some considerations to use when determining criticality:
 - What business objective/goal does this function support?
 - How often does this function occur?
 - How many business units (departments) or people perform this function?
 - Does the successful completion of this function depend on any other functions?
 - Are other functions dependent on this function for its successful completion?
 - Is there a potential for revenue loss if this function is not completed?
 - Is there a potential for fines, litigation, additional downtime, or other punishment for noncompliance due to a regulatory requirement (PUCT, NERC, or ISO)?
 - What priority ranking would you give this function as compared to other functions?

Required Resources:

- People: Identify the number of employees required for this function. Also identify if a staggered resumption of employees is an option.
- Equipment: Identify the type of equipment and how many would be required in order to get this function back in operation.
- Supplies: Identify any unique supplies required for this function (do not list items that could be easily purchased from an office supply store). This would include any paper forms or documents needed.
- Information Technology: Identify software (e.g., Microsoft Office, QuickBooks, etc.), systems, applications, and electronic documentation needed to complete the function.
- Interdependencies: List other business functions this function relies on to be operational.

Identification of Staff Required to Continue Business Operations:

In the event of a pandemic or epidemic, work absences, due to medical issues attributed to the widespread medical event, can lead to dramatic decreases in productivity, potentially leading to the shutdown of facilities. To maintain the best possible operational posture, it is imperative to communicate duties to the appropriate personnel, helping to ensure Ammper Power's facilities can remain operational to the greatest extent possible. In many cases, employees may log in remotely and perform their duties, fostering as much of an illness-free atmosphere possible, however, there will be the need for onsite staff to maintain and operate facilities, leading to the identification of mission essential staff and reporting structures. Ammper's senior management will identify those mission- essential individuals and will communicate tasks to them. As each case may differ, there will be no "One-size-fits-all" approach, and each response to a pandemic or epidemic will require its own set of responsible personnel and tasks. It is imperative that all possible measures are taken to keep Ammper Power staff from contracting or spreading the illness. Maintaining social distancing, where appropriate and possible, wearing proper PPE, and maintaining hygienic work and living spaces is crucial to combatting a widespread medical event. Depending on the nature of the event, the measures below may serve to facilitate the continued operations of Ammper Power facilities:

- Wearing of PPE
 - Masks (N-95 or similar)
 - Social distancing
 - Proper hygiene
 - Eye, face, hand, or other protection (as applicable)
- Remote work, where appropriate and possible
- Encourage the use of approved medications and/or vaccine(s)

TABLE 1

Ammper Power Critical Business Function				
Critical Business Function 1: Market Operations				
Business Process To Complete: Operations process, confirm access to ISO website and company information cloud, First of all in headquarters and as a backup in another remote location.				
Supporting Elements				
Supporting Activities (Describe)	Lead POC	Vendors and External Contacts	Vital Records	Maximum Allowed Down Time
	Alternate			Criticality
Bids and offers	Operations Manager	ERCOT, and any client main contact	All information needed must be in company cloud	Less than 5 hours
	Operations Subdirector			High
Trading	Operations Manager	ERCOT,	All information needed must be in company cloud	Less than 5 hours
	Operations Subdirector			High
Reporting	Operations Manager	ERCOT, and any client main contact.	All information needed must be in company cloud	Less than 12 hours
	Operations Subdirector			High
Implications if not Conducted: Interruption and/or loss of this function would interrupt market operations. Furthermore, it would result in a delay of the capability of communicating with ERCOT. Operations interruption may cause a market default or a breach of contract with some of our customers				
Calendar Dependent: (e.g., this function is always occurring, this function only occurs in summer months, this function is active during inclement winter weather, etc.). The activities listed above occur every day and some depend on contracted conditions by costumers.				
Required Resources: Staff, equipment, supplies, Information Technology, and other resources. IT equipment				
Facilities: Standard office space that can accommodate up to 2 people at any time. Traditional office equipment and space for phones, computers, etc., with network access to Internet, radio, and other telecommunications services.				
Supporting Partners: List private sector or public sector supporting partners.				

