UNIVERSITY OF Cincinnati Clermont College **Category:** Information Technology **Applicable for:** Faculty/Staff/Affiliates	*Procedure/Guideline Title:* **Data Classification** **Effective Date:** 03.22.2017 **Prior Effective Date:** **Enabling Act:** Technology Steering Committee Approval	*Number:* **034.TS.107** **Owner:** Technology Steering Committee **Responsible Office(s):** Technology Services

Background

As an institution of higher learning, UC Clermont uses a variety of data in support of daily operations, instruction, research, and outreach missions. As a valued resource the University of Cincinnati (UC) and UC Clermont must govern, classify, and protect its data. Additionally, federal and state laws require the university to limit access to certain data categories to protect the privacy of employees, students, subjects, affiliates, and patients.

All University of Cincinnati personnel are responsible for the protection of sensitive data entrusted to our care; therefor, The UC Office of Information Security (IOS) created the Data Governance & Classification Policy to provide simplified guidance and direction for compliance in a complex environment.

The Data Governance & Classification Policy requires safeguards for Export, Restricted and Controlled data; see Minimum Safeguards and Data Classification and Data Types for details. The UC Clermont Data Classification Procedure has been created in order to identify, classify, and maintain compliance with the UC Data Classification Policy.

Procedure

Identify

- Discover export, restricted, and controlled data storage/usage utilizing a data classification questionnaire, which will be used to survey each faculty/staff member for data type usage. Process to be performed annually.

- Review data classification questionnaire and obtain more information from departments or employees as necessary.

Classify

- Classify data usage/storage based on questionnaire. Classifications may result in standards being implemented departmentally, individually, or college wide (i.e. Laptop data encryption policy.). All data will be managed and handled according to the University approved Minimum Safeguards.

Compliance and Remediation

In order to support the requirements outlined in the Data Governance & Classification Policy and the Minimum Safeguards the UC Clermont Technology Services Department will:

- Work with the college to determine specific data needs and whether usage of controlled or restricted data is necessary.
- Provide strategic direction to the college to meet these requirements.
- Implement the necessary safeguards (i.e. encryption, patching, A/V, firewalls, etc...) to ensure data is secure and requirements are met.
- Provide education in conjunction with OIS regarding compliance with this policy.
- Provide new employees with information regarding the Data Governance & Classification Policy and the Minimum Safeguards. Provide strategic direction to meet these requirements.
- When non-compliance is found work with departments or individuals to: provide consulting/review and remediation in order to bring data usage/storage into compliance.

Use of Information Technology
http://www.uc.edu/content/dam/uc/infosec/docs/policies/Use_of_Information_Technology_Policy.pdf

Contacts
Technology Services 513.732.5216