Marywood University

Policies and Procedures

Information Classification and Management Policy

Policy Statement:

The purpose of the Marywood University Information Classification and Management Policy is to provide a system for classifying and managing Information Resources according to the risks and regulations associated with its storage, processing, transmission, and destruction.

Procedures: Information Handling

Public:

- Disclosure of Public Information must not violate any pre-existing, signed non-disclosure agreements.

Internal:

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
- Must be protected by a confidentiality agreement before access is allowed.
- Must be stored in a closed container (i.e., file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Is the "default" classification level if one has not been explicitly defined.

Confidential:

- When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords.
- Must be encrypted
- Must be stored in a locked drawer, room, or area where access is controlled to prevent unauthorized access by members of the public, visitors, or other persons without a need to know.

Must not be transferred via unsecure communication channels, including, but not limited to:

- Unencrypted email
- Text messaging
- Instant Messaging
- Unencrypted FTP
- Mobile devices without encryption
- When sent via fax, it must be sent only to a previously established and used number or one that has been verified as using a secure location.
- When transmitted via USPS or other mail services, it must be enclosed in a sealed security envelope.

- Must not be posted on any public website.
- A person who learns or becomes aware that information classified as Confidential has been or is suspected of being lost or disclosed to unauthorized parties must immediately notify both Office of Information Technology (OIT) and their direct supervisor.

Information Storage:

The chart below defines acceptable storage locations for information:

Storage Location	**Description**	**Confidential Protected Level 1**	**Internal Protected Level 2**	**Public Protected Level 3**
Google Drive	An enterprise solution that allows faculty/staff users to store, share and edit files as part of Google G Suite	🚫	🚫	✓
OneDrive	An enterprise service that allows students, faculty, and staff to store, share and edit files within online apps as part of Microsoft Office 365	🚫	✓	✓
SharePoint	An online collaboration space that is part of Office 365	🚫	🚫	✓
IT Network File Shares	Network drives only accessible on the MU Network and managed by MU IT staff	🚫	🚫	✓
University owned devices	Local workstation or laptop managed by MU	🚫	🚫	✓
NON-University owned devices	Personal Computers or devices not owned or managed by MU	🚫	🚫	✓
Portable Storage	Thumb drives, portable hard drives, or any other portable device that is capable of storing files	🚫	🚫	✓
System of Record	Slate, Colleague, Raisers Edge	✓	✓	✓

Definitions:

Information Classification

Information owned, used, created or maintained by Marywood University should be classified into one of the following three categories:

Public – Protected Level 3

- Is information that may or must be open to the general public.
- Has no existing local, national, or international legal restrictions on access or usage.

- While subject to Marywood University disclosure rules, it is available to all Marywood University employees and all individuals or entities external to the corporation. Examples of Public Information include:
- Publicly posted press releases, ● Publicly available marketing materials, ● Publicly posted job announcements.

Internal – Protected Level 2

- Is information that must be guarded due to proprietary, ethical, or privacy considerations.
- Must be protected from unauthorized access, modification, transmission, storage or other use.
- Is restricted to personnel designated by Marywood University, who have a legitimate business purpose for accessing such Information.
- Is information that must be guarded due to proprietary, ethical, or privacy considerations.
- Must be protected from unauthorized access, modification, transmission, storage or other use.
- Is restricted to personnel designated by Marywood University, who have a legitimate business purpose for accessing such Information.

Examples of Internal Information include:

- FERPA: Student information, Educational Records not defined as directory information, Grades, courses taken, schedule, Test scores, advising records, educational services received, disciplinary actions, student photo
- Campus Financials
- Campus Attorney-Client information
- Employee Information: Name with home address, personal email, home phone, marital status, gender, evaluation, personnel actions
- Organizational charts, contracts Internal Information must be:
- Restricted to personnel who have a legitimate business purpose
- Guarded/protected from unauthorized access

Confidential Information – Protected Level 1

- Is information protected by statutes, regulations, Marywood University policies or contractual language. Information Owners may also designate Information as Confidential.
- Is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a "need-to know" basis only.
- Disclosure to parties outside of Marywood University must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.

Examples of Confidential Information include:

- HIPAA, Health Records, Health Insurance Data
- Personally Identifiable Information (PII) – Name with Personally identifiable information SSN, Passport, Visa, etc.
- Gramm-Leach-Bliley Act (GLBA) – Name with Financial Information, Bank Accounts, Tax Returns, etc.
- Federal Tax Information (FTI) included on the FAFSA used to determine an applicant's eligibility for student aid.
- Payment Card Industry Data Security Standard (PCI-DSS): Payment card information, Credit Card Numbers, Bank Account and Routing numbers, Law Enforcement Records: Name with Driver's License, Criminal Background.

Campus Access Credentials:

- Passwords or credentials that grant access to Level 1 and Level 2 data Confidential Information must:
- Be encrypted at rest
- Be protected by statutes and regulations
- Never be sent through email

Policy History: 2025-05-22: The President approved this policy as recommended by the Policy Committee of the University at their May 9, 2025 meetings.

Related Committees and Policies:

Records Management and Archives Policy

MARYWOOD UNIVERSITY
POLICIES AND PROCEDURES

Mary Theresa Gardier Paterson, Esquire Secretary of the University and General Counsel