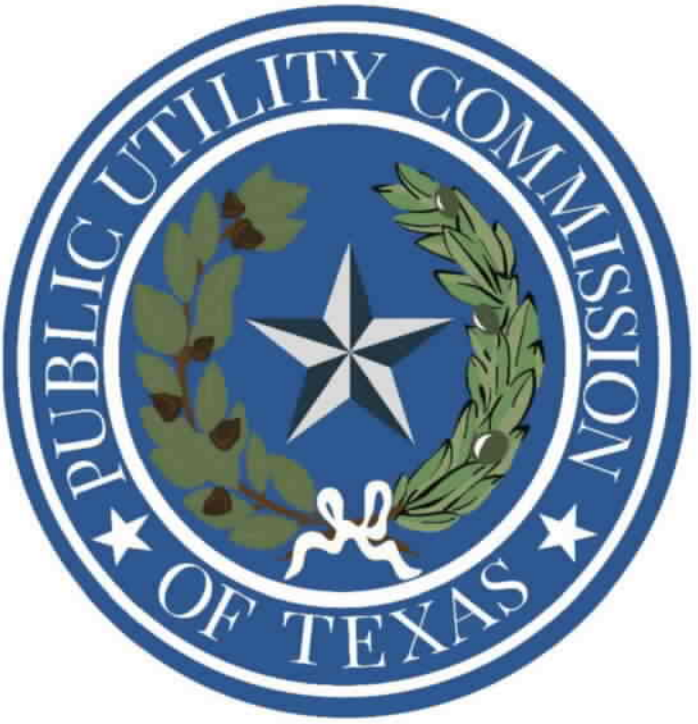

Filing Receipt

Filing Date - 2024-03-08 12:20:16 PM

Control Number - 53385

Item Number - 1833

AE-Telview ESS
Emergency Operations Plan
(PGC No. 20734)[1]

[1] AE-Telview ESS was originally registered with the PUCT as "Goddess Storage ESS".

Table of Contents

Executive Summary

AE-Telview ESS LLC ("AE-Telview") is a Power Generation Company ("PGC") located in Houston, Texas. This Emergency Operation Plan (the Plan) adheres to the requirements set forth by the Public Utility Commission of Texas Electric Substantive Rules, Chapter 25, Section 25.53 – Electric Service Emergency Operations Plans. The Plan addresses AE-Telview's common operational functions that are relevant across emergency types and outlines the entity's response to and policies on specific types of emergencies, including weather related emergencies, restoration of service, cyber security issues, and physical security of the project site.

Record of Distribution

Record of Distribution		
Title	**Name**	**Date of Training on EOP**
SVP Asset Management	Jeffrey Perry	2/14/2024
Director of Interconnection	Richard Labrecque	2/14/2024

Primary and Backup Emergency Contacts (filed separately)

Affidavit

See attached.

Affidavit

AE-Telview ESS, LLC

Agilitas Energy Inc. ("Agilitas Energy") has prepared this Emergency Operation Plan ("EOP") for AE-Telview ESS, LLC ("AE-Telview"). As of the submission of this affidavit, AE-Telview is not yet operational and is still in construction or development. Barrett Bilotta, President and CEO of Agilitas Energy, hereby makes his statement and General Affidavit upon oath and affirmation of belief and personal knowledge that the following matters, facts and things set forth are true and correct to the best of his knowledge:

I, Barrett Bilotta, as Managing Principal of AE-Telview ESS LLC affirm the following:

I. Key operating personnel will be familiar with and will have received training on the applicable contents and execution of the EOP on or before AE-Telview becomes operational, and such personnel will be instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate because of specific circumstances during an emergency,
II. The EOP has been reviewed and approved by the appropriate executives,
III. Drills will be conducted to the extent required by 16 TAC Section 25.53(f),
IV. As appropriate, the EOP or an appropriate summary will be distributed to local jurisdictions as needed,
V. The AE-Telview ESS LLC entity maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident, and
VI. On or before AE-Telview becomes operational, any AE-Telview ESS LLC's emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events will receive (or have received) the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System training.

