University of CINCINNATI	*Policy Title:* **Data Governance & Classification**	*Policy Number:* **9.1.1**
Category: Information Technology	**Effective Date:** 1/25/2017	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: Faculty/Staff/Students/ Affiliates	**Prior Effective Date:** 08/01/2015	**Responsible Office(s):** IT@UC Office of Information Security

Background

The University of Cincinnati (UC) 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, (i.e., hard copy). This policy applies regardless of the place of storage and whether used for administration, research, teaching or other purposes.

Data governance is a quality control 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 Export Controlled data, Restricted data, Controlled data and Public data. See Data Classification and Data Types for additional information and examples.

- **Export Controlled**: As a means to promote national security, the U.S. Government controls export of sensitive data, equipment, software and technology. This data is labeled Export Controlled. Trustees, Stewards, Custodians and Users of Export Controlled data must follow all safeguards for Restricted data plus additional safeguards as directed by the Export Controls Office. Trustees, Stewards and

Custodians of systems that have Export Controlled data are responsible to work with the Export Controls Office to identify appropriate additional safeguards.

- **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 Export Controlled, 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 safegards 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

University community members must report actual or suspected criminal activity to the Department of Public Safety or, if off campus, other appropriate law enforcement agencies. Incidents involving Export Controlled data must be immediately reported to the unit head, the IT@UC Office of Information Security (OIS) via e-mail at abuse@uc.edu and to 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

Export Controlled data is not permitted to be stored or shared via cloud based file storage of any kind. Only university approved cloud based file storage may be used for Restricted and Controlled data. See Cloud Based File Storage for more information.

Contact Information

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

Related Links

The Data Governance and Classification Policy subparts:

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

Export Controls Office

Revision History

Issued: 07/01/2009
Revised: 08/01/2014
Revised: 08/01/2015
Revised: 1/25/2017