Vital Records: *List relevant vital records and their location, if appropriate.*

PLAN ACTIVATION PROCEDURES

Plan Activation During Normal Business Hours:

If it is determined that the facility cannot be reinhabited, the ODM, OM, or designee will inform personnel on next steps. Employees may be instructed to go home to await further instructions or move to an alternate site. Further communications, such as instructions on where and when to report for work will be made using communication methods such as email, phone calls, texts, or other communication methods.

Plan Activation Outside Normal Business Hours:

If an event occurs outside normal business hours that renders a facility uninhabitable, the ODM, OM or designee will activate the PRP using email, phone calls, texts, or other communication methods.

Actions upon Activation:

Upon activation of the PRP, the ODM, OM or designee will be responsible for notifying all affected personnel of their duties and where they will be performing those duties (remotely or at a site).

ORDERS OF SUCCESSION AND DELEGATIONS OF AUTHORITY

Overview:

Orders of succession are prepared to provide clarity of senior leadership roles in the event that individuals in these roles, whether they be decision-making or management roles, are unavailable due to effects of a pandemic or epidemic. A delegation of authority provides successors with the authorization to act on behalf of critical positions within the organization for specific purposes and duties during emergency circumstances.

Orders of Succession:

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

Delegations of Authority:

Delegations of authority are the authorization to act on behalf of critical positions within the organization for specific purposes and duties. In order to ensure the rapid response to any situation requiring the activation of a PRP employees who serve in key senior leader positions must develop and maintain pre-delegated authorities for policy determinations and decisions, as needed. The delegations of authority

Annex F power

Annex F - AP-EOP-001-Pandemic Response Plan

should include what type of authority is being delegated, such as signatory or credit card authorization for purchasing, and also limitations of the delegated authority. All duties of each senior leader are delegated to the position in the orders of succession when the incumbent cannot fulfill that authority for any reason, including but not limited to:

- Absence
- Illness
- Leave
- Death

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

How to Complete the Delegation Table (Table 2)

This table is customizable and has no limit to how much information should be included. Please copy/paste to create a table for each position that must be continually occupied.

Position to be succeeded - This should be the title of the position that will need to be filled in the event a staff member becomes unavailable.

Successors - This should be the title of the position, not an individual, that will need to fill the position identified in the first column. They should be listed in sequential order.

Delegated authorities - These are the task and responsibilities held by the position delineated in the first column.

Activation and termination triggers - Select from incapacitated, unavailable, or selective decision as a reason for activation, per each position. Termination can be identified as sample language suggests or alternations can be made to termination thresholds.

Table 2

Position to be Succeeded	Successors	Delegated Authorities	Activation and Termination Triggers
Operations Manager	Operations Subdirector	Managing, coordinate and do all activities related to ERCOT	<u>Activate:</u> Incapacitated, unavailable. <u>Terminate:</u> Return of Operations Manager
	Operations Analyst	Coordinate and do all activities related to ERCOT	<u>Activate:</u> Incapacitated, unavailable. <u>Terminate:</u> Return of Operations Manager
	General Manager	Managing, coordinate and do all activities related to ERCOT	<u>Activate:</u> Incapacitated, unavailable. <u>Terminate:</u> Return of Operations Manager
	Operations Director	Managing, coordinate and do all activities related to ERCOT	<u>Activate:</u> Incapacitated, unavailable. <u>Terminate:</u> Return of Operations Manager or Subdirector

PLAN DEACTIVATION

Overview:

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

Criteria for PRP Deactivation:

The business owner or designee will determine, based on input from medical authorities, staff, or other entities when it is safe and when the organization is prepared to restore or transfer critical business functions to a facility for long term usage. Critical business functions must be restored in priority sequence based upon the classification and criticality of the function. The following elements are typically completed prior to plan deactivation.

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

Resumption Process:

Provide information as to how each function outlined in Table 3 will be resumed and which staff members need to be active participants in this process.

How To Complete The Plan Deactivation Table - The following information details how to complete elements of Table 3 below. When completing this table, minimize the use of acronyms and describe actions in plain terms so that staff members who may be unfamiliar with the function will be able to use the document to resume and sustain the critical business function, if necessary.