DATED this the 8th day of March 2024

03/08/2024 10:07 AM CST

Signature of Affiant

Sworn and subscribed before me this 8th day of March, 2024.

03/08/2024 10:11 AM CST

Notary Public in and for
the State of Texas.

JENNIFER B. ROGERS
Notary Public, State of Texas
Notary ID# 124513507
My Commission Expires
MARCH 28, 2027

Online Notary Public. This notarial act involved the use of online audio/video communication technology. Notarization facilitated by SIGNiX®

Approval and Implementation

The AE-Telview ESS LLC Emergency Operation Plan ("EOP") addresses how the entity plans to respond in an emergency involving specific hazards or threats as detailed in Texas Administrative Code, Chapter 25, Substantive Rules Applicable to Electric Service Providers. This EOP will be used to train and advise the relevant operating personnel on the procedures, drills, and protocols in the case of an emergency, including weather emergencies, restoration of service emergencies, and cyber security emergencies.

Jeffrey Perry, SVP Asset Management, is responsible for maintaining and implementing the EOP. Jeffrey Perry and Richard Labrecque, Director of Interconnection have the authority to change the EOP on an as-needed basis. As this is the first filing of this EOP, dated and approved on February 14, 2024, there is yet to be included a revision control summary.

Communication Plan

All key personnel will be informed about the importance of a plan for communication during an emergency. Following are the procedures during an emergency for communicating with the media; the commission; OPUC; fuel suppliers; the applicable reliability coordinator; and local and state governmental entities, officials, and emergency operations centers, as appropriate in the circumstances for the entity.

1. Utilize call tree established between internal primary and backup emergency contacts
2. Establish liaison to communicate with key external organizations and stakeholders; by default this will be Jeffrey Perry, SVP Asset Management.
3. Communicate with primary stakeholders, utilizing external call tree (text, phone, email)
4. Communicate with secondary stakeholders, utilizing external call tree (text, phone, email)
5. Where appropriate, prepare public service announcement
6. Where appropriate, use social media for outreach (website)
7. When the incident is resolved, provide an update through the same channels
8. Within the next 24 hours, prepare an update addressing what happened

Tasks that will be performed on an ongoing basis:

- Establish and test communication channels before an emergency
- Confirm internal points of contact are up to date
- Confirm external points of contact are up to date and upkeep contact information spreadsheet
- Update Communication Plan based on event experience
- Document incident: what happened, what was done, the results and the outcomes

Plan for Maintaining Pre-identified Supplies for Emergency Response

All key personnel will be informed about the importance of a plan for maintaining pre-identified supplies for emergency response. This plan will emphasize the need to ensure the availability of necessary resources during emergencies.

Key aspects of the plan for maintaining pre-identified supplies for emergency response will include:

1. Identification of Essential Supplies:
    - Consistent with best practices for lithium-ion battery projects, prepare a list of specific supplies required for emergency response. Supplies will include:
        A. Personal Protective Equipment (PPE):
            I. Ensure an adequate supply of PPE for personnel involved in emergency response.
            II. PPE may include safety glasses, gloves, flame-resistant clothing, respiratory protection, and any other gear specific to battery-related hazards.
            III. Where appropriate, train personnel on the proper use and maintenance of PPE.
        B. Fire Suppression and Containment:
            I. Where appropriate, have appropriate fire suppression equipment readily available, such as fire extinguishers, fire blankets, and foam-based fire suppression systems.
            II. Where appropriate, establish procedures for containing and controlling fires in and around battery storage areas.
            III. Where appropriate, ensure that fire suppression systems are regularly inspected, maintained, and tested.
        C. Spill Response:
            I. Lithium-ion batteries contain chemicals that can pose environmental hazards if leaked or spilled.
            II. Where appropriate, have spill response kits on hand to address potential chemical spills.
            III. Where appropriate, train personnel on proper spill containment and cleanup procedures, including the use of absorbents and appropriate personal protective equipment.
        D. Emergency Lighting and Communication:
            I. As appropriate, install emergency lighting systems to ensure visibility during power outages or emergencies.

