ILLINOIS WESLEYAN UNIVERSITY	*INFORMATION CLASSIFICATION POLICY*
Effective Date: 03/20/2025	Version 1.0

CONTENTS

Purpose

The purpose of this policy is to define the data classification requirements for 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 organization. This policy has been developed to assist Illinois Wesleyan University and provide direction to the organization regarding identification, classification, and handling of information assets.

Scope

The scope of this policy includes all information assets governed by Illinois Wesleyan University. All personnel and third parties who have access to or utilize information assets to process, store and/or transmit information for or on behalf of Illinois Wesleyan University shall be subject to these requirements. Because course materials and faculty research generally do not contain Personally Identifiable Information (PII), such materials are exempt from the Information Classification Policy. Faculty can refer to the Intellectual Property Policy regarding ownership of course materials and the Institutional Review Board policy and procedures for information about ethical research practices, including the collection, storage, and sharing of research data, respectively.

Roles and Responsibilities

- Data Governance Committee – Responsible for creating and managing asset inventories used to store, process, transmit or provide access to electronic information. IT Security is the custodian for this policy.
- CIO – Responsible for monitoring the implementation of this policy and reporting to senior management on any abnormal findings or exceptions.
- All Employees –
    - Responsible for classifying and marking all created or modified information, including any reproductions that are made (e.g. reports).
    - Responsible for appropriate handling of all classified information (electronic or non-electronic).
- Data Administrators - members of the President's Cabinet**,** are responsible for the overarching principles of data governance and usage in each functional area of the University. This group helps communicate the value of data governance

throughout the University. As such, they approve the policies, standards and procedures developed by the Data Governance Committee and will ensure that the data governance program is aligned with business needs and that goals and policies are enforced.

- Data Stewards - individuals, roles, or committees primarily responsible for information assets. These individuals are responsible for:
    - Identifying the organization's information assets under their areas of supervision; and
    - Maintaining an accurate and complete inventory for data classification and handling purposes.
    - Ensuring information assets receive an initial classification upon creation.
    - Re-classification of an information asset should be performed by the asset owners whenever the asset is significantly modified.
    - Reporting deficiencies in security controls to management.

Policy

Illinois Wesleyan University has established the requirements enumerated below regarding the classification of data to protect the organization's information.

Data Classification

Classification of data will be performed by the data asset owner based on the specific, finite criteria. Refer to the descriptions in Appendix B of the Data Classification and Handling Procedure to determine how data should be classified. Data classifications will be defined as follows:

- *RESTRICTED* - Information whose loss, corruption, or unauthorized disclosure would cause **severe** personal, financial, or reputational harm to the organization, organization staff or the constituents we serve. Federal or state breach notification would be required, identity or financial fraud, extreme revenue loss, or the unavailability of extremely critical systems or services would occur. Common examples include, but are not limited to, social security number, banking and health information, payment card information and information systems' authentication data.

- *PRIVATE* – Information whose loss, corruption, or unauthorized disclosure would likely cause **limited** personal, financial, or reputational harm to the organization, organization staff or the constituents we serve. Federal or state breach notification would not be required, limited identity theft and very little revenue loss would occur, and the availability of critical systems would not be affected. Common examples include, but are not limited to, some data elements found in HR employment records, unpublished research data, and passport and visa numbers.

- *PUBLIC* – Information whose loss, corruption, or unauthorized disclosure would cause **minimal or no** personal, financial or reputational harm to the organization, organization staff or the constituents we serve. Common examples include, but are not limited sales and marketing strategies, promotional information, published research data, and policies.

DIRECTORY INFORMATION

Directory Information in this context does not refer to the University Directory published on the IWU website. Rather it is a set of data which is considered to be unrestricted and the release of which is likely to result in little or no risk to the University or individual. This data should be considered information that may be shared, but whose use is limited by both circumstances and best practices, e.g., the Registrar's Office for student information and Human Resources for workforce information.

Workforce Information is defined as the following:

- Name
- Date of hire
- Date of separation
- Current position title
- Employment status
- Department of assignment, including office telephone number and office address

Student Directory Information is defined as the following:

- Name of student

- Telephone number
- Email address
- Class level
- Dates of attendance
- Major field of study
- Number of course units in which student is enrolled
- Degrees and honors received
- Last school attended
- Participation in official student activities
- For intercollegiate athletic team members only:
    - Name
    - Height
    - Weight

Data Handling

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods.

To assist and support authorized users, additional guidance on classifying data and requirements for handling data in specific scenarios is outlined in Appendices B and C of the Data Classification and Handling Standard and Procedure. <Link to Information Handling Guidelines>

Labeling

Information labeling is the practice of marking an information system or document with its appropriate classification levels that others know how to appropriately handle the information.

There are several methods for labeling information assets.

- **Printed/Emailed**: Restricted information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain Illinois Wesleyan University's classification in the document.

- **Displayed**: Restricted or Internal information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.
- Materials that will be utilized internally at Illinois Wesleyan University are expected to be handled in accordance with their classification based on the training provided to employees.

Re-Classification

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

Classification Inheritance

Logical or physical assets 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.

Access

Information Stewards are responsible for ensuring all workforce are provisioned appropriate access to information and information systems. Access to information and information systems will be provisioned on a least privilege basis. Should additional access be required to perform job functions, reference the organization's Access Control Procedure for steps on how to request additional access:

[Insert Link to Access Control Procedure]

Retention & Destruction

Information will be retained in compliance with organization defined retention schedules

[Insert Link to Retention Schedule]

Information will be destroyed in compliance with organization defined destruction procedures:

[Insert Link to Destruction Procedure]

Asset Inventory

See Asset Inventory matrix located here: [Insert Link to Asset Inventory and Information Classification].

Enforcement

Users who violate this policy may be denied access to the organization's resources and may be subject to penalties and disciplinary action both within and outside of the organization. The organization may temporarily suspend or block access to an account prior to the initiation or completion of such procedures, when it appears reasonably necessary to do so in order to protect the integrity, security or functionality of the organization or other computing resources or to protect the organization from liability.

Exceptions

Exceptions to this policy must be approved in advance by the Chief Information Officer, at the request of the responsible data asset owner. Approved exceptions must be reviewed and re-approved by the asset owner annually.

References

- Federal Information Processing Standard Publication 199 (FIPS-199)
- NIST Special Publication 800-53 r5

Related Policies

- Acceptable Use Policy
- Information Security Policy

Compliance

Any employee found to have violated the provisions in this plan will be subject to Illinois Wesleyan University disciplinary procedures, as defined in the employee handbook and other relevant policies.

Ownership and Review

This document is owned by the CIO.

This document shall be reviewed on an annual basis.

DOCUMENT PROPERTIES

PROPERTIES	
Property	**Description**
Circulation	Internal Use Only.
Next Scheduled Review	Click or tap to enter a date.

DOCUMENT APPROVALS		
Name	**Title**	Date
		Click or tap to enter a date.
		Click or tap to enter a date.
		Click or tap to enter a date.

REVISION HISTORY			
Version	**Date**	**Description of Changes**	**Revised by**
0.1	10/24/2024	Initial draft version	Data Governance Team
1.0	02/19/2025	**Final Draft**	Data Governance Team
1.0	03/20/2025	**Reviewed by President's Cabinet**	No revisions