Table 3

Item	Function	Supplies	Required Resources
1	ISO connection	Internet, computer, phone line	Configure connection to ISO Website and confirm communication with ERCOT personnel by phone in headquarters
2	Company information	Internet, computer, phone line	Configure computer to have access to company information cloud in headquarters

14

Table 5

[illegible]



Review and Approval

Gustavo Cedillo	ERCOT Operations Manager
Fernanda Barrios	Organization Development and Communication Manager
Andrés Sánchez	Integrated Management System Manager
Alfonso Mejía	Chief Legal Officer; Safety and Hygiene Committee Head
Juan Ignacio Romo	VP & General Manager

Annex W - Hurricane & Weather- Related Emergencies Plan

Ammper Power, LLC

Version 1.0

Effective Date: 10/01/2022

In the event of a hurricane, the first priority is always the health and safety of Ammper Power, LLC's ("Ammper") personnel. Ammper's Hurricane response process is as follows:

- Ensure all Ammper personnel and any potentially affected members of the public are not in danger.
- By using the evacuation routes at the links below, Ammper personnel must evacuate at a time recommended by local authorities.
- Ammper facilities should be hardened, to the extent possible, against lasting damage from a hurricane. Some of these hardening details are listed below:
 - Ensure all loose material or equipment is secured, as appropriate.
 - Ensure proper draining channels exist and are functional, as appropriate.

Ammper Power facilities in Region 1, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

Ammper Power facilities in Region 2, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

Ammper Power facilities in Region 3, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

Ammper Power facilities in Region 4, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

Ammper Power facilities in Region 5, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

Ammper Power facilities in Region 6, as specified by TDEM, shall use the hurricane evacuation routes published by the Texas Department of Transportation.

Checklist(s) for Ammper's facility personnel to address emergency events

Ammper shall use the checklist in Annex C to identify which personnel shall address events that arise during the emergency.

For re-entry to Ammper's facility, the route should be surveyed, to the extent possible, to gauge safety and accessibility. Should accessibility be obstructed, pre-identified equipment, such as chain saws, tire chains, or other emergency equipment must be on-hand and available to clear a path. At all times, proper

Personal Protective Equipment (“PPE”) must be worn and communication between designated Ampper staff and leadership must be maintained.

Appendix – Cyber Security Emergency Plan

Ammper Power, LLC

Version 1.0

Effective Date: 10/01/2022

Purpose

The Cyber Security Plan defines and addresses the actions and procedures to follow in the event of a cyber security incident.

Identification of a cyber security incident

A cyber security incident is defined as any occurrence that imminently jeopardizes, without lawful authority, the integrity, operation, reliability, or availability of the information or systems that are essential to the daily operation of Ammper Power, LLC ("Ammper").

A cyber security incident can be identified by the following events:

- Attempts to gain unauthorized access to a computer system and/or data.
- The unauthorized use of systems for the processing or storing of data.
- Changes to the firmware, software, or hardware of a system without the consent of the owner of the system.
- Malicious disruption and/or denial of service.
- Programs or systems not running properly.

This list includes some cyber security incidents; however, if Ammper personnel are unsure of a possible event, they must contact and report the incident to the IT department.

Cyber security incident response

Before an incident occurs, the IT team oversees the following activities to be prepared for any emergency:

- Participate in the analysis and updates to which the organization is vulnerable and requires a response procedure and identify critical areas related to security of information.
- Coordinate and/or participate in assessment reviews or prevention activities related to information security.
- Develop and implement testing programs or prevention activities to protect information.
- Verify that the information, resources, or actions to address a cyber security emergency are developed within the organization.
- Coordinate and lead all efforts to address any cyber security emergency.
- Maintaining necessary resource inventory to respond to a cybersecurity emergency, as well as an emergency contact directory.

Once a cyber security event occurs or is identified, immediately notify the following e-mail itsupport@ammper.com or to the following people of the IT department:

- 1.- Nestor Flores - nflores@ammper.com – 844-536-5219
- 2.- Gustavo Cedillo - gcedillo@ammper.com - 469 905 6880
- 3.- Juan I Romo - jromo@ammper.com – 469-462-9895

While particular emergency events may require a particular response, Ammper will generally respond to emergency events as follows:

For any issue that does not affect the operation:

- Report the issue to the following email: itsupport@ammper.com.
- The IT department will analyze the incidents, including triage and prioritization.
- If possible, an immediate solution will be implemented. Preliminary mitigating measures will be implemented if an immediate solution is not possible.
- The IT department is responsible for communicating the status of the incident, according to Appendix 1.

