Digital Records & Cloud Governance

Document No.: POL-01-003 Effective Date: 05/2026

Purpose

To ensure secure storage, controlled access, and lawful retention of electronic records.

Authorized Platforms

All official digital records must be stored in:

- Board-approved cloud storage
- Official Association email accounts
- Approved accounting software

Personal email or personal cloud storage may not be used for official records. All platforms must be approved at a general meeting before use.

platforms Access Control

1. Access is limited to authorized officers.
2. Administrative access is restricted to no more than two individuals.
3. Shared passwords are prohibited.
4. Passwords must be updated immediately upon officer transition.
5. Multi-factor authentication (MFA) is strongly recommended.

Email Governance

- Official business must be conducted through Association email accounts.
- Important decisions must be preserved in meeting minutes.
- All emails must be archived.

Backup & Continuity

1. Digital records must be backed up regularly.
2. Access credentials must be documented securely for continuity.
3. Upon officer transition:
    - Access must be transferred within 7 days
    - Former officers' access must be revoked

Digital Destruction

Electronic records must follow the Record Retention Schedule.

Deletion must be permanent and must not occur during a Litigation Hold.

Data Security

The Association shall:

- Protect donor information
- Protect student information
- Restrict access to financial data
- Avoid storing sensitive personal information unnecessarily