MID-CAROLINA ELECTRIC COOPERATIVE, INC.

LEXINGTON, SOUTH CAROLINA

MINUTES OF REGULAR MEETING OF BOARD OF TRUSTEES

August 25, 2025

AGENDA ITEM # 1

CALL TO ORDER: (9:30 a.m.)	Marvin W. Sox, President/Chairman Alan R. Lunsford, Vice-President/Vice-Chairman Donette B. Kirkland, Secretary J. Allan Risinger, Treasurer J. Carey Bedenbaugh, Jr. Eddie C. Best, Jr. Kenneth E. Lindler Mark A. Svrcek via Zoom Justin B. Watts
STAFF PRESENT:	R. Robert "Bob" Paulling, President and CEO Theresa D. Crepes. VP, Finance and Accounting Robert A. Wilbur, VP, Operations Lee H. Ayers, VP, Engineering Troy A. Simpson, VP, Member Services Steven G. Davidson, VP, Information Technology Vicki E. Ross-Bell, Administrative Services Manager
ATTORNEY PRESENT:	J. David Black via Zoom
INVOCATION:	Donette Kirkland

PLEDGE OF ALLEGIANCE

AGENDA ITEM # 2

APPROVAL OF MINUTES: Chairman Sox called the meeting to order. He then asked if there were any corrections, additions, or deletions to the minutes of the last monthly meeting held on July 28, 2025. Mr. Lindler made a motion to approve the minutes, as presented. The motion was seconded by Mr. Lunsford and unanimously passed.

See Resolution # 1

AGENDA ITEM # 3

UNFINISHED BUSINESS: There was no unfinished business to come before the Board.

AGENDA ITEM # 4

FORM 990 REVIEW: Chairman Sox called on Mr. Paulling, who introduced Mr. Terry McMichael, CPA, who was on a Zoom call. Mr. McMichael reviewed the Cooperative's 2024 Form 990. After the review and discussion, Chairman Sox thanked Mr. McMichael for his report. Mr. Risinger made a motion to approve the 2024 Form 990, as presented. The motion was seconded by Mr. Best and unanimously passed.

AGENDA ITEM # 5

DEPARTMENTAL REPORTING:

FINANCE AND ACCOUNTING: Chairman Sox called on Mrs. Crepes for the Finance and Accounting report. Mrs. Crepes reported the year-to-date revenue was $106,791,574, which is $1,072,797 over budget at the end of July. The year-to-date cost of wholesale power was $60,448,029, which is over budget by $952,320. The year-to-date margins were $5,864,553, which is ($370,009) below budget. Mrs. Crepes reported that equity was 23.13% at the end of July for a decrease of -0.18%. The deferred credits account balance changed by $1,728,721, and the ending balance was $6,968,708.

Mrs. Crepes then presented a rate comparison chart showing an average residential usage of 1,289 kWh in July. Mid-Carolina's average bill was $236.07 (account charge $39.00) compared to Dominion's $288.05 (account charge $9.50), Duke – Carolina's $243.29 (account charge $11.96), and Duke – Progress $256.41 (account charge $11.78). She then presented a comparison chart showing an average annual usage of 16,331 kWh. Mid-Carolina's average annualized bill was $2,309.19 (account charge $474.50) compared to Dominion's $2,397.70 (account charge $114.00), Duke – Carolina's $2,360.48 (account charge $143.52), and Duke – Progress $2,301.79 (account charge $141.36).

Mrs. Crepes reported that Mid-Carolina has received $3,896,924 from CarolinaConnect year-to-date. There were no further questions or comments, and Chairman Sox thanked Mrs. Crepes for her report.

OPERATIONS: Chairman Sox called on Mr. Wilbur for the Operations report. Mr. Wilbur reported on the locations the Mid-Carolina and contractor crews worked in July. He reported the right-of-way crews are still working in the Lake Murray, Pelion, Hollywood, and Irmo areas. Mr. Wilbur stated the System Inspectors are still working in the Holley Ferry area. He reported that work is ongoing with the Carolina Crossroads project. There were no further questions or comments, and Chairman Sox thanked Mr. Wilbur for the report.

ENGINEERING: Chairman Sox called on Mr. Ayers for the Engineering report. Mr. Ayers reported that routine inspection and maintenance were completed. The work at Lake Murray Substation continues and the foundation and structures have started. The transmission line rebuild is still on schedule to start after Labor Day.