For any issues that affect the operation:

- Report the issue through a call to any member of the IT department mentioned in this document.
- The IT department provides an immediate response to execute or offers alternatives to resume operation
- After any issues are resolved, they will be analyzed to define a definitive approach for future issues.
- The IT department is responsible for communicating the status of the incident until it is closed. Communication is made according to Appendix 1.

Communication Plan

External communication shall be carried out by Ammper emergency personnel according to Appendix 1. Any communication to ERCOT, PUCT, OPUC, media and other entities must preferably be made by Ammper Power's phone lines: (844) 536-5219 or (469) 945-7310. Please refer to Annex 1.

Any internal communication related to cyber security must be addressed through official channels such as the: corporate e-mails or cell phone numbers of the following IT department staff in the following order:

- 1.- Nestor Flores - nflores@ammper.com – 844-536-5219
- 2.- Gustavo Cedillo - gcedillo@ammper.com - 469 905 6880
- 3.- Juan I Romo - jromo@ammper.com – 469-462-9895

Review and Approval

Nestor Flores	IT Director
Gustavo Cedillo	ERCOT Operations Manager
Juan Ignacio Romo	VP & General Manager

APPENDIX 1

EMERGENCY OR EVENT	TYPE	WHO	WHEN	WHAT	HOW
INFORMATION SECURITY INCIDENT	INTERNAL	EMPLOYEES	IN CASE OF EVENT	-GIVE INFORMATION REGARDING THE EMERGENCY -INCIDENTS SOLUTIONS AND FURTHER RECOMMENDATIONS	-EMAIL -BUSINESS COMMUNICATION PLATFORM (TEAMS)
	EXTERNAL	CLIENTS CONTRACTORS NEIGHBORS MEDIA AUTHORITIES	EVENT HAS A HIGH IMPACT IN THE EXTERNALS	-INCIDENTS IMPLICATIONS	-CALL -EMAIL -WHATSAPP
			MASSIVE COMMUNICATION IS NEEDED	-NEED OF MASSIVE COMMUNICATION	-CALL
			ASSISTANCE IS NEEDED	-NEED OF ASSISTANCE / HELP	-CALL -EMAIL

Annex – Physical Security Plan

Ammper Power, LLC

Version 1.0

Effective Date: 10/01/2022

Purpose

This document provides the Physical Security Plan for Ammper Power's, LLC's ("Ammper") facilities in accordance with PUCT Rule § 25.53. This plan describes procedures to identify, plan, respond, prepare, and improve Ammper's response to potential emergencies. This document describes the controls to prevent unauthorized physical access, damage, and/or interference to the organization's information, equipment, and facilities.

Physical Security Procedure

Ammper has implemented physical security controls based on the need to protect facilities and ensure operational continuity to reduce or mitigate the risk of unauthorized access, environmental threats, and to maintain people's and equipment safety.

Physical Entry Controls.

Ammper's facilities and its restricted areas are controlled against unauthorized access as described below:

Access	Entry Control	Description
Head Office	Building Access Control	Visitors must register at the front desk to get access to the organization's offices
Data Center	Building Access Control + Access Control System	Key card access control to authorized personnel
Operation rooms	Building Access Control + Access Control System	Key card access control to authorized personnel
Archive	Building Access Control + Access Control System	Key card access control to authorized personnel
PPE warehouse	Building Access Control + Key	Key card access control to authorized personnel

Physical Security Perimeter.

Ammper implements security perimeters to avoid unauthorized access to restricted areas that contain critical information, equipment, devices, and other assets inside the facilities.

Monitoring

- Access control system (ACS) → Restricted areas area controlled with key card readers. Authorized accesses are monitored and updated monthly.
- Closed-circuit Television (CCTV) video monitoring → Main office space (included restricted areas) is monitored.
- Security patrols → Twice at night, security patrols are performed to verify physical conditions.

