MCLA MASSACHUSETTS COLLEGE of Liberal Arts

PL12 - Business Continuity

Version: 1.0
Issued: 2/19/2016

PURPOSE

The purpose of this policy is to define how Massachusetts College of Liberal Arts (MCLA) will prepare and respond to disruptions to availability of organizational information resources and define the process for the recovery.

SCOPE

This policy applies to the MCLA Business Continuity Plan as well as supporting backup and recovery processes for MCLA information resources.

POLICY

Business Continuity Planning:

The Business Continuity Plan and recovery procedures shall ensure that information security is maintained to protect non-public information as required in normal operations during the recovery process and while operating in alternate facilities and using alternate processes.

A high-level recovery plan will be documented and communicated to applicable personnel on at least an annual basis. The plan shall include the process to declare an emergency and the logistics of contacting key individuals that will be responsible for recovering the systems.

When enacted, the plan achieves the following objectives:

- Ensure employee safety
- Address all possible disasters, emergencies, or disruptive incidents which could have a negative impact on the operations of the organization
- Identify staff necessary to perform critical functions defined within the plan
- Contain a call tree with information on emergency contact details, strategies to mitigate impact, procedures to be implemented, and communication processes to be followed in response to a critical, serious, or irritating disruptive event
- Take inventory of information systems assets such as computer hardware and software
- Provide the means necessary to handle all incidents in a controlled and structured manner
- Assist management in providing swift and decisive leadership for a successful recovery
- Minimize disruptions of service to the organization
- Reduce the risk of the organization's inability to operate in the face of various crisis situations, thereby limiting potential losses.
- Afford the employees the means to efficiently and effectively carry out their tasks and responsibilities
- Prioritization of key organizational functions
- Creation of a public relations plan to assist with effective handling of an incident
- The plan will be reviewed at least annually, and when a restructuring of the organization occurs, new products or services are introduced or significant changes in the information technology architecture takes place to ensure appropriate systems, staff, assignments, and contact information are all accurate
- Training for all staff regarding the business continuity plan and their responsibilities based on their role will take place at a minimum on an annual basis and when there are significant changes to the plan

- Testing of the plan will be coordinated by the IT Manager and/or the Chief Operating Officer and will be tested on an annual basis at minimum
- Testing of the plan shall take place in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed
- Test results will be documented indicating successes, deficiencies, and improvements with a plan developed to remediate the deficiencies

Backup and Recovery:

- All critical systems and data must be backed up on a defined and regular scheduled basis based on organizational need and risk.
- The backup scheme must provide more than one (1) level of backup to a previous point in time, to cover the organization in case of the failure of the primary backup mechanisms.
- Restricted and Confidential data shall be encrypted on backup media.
- Backup and archive media shall be inventoried at least every twelve (12) months to ensure that all media is accounted for and is available for use when necessary.
- Recovery procedures must be tested at least every twelve (12) months to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery
- Backup and recovery documentation must be reviewed and updated on an annual basis at minimum to account for new technology, business changes, and migration of applications to alternative platforms
- Backups and archives will be treated with the same level of criticality and sensitivity as the data and applications stored on them

ENFORCEMENT

Any employee found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including termination of employment.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
IT Manager	Ensure the BCP and supporting procedures can be executed by Information Technology. Ensure information security is built into the plan to address security and privacy laws, regulations and standards. Provide mechanisms to ensure backup and archival process are implemented following the guidelines of Organizational Management and Legal Counsel. Perform reviews to ensure compliance with this policy.
IT Staff	Define data and systems to be backed up including the content, frequency, and retention time. Define data to be archived for legal and/or regulatory purposes in conjunction with the IT Manager

PL12 - Business Continuity

Version: 1.0
Issued: 2/19/2016

ROLE	RESPONSIBILITY
Management Team	Identify and document key organizational processes, data and their priority as part of this policy. Ensure the BCP is up to date, training takes place and the plan is tested at a minimum annually.

REFERENCES

Framework

Name	Reference
CoBiT 4.1	DS4 DS5
ISO 27001	A.11.1.4 Protecting against external and environmental threats A.12.3.1 Information backup A.17.1.1 Planning information security A.17.1.2 Implementing information security continuity A.17.1.3 Verify, review and evaluate information security continuity A.17.2.1 Availability of information processing facilities A.18.1.3 Protection of records
SANS CSC V6	CSC 10: Data Recovery Capability
SANS CSC V6	CSC 10: Data Recovery Capability

Regulations and Requirements

Name	Reference
PCI DSS 3.1	Requirement 2 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