Mr. Ayers then showed a chart graphing MWh purchased each month year-to-date from 2021-2025 with a five-year running average. The next chart showed the MW Demand purchased each month year-to-date from 2021-2025 with a five-year running average. The monthly outage report and notes for July were discussed. There were no further questions or comments, and Chairman Sox thanked Mr. Ayers for his report.

MEMBER SERVICES: Chairman Sox called on Mr. Simpson for the Member Services report. Mr. Simpson shared ways the Cooperative has recently connected with the community. He discussed the new Mid-Carolina Community Leadership Council program that will be launched in January 2026.

Mr. Simpson reported on the Member Service walk-in statistics for July compared to the 2024 statistics showing an increase. He shared the recent social media engagement and reviewed the quarterly schedule for the *South Carolina Living* magazine through the October 2025 issue. There were no further questions or comments, and Chairman Sox thanked Mr. Simpson for his report.

INFORMATION TECHNOLOGY: Chairman Sox called on Mr. Davidson for the Information Technology report. Mr. Davidson reported there were 43,397 accounts enrolled in SmartHub as of August 1, 2025, which represents 71.12% of active accounts enrolled. He stated that 87.63% of all July payment transactions were made electronically. Mr. Davidson reported that an additional 1,458 members enrolled in TextPower this month, bringing the enrollment total to 56,841. He then reported on the Cooperative's process in backing up all databases.

Mr. Davidson reported there were 40,517 emails received during the month, and 15,051 emails were blocked prior to reaching the Cooperative's email servers, and 27 of those emails contained viruses. He then gave an update on the S.C. Hands-Free Driving Act. There were no further questions or comments, and Chairman Sox thanked Mr. Davidson for his report.

ADMINISTRATION: Chairman Sox called on Mrs. Ross-Bell for the Administration report. Mrs. Ross-Bell referred to the monthly Operation Round-Up report. The Trust Board did not meet in July. The donation to the five Christian Ministries totaled $13,198 in July, leaving a balance of $57,000 in the Trust Fund. She then reviewed the Board calendars through October 2025. There were no further questions or comments, and Chairman Sox thanked Mrs. Ross-Bell for her report.

AGENDA ITEM # 6

CEO'S REPORT: Chairman Sox called on Mr. Paulling for his report. Mr. Paulling discussed that there were no recordable accidents in July. He then reported that a new Fleet intern will be starting September 2, 2025. There is active recruitment for a Line Superintendent.

Mr. Paulling gave an update on Central and Statewide. He then showed pictures and discussed the Co-op Media Day that was held at Mid-Carolina's office on Friday, August 22, 2025. There were no further questions or comments, and Chairman Sox thanked Mr. Paulling for his report.

AGENDA ITEM # 7

LEGAL DISCUSSION: Chairman Sox called on Mr. Black for the legal report. Mr. Black discussed several pending legal matters. There were no further questions or comments, and Chairman Sox thanked Mr. Black for his report.

AGENDA ITEM # 8

CHAIRMAN'S REPORT: Chairman Sox read two thank you notes. He had nothing further to report at this time.

AGENDA ITEM # 9

COMMITTEE REPORTS: Chairman Sox stated the Compensation Committee met just prior to the meeting today, and more information will be discussed in the executive session.

Chairman Sox then called on Ms. Kirkland for the Policy Committee Report. Ms. Kirkland reported the Policy Committee has approved new Board Policy 306 – Cybersecurity and the Information Technology and Operation Technology Incident Response Plans. All documents were received by the Board to review prior to the meeting today. After a discussion, Mr. Lindler made a motion to approve the new policy, as presented. The motion was seconded by Mr. Lunsford and unanimously passed.

See Resolution # 2

There were no other committee reports at this time.

AGENDA ITEM # 10

ASSOCIATED MEETING REPORTS: Chairman Sox stated that CarolinaConnect's Board Meeting will be held the next day on August 26, 2025. CarolinaConnect currently has over 45,000 customers.

Ms. Kirkland stated that CEEUS is doing well. They are looking for additional parcels for outside storage. She gave an update on the recent Executive Committee meeting at Statewide.

There were no other reports at this time.

AGENDA ITEM # 11

NEW BUSINESS: Chairman Sox called for any new business. There was no new business to come before the meeting at this time. Mr. Watts made a motion to enter executive session. The motion was seconded by Mr. Bedenbaugh and unanimously passed.

AGENDA ITEM # 12

EXECUTIVE SESSION: During executive session, the Board conducted the annual review of the CEO. The Board unanimously approved an appropriate salary increase, as recommended by the Compensation Committee.

