IS0006 - Incident Management Policy

Purpose

The purpose of the MLC Incident Management Policy is to describe the requirements for dealing with information security incidents.

Scope

The policy applies to executive management and other individuals responsible for protecting MLC Information Resources.

Definitions

Policy

Incident Handling Team (IHT)

The IHT is responsible for:

- ensuring that incident response activities are carried out in accordance with legal, contractual, and regulatory requirements.
- internal and external communications pertaining to information security incidents.
- ensuring that personnel are trained on how to report a potential incident.

The IHT is made up of the following individuals:

- Vice President of Administration
- Director of Information Technology
- Director of Human Resources
- Director of Financial Services
- Director of Public Relations
- WELS Information Security Analyst

Response Team

- An Incident Response Commander will be appointed to oversee and direct incident response activities by the IHT.
- The Incident Response Commander will assemble and oversee a Cyber Security Incident Response Team (CSIRT).

- The CSIRT will respond to identified cyber security incidents following the Incident Response Plan.
- The Incident Response Commander is responsible for appropriately reporting incidents to the IHT.

Incident Response Plan (IRP)

- The Incident Response Commander is responsible for overseeing the creation, implementation, and maintenance of an Incident Response Plan (IRP).
- IS0007 - Incident Response Plan must be reviewed by the Information Security Committee annually.

Incident Reporting

- Management must provide a means for all personnel to report potential incidents. Reporting methods should ensure that a potential incident is promptly escalated to the appropriate person.
- IT Services is responsible for monitoring event logging, vulnerability management, and other logs for suspicious activities.
- All reported incidents must be assessed by a qualified member of IT Services to determine the threat type and activate the appropriate response procedures. Any personnel assessing possible threats must be familiar with how to assess and escable a potential incident.
- IT leadership must report any potential breaches and/or incidents involving customer or stakeholder data to the Incident Handling Team (IHT) promptly.

Notification and Communication

The IHT is responsible for ensuring that notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements take place in a timely manner.

All Information concerning an incident is considered confidential, and at no time should any information be discussed with anyone outside of Martin Luther College without approval of executive management and our legal counsel.

Personnel

- Personnel should be notified whenever an incident or incident response activities may impact their work activities.
- Internal communications should aim to avoid panic, avoid the spread of misinformation, and notify personnel of appropriate communication channels.

Interaction with Law Enforcement

- Interaction between law enforcement and emergency services personnel should be coordinated by the Incident Response Commander or a member of the IHT.
- Legal counsel should be consulted in communications with law enforcement.

Customers and Partners

- All customers and partners who are affected by the incident must be notified according to applicable contract language, service level agreements (SLAs), applicable statutes and/or regulations.
- Communications with customers and partners must be consistent, with the same or similar message delivered to each.

Regulatory Authorities

- Only members of the IHT are permitted to discuss the nature and/or details of an incident with any regulatory agencies.
- The IHT must contact regulators as required or as soon as practical.

Public Media

- The IHT or executive management will assign a designated spokesperson responsible for communication with the media.
- Inquiries from media agencies must be directed to the designated spokesperson and the IHT.

References

The following documents are referenced above:

- IS0007 - Incident Response Plan

Exceptions

Exceptions to any policies, provisions, 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
Feb 19, 2024	Reviewed	Information Security Committee
May 1, 2026	Reviewed and revised	Director of IT