II. Where appropriate, maintain a reliable communication system, including two-way radios, to facilitate coordination and communication among emergency response personnel.

E. First Aid and Medical Supplies:

I. Where appropriate, keep fully stocked and easily accessible first aid kits in designated areas.

II. Include supplies specific to battery-related injuries or chemical exposures.

III. Where appropriate, provide appropriate training to personnel on first aid response and emergency medical procedures.

2. Documentation and Training:
   - Where appropriate, maintain accurate records of emergency response supplies, including inventory, inspection reports, maintenance records, and training documentation.
   - Where appropriate, conduct regular training sessions for personnel involved in emergency response, covering topics such as equipment use, evacuation procedures, and communication protocols.
3. Inventory Management:
   - Where appropriate, establish a system for maintaining an inventory of emergency supplies, including a detailed list of all supplies, including quantities, expiration dates, and storage locations.
   - Regularly update the inventory to ensure accuracy and account for any changes.
4. Storage and Maintenance:
   - Where appropriate, designate appropriate storage areas for emergency supplies.
   - Ensure that storage areas are secure, easily accessible, and protected from environmental factors.
   - Where appropriate, store supplies in a way that allows for easy identification and retrieval during emergencies.
   - Where appropriate, regularly inspect and maintain the supplies to ensure they are in proper working condition and within expiration dates.
5. Restocking Procedures:
   - Determine restocking procedures based on supply usage and expiration dates.
   - Develop a schedule for routine restocking and rotation of supplies.
   - Where appropriate, assign responsibility to specific individuals or departments for restocking activities.
   - Where appropriate, establish relationships with suppliers to ensure timely restocking and availability of emergency supplies.
6. Training and Awareness:
   - As appropriate, provide training to relevant personnel on the importance of maintaining emergency supplies.
   - As appropriate, conduct training sessions on the proper use and storage of specific supplies.

- Promote awareness among employees about the location and purpose of emergency supplies.

7. Documentation and Record Keeping:
    - As appropriate, maintain accurate records of all supply purchases, restocking activities, and inspections.
    - As appropriate, document any supply usage during emergency events.
    - As appropriate, keep records of any maintenance or repairs performed on emergency supplies.
8. Regular Audits and Reviews:
    - Conduct periodic audits of the emergency supply inventory to assess adequacy and identify any gaps.
    - Review the plan for maintaining emergency supplies on a regular basis.
    - Consider feedback from drills, incidents, and lessons learned to make necessary adjustments to the plan.
9. Communication and Coordination:
    - Establish clear communication channels for requesting and accessing emergency supplies.
    - Ensure all relevant personnel are aware of the process for obtaining supplies during emergencies.
    - As appropriate, coordinate with the emergency response team and relevant stakeholders to align supply needs with response strategies.

Plan to Address Staffing During Emergency Response

All key personnel will be informed about the importance of a plan to address staffing during emergency response. This plan will explain the purpose and importance of the plan to address staffing during emergency response, emphasize the need for adequate staffing to effectively manage emergencies and state the objectives of the plan.

Key aspects of the plan to address staffing during emergency response will include:

1. Establish Emergency Response Team:
    - Establish an emergency response team comprising key personnel responsible for managing emergencies.
    - Clearly define roles and responsibilities for each team member. Identify critical roles and responsibilities needed for emergency response.
    - As appropriate, ensure that team members have appropriate training and qualifications for their designated roles.
    - Designate a team leader or incident commander responsible for overall coordination and decision-making during emergencies.
2. Call-out Procedures:

- Establish communication protocols and contact lists for notifying staff members and local consultants during emergencies.
- Include alternate contact methods in case primary methods are unavailable.