General Response Plan

1. Any employee that detects a security breach must notify immediately to the Office Manager ("OM") and Property Security Personnel that a physical security incident has occurred.
2. The OM must communicate immediately the incident to personnel and local authorities, as applicable.

3. Employees must remain inside the secure areas in the event that unauthorized people enter the Head Office. In case of a natural disaster, people should go to the assembly point and follow the indications of the OM or the Emergency Response Team.
4. Once the facilities are under control and there are no potential threats, employees will be notified that the building is safe and clear so that they can enter the facilities and resume their duties. The Communication team will notify workers by corporate email and corporate chat such as Microsoft Teams or other authorized communication programs.

Protecting against external and environmental threats

Below is a list of the various types of threats intended to be addressed under this plan:

- Natural:
 - Earthquakes
 - Lightnings - Electrical storm
 - Fire
 - Hurricanes
 - Flood
 - Extreme winds
 - Tornados
- Technological (failure of systems created by humans):
 - Energy shortage
 - Building Fire – inside facilities or surroundings areas –
 - Any incident or accident inside facilities or on-site visits
 - Water leakage
 - Explosions
 - Aircraft crash
- Social:
 - Labor strike
 - Robbery
 - Terrorism
 - Vandalism
 - Active shooter

To mitigate, prevent, and improve responses to any emergency, personnel in facilities must follow the actions as described below

Ammper Power Personnel

- Ammper's employees must register in the access control system their entries and exits to/from the facilities
- Any danger or insecure activity must be reported immediately to Office Manager (OM) or Manager of the Integrated Management System (MIMS)
- Must act according to each specific emergency program
- Participate in drills as required

- In case of emergency, follow the instructions of trained personnel (Emergency Response Team)

Visitors

- Review security instructions given before entering the facilities
- Must register in system upon arriving at Ammpower facilities

Emergency Alerts

To communicate the emergency, Seismic Alarm Systems (SAS) and Fire Alarm Systems (FAS) have been installed inside the facilities. The SAS will reproduce the seismic alarm sound and the Fire Alarm System will warn people through visual and audio appliances (sound strobe), reproducing repetitively three consecutive loud sounds and intermittent flashes from strobes.

In case of a system failure in the SAS or FAS, the OM or trained personnel must blow a whistle: once for earthquake, three times for fire emergencies. Any other information will be sent by email or internal communication channels as soon as possible.

Requirements

Ammper must maintain an emergency kit inside facilities and at any designated assembly point that includes first aid kit, bottled water, high energy foods, and blankets. Also, fire extinguishers will be kept in all facilities and a generator in case of electrical emergency shortage.

OM and MIMS must have an emergency contact address for employees, and the emergency addresses for fireman, policemen and clients, also an emergency map with evacuation route defined, fire extinguisher location(s) and emergency exits.

Communication Plan

Any external communications, e.g., to ERCOT, the PUCT, OPUC, police, fire department, etc., must be done by the personnel in charge of the emergency.

General

1. All employees and contractors must report any observed security events or weaknesses to the Office Manager and/or IT Team in the case of a cybersecurity emergency.
2. EXTERNAL communication is performed when the emergency or event has an impact or potential to damage Clients, Visitors, Contractors, Neighbors, etc. Communication with the Authorities when they are needed to address the emergency. And communication with Media when it is needed to inform the community/public of potential risks.
3. INTERNAL communication is performed by email or other authorized medium to inform all employees regarding the emergency and instruct them on any necessary actions.

SPECIFIC

SUBANNEX A.1

Review and Approval

Gustavo Cedillo	ERCOT Operations
Guadalupe Roa	Office Manager; Emergency Response Team Leader
Andrés Sánchez	Integrated Management System Manager
Alfonso Mejía	Chief Legal Officer; Safety and Hygiene Committee Head
Juan Ignacio Romo	VP & General Manager