AGENDA ITEM # 13

ADJOURNMENT: There was no further business, and the meeting was adjourned at 12:50 p.m.

Donett B. K
Donette B. Kirkland, Secretary

APPROVAL:

Marvin W Sox
Marvin W. Sox, President/Chairman of the Board

S.C. 37 LEXINGTON

MID-CAROLINA ELECTRIC COOPERATIVE, INC.

RESOLUTION

1

WHEREAS, the Board of Trustees reviewed and had no changes to the minutes of the regular monthly meeting held on July 28, 2025;

NOW THEREFORE BE IT RESOLVED, that the Board of Trustees of Mid-Carolina Electric Cooperative, Inc. hereby approves the minutes for the last regular monthly meeting held on July 28, 2025.

I, Donette B. Kirkland, Secretary of Mid-Carolina Electric Cooperative, Inc., do hereby certify that the above is a true and correct copy of a resolution adopted by the Board of Trustees of Mid-Carolina Electric Cooperative, Inc. at a regular meeting duly assembled on the 25th day of August 2025, at which meeting a quorum was present.

Donette B. Kirkland

Donette B. Kirkland, Secretary

S.C. 37 LEXINGTON

MID-CAROLINA ELECTRIC COOPERATIVE, INC.

RESOLUTION

2

WHEREAS, the Policy Committee approved a new Board Policy 306 – Cybersecurity; and

WHEREAS, the policy includes an Information Technology Incident Response Plan; and

WHEREAS, the policy also includes an Operations Technology Incident Response Plan; and

WHEREAS, the policy and incident response plans were presented to the Board for approval; and

WHEREAS, the Board reviewed the information and agreed with the Policy Committee's recommendation;

NOW THEREFORE BE IT RESOLVED, that the Board of Trustees of Mid-Carolina Electric Cooperative, Inc. hereby approves Board Policy 306 – Cybersecurity along with the Information Technology and Operations Technology Incident Response Plans, which are attached hereto.

I, Donette B. Kirkland, Secretary of Mid-Carolina Electric Cooperative, Inc., do hereby certify that the above is a true and correct copy of a resolution adopted by the Board of Trustees of Mid-Carolina Electric Cooperative, Inc. at a regular meeting duly assembled on the 25th day of August 2025, at which meeting a quorum was present.

Donette B Kirkland

Donette B. Kirkland, Secretary

MID-CAROLINA ELECTRIC COOPERATIVE, INC.
BOARD OF TRUSTEES POLICY 306

SUBJECT: CYBERSECURITY POLICY

I. OBJECTIVE

This board policy provides the governance framework for the Cooperative to help mitigate its cybersecurity risk. The Cooperative's Board of Directors ("Board") recognizes that cybersecurity poses a risk to the Cooperative and requires a strategic enterprise-wide approach to mitigate that risk. The Cooperative will maintain an insurance rider for Cybersecurity, which is classified as Cyber Liability coverage.

II. POLICY CONTENT

The Board expects management to develop, implement, and comply with a cybersecurity risk mitigation plan that includes policies, procedures, practices and training (collectively "Cybersecurity Incident Response Plans") commensurate with the Cooperative's cybersecurity risk profile and consistent with applicable laws. As part of its governance responsibility, the Board will approve and oversee the Cybersecurity Incident Response Plans and evaluate management's effectiveness by implementing it.

A. Directors will:

1. Maintain a reasonable understanding of the Cooperative's cybersecurity risk profile.

2. Maintain a reasonable understanding of the Cybersecurity Incident Response Plans.

3. Have reasonable access to cybersecurity expertise as needed to become and remain reasonably informed about the Cooperative's cybersecurity risk profile and Cybersecurity Incident Response Plans including, but not limited to, maintaining a reasonable understanding of cybersecurity legal requirements that apply to the Cooperative.

4. On a regular basis, participate in a reasonable amount of education and training aimed at assisting directors with understanding their governance responsibilities as it relates to cybersecurity.

B. The Board will:

1. Require management to develop, implement, and comply with Cybersecurity Incident Response Plans that are commensurate with the Cooperative's cybersecurity risk profile consistent with applicable laws. The Cybersecurity Incident Response Plans should take into consideration the Cooperative's circumstances and address what risks to accept, mitigate or transfer.

2. Require the Cybersecurity Incident Response Plans include reasonable internal controls to determine that management is effectively implementing the plans.