3. Communication and Coordination:
    - Establish a communication system to facilitate real-time updates and coordination among staff members during emergency response.
    - As appropriate, use two-way radios, mobile phones, or other reliable communication devices.
    - Define communication channels and protocols to ensure effective information flow.
4. Documentation and Record Keeping:
    - As appropriate, maintain accurate records of staff assignments, contact information, and training certifications.
    - Document staff attendance and involvement in emergency response activities.
    - Keep records of lessons learned and feedback from staff members for continuous improvement.

Plan to Address Weather-related Hazards

All key personnel will be informed about the importance of a plan to address weather related hazards This plan will address weather-related hazards for lithium-ion battery projects and emphasize the importance of identifying and mitigating weather-related risks.

Key aspects of the plan to address weather related hazards will include:

1. Weather Risk Assessment:
    - Conduct a thorough weather risk assessment for Houston Texas, including potential for hurricanes, lightning storms, and floods.
    - Evaluate the potential impacts of these hazards on the lithium-ion battery project.
    - The emergency response team identified above will be responsible for managing weather-related emergencies.
2. Monitoring and Early Warning Systems:
    - Personnel will utilize weather forecasting services to receive early warnings of potential weather hazards and utilize protocols for disseminating weather-related information to project personnel.
3. Hazard Mitigation Measures:
    - Secure battery storage facilities and equipment to withstand severe weather conditions.
    - Implement lightning protection systems to safeguard against lightning strikes.
    - Incorporate flood prevention measures such as proper drainage and elevation.

4. Evacuation Plan:
    - Coordinate with local government authorities to identify evacuation routes and assembly points away from hazardous areas;
    - establish communication methods to account for all personnel during and after evacuation;
    - where appropriate, consider the specific needs of vulnerable individuals, such as those with disabilities or special medical requirements.

Annexes

Weather Emergency Annex

All key personnel will be informed about the importance of operational plans for responding to a cold or hot weather emergency. Given the nature of a lithium-ion battery project, this weather emergency annex does not need verification of the adequacy and operability of fuel switching equipment.

Following is a checklist for generation resource personnel to use during a cold or hot weather emergency response that includes lessons learned from past weather emergencies to ensure necessary supplies and personnel are available through the weather emergency.

1. Weather Preparedness:
    - Monitor weather forecasts and warnings from reliable sources.
    - Stay informed about the specific weather conditions expected during the emergency.
    - Review lessons learned from past weather emergencies and incorporate best practices into your response plan.
2. Personnel Readiness:
    - Ensure that all essential personnel are aware of their roles and responsibilities during cold or hot weather emergencies.
    - Verify contact information for all personnel and establish communication protocols.
    - Conduct training sessions to refresh knowledge on emergency response procedures.
3. Supplies and Equipment:
    - Review and update the inventory of necessary supplies and equipment for cold or hot weather emergencies.
    - Where appropriate, ensure an adequate stock of fuel, lubricants, coolant, and other consumables specific to weather-related operations.
    - Verify the availability and functionality of generators, heating systems, cooling systems, and other critical equipment.
4. Fuel and Power Availability:

- Establish relationships with fuel suppliers and ensure the availability of fuel during weather emergencies.
- Monitor fuel levels and arrange for timely refueling to maintain uninterrupted operation.
- Develop contingency plans for alternative fuel sources in case of disruptions.

