Board of Directors Policies

Policy Number: 303	**Subject:** Acceptable Use of Technology by Directors
Effective Date: 09/30/2025	**Previous Version:** 08/22/2023

OBJECTIVE

To establish guidelines for Board of Director (Board) access and acceptable use of Delta-Montrose Electric Association (DMEA) information systems and devices, ensuring security, responsible use, and consistency with organizational standards.

ACCOUNTABILITY

Board of Directors

POLICY

1. **Definitions.**

   a. **Device**. Any laptop, workstation, desktop, phone, or tablet and related equipment used by a Director to access DMEA information systems.

   b. **Information System**. The collection of resources, including, but not limited to, applications, devices, data, and networks that DMEA uses to manage and process information (e.g., email).

2. **Access to DMEA Resources.**

   a. **Electronic Access.** Upon election or appointment to the Board and completion of required cybersecurity training, Directors shall be granted access to DMEA's essential information systems for use in the performance of their duties as a Director. The purpose of such access is to facilitate business communications and research, send and receive information, exchange ideas, and share files.

   b. **Physical Access.** Directors will be provided with an access control card granting limited access to DMEA facilities. It is the responsibility of the Director to securely store the access control card and immediately report any lost or stolen cards to the Chief Executive Officer (CEO). Unauthorized use or duplication of an access control card is strictly prohibited.

   c. **Termination of Access.** Access to DMEA's information systems and facilities will be terminated when a Director's term concludes, when a Director voluntarily resigns, or when a Director is involuntarily removed from the Board for any reason. Additionally, access may be revoked at any time by (i) a majority vote of the Board; or (ii) temporarily for justifiable security reasons by the CEO.

   d. **Access Limitations.** DMEA will use reasonable efforts to grant Directors access to only those information systems necessary for the Directors to fulfill their duties effectively.

Directors are prohibited from accessing information systems which are not directly related to their official responsibilities.

e. **Passwords.** Directors are required to use passwords that comply with DMEA's password policy guidelines. Passwords shall not be shared with others. When available, DMEA may require Multifactor Authentication (MFA) as a mandatory enhancement to provide additional security when accessing DMEA information systems. Only MFA applications approved by DMEA shall be used.

f. **Cooperative Property.** All information systems, including the data and information contained therein, shall remain the property of DMEA. This includes all communications and files sent, received, or stored via email or other systems.

3. **Director Use of Information Systems.**

a. **Monitoring and Privacy Expectations**. DMEA reserves the right to monitor networks, systems, and devices to detect security threats and maintain confidentiality, integrity, and availability of DMEA's information systems and devices. Directors should have no expectation of privacy when using DMEA information systems or devices. Usage may be intercepted, recorded, or reviewed in accordance with applicable laws, regulations, and DMEA policies. Unauthorized use is prohibited. By serving as a Director, Directors acknowledge and consent to such monitoring by using DMEA information systems and devices.

b. **Confidentiality.** Directors may be exposed to privileged information while using DMEA information systems. Privileged information may include confidential, legally privileged, or sensitive information, including personally identifiable information. Directors shall only access, use, or share privileged information to the extent authorized by DMEA and necessary to fulfill their duties as directors.

c. **Acceptable Use.** Directors may engage in occasional and incidental personal use of DMEA-issued devices, provided such use is limited in scope, does not interfere with Board responsibilities, does not compromise security, and is in compliance with all relevant laws and regulations. DMEA reserves the right to revoke or limit this privilege at any time.

d. **Incidental Personal Use.** Directors may engage in reasonable, incidental personal use of DMEA-issued devices so long as it does not interfere with their duties or compromise the DMEA's security or operations.

e. **Unacceptable Use.** Directors are prohibited from using any DMEA information systems or devices in a manner that violates any applicable law, policy, or regulation. Unacceptable use includes, but is not limited to, the following activities:

i. Attempting to access or accessing devices or information systems for which the Director does not have proper authorization;

ii. Invading the privacy of others, including fellow Directors, employees, or members, by accessing or sharing their personal information without proper authorization or consent;

iii. Engaging in any activities that may harm, disrupt, or compromise the security, integrity, or availability of DMEA's devices and information systems;

iv. Sending unsolicited junk emails, messages, or other communications;

v. Creating, accessing, downloading, or distributing any content that is offensive, defamatory, discriminatory, harassing, or in violation of the intellectual property rights of DMEA or others;

vi. Trolling, bullying, intimidating, or harassing other individuals;

vii. Using DMEA-issued devices for personal use to the extent that personal use interferes with DMEA's business or other directors' duties;

viii. Engaging in any illegal or unethical activities, such as hacking or fraud;

ix. Connecting unauthorized devices to DMEA-authorized networks;

x. Permitting any unauthorized person(s) to access DMEA's information systems or devices;

xi. Using DMEA-issued devices and information systems for commercial ventures, religious or political causes, or personal gain; or

xii. Engaging in activities that may damage the reputation of DMEA.

