

 <p><b>Category:</b> Information Technology</p> <p><b>Policy applicable for:</b> Faculty/Staff</p>	<p><i>Policy Title:</i> <b>Data Protection</b></p> <p><b>Effective Date:</b> 07/01/2009</p> <p><b>Prior Effective Date:</b> mm/dd/yyyy</p> <p><b>Enabling Acts:</b> HIPAA, FERPA, GLB, PCI, