University of CINCINNATI	*Policy Title:* **Data Governance & Classification**	*Policy Number:* **9.1.1**
Category: Information Technology	**Effective Date:** 09/03/2021	**Policy Owner:** VP & CDO, Digital Technology Solutions
Policy applicable for: Faculty/Staff/Students/ Affiliates	**Prior Effective Date:** 09/25/2019	**Responsible Office(s):** Office of Information Security

Background

The University of Cincinnati uses a variety of data in support of its teaching, research and outreach missions. Data is a valued resource the university must govern, classify and protect. In addition, federal and state laws require that the university must limit access to certain categories of data to protect the privacy of employees, students, subjects, affiliates and patients.

Policy

The purpose of this policy and suite of accompanying resources is to help ensure the governance, classification and protection of university data from unauthorized access, damage, alteration or disclosure while preserving the ability of authorized users to access and use institutional data for appropriate university purposes. This policy refers to all university data, electronic as well as paper. This policy is applicable to all data storage locations and is applicable to all university data used for administration, research, teaching or other purposes.

Data governance is a discipline for assessing, managing, using, improving, monitoring, maintaining and protecting university data. Data governance is used by organizations to exercise control over processes and methods used by their Data Stewards and Data Custodians in order to improve data quality and integrity. When data is created the Data Trustee must classify the data and establish a governance framework for the data that corresponds to the university rules for that data type and applicable federal and state laws.

Data Classification and Data Types

This policy describes the actions necessary to secure and protect university data defined as Controlled Unclassified Information, Restricted data, Controlled data and

Public data. See Data Classification and Data Types for additional information and examples.

- **Controlled Unclassified Information (CUI):** Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act. Export Controlled data is a subset of CUI. Export Controlled data often comes as a specific clause within the Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012)
- **Restricted**: Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates. Users of Restricted data must follow all safeguards for Controlled data plus additional safeguards identified for Restricted data. High levels of security safeguards must be applied to Restricted data.
- **Controlled**: Data is classified as Controlled when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. By default, all institutional data that is not explicitly classified as CUI, Restricted or Public data must be treated as Controlled data. A reasonable level of security safeguards must be applied to controlled data.
- **Public**: Data that is readily available to the public. This data requires no confidentiality or integrity protection. Public data needs no additional protection.

Minimum Safeguards

The responsibility of protecting university data is shared by everyone that uses, accesses or stores such data. Required safeguards depend on the data classification. See Minimum Safeguards for more information.

Roles and Responsibilities

There are four data user roles with differing levels of responsibilities. See Roles and Responsibilities for more information.

- **Trustees**: Senior university officials or their designees who have planning and policy level responsibility for data within their functional areas and management responsibility for defined segments of institutional data.
- **Stewards**: University officials having direct operational-level responsibility for the management of one or more types of institutional data. Data Stewards in coordination with Data Custodians must implement and apply safeguards that meet or exceed the Minimum Safeguards of each data classification.

- **Custodians**: Central or distributed university units or computer system administrators responsible for the operation and management of systems and servers which collect, manage and provide access to institutional data.
- **Users**: University units or individual university community members who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the university.

Collectively these parties are responsible for identifying and implementing safeguards for the different data types. Many university activities involve multiple departments; for such activities that involve access to, or storage of, university data, the procedures and safeguards must be coordinated by all Trustees, Stewards, Custodians and Users involved.

Compliance and Remediation

Incidents involving CUI data must be immediately reported to the Office of Information Security (OIS) via e-mail at abuse@uc.edu. Incidents involving Export controlled data must be reported to OIS and the Export Controls Office via e-mail at exportco@uc.edu. In addition, any breach, loss, or unauthorized exposure of Restricted or Controlled data shall be immediately reported to the unit head and OIS via e-mail at abuse@uc.edu. OIS will then determine the appropriate actions to comply with university Policy and local, state and federal law. See Compliance and Remediation and the Incident Management and Response Policy for additional information.

Cloud Based File Storage

Only university approved cloud based file storage may be used for Restricted and Controlled data. See Cloud Based File Storage for more information.

Controlled Unclassified Information

All departments, colleges or individuals that process, store or transmit CUI must follow all the security controls for restricted data plus additional controls as outlined in **Controlled Unclassified Information** document.

Contact Information

Office of Information Security	513-558-ISEC (4732)	infosec@uc.edu

Related Links

The Data Governance and Classification Policy Supporting Documents:

- Data Classification and Data Types
- Minimum Safeguards
- Roles and Responsibilities
- Compliance and Remediation
- Cloud Based File Storage
- Controlled Unclassified Information

Export Controls Office