SUBANNEX A.1 AMMPER POWER COMMUNICATION PLAN

EMERGENCY OR EVENT	TYPE	WHO	WHEN	WHAT	HOW (CHANNEL)
EARTHQUAKE	INTERNAL	EMPLOYEES	BEFORE	EMERGENCY PROCEDURES	-VERBAL INSTRUCTIONS -BUSINESS COMMUNICATION PLATFORM (TEAMS)
			DURING	-Alert people (SAS or 1 whistle) - Get up and walk (do not run) towards the safe area (internal assembly point) -Place yourself parallel to the wall, put a hand on the wall to make contact, and stand still or get on your knees until the movement finishes.	-SEISMIC ALARM SYSTEM -WHISTLE
			AFTER	- Follow the instructions of the Emergency Response Unit and OM. - Never evacuate unless the OM gives the specific instruction to evacuate (using the stairs). - Should evacuation of the building is needed, get to the external assembly point.	VERBAL INSTRUCTIONS

Amnper power

Annex -AP-EOP-001 Physical Security Plan

	EXTERNAL	VISITORS CONTRATORS (ON-SITE)	PRIOR TO ACCESS FACILITIES	EMERGENCY PROCEDURES	REGISTER TABLETS EMAIL
		AUTHORITIES CIVIL PROTECTION	AFTER AN EARTQUAKE	NEED OF ASSITANCE / HELP	CALL
FIRE	INTERNAL	EMPLOYEES	BEFORE	> EMERGENCY PROCEDURES	-VERBAL INSTRUCTIONS -BUSINESS COMMUNICATION PLATFORM (TEAMS)
			DURING	-Alert people (FAS or 3 whistles) - Get up and walk quickly (do not run) towards the safe area (internal assembly point). - Follow OM and ERT instructions to evacuate, move or stay inside the building	-FIRE ALARM SYSTEM -VERBAL INSTRUCTIONS
	EXTERNAL	VISITORS CONTRATORS (ON-SITE)	PRIOR TO ACCESS FACILITIES	EMERGENCY PROCEDURES	-VERBAL INSTRUCTIONS -REGISTER TABLETS (MAIL)
		AUTHORITIES FIRE DEPARTMENT CIVIL PROTECTION	DURING A FIRE	NEED OF ASSITANCE / HELP	CALL
STRIKES	INTERNAL	EMPLOYEES (NOT INSIDE)	DURING	-DO NOT APPROACH TO THE BUILDING OR PROTESTERS -STAY ALERT TO COMMUNICATION UPDATES	-EMAIL -BUSINESS COMMUNICATION PLATFORM (TEAMS)

Amnper power

Annex -AP-EOP-001 Physical Security Plan

	EXTERNAL	EMPLOYEES (INSIDE THE FACILITIES)	DURING	-STAY INSIDE THE FACILITIES	CALL
		VISITORS CONTRATORS (ON-SITE)	A VISIT IS PLANNED	-CANCEL APPOINTMENTS/MEETINGS	EMAIL
		POLICE	DURING A STRIKE	NEED OF ASSITANCE / HELP	CALL
ANY OTHER EMERGENCY	INTERNAL	EMPLOYEES	IN CASE OF EVENT	-FOLLOW THE INSTRUCTIONS OF OM and ERTs. -KEEP AN EYE ON YOUR EMAIL, TEAMS AND CELLPHONE FOR INSTRUCTION UPDATES	-EMAIL -BUSINESS COMMUNICATION PLATFORM (TEAMS)
	EXTERNAL	CLIENTS	EVENT HAS A HIGH IMPACT IN THE EXTERNALS	-RECOMMENDATIOS REGADING KEEPING SAFE	-CALL -EMAIL -WHATSAPP
		CONTRACTORS			
		NEIGHBORS			
		MEDIA	MASSIVE COMMUNICATION IS NEEDED		CALL
		AUTHORITIES	ASSISTANCE IS NEEDED	-NEED OF ASSISTANCE / HELP	CALL

Ampper power

Annex -AP-EOP-001 Physical Security Plan

ANY EMERGENCY	EXTERNAL	BUILDING SECURITY/EMERGENCY UNIT	DURING EVENT	-RECIEVE AND FOLLOW INSTRUCTIONS FROM THE BUILDING MANAGEMENT -NEED TO EVACUATE BUILDING -GIVE INFOMRATION REGARDING THE EMERGENCY -GIVE STATUS OF PERSONNEL	RADIO
		SISTERS COMPANIES SECURITY/EMERGENCY UNITS		-RECIEVE AND FOLLOW INSTRUCTIONS FROM THE CORPORATIVE SECURITY MANAGEMENT -GIVE INFORMATION REGARDING THE EMERGENCY -GIVE STATUS OF PERSONNEL	RADIO