f. **Off-Site Transmission and Storage Restrictions.** Off-site transmission or storage of privileged information should only occur through DMEA approved and secure methods. Directors may not store DMEA information on third-party or personal cloud-storage accounts, web-applications, or non-DMEA devices.

g. **Email Systems.** Directors shall use DMEA email for conducting all DMEA business. Use of personal email for DMEA-related communications is prohibited unless explicitly authorized by the Board President.

h. **Social Media.** Only authorized DMEA employees are permitted to post or reply to social media accounts or posts on behalf of DMEA. Directors may not use personal social media accounts to conduct DMEA business.

i. **Reporting Security Incidents.** Directors are responsible for promptly reporting any actual or suspected security incidents, data breaches, or other security-related issues to the CEO. Directors shall provide all relevant details and any available evidence related to the security incident to facilitate the investigation and response process. Directors must maintain confidentiality and handle sensitive information in a secure manner during the reporting and investigation of security incidents.

j. **Security Response.** DMEA reserves the right to take immediate action in response to any identified security risk on DMEA-issued devices. This includes the ability to uninstall applications deemed to pose a threat to the integrity of the device, other information systems, or DMEA data.

4. Devices

a. **Device Assignment.** DMEA recognizes the importance of equipping Directors with suitable devices and related equipment to access DMEA information systems for the effective performance of their duties. Upon election or appointment to the Board, Directors will be provided with a DMEA-issued device or reimbursement for the use of their personal device. Given the average life span of such devices, Directors, at their option, may be provided with a new device or reimbursement for a personal device upon re-election.

   i. Directors electing to receive a DMEA-issued device will receive a standard pre-configured device and necessary application, security software, and essential accessories required to access DMEA information systems. The purchase of non-essential accessories (e.g., keyboard, mouse, etc.) is the responsibility of the Director. Directors will be required to return to DMEA all devices and equipment exchanged for new or different devices or equipment. Unless otherwise agreed to by DMEA and a Director, DMEA will retain ownership of any device or equipment issued to a Director.

   ii. Alternatively, Directors may elect to receive a reimbursement for use of a personal device instead of receiving a DMEA-issued device. The reimbursement amount, determined solely by DMEA, will be approximately the same as the DMEA-issued device. Directors choosing the reimbursement must ensure, and at their own expense, that their device meets the minimum security and technical requirements as determined by DMEA. Directors shall be solely responsible for repairing or replacing Director-owned devices.

b. Internet Access. DMEA-issued devices will be provided with a mobile data plan. Directors electing to receive a device reimbursement shall also receive a monthly mobile data plan reimbursement equivalent in value to the mobile data plan provided by DMEA for DMEA-issued devices.

c. Device Management. To protect DMEA's information systems and devices, DMEA may require installation of a Mobile Device Management (MDM) solution or other designated device manager for managing and securing DMEA-issued devices. This includes, but is not limited to, the following functions:

i. Enforcing security policies;

ii. Remote management to remotely lock or wipe a device or to perform routine maintenance;

iii. Installing or managing applications and preventing the installation of potentially harmful applications; or

iv. Monitoring the device to identify potential security threats and to ensure compliance with DMEA policies.

d. Unattended Devices. Devices must not be left unsecured in transit (e.g., airline luggage systems). Devices containing DMEA information must remain attended or physically secured at all times.

e. Device Backups. DMEA does not provide a backup of data on DMEA-issued or Director-owned devices. DMEA recommends that Directors regularly back up the data on their equipment to DMEA-approved systems to protect against data loss.

f. Loss of Devices. Directors shall immediately report the theft or loss of any device used to access DMEA information systems. The Director shall provide a written report describing the circumstances surrounding the loss or theft. The Board may require the Director to reimburse DMEA for the cost of replacing a DMEA-issued device.

5. <u>Training and Support</u>.

a. Cybersecurity Training. Directors must remain current with periodic cybersecurity training requirements consistent with DMEA-wide security expectations.

b. Technical Support. DMEA will provide Directors with technical support during business hours for all information systems and DMEA-issued devices essential for performing their duties as Directors. After-hours technical support may be granted at CEO discretion. On

Board or committee meeting days, the IT department will prioritize Director requests for support.

c. **Director-owned Device Support.** For Director-owned devices, technical support will be limited to facilitating access to the information systems and applications necessary for Directors to fulfill their duties. DMEA will not provide support for personal use.

6. **Failure to Comply.** Violations may result in restricted access, referral to the Board for action, and/or reporting to law enforcement where applicable.

Board of Directors President

9/30/25
Date