



Board of Directors Policies

Policy Number: 302	Subject: Information Security
Effective Date: 08/26/2025	Previous Version: 08/22/2023

OBJECTIVE

The purpose of this policy is to ensure the confidentiality, integrity, and availability of all Delta-Montrose Electric Association (DMEA) information assets. This policy provides a framework for managing information security risks at a strategic level and establishes the Board's commitment to protecting these assets.

ACCOUNTABILITY

The Board of Directors (Directors) and the Chief Executive Officer (CEO).

POLICY

- 1. Designation of Information Security Officer.** The CEO shall designate an Information Security Officer (ISO) to serve as the primary contact for cybersecurity matters and oversee cybersecurity for both information technology (IT) and operational technology (OT) for DMEA. The ISO shall be responsible and accountable for ensuring compliance with applicable cybersecurity standards, conducting risk assessments, coordinating training, and managing cybersecurity incidents. The CEO shall be responsible for periodically updating the Board on DMEA's cybersecurity status and any open risks.
- 2. Third-Party Contract Reviews.** All contracts and agreements, excluding those covered by the Disclosure of Information Policy, that involve third-party access to DMEA's privileged information or systems will be reviewed by the ISO, in conjunction with management and/or legal counsel. The purpose of the ISO's review is to understand the nature of the data and system access given to third parties, assess associated risks, confirm third-party adherence to DMEA's security standards, and ensure third parties have adequate protective measures in place to secure DMEA's information and systems.
- 3. Data Classification.** The CEO shall oversee the development and implementation of a data classification policy and data protection standards to ensure proper handling and protection of DMEA information.
- 4. Data Protection and Privacy.** DMEA shall comply with all applicable data and privacy laws, regulations and required standards, including, but not limited to, Federal Trade Commission Fair and Accurate Credit Transactions Act (FACT) Red Flags Rules, Payment Card Industry Data Security Standards (PCI DSS) and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), and may voluntarily elect to comply with other data and privacy standards that may be issued from time to time.
- 5. Incident Response and Disaster Recovery.** The CEO shall be responsible for establishing

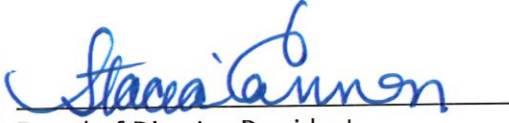


Board of Directors Policies

Policy Number: 302	Subject: Information Security
Effective Date: 08/26/2025	Previous Version: 08/22/2023

and maintaining a Cyber Incident Response Plan, an IT Disaster Recovery Plan, and a Crisis Communications Plan. The purpose of these plans is to ensure prompt and effective handling of cybersecurity incidents, swift recovery of critical systems, and efficient communications during an incident or disaster.

- 6. Internal Policies.** The CEO shall be responsible for establishing and enforcing internal policies to promote information security best practices and safeguard the cooperative's assets. These policies shall include, at minimum, an Employee Acceptable Use Policy to ensure responsible and secure use of technology resources; a Cyber Operating Policy for IT and OT to establish guidelines for the secure operation and management of systems; and a Physical Security Policy to outline measures to protect DMEA's physical information technology assets and sensitive information. Other internal policies may be developed as necessary to maintain secure operations and safeguard against unauthorized access or damage.

 Board of Director President	<u>8/26/25</u> Date
--	------------------------