LE MOYNE
Greatness meets Goodness

POLICY:
INFORMATION SECURITY

DOCUMENT #: POL-0001
EFFECTIVE: 01-JAN-2017
OWNER: ISO

CONTENTS

LE MOYNE
Greatness meets Goodness

1.0 INTRODUCTION

This Information Security Policy assists Le Moyne College (LMC or College) in its efforts to fulfill its fiduciary responsibilities relating to the protection of information assets, and comply with regulatory and contractual requirements involving information security and privacy. This policy framework consists of eighteen (18) separate policy statements, with supporting Standards documents, based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-53 r4.

Although no set of policies can address every possible scenario, this framework, taken as a whole, provides a comprehensive governance structure that addresses key controls in all known areas needed to provide for the confidentiality, integrity and availability of LMC's information assets. This framework also provides LMC administrators with guidance necessary for making prioritized decisions, as well as justification for implementing organizational change.

2.0 PURPOSE

The purpose of this Information Security Policy is to clearly establish that each member of the College community has a role in protecting LMC's information assets, and to communicate minimum expectations and requirements. Fulfilling these objectives enables LMC to implement a comprehensive, system-wide Information Security Program.

3.0 SCOPE

The scope of this Policy includes all information assets governed by LMC. All personnel and service providers who have access to or utilize assets of LMC, including data at rest, in transit or in process must be subject to these requirements. This Policy applies to all information assets and IT resources operated by LMC; all information assets and IT resources provided by LMC through contracts, subject to the provisions and restrictions of the contracts; and all authenticated users of LMC information assets and IT resources.

All third parties with access to LMC's non-public information must operate in accordance with a service provider contract containing security provisions consistent with the requirements promulgated under the Gramm-Leach-Bliley Act.

4.0 IMPLEMENTATION

LMC needs to protect the availability, integrity and confidentiality of data while providing information resources to fulfill its academic mission. Administration is responsible for the development, implementation and maintenance of a comprehensive Information Security Program for LMC that is risk-based. This includes security policies, standards and procedures which reflect best practices in information security.

LMC's administration recognizes that fully implementing all controls within the NIST Standards is not possible due to organizational limitations and resource constraints. Administration must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practicable.

5.0 ROLES AND RESPONSIBILITIES

LMC has assigned the following roles and responsibilities:

1) Director for Information Technology: The Director for Information Technology is responsible for the implementation of the Information Security Program including:

    a) Security Policies, Standards, and Procedures; and

    b) Security Compliance including managerial, administrative and technical controls.

2) Information Security Committee: The Committee is responsible for the design, implementation, operations and compliance functions of the Information Security Program for all LMC constituent units. The Committee is comprised of Senior Staff and functions as the Information Security Program Office.

6.0 INFORMATION AND SYSTEM CLASSIFICATION

LMC must establish security categories for both information and information systems. For more information, reference the Data Classification Policy.

7.0 PROVISIONS FOR INFORMATION SECURITY STANDARDS

The LMC Security Program is framed on National Institute of Standards and Technology (NIST) and controls implemented based on SANS Critical Security Controls priorities. LMC must develop appropriate control standards and procedures required to support the College's

Information Security Policy. This Policy is further defined by control standards, procedures, control metrics and control tests to ensure functional verification.

The LMC Security Program is based on NIST Special Publication 800-53; this publication is structured into 18 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements, including but not limited to the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), New York State Information Security Breach and Notification Act, and the Payment Card Industry Data Security Standard (PCI-DSS).

7.1 ACCESS CONTROL (AC)

LMC must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

7.2 AWARENESS AND TRAINING (AT)

LMC must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of LMC information systems; and (ii) ensure that LMC personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

7.3 AUDIT AND ACCOUNTABILITY (AU)

LMC must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

7.4 ASSESSMENT AND AUTHORIZATION (CA)

LMC must: (i) periodically assess the security controls in College information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in College information systems; (iii) authorize the operation of College information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

7.5 CONFIGURATION MANAGEMENT (CM)

LMC must: (i) establish and maintain baseline configurations and inventories of College information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in College information systems.