Annex W - Extreme Weather- Related Emergencies Plan

Ammper Power, LLC

Version 1.0

Effective Date: 10/01/2022

Preparations for Operations During Extreme Cold Weather Conditions

For severe cold weather, Ammper Power, LLC (“Ammper”) will identify, through inspection, areas of its facility(ies) that may be most vulnerable to malfunction during extreme cold events. Ammper’s staff shall ensure the following:

- Staff will ensure heat tracing is present and functional for all appropriate exposed instrumentation and/or equipment, where applicable.
- Where appropriate and necessary, temporary barriers shall be erected to shield sensitive or exposed equipment and instrumentation from wind and freezing precipitation, etc..
- If needed, temporary barriers may be constructed of plastic sheeting or other material that is sufficient to protect exposed equipment and instrumentation, and may contain, if conditions warrant, a portable heat source to keep temperatures above freezing in the designated area(s).
- Other measures may be taken, as the Ammper facility staff see fit, to protect the facility during an extreme cold weather event.
- Ensure business continuity measures are taken, as appropriate, to continue essential operations during the extreme weather event.

Preparations for Operations During Extreme Hot Weather Conditions

For extreme hot weather, Ammper staff shall ensure the following:

- Proper ventilation is present and functional for any areas where extreme hot temperatures may negatively impact operations, as necessary.
- In addition to this, portable fans may be mobilized to force air around potentially affected areas, as necessary.

In all cases, Ammper’s staff will ensure that any operating equipment that it owns is properly weatherized. This includes the following:

- Ensuring all operational tools are accessible and serviceable and can be remotely accessed, as applicable.
- Ensuring all communications paths are operational.

It is important, after any weather-related emergency, to analyze the performance of the staff and facility(ies), identify any operational failures that occurred (if any), and develop an action plan to address those issues. These issues may include the following:

- A list of equipment that failed during the cold or hot weather event must be identified and addressed. Additionally, any critical failure points identified must

be tracked through the normal maintenance processes to ensure appropriate maintenance has taken place for the identified tool(s) or equipment. Any facility equipment design limits that could limit generator output must be identified and addressed, to the extent possible, to ensure no interruption of operations occurs during an extreme weather event.

- Ammper's staff shall actively monitor all potential extreme weather events that may affect their facilities, to include severe weather and operational circumstances arising from those events. Ammper's staff will continue monitoring weather forecasts and ERCOT operational data to aid in predicting conditions that may impact operations.
- If the facility is located in an area where ingress and egress may be impacted by extreme heat or cold events, it is imperative to ensure entry and egress routes are hardened to the extent possible. Staff must ensure to elevate and/or secure equipment that may be subject to being carried away by flooding, and ensure structures are weatherproofed to the extent possible.

**Ammper Power, LLC
Emergency Operations Drill
Instructions**

Introduction:

It is imperative to consider as many emergency-related issues as possible when developing the tasks for the Emergency Operations Drill (Drill) pursuant to 16 TAC § 25.53(f). Equally as important is determining the appropriate staff to address these issues, timing, contracts (if necessary) and dependencies on external entities, all while maintaining clear and unambiguous instructions. This Drill is designed to help Ammper Power, LLC ("Ammper") address as many of these issues as possible, to ensure the continued operations of its facilities, and the performance of essential tasks during emergency conditions.

Staffing:

All Ammper personnel participating in the Drill will be notified prior to the Drill directly with a clear set of tasks to be completed. Should the tasks need to be performed in a sequential order, appropriate personnel shall be instructed on the timing and order of tasks. For example, if an operator is required to perform an action, it is important to identify adequate staff to complete the necessary tasks to ensure continuous operation of the REP, to the extent possible.

Task Identification:

By identifying the range of tasks that are required for continuous operation in the event of an emergency, Ammper is able to focus on and prioritize critical activities.

