IS0004 - Information Security Audit Policy

Purpose

The purpose of the MLC Information Security Audit Policy is to establish the requirements for conducting audit-related reviews on information security resources, policies, and practices at MLC institutions.

Scope

The Information Security Audit Policy applies to any entity or process that maintains or has access to MLC information resources in any tangible manner.

Definitions

Policy

- All information resources that create, collect, store, and/or process confidential information must be audited on a regular basis, according to a documented schedule.
- The scope and conduct of information resource audits must be done in accordance with documented standards and/or procedures. The scope of these audits must fulfill all compliance requirements established in the MLC Information Security Policy. These include but are not limited to GDPR, FERPA, GLBA, and PCI compliance.
- System security audits must be led by information security personnel with the specialized training necessary to conduct such audits.
- Personnel conducting system security audits should communicate the following information to information resource owners, custodians, and users, prior to conducting an audit:
    - The date in which the audit will begin,
    - The date in which the audit will end,
    - The scope of the audit,
    - The purpose of the audit,
    - The potential, even if slight, of service disruption.
- Information resource owners and custodians must provide reasonable access to information resources in order for audit personnel to conduct security audits in accordance with the documented purpose and scope of the audit.
- All pertinent security audit activities and results must be documented.

- Every security audit deficiency must be accompanied with a recommendation.
- Audit summary reports must be created for each system security audit conducted, and the reports must be provided to the Information Security Committee and Administrative Council at the conclusion of the audit.
- The security of exchanges of information, are the subject of policy development and compliance audits.
- The Information Security Team will conduct an internal audit each year.
- A third-party vendor approved by the Information Security Committee will conduct an audit at least every three years. A third-party audit may be conducted ad hoc at the discretion of the Information Security Committee. The above entities are subject to this audit.
- All audit data must be stored in compliance with the procedure document for the specified audit.
- All audit results will be reported to the MLC Information Security Team and other relevant persons and groups as determined by the procedure for the audit in question. This will include, but is not limited to, the Administrative Council, the Information Security Committee, as well as designated individuals from any of the subject entities.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties. Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

References

The following documents are referenced above:

- None

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.

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