Policy Number: B-17
Subject: Information and Cyber Security Policy
Review Requirement: 3 years
Original Issue Date: October 11, 2018
Date of Last Review: September 11, 2025
Date of Last Revision: September 11, 2025
Previous Revisions: 06/09/2020, 08/11/2022

I. OBJECTIVE

Mountain Parks Electric, Inc.'s (the "Cooperative") Directors recognize the need to protect the Cooperative, our members, and both Cooperative and member data, and systems, from growing information and cyber security threats. This policy establishes an Information & Cyber Security Program within the Cooperative to ensure adequate measures are taken and controls are in place to mitigate threats and protect those company resources.

This policy is intended for establishment of an overall Information Security Program at the Board level with Policy and Procedure management handled at the executive staff/IT Management level. Information Security is not solely an Information Technology concern but touches all departments, all employees, and all types of information transactions. The purpose of this policy is to ensure that the Cooperative's technology assets are protected against all internal, external, deliberate and accidental threats. Information, in all its forms, written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorized modification, or destruction throughout its life cycle. Policies and Procedures established by executive staff/IT Management ("Information & Cyber Security Policies and Procedures") shall be administered by executive staff/IT Management to protect Cooperative data acquisition and control systems across the enterprise.

II. SCOPE

All employees, contractors, temporary and other workers at the Cooperative and its subsidiaries must adhere to all policies and procedures authorized and approved under this program. This applies to Cooperative data sets and technology equipment that is owned, operated, or leased by the Cooperative. The Information & Cyber Security Policies and Procedures describe the technology and information assets that must be protected and identify many of the threats to those assets. The equipment, software, and storage medium used to process, store, and transmit information will be protected by appropriate controls.

All third-party service providers, vendors, and contractors with access to Cooperative systems or data must adhere to security standards consistent with this Policy and the Cooperative's Information & Cyber Security Policies and Procedures. Contracts and agreements shall require appropriate data protection, monitoring, and compliance measures.

III. POLICY

A. The Information & Cyber Security Policies and Procedures will ensure that:

1. Sensitive, protected and/or privileged information and technology systems will be safeguarded against any unauthorized access;

2. Confidentiality of sensitive, protected and/or privileged information will be assured;

3. Integrity of information will be maintained;

4. Availability of information for business purposes will be maintained;

5. Legislative and regulatory requirements will be met;

6. Business continuity and disaster recovery plans will be developed, maintained, and tested annually;

7. All Cooperative employees will be provided information security and awareness training on a regular basis annually at a minimum;

8. Any actual or suspected information security breaches will be reported to designated management at the Cooperative. All breaches will be investigated thoroughly and logged.

9. The Cooperative shall maintain an Incident Response Plan to guide the detection, response, escalation, communication, and recovery from cybersecurity incidents. Incident reporting obligations, including regulatory or member notifications when required, shall be followed.

10. The Cooperative recognizes the growing role of Artificial Intelligence (AI) in business operations and information management. To ensure responsible and secure adoption of AI tools and processes, all use of AI within the Cooperative shall comply with the Cooperative's established AI Standard Operating Procedure (SOP AI). This includes, but is not limited to, safeguards for data privacy, protection of member and Cooperative information, mitigation of security risks, and adherence to ethical and regulatory standards.

11. The Cooperative shall conduct regular information security risk assessments, audits, and penetration testing, as appropriate, to evaluate the

effectiveness of security controls and identify emerging threats. Findings will inform updates to security measures and staff training.

B. Policies and Procedures have been established to support this program, including appropriate controls and continuity plans and shall be administered by executive staff/IT Management.

C. Business requirements for availability of information systems will be met.

Definition of Terms:

Because modern technology is subject to rapid change, and because social, cultural, and legal standards and expectations regarding technology are ever evolving, it is not possible for these Information & Cyber Security Policies and Procedures to address every possible situation which might develop. Nonetheless, the philosophy, principles and procedures of these Information & Cyber Security Policies and Procedures shall be used whenever possible to guide the development of, the compliance with, and the administration and enforcement of all matters relating to the effective acquisition and utilization of technology.

The term Technology is intended to be defined broadly and includes all:

A. Electronic hardware, software and services, including but not limited to desktops, laptops, rugged computers, tablets, workstations, monitors, printers, plotters, faxes, scanners, multifunction print devices, smartphones, cellular phones, satellite phones, wireless broadband cards, pagers, servers, PBX equipment, telecommunications equipment, circuits, switches, routers, storage devices, recording devices, digital cameras, email, text messaging, instant messaging, Internet, firmware, operation systems, software, business applications, Software as a Service ("SaaS") applications, Infrastructure as a Services ("IaaS"), Platform as a Service ("Paas"), peripherals used in conjunction with the devices and software listed above, and all other electronic devices or software used to run software or create, record, store, transmit and/or receive video, voice or data.

B. Electronic information, including but not limited to email addresses, phone numbers, IP addresses, email messages, text messages, instant messages, word processor documents, spreadsheets, presentations, drawings, images, photos, videos, music, voice, databases, application data, and all other electronic data; and personally identifiable information.

C. Electronic communications, including but not limited to voice, email, text messages, instant messages, voice messages, internet postings, facsimiles, and all other forms of electronic communications.

D. For purposes of this Policy, Artificial Intelligence (AI) refers to computer systems and software capable of performing tasks that typically require human intelligence, including but not limited to learning, reasoning, pattern recognition, natural language processing, and decision-making.

IV. RESPONSIBILITY

Responsibilities for this Information and Cyber Security Program Policy are delineated as follows:

A. The Board of Directors of the Cooperative is responsible for the content of this policy and its implementation.

B. The Chief Executive Officer of the Cooperative shall be responsible for the overall administration of this policy.

C. The Vice President of IT shall direct and monitor the implementation of the Information & Cyber Security Policies and Procedures in accordance with this policy.

D. All Cooperative personnel are responsible for following the guidelines and procedures laid out in the Information & Cyber Security Policies and Procedures as well as for reporting known violations of the policies and procedures.

APPROVED BY THE BOARD OF DIRECTORS ON SEPTEMBER 11, 2025