3. Budget reasonable resources needed to implement the Cybersecurity Incident Response Plans.

4. Reflect in Board meeting agendas and meeting minutes that cybersecurity was discussed. Any written reports on cybersecurity provided to the Board should be included as an exhibit to the minutes (or executive session minutes), as appropriate. Appropriate confidentiality practices, procedures, and protections should be maintained, including, but not limited to, conducting discussions on cybersecurity during executive session.

5. The Board should receive regular reports regarding management's performance in implementing the Cybersecurity Incident Response Plans. The reports should include, but not be limited to:

   i. Any major cyber-attack attempts or actual cybersecurity incidents impacting the Cooperative, regardless of whether a major cyber-attack attempt was prevented.

   ii. The adequacy of resources budgeted to support the Cybersecurity Incident Response Plans.

   iii. The adequacy of the Cooperative's cybersecurity insurance coverage.

   iv. Evaluations of the Cooperative's implementation of the Cybersecurity Plan, including, but not limited to, penetration testing. The evaluations should be conducted by qualified and impartial internal staff or a qualified and impartial external contractor.

   v. Evaluations of the Cooperative's cybersecurity risk profile, including risks associated with third-party service providers including, but not limited to, Information Technology and Operations Technology outsourcing, business process outsourcing, and cloud solutions. The evaluations should be conducted by qualified and impartial internal staff or a qualified and impartial external contractor.

6. Verify that the Cooperative has established and maintains relationships with the appropriate federal, state, and local governmental authorities responsible for cybersecurity or cybersecurity related law enforcement, such as the Federal Bureau of Investigation.

7. Verify that the Cooperative engages in cyber threat information sharing within the industry, such as the E-ISAC.

8. The Cooperative will maintain an insurance rider for Cybersecurity, which is classified as Cyber Liability coverage.

9. Review this policy on a regular basis and update it as reasonably necessary.

III. RESPONSIBILITY

A. The Board of Trustees shall be responsible for this policy being carried out.

B. The CEO shall be responsible for all expectations of the Cooperative's management set for by this policy.

Mid-Carolina Information Technology
Cybersecurity Incident Response Plan

Date: 28-Jan-2022 (Draft)
4-Feb-2022 (1st Edit)
10-Feb-2022 (2nd Edit)
16-Apr-2024 (3rd Edit)
22-Jan-2025 (4th Edit)
28-July 2025 (5th Edit)

Introduction

To maintain the trust of our employees, members, and partners and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a cyberattack. The better prepared we are to respond to a potential cyberattack, the faster we can eradicate any threat and reduce the impact on our business.

This document describes the plan for responding to cybersecurity incidents at Mid-Carolina Electric Cooperative, Inc. and explains how to detect and react to these incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders. Effective incident response involves every part of our organization, including IT teams, Board, executive staff, human resources, corporate communications, and business operations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be periodically reviewed and updated to reflect organizational changes, new technologies and new compliance requirements that inform our cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response. This document is divided into sections which describe the various events and those teams responsible for action during and after a cybersecurity incident.

Cybersecurity – a definition: While it is incumbent on us to protect confidential information for our members, employees and other stakeholders, cybersecurity is mainly concerned with protecting data that is in an electronic or digital format.

Incident Response Team:

The IR Team is divided into two main sections, Primary and Secondary, each with specific roles.

Primary IR Team:

VP, Information Technology	Steven Davidson	sdavidson@mcecoop.com
	803.629-4141 (m)	803.746.6540 (o)
Systems & Network Administrator	Michael Blanton	mblanton@mcecoop.com
	803.873.1294 (m)	803.749.6541 (o)

Secondary IR Team:

IT Personnel	Lisa Dawkins	lisa_d@mcecoop.com
	803.315.6062 (m)	803.749.6545 (o)
	Robert Webb	rwebb@mcecoop.com
	843.494.4667 (m)	803.749.6544
	Aleshia Bailey	Aleshia_d@mcecoop.com
	803.730.1691 (m)	803.749.6546 (o)
	Melanie Dodson	melanie@mcecoop.com
	803.530.6943 (m)	803.749.6446 (o)

Cross-Functional Members:

CEO	Bob Paulling	bobp@mcecoop.com
	803.206.5576 (m)	803.7498.6450 (o)
VP, Member Services	Troy Simpson	troy@mcecoop.com
	803.391.0061 (m)	803.749.6411 (o)
VP, Engineering	Lee Ayers	lee@mcecoop.com
	803.413.5437 (m)	803.749.6454 (o)
VP, Operations	Bobby Wilbur	bobby@mcecoop.com
	803.315.0247 (m)	803.749.6456 (o)
VP, Finance and Accounting	Theresa Crepes	theresa@mcecoop.com
	803.315.1826 (m)	803.749.6468 (o)

