MCLA Massachusetts College of Liberal Arts

PL11 - Acquisition and Development

Version: 1.1
Issued: 1/12/2022

PURPOSE

The purpose of this policy is to define the process for the development and acquisition of Massachusetts College of Liberal Arts (MCLA) applications and information systems.

SCOPE

This policy applies to all internally developed applications and all acquisition of information systems.

POLICY

Development:

- Development of applications shall be conducted using secure coding techniques and must in accordance with the SDLC procedures.
- All internally developed applications shall have source code securely maintained with appropriate revision controls.
- Applications shall have source code reviewed and must be tested prior to deployment.
- Database and application test environments shall be separated from the production environment.

Acquisition:

- All systems (hardware or applications) shall meet applicable compliance requirements for laws, regulations, and industry requirements.
- Acquired systems shall be reviewed to ensure that proper review of the following
    - Security capabilities, deficiencies, and vulnerabilities
    - Hardware and software requirements to interface with existing systems
    - Existing systems ability to perform the same functions
    - Licensing agreements for all software.
    - Hidden costs of ownership (licensing, ownership, provisioning)
- Prior to the acquisition of major systems or applications, internal evaluation shall be conducted by the CIO to account for internal costs, including administration, training, networking support, and other costs. *Note: This does not apply to group acquisitions or purchases.*

ENFORCEMENT

Any employee found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action subject to the appropriate collective bargaining agreement.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
CIO, Chief Information Officer	Review and approve requirements, requests, and trade studies for new systems and applications.
IT Staff	Acquire and/or develop IT software/systems according to the policy.
Management Team	Involve Information Technology on any acquisition of hardware or software. Approve the requirement for new systems and software.

PL11 - Acquisition and Development

Version: 1.1
Issued: 1/12/2022

REFERENCES

Framework	**Name**	**Reference**
	CoBiT 4.1	PO3 PO5 PO8 AI1 AI2 AI3
	ISO 27001	A.6.1.5 Information security in project management A.14.1.1 Information security requirements analysis and specification A.14.2.1 Secure development policy A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing
	SANS CSC V6	CSC 18: Application Software Security
	SANS CSC V6	CSC 18: Application Software Security
Regulations and Requirements	**Name**	**Reference**
	PCI DSS 3.1	Requirement 6 Requirement 12
	MA 201 CMR 17	§ 17.04
Supporting Standards and Procedures		

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	2/19/2016	Compass ITC	Initial Draft
1.1	01/06/2022	Ian Bergeron	Proposed Policy