7.6 CONTINGENCY PLANNING (CP)

LMC must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the College's information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

7.7 IDENTIFICATION AND AUTHENTICATION (IA)

LMC must identify information system users, processes acting on behalf of users, or devices and authenticate the identities of those users, processes, or devices, as a prerequisite to allowing access to LMC information systems.

7.8 INCIDENT RESPONSE (IR)

LMC must: (i) establish an operational incident handling capability for College information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate College officials and/or authorities.

7.9 MAINTENANCE (MA)

LMC must: (i) perform periodic and timely maintenance on College information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

7.10 MEDIA PROTECTION (MP)

LMC must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; (iii) use encryption, where

applicable, and (iiii) sanitize or destroy information system media before disposal or release for reuse.

7.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

LMC must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

7.12 PLANNING (PL)

LMC must develop, document, periodically update, and implement security plans for College information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

7.13 PERSONNEL SECURITY (PS)

LMC must: (i) ensure that individuals occupying positions of responsibility within the College are trustworthy and meet established security criteria for those positions; (ii) ensure that College information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with LMC security policies and procedures.

7.14 RISK ASSESSMENT (RA)

LMC must periodically assess the risk to College operations, College assets, and individuals, resulting from the operation of College information systems and the associated processing, storage, or transmission of College information.

7.15 SYSTEM AND SERVICES ACQUISITION (SA)

LMC must: (i) allocate sufficient resources to adequately protect College information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures, through federal and New York

state law and contractual obligation, to protect information, applications, and/or services outsourced from the College.

7.16 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

LMC must: (i) monitor, control, and protect College communications (i.e., information transmitted or received by College information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within College information systems.

7.17 SYSTEM AND INFORMATION INTEGRITY (SI)

LMC must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within College information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

7.18 PROGRAM MANAGEMENT (PM)

LMC must implement Security Program management controls to provide a foundation for the College Information Security Program.

8.0 ENFORCEMENT

LMC may temporarily suspend or block access to any individual or device when it appears necessary to do so in order to protect the integrity, security, or functionality of the College and computer resources. Violations of this policy may result in penalties and disciplinary action in accordance with the Student Handbook, Faculty Handbook and/or rules governing employment at LMC.

9.0 PRIVACY

Users do not acquire a right of privacy for data transmitted or stored on College information systems. LMC may access, review, monitor or disclose data associated with an individual's account in response to a judicial order or any other action required by law, or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the College.

10.0 EXCEPTIONS

Exceptions to the policy may be granted by the Director for Information Technology, or his or her designee. All exceptions must be reviewed annually.

11.0 DISCLAIMER

LMC disclaims any responsibility for and does not warrant information and materials residing on non-LMC systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of LMC, its faculty, staff or students.

12.0 REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- New York State Information Security Breach and Notification Act
- NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April, 2013.)
- FIPS-199 (Standards for Security Categorization of Federal Information and Information Systems, Feb, 2004.)
- PCI DSS 3.1 (Data Security Standard, version 3.1. and Associated Documents)
- NIST Cybersecurity Framework (NIST Framework for Improving Critical Infrastruture Cybersecurity, version 1.0, Feb 12, 2014.)

13.0 RELATED POLICIES

- Le Moyne College Data Classification Policy, Procedure and Quick Reference Guide
- Acceptable Use Policy

14.0 RESPONSIBLE DEPARTMENT

Information & Technology Services (a.k.a. Information Technology)

15.0 POLICY AUTHORITY

This policy is issued by the Information Security Committee for Le Moyne College.

Le Moyne College

LE MOYNE
Greatness meets Goodness

16.0 REVISION HISTORY

Version	Date	Author	Revisions
1.00	04-14-16	GreyCastle Security	Initial Draft
1.01	04-21-16	GreyCastle Security	Policy Updates
1.02	05-11-16	GreyCastle Security	Policy Updates
1.03	06-24-16	GreyCastle Security	Final Draft
1.04	01-01-2017	Le Moyne College	

17.0 APPROVALS

Executive	Information Security Officer
Name	Name
Title	Title
Date	Date
Signature	Signature