5. Heating and Cooling Systems:
    - Inspect and maintain heating systems, boilers, and related infrastructure before the onset of cold weather emergencies.
    - Test and verify the functionality of cooling systems, chillers, and air conditioning units prior to hot weather emergencies.
    - Have backup heating or cooling systems available in case of equipment failures.
6. Safety Measures:
    - Ensure that all personnel are trained on safety procedures specific to cold or hot weather emergencies.
    - As appropriate, provide appropriate personal protective equipment (PPE) for extreme weather conditions.
    - Conduct regular safety inspections and address any identified hazards promptly.
7. Emergency Communication:
    - Establish clear communication channels and protocols for internal and external communications.
    - Ensure that all personnel have access to reliable communication devices, such as radios or mobile phones.
    - Maintain updated contact information for key stakeholders, including emergency services and local authorities.
8. Collaborative Partnerships:
    - Establish partnerships or agreements with local emergency management agencies or organizations.
    - As appropriate, coordinate with utility providers, neighboring facilities, and relevant stakeholders to support mutual aid efforts during weather emergencies.
    - Share lessons learned and best practices with partner organizations for collective improvement.
9. Regular Drills and Exercises:
    - As appropriate, conduct regular drills and exercises to test the response plan and identify areas for improvement.
    - Simulate cold or hot weather emergency scenarios and evaluate the effectiveness of personnel, supplies, and procedures.
    - Document lessons learned from each exercise and incorporate them into future planning and training.
10. Plan Review and Updates:
    - Schedule regular reviews of the emergency response plan, considering feedback, lessons learned, and changes in weather patterns.

- Stay informed about evolving best practices, regulations, and recommendations related to weather emergency response.
- Update the checklist and response plan accordingly to ensure its relevance and effectiveness.

Water Shortage Annex

Given that the AE-Telview ESS project does not use any water, this water shortage annex, which addresses supply shortages of water used in the generation of electricity, is not applicable.

Restoration of Service Annex

The AE-Telview ESS project will develop a systematic process for restoration of service. This process will identify key components of the lithium-ion battery project that may require repair or replacement. The process will also consider the criticality of different system components and prioritize their restoration based on impact and functionality.

AE-Telview ESS key personnel will determine the resources needed for service restoration, such as skilled labor, equipment, spare parts, and materials. These personnel will also develop a mechanism to quickly mobilize resources based on identified priorities.

All restoration of service activities will comply with safety regulations and standards. This includes providing appropriate personal protective equipment (PPE) and ensure its use during restoration operations. This also includes conducting safety assessments and inspections to identify and mitigate potential hazards during the restoration process.

Repair and Replacement Procedures include:

- Developing detailed procedures for repairing and replacing damaged components of the lithium-ion battery project.
- Providing step-by-step instructions for restoration activities, including proper handling and installation of components.
- Ensuring that personnel involved in restoration activities are trained on the specific procedures.
- Establishing protocols for testing and verifying the restored system components.
- Conducting comprehensive testing to ensure the proper functioning and integrity of the restored system.

Pandemic and Epidemic Annex

The AE-Telview ESS project will develop a thorough risk assessment to identify potential risks and vulnerabilities related to pandemics or epidemics. The risk assessment will assess the potential impact on the lithium-ion battery system's operations, workforce, and supply chain.

In the event of a pandemic or epidemic, AE-Telview ESS key personnel will implement a plan that includes the following:

1. Preparedness and Response Team:
    - Establish a preparedness and response team responsible for managing pandemic or epidemic situations.
    - Assign specific roles and responsibilities to team members.
    - Ensure team members are adequately trained on pandemic or epidemic response procedures and protocols.
2. Communication and Information Sharing:
    - Implement a communication plan to disseminate timely and accurate information to project personnel.
    - Establish channels for internal and external communication during a pandemic or epidemic.
    - Stay updated on official guidelines and recommendations from relevant health authorities.
3. Health and Safety Measures:
    - Where applicable, implement health and safety measures to prevent the spread of infectious diseases among the workforce.
    - Promote good hygiene practices such as handwashing, respiratory etiquette, and proper sanitation.
    - Provide personal protective equipment (PPE) as necessary and ensure its proper use and disposal.
4. Workforce Management:
    - Develop a workforce management plan to address potential staffing shortages during a pandemic or epidemic.
    - Identify critical roles and functions and establish backup personnel or cross-training procedures.
    - Implement remote work policies and telecommuting options where feasible.
    - Establish protocols for monitoring employee health and implementing quarantine measures, if necessary.
5. Supply Chain Management:
    - Assess the vulnerabilities in the supply chain and identify alternative suppliers or contingency plans.