Ammper will list all tasks to be performed in Attachment B of the Emergency Operations Plan, as well as assign the tasks to the appropriate personnel. It is important to note that severe conditions may warrant more resources to execute a task than normal operating conditions, so it is imperative that equipment like snow chains (if necessary), de-icing solution(s) for walkways and roads, and extra fuel, etc., are available. Action items will be assigned to personnel (listed by name), a description of the task, date, completion status (for tracking purposes), and any notes or comments taken during the drill.

Sample Tasks:

- Identification/procurement of personnel required to perform tasks.
- Management of transportation for personnel participating in the Drill.
- Establishment of emergency operations communications, cell phones, satellite phones, radios, etc.
- Communication of tasks and continual updates via the communication platforms used in the Drill.
- Procurement and placement of portable heaters and extra fuel (if needed).
- All necessary PPE is on hand and available for staff.
- Establish communication with ERCOT, QSE (if applicable), and regulatory staff at PUCT, to keep them informed of any developing issues that may impact operation of the facility. Communications are covered in the main EOP (AP-EOP-001).
- Ensure proper equipment is on hand and available for clearing paths to the facility, should there be downed vegetation or obstructions (if required).

Review and Correction:

If vulnerabilities or issues were identified during the Drill, appropriate Ammper staff shall conduct a review of the Drill, corrective actions to be taken, and document those corrective actions in Attachment B. This review should include an extent of conditions assessment and root cause analysis to address any latent issues that may exist in other areas.

AFFIDAVIT

STATE OF TEXAS §
 §
COUNTY OF HARRIS §

Before me, the undersigned notary public, on this day personally appeared Juan Bautista Guichard Cortina, to me known to be the person whose name is subscribed to the foregoing instrument, who being duly sworn according to law, deposes and says:

“1. My name is Juan Bautista Guichard Cortina. I am over the age of eighteen and am a resident of Mexico. I am competent to testify to all the facts stated in this Affidavit, and I have the authority to make this Affidavit on behalf of Ammper Power, LLC as the highest-ranking representative, official, or officer with binding authority over Ammper Power, LLC.

2 I swear or affirm that in my capacity as CEO of Ammper Power, LLC I have personal knowledge of the facts as stated in this Affidavit which is given in support of Ammper Power, LLC’s Emergency Operations Plan (“EOP”) submission to the Public Utility Commission of Texas (“PUCT”) and to the Electric Reliability Council of Texas (“ERCOT”) as required by 16 Tex. Admin. Code (“TAC”) § 25.53. I further swear or affirm that all of the statements and/or representations made in this affidavit are true, complete, and correct to the best of my knowledge.

3. I further swear or affirm that relevant operating personnel are familiar with and have received training on the applicable contents and execution of the EOP, and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency.

4. I further swear or affirm that the EOP has been reviewed and approved by the appropriate executives.

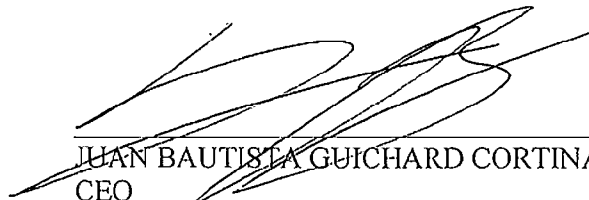
5. I further swear or affirm that Ammper Power, LLC intends to conduct a drill consistent with 16 TAC § 25.53(f) before December 1, 2022 and will provide notice to the Commission at least 30 days before that drill is conducted. Once that drill is conducted, Ammper Power, LLC will notify the Commission.

6. I further swear or affirm that the EOP or an appropriate summary has been distributed to local jurisdictions as needed.

7. I further swear or affirm that Ammper Power, LLC maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident.


8. I further swear or affirm that Ammper Power, LLC’s emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events have received the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training on or before October 1, 2022.”

Further affiant sayeth not.


JUAN BAUTISTA GUICHARD CORTINA
CEO
AMMPER POWER, LLC

SWORN TO AND SUBSCRIBED TO BEFORE ME on the 13th day of October, 2022.

[Affix seal here.]


Notary Public in and for the
State of Texas