Member Services Manager	Christina Rish	christina@mcecoop.com
	803.312.1038 (m)	803.749.6449 (o)
Administrative Services Manager	Vicki Ross-Bell	vicki@mcecoop.com
	803.315.8249 (m)	803.749.6475 (o)

External Organizations:

Corporate Attorney	David Black	dblack@mcecoop.com
	803.609.1650 (m)	803.771.8900 (o)
Law Enforcement	SLED	803.737.9000
	FBI	803.551.4200
Sherriff	Richland County	803.576.3000
Sherriff	Lexington County	803.785.8230
Sheriff	Saluda County	864.445.2112
Sheriff	Aiken County	803.642.1761
Sheriff	Newberry County	803.321.2211
ECSC (Statewide)	Chris Koon	chris.koon@ecsc.org
	803.622.5888 (m)	803.796.6060 (o)
Federated	Cyber Department	800.356.8360

Note: There may be outside vendors such as NISC, Oracle, Milsoft, Gridbright, or Training Concepts that will play a part in the processes we utilize to analyze and resolve any incidents.

Process and Stages:

Step 1 is always to contact a member of the IR Response Team (Primary) to inform them of the suspected breach or attack. If the Primary Team is unavailable, please contact a member of the Secondary Team. If possible, please discontinue operations on the workstation in question until a member of one of the teams can assess the situation.

Each step in the following procedure should be recorded in a log for review, training, insurance reporting etc.

Step 2 – Assessment:
The Primary or Secondary Team Member should initially determine whether a network disconnect should be undertaken to eliminate the possibility of further infection. It is also imperative to determine if this case is isolated or if other systems/workstations/devices have been infected. Then the remaining members of the Primary and Secondary teams should be notified as to the specifics of the breach.

Step 3 – Analysis and Operation:
Designate an Incident Commander(s) – to oversee and manage the incident (VP, Information Technology and Systems & Network Administrator).
Contact cross-functional team members that need to be aware of the ongoing incident.
Determine what happened. What are the symptoms? How many users are affected? (Scope)
Can the breach be mitigated in-house? If not, which outside partners will need to be involved?
Will Law Enforcement assistance or reporting be required?

Step 4 – Recovery (after the breach is mitigated):
Determine if data needs to be recovered and the impact on others in the organization.
Are outside partners needed to assist in recovery?
Contact all parties needed to get recovery or remediation started.

Step 5 – Post Incident:
Determine any reporting requirements (Federated, Law Enforcement, Business Partners, Other Cooperatives, Vendors)
Determine the severity of the incident.
Determine whether a forensic analysis is needed and if so, who will perform it.

Step 6 – Prevention:
Should policies and/or procedures be updated to prevent this type of incident from happening in the future?
Do firewall and other security systems need to be hardened or updated?
Execute a post-incident roundtable with the Primary and Secondary Teams.

Step 7 – Close this case.

Mid-Carolina Operations Technology
Cybersecurity Incident Response Plan

Date: 11-June-2025 (Draft)

28-July-2025 (1st Edit)

Introduction

To maintain the trust of our employees, members, and partners and meet regulatory requirements, it is essential that we do everything we can to protect the operational technology systems in the face of a cyberattack. The better prepared we are to respond to a potential cyberattack on our operational technology infrastructure, the faster we can eradicate any threat and reduce the impact on our business.

This document describes the plan for responding to cybersecurity incidents affecting Mid-Carolina Electric Cooperative's Operational Technology and explains how to detect and react to these incidents, determine their scope and risk, respond appropriately, and communicate the results and risks to all stakeholders.

Effective operational technology incident response involves every part of our organization, including engineering teams, dispatch, Board, executive staff, IT teams, human resources, corporate communications, and business operations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be periodically reviewed and updated to reflect organizational changes, new technologies and new compliance requirements that form our operational technology cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

This document is divided into sections which describe the various events and those teams responsible for action during and after a cybersecurity incident affecting operational technology systems.

Operational Technology Cybersecurity – a definition: Operational technology cybersecurity is mainly concerned with protecting control systems, SCADA networks, and other operational technology that is critical to our electric utility operations and member service delivery.

Incident Response Team:

The IR Team is divided into two main sections, Primary and Secondary, each with specific roles.