- Maintain open lines of communication with suppliers to monitor potential disruptions and delays.
- As appropriate, stockpile critical materials and spare parts to mitigate supply chain disruptions.

6. Facility Operations:
    - Where appropriate, implement enhanced cleaning and disinfection protocols in facilities housing the lithium-ion battery system.
    - Establish procedures for monitoring and responding to suspected or confirmed cases of infectious diseases among on-site personnel.
    - Ensure proper ventilation and air filtration systems to minimize the risk of airborne transmission.
7. Continuity of Operations:
    - Develop a business continuity plan to ensure the ongoing operation of the lithium-ion battery system during a pandemic or epidemic.
    - Identify critical processes and establish contingency plans to maintain essential functions.
    - Test and update the continuity plan regularly to address emerging challenges.

Hurricane Annex

Key personnel for the AE-Telview ESS project will be trained in the importance of preparedness and response to hurricane events. Key personnel will be educated on the vulnerabilities and potential risks to the lithium-ion battery project based on project location and potential impacts.

The AE-Telview ESS Hurricane preparedness and response plan includes the following elements:

1. Preparedness and Response Team:
    - Key personnel will be responsible and accountable for management during hurricane events. These personnel will ensure that team members are trained on hurricane response procedures and protocols.
2. Early Warning Systems and Communication:
    - Establish access to reliable and up-to-date hurricane tracking information from recognized meteorological sources.
    - Develop a communication plan to disseminate timely and accurate information to key project personnel.
    - Establish communication channels for internal and external communication during hurricane events.
3. Facility Readiness:

- The design phase of the project will ensure that the structural integrity of the lithium-ion battery facility can withstand hurricane-force winds and potential flooding.
- Operations and Maintenance (O&M) personnel will secure loose objects, equipment, and materials to prevent them from becoming projectiles during high winds.
- In the design phase and during O&M, AE-Telview ESS personnel will implement flood prevention measures such as proper drainage systems and elevated equipment placement.

4. Supply Chain Management:
    - In advance of any hurricane or weather event, AE-Telview ESS personnel will identify critical supplies, spare parts, and materials required for post-hurricane recovery. This will include a plan for expedited procurement and delivery of necessary supplies post-hurricane.
5. Damage Assessment and Recovery:
    - AE-Telview ESS personnel will develop procedures for conducting post-hurricane damage assessments of the lithium-ion battery system.
    - Personnel will also establish a process for documenting and reporting damages to the facility, equipment, and infrastructure, including a plan for prioritizing and implementing repairs and restoration activities based on the severity of damages.

Cyber Security Annex

All key personnel will be informed about the importance of a plan to address cyber security issues. AE-Telview ESS LLC cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. We have implemented a number of security measures and prepared instructions to help mitigate security risks.

1. Confidential data
    - Confidential data is secret and valuable. Common examples are:
        A. Unpublished financial information
        B. Data of customers/partners/vendors
        C. Patents, formulas or new technologies
        D. Customer lists (existing and prospective)
    - All employees are obliged to protect this data and will be trained on how to avoid security breaches.

2. Protect personal and company devices
    - When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both

their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

A. Keep all devices password protected.
B. Choose and upgrade a complete antivirus software.
C. Ensure they do not leave their devices exposed or unattended.
D. Install security updates of browsers and systems monthly or as soon as updates are available.
E. Log into company accounts and systems through secure and private networks only.

