IS0011 - Asset Management Policy

Purpose

The purpose of the Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by Martin Luther College.

Scope

This policy applies to individuals who are responsible for the use, purchase, implementation, management, and/or maintenance of Martin Luther College information resources.

Definitions

Policy

Hardware, Software, Applications, and Data

- All hardware, software, and applications must be approved, inventoried, and purchased by MLC IT Services.
- Installation of new hardware or software, or modifications made to existing hardware or software, must follow approved procedures and change control processes.
- All purchases must follow the defined and appropriate processes outlined by MLC.
- Software used by MLC employees, contractors, and/or other approved third parties working on behalf of MLC must be properly licensed.
- Software installed on MLC computing equipment, outside of that noted in the Approved Software List, must be approved by IT Services management or MLC leadership and installed by IT Services personnel.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g., personally identifiable information (PII), protected health information (PHI), student data and information, organizational financial data, etc.
- Two-factor authentication is required for external cloud computing applications with access to any confidential information for which MLC has a custodial responsibility unless an exception form is formally approved.
- Contracts with cloud computing application providers must address data retention, destruction, data ownership, and data custodian rights regarding stored MLC data.

- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- A general inventory of information (data) must be mapped and maintained on an ongoing basis.
- All MLC assets must be formally classified with ownership assigned.
- Maintenance and repair of organizational assets must be performed and logged in a timely manner and managed by IT Services.
- If an MLC asset is being taken to a “High-Risk Area,” as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by IT Services before being taken offsite and before reconnecting to any MLC network.
- Confidential information must be transported either by a designated MLC employee or a suitable courier, method, or service approved by IT Services.
- Upon termination of employment, contract, or agreement, all MLC assets must be returned to MLC IT Services or leadership and documented accordingly.

Mobile Devices

- The use of a personally owned mobile device to connect to the MLC network, besides the guest network, is a privilege granted to employees and requires successful registration of the device by the owner.
- Mobile devices used to connect to the MLC network, besides the guest network, may be required to use the approved Mobile Device Management (MDM) or Mobile Application Management (MAM) solution, defined by IT Services, at any time.
- Mobile devices that access MLC email must have a PIN or other authentication mechanism enabled.
- Confidential data should only be stored on devices that are encrypted in compliance with IS0001 - Encryption Policy.
- All mobile devices with access to MLC data should maintain up-to-date versions of all operating systems and applications.

Media Destruction & Reuse

- Media that may contain confidential or internal information must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- All decommissioned media must be stored in a secure area prior to destruction.
- Media reuse and destruction practices must be tracked and documented.
- All information must be destroyed when no longer needed, including encrypted media.

Backups

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.

- The MLC backup and recovery process for each system must be documented and periodically reviewed according to the defined review schedule, approved by MLC leadership.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems.
- Backup media must be protected in accordance with the highest sensitivity level of information stored.
- Backups must be periodically tested to ensure that they are recoverable in accordance with the backup standard.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Backups containing confidential information must be encrypted in accordance with IS0001 - Encryption Policy.
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
    - Creation Date
    - Sensitivity Classification

Removable Media

- The use of removable media for storage of MLC information must be supported by a reasonable business case.
- All removable media must be approved by IT Services or leadership prior to use.
- Personally owned removable media use is not permitted for storage of MLC information.
- Users are not permitted to connect removable media from an unknown origin.
- Confidential and internal information must not be stored on removable media without the use of encryption.
- The loss or theft of a removable media device that may have contained any information, regardless of sensitivity, must be reported to IT Services.

References

The following documents are referenced above:

- IS0001 - Encryption Policy

Exceptions

Exceptions to any policies, provision, guidelines, procedures, etc. of the MLC Information Security Program can be sought out by following IS0008 - Information Security Exception Policy.

Compliance

Your signature of acknowledgment as part of the annual Lay and Called Worker Handbook Acknowledgement, indicates that you have read all of the MLC Information Security Policies, including this policy, and that you will abide by the regulations set forth in the Information Security Policies.

Revisions

Date	Comment	Approver
Nov 20, 2023	Initial draft	
Nov 20, 2023	Recommended for adoption	Information Security Committee
Nov 30, 2023	Approved for adoption	MLC Administrative Council
Oct 21, 2024	Reviewed	Information Security Committee
May 1, 2026	Reviewed and revised	Director of IT