OHIO CHRISTIAN
UNIVERSITY

Information Technology

1476 Lancaster Pike
Circleville, OH 43113
it.ohiochristian.edu
blazertech@ohiochristian.edu
740-420-5907

DOCUMENT #:POL-0003
EFFECTIVE: XX-XXX-2021
OWNER: ISO

DATA CLASSIFICATION

CONTENTS

1.0 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 the impact that theft, corruption, loss, or exposure would have on the university. This policy has been developed to assist Ohio Christian University and provide direction to the university regarding identification, classification, and handling of information assets.

2.0 SCOPE

The scope of this policy includes all information assets governed by Ohio Christian 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 Ohio Christian University shall be subject to these requirements.

3.0 ROLES AND RESPONSIBILITY

- Assistant Director of IT Services and Security Compliance – 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.
- Executive Director of IT– 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 university'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.

4.0 POLICY

Ohio Christian University has established the requirements enumerated below regarding the classification of data to protect the university'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 university, university's staff, or the constituents/people 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, university account numbers, accounts receivable ledgers and schedules, bank statements and reconciliations, deeds, mortgages, bills of sale, contracts, property records, and information systems' authentication data.
- *INTERNAL* – Information whose loss, corruption, or unauthorized disclosure would likely cause **limited** personal, financial, or reputational harm to the university, university's staff, or the constituents/people 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 university, university's staff, or the constituents/people we serve. Common examples include, but are not limited to sales and marketing strategies, promotional information, published research data, and policies.

4.2 DIRECTORY INFORMATION

Workforce Information is defined as the following:

- Name
- Current position title
- Email
- Department of assignment
- Office telephone number
- 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. The specific methods must be described in REF04-Information Handling Guidelines.

4.4 LABELING

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

There are several methods for labeling information assets.

- **Printed/Emailed**: Internal information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain Ohio Christian University's classification in the document.
- **Displayed**: 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 Ohio Christian University 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 restricted 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 that all workforce individuals 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 university's Access Control Procedure for steps on how to request additional access:

4.8 RETENTION & DESTRUCTION

- Information will be retained in compliance with the university's defined retention schedules.
- Information will be destroyed in compliance with the university's defined destruction procedures.

5.0 ENFORCEMENT

Users who violate this policy may be denied access to the university's resources and may be subject to penalties and disciplinary action both within and outside of the university. The university 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 university's computing resources or to protect the university from liability.

6.0 EXCEPTIONS

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

7.0 REFERENCES

- Federal Information Processing Standard Publication 199 (FIPS-199)
- NIST Special Publication 800-171r2

8.0 RELATED POLICIES

- Acceptable Use Policy
- Information Security Policy

9.0 RESPONSIBLE DEPARTMENT

Human Resources

10.0 REVISION HISTORY

Version	Date	Author	Revisions
1.0		Information Technology	Initial Draft

11.0 APPROVALS

Executive	Information Security Officer
Ted Perry	Amber Smith
CFO/COO	Executive Director of Information Technology
Date	Date
Signature	Signature