- We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

3. Training
   - All employees will be trained on cyber-security issues upon commencement of employee's job assignment. Employees will receive regular training, via periodic email communication and one-time updates associated with new protocols that must be implemented immediately. Supervisors are responsible for training employees.
   - Training will consistent of the following protocols:
     A. Email safety. Emails often host scams and malicious software (e.g. worms). To avoid virus infection or data theft, we instruct employees to:
        I. Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "Watch this video, it's amazing")
        II. Be suspicious of clickbait titles (e.g. offering prizes, advice)
        III. Check email and names of people they received a message from to ensure they are legitimate
        IV. Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks)
        V. If an employee isn't sure that an email they received is safe, they can refer to our IT Specialist

4. Password Management
   - Password leaks are dangerous since they can compromise our entire infrastructure. To avoid hacking, passwords should remain secure and secret. For this reason, we advise our employees to:
     A. Create their own usernames and personal passwords, not to be shared with others.

B. Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays)
C. Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
D. Exchange credentials only when necessary, in person. When this is not possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
E. Change their passwords every two months.

- Remembering many passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

5. Incident Response
   - In the event of a Cybersecurity Incident, defined as an event that causes a data or privacy breach, the following steps shall apply.
     A. Immediately notify the Managing Principal, with information that identifies and records details regarding the incident.
     B. Personnel involved with the event should follow these steps:
        I. Run scans to detect any viruses or malware.
        II. Review files and folders to check for suspicious activity.
        III. Monitor accounts and credentials for unauthorized changes.
        IV. Perform a traffic analysis.
   - AE-Telview ESS LLC takes cyber security seriously and the Company's Security Incident Response Plan includes immediate escalation to the Managing Principal, who will collaborate with personnel involved in the incident to identify any threats and take steps to contain any infections. AE-Telview ESS LLC will hire a third party to eradicate the threats, recover any affected systems and perform a review to see if there are any lessons that can be learned.

6. Disciplinary Action
   - We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action.
     A. First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
     B. Intentional, repeated or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

- Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.
- AE-Telview ESS LLC retains the right to monitor employees for excessive or inappropriate use of their cell phones. If an employee's phone usage causes a decline in productivity or interferes with our operations, we'll ban that employee from using their cell phones.
- Employees may face severe disciplinary action up to and including termination, in cases when they:
    A. Cause a security breach.
    B. Violate our confidentiality policy.
    C. Cause an accident by recklessly using their phones.

Physical Security Incident Annex

Key personnel for the AE-Telview ESS project will be trained on the importance of physical security. This training will emphasize the importance of maintaining a secure environment to protect personnel, assets, and operations.

Physical security for a lithium-ion energy storage facility will include the following elements:

1. Threat Assessment:
    - Preparation of a threat assessment that identifies potential security threats, including unauthorized access, theft, vandalism, sabotage, terrorism, or other criminal activities. The assessment will analyze the potential impact of these threats on the plant's operations and infrastructure.
    - The threat assessment will also evaluate the effectiveness of access control systems, perimeter fencing, surveillance cameras, lighting, alarms, and other security infrastructure, including identifying any vulnerabilities or gaps in the current security measures.
2. Access Control and Security Monitoring and Surveillance
    - Where appropriate, AE-Telview ESS personnel will develop and implement robust access control procedures for the plant, including perimeter access points, buildings, sensitive areas, and critical infrastructure.
    - Where appropriate, project personnel will install and maintain a comprehensive security monitoring and surveillance system, including cameras, alarms, and intrusion detection systems.
    - Where appropriate, project personnel will also establish protocols for real-time monitoring of security systems and regular review of recorded footage.
3. Security Training and Coordination with External Agencies:

- Where appropriate, AE-Telview ESS personnel will train employees on recognizing and reporting suspicious activities, proper use of access control systems, and emergency response procedures.
- Where appropriate, AE-Telview ESS will establish relationships and protocols for coordination with local law enforcement, emergency services, and relevant government agencies. It is recognized that collaborating with these agencies will give an opportunity to share threat intelligence, conduct joint exercises, and develop coordinated response plans.