THE Wesleyan Way KENTUCKY WESLEYAN COLLEGE	*Information Classification*
Effective Date 1/1/2023	Version 1.0

Contents

THE Wesleyan Way KENTUCKY WESLEYAN COLLEGE	*Information Classification*
Effective Date 1/1/2023	Version 1.0

1. 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 Kentucky Wesleyan College and provide direction to the organization regarding identification, classification and handling of information assets.

2. Scope

The scope of this policy includes all information assets governed by Kentucky Wesleyan College. All personnel and third parties who have access to or utilize information assets to process, store and/or transmit information for or on the behalf of Kentucky Wesleyan College shall be subject to these requirements.

3. Roles and Responsibility

Director of Information Technology

- 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.
- 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 owners - 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.

4. Policy

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

4.1 Data Classification

Classification of data will be performed by the data asset owner based on the specific, finite criteria. Refer to 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 college, college staff, faculty or the students 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.

- *SENSITIVE or INTERNAL* – Information whose loss, corruption, or unauthorized disclosure would likely cause **limited** personal, financial or reputational harm to the college, college staff, faculty or the students 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 college, college staff, faculty or the students we serve. Common examples include, but are not limited sales and marketing strategies, promotional information, published research data, and policies.

4.2 Directory 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

4.3 Data Handling

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

4.4 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 Kentucky Wesleyan College'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 Kentucky Wesleyan College are expected to be handled in accordance with their classification based on the training provided to employees.

4.5 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.

4.6 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.

4.7 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 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:

ITS Policy Handbook

4.8 Retention & Destruction

Information will be retained in compliance with organization defined retention schedules

ITS Policy Handbook

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

ITS Policy Handbook

4.9 Asset Inventory

See Asset Inventory matrix located in:

Commented [RS1]: Does this exist?

Asset Panda

Information Classification Policy

5. 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.

6. Exceptions

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

7. References

- Federal Information Processing Standard Publication 199 (FIPS-199)
- NIST Special Publication 800-171

8. Related Policies

- Acceptable Use Policy
- Information Security Policy

9. Responsible Department

Information Technology

10. Revision History

Version	**Date**	**Author**	**Revisions**
1.00		GreyCastle Security	Original
1.1			

11. Approvals

Executive	**Director of Information Technology**
Name	Name
Title	Title
Date	Date

Signature	Signature