LE MOYNE
Greatness meets Goodness

POLICY:
DATA CLASSIFICATION

DOCUMENT #: POL-0003
EFFECTIVE: 01-JAN-2017
OWNER: ISO

CONTENTS

LE MOYNE
Greatness meets Goodness

1.0 PURPOSE

The purpose of this Data Classification Policy is to define the data classification requirements for Le Moyne College's (LMC or College) information assets and to ensure that data is secured and handled according to its sensitivity and impact that theft, corruption, loss or exposure would have on the Institution. This Policy has been developed to assist LMC and provide direction to the Institution regarding identification, classification and handling requirements of information assets.

2.0 SCOPE

The scope of this Policy includes all information assets governed by Le Moyne College. 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.

3.0 POLICY

LMC has established the requirements enumerated below regarding the classification of data to protect the Institution's information.

3.1 DATA OWNERSHIP AND ACCOUNTABILITY

Data owners are identified as the individuals, roles or committees primarily responsible for information assets. These individuals are responsible for identifying the Institution's information assets under their areas of supervision, and maintaining an accurate and complete inventory for data classification and handling purposes.

Data owners are accountable for ensuring that their information assets receive an initial classification upon creation and a re-classification whenever reasonable. Re-classification of an information asset should be performed by the asset owners whenever the asset is significantly modified. Data owners are also responsible for reporting deficiencies in security controls to College Administration.

3.2 DATA CLASSIFICATION

Classification of data will be performed by the data asset owner based on the specific, finite criteria as identified in the Federal Information Processing Standard Publication 199 (FIPS-199) for confidentiality, integrity and availability. Refer to the Data Classification and Handling

Procedure to determine how data should be classified. Data classifications will be defined as follows:

- *PROTECTED* - Information assets whose loss, corruption, or unauthorized disclosure would cause financial loss or would result in regulatory or government sanctions such as violations of federal or state laws or security breaches that result in the compromise of customer or associate private information. Common examples include but are not limited to banking, health and payment card information; personnel records; and information systems' authentication data.

- *SENSITIVE* - Information assets whose loss, corruption, or unauthorized disclosure would not seriously impair business functions but is otherwise private. Examples include financial statements, contracts and legal information.

- *PUBLIC* - Information assets whose loss, corruption, or unauthorized disclosure would not impair business functions. Examples include sales and marketing strategies, web site content, building plans and promotional information.

- *RESEARCH*: Recorded factual material commonly accepted in the scientific community as necessary to validate research findings. Security controls addressing information classified as "Research" are at the discretion of the College.

3.3 DATA HANDLING

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods. The specific methods must be described in the Data Classification Procedure.

3.4 RE-CLASSIFICATION

A re-evaluation of classified data assets will be performed at least once per year by the responsible data owners. Re-classification of data assets should be considered whenever the data asset is modified, retired or destroyed.

3.5 CLASSIFICATION INHERITANCE

Assets, logical or physical, that "contain" a data asset may inherit classification from the data asset(s) contained therein. In these cases, the inherited classification shall be the highest classification of all contained data assets.

4.0 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, Employee Handbook, Faculty Handbook and/or other policies and procedures governing acceptable employee and student behavior.

5.0 EXCEPTIONS

Exceptions to this Policy must be approved in advance by the Director for Information Technology, at the request of the responsible data asset owner. Approved exceptions must be reviewed and re-approved by the asset owner annually.

6.0 REFERENCES

- Procedure – Data Classification and Handling
- Federal Information Processing Standard Publication 199 (FIPS-199)
- NIST Special Publication 800-53 r4

7.0 RELATED POLICIES

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

8.0 RESPONSIBLE DEPARTMENT

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

9.0 POLICY AUTHORITY

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

LE MOYNE
Greatness meets Goodness

10.0 REVISION HISTORY

Version	Date	Author	Revisions
1.00	04-20-16	GreyCastle Security	Original
1.01	05-11-16	GreyCastle Security	Policy Updates
1.02	06-24-16	GreyCastle Security	Final Draft
1.03	01-01-2017	Le Moyne College	

11.0 APPROVALS

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