Primary IR Team:

VP, Engineering	Lee Ayers	LEE@mcecoop.com
	803.413.5437 (m)	803.749.6454 (o)
OT Systems & Network Administrator	Clark Reboul	clark@mcecoop.com
	440.591.9299 (m)	803.749.6459 (o)

Secondary IR Team:

OT Personnel	Lew Dubose	lew@mcecoop.com
	803.730.8502 (m)	803.749.6441 (o)
	Chris Strickland	strickland@mcecoop.com
	803.622.0223 (m)	803.749.6457 (o)
	Jill Parker	jill@mcecoop.com
	803.767.3749 (m)	803.749.6458 (o)

Cross-Functional Members:

CEO	Bob Paulling	bobp@mcecoop.com
	803.206.5576 (m)	803.7498.6450 (o)
VP, Member Services	Troy Simpson	troy@mcecoop.com
	803.391.0061 (m)	803.749.6411 (o)
VP, Information Technology	Steven Davidson	sdavidson@mcecoop.com
	803.629.4141 (m)	803.746.6540 (o)

VP, Operations	Bobby Wilbur	bobby@mcecoop.com
	803.315.0247 (m)	803.749.6456 (o)
VP, Finance and Accounting	Theresa Crepes	theresa@mcecoop.com
	803.315.1826 (m)	803.749.6468 (o)
Member Services Manager	Christina Rish	christina@mcecoop.com
	803.312.1038 (m)	803.749.6449 (o)
Administrative Services Manager	Vicki Ross-Bell	vicki@mcecoop.com
	803.315.8249 (m)	803.749.6475 (o)

External Organizations:

Corporate Attorney	David Black	dblack@mcecoop.com
	803.609.1650 (m)	803.771.8900 (o)
Law Enforcement	SLED	803.737.9000
	FBI	803.551.4200
Sheriff	Richland County	803.576.3000
Sherriff	Lexington County	803.785.8230
Sherriff	Saluda County	864.445.2112
Sherriff	Aiken County	803.642.1761
Sherriff	Newberry County	803.321.2211
ECSC (Statewide)	Chris Koon	chris.koon@ecsc.org
	803.622.5888 (m)	803.796.6060 (o)
Federated	Cyber Department	800.356.8360

Note: There may be outside vendors such as AspenTech, Emerson, Oracle, Microsoft, Schweitzer Engineering Labs, Burns & McDonnell, 1898 & Co. or Training Concepts that will play a part in the processes we utilize to analyze and resolve any OT incidents.

Process and Stages:

Stage 1 is always to contact a member of the IR Response Team (Primary) to inform them of the suspected breach or attack. If the Primary Team is unavailable, please contact a member of the Secondary Team. If possible, please discontinue operations on the associated operational device in question until a member of one of the teams can assess the situation.

Each step in the following procedure should be recorded in a log for review, training, insurance reporting etc.

Step 2 – Assessment:

The Primary or Secondary Team Member should initially determine whether a network disconnect should be undertaken to eliminate the possibility of further infection. It is also imperative to determine if this case is isolated or if other OT devices have been infected.

Step 3 – Analysis and Operation:

Designate an Incident Commander(s) – to oversee and manage the incident (VP, Engineering and OT Systems & Network Administrator).

Contact cross-functional team members that need to be aware of the ongoing incident.

Determine what happened. What are the symptoms? How many users/systems are affected? (Scope)

Critical OT-specific considerations: Impact on electric grid operations and reliability, safety implications for field personnel and equipment, effect on member service and power delivery

Can the breach be mitigated in-house? If not, which outside partners will need to be involved?

Will Law Enforcement assistance or reporting be required?

Step 4 – Recovery (after the breach is mitigated):

Determine if data needs to be recovered and the impact on other systems in the organization.

OT-specific recovery priorities: Restore critical control systems and SCADA networks, verify integrity of protection and safety systems, validate power system operations and grid stability, confirm communication systems functionality

Are outside partners needed to assist in recovery?

Contact all parties needed to get recovery or remediation started.

Step 5 – Post Incident:

Determine any reporting requirements (Federated, Law Enforcement, Business Partners, Other Cooperatives, Vendors, NERC, CISA, DOE)

Determine the severity of the incident.

Determine whether a forensic analysis is needed and if so, who will perform it.

Step 6 – Prevention:

Should policies and/or procedures be updated to prevent this type of incident from happening in the future?

Do firewalls and other security systems need to be hardened or updated?

Execute a post-incident roundtable with the Primary and Secondary Teams.

Step 7 – Close this case.