# MOUNTAIN PARKS ELECTRIC, INC.
## BUSINESS FUNCTIONS POLICIES AND PROCEDURES

| SUBJECT: **INFORMATION AND CYBER SECURITY POLICY** | POLICY NO. **B-17** |
|---|---|
| EFFECTIVE DATE: **OCTOBER 11, 2018** | PAGE 1 OF 3 |
| REVISED DATE: **JUNE 9, 2020, AUGUST 11, 2022** | |

OBJECTIVE

Mountain Parks Electric, Inc. ("MPE") Directors recognize the need to protect MPE, our members, and both cooperative and member data, and systems, from growing information and cybersecurity threats. This policy establishes an Information & Cyber Security Program within MPE 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 informational transactions. The purpose of this policy is to ensure that MPE 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 technology systems and data, member financial and protected information, and cooperative data acquisition and control systems across the enterprise.

Scope:

All employees, contractors, consultants, temporary and other workers at MPE 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 MPE. The Information & Cyber Security Policies and Procedures describe the technology and information assets that must be protected and identifies 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.

POLICY

A. The Information & Cyber Security Policies and Procedures will ensure that:
   a. Sensitive, protected and/or privileged information and technology systems will be safeguarded against any unauthorized access;
   b. Confidentiality of sensitive, protected and/or privileged information will be assured;
   c. Integrity of information will be maintained;

d. Availability of information for business purposes will be maintained;
e. Legislative and regulatory requirements will be met;



f. Business continuity and disaster recovery plans will be developed, maintained and tested annually;
g. All MPE employees will be provided information security and awareness training on a regular basis;
h. Any actual or suspected information security breaches will be reported to the designated management at MPE. All breaches will be investigated thoroughly and logged

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 Service (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 received 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

**Responsibilities:**

A. Responsibilities for this Information and Cyber Security Program Policy are delineated as follows:
   a. The Board of Directors of MPE is responsible for the content of this policy and its implementation.
   b. The General Manager of the Association shall be responsible for the overall administration of this policy.
   c. The Manager of IT shall direct and monitor the implementation of the Information & Cyber Security Policies and Procedures in accordance with this policy.
   d. All MPE 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.

, PRESIDENT DATE: 08/11/22

4849-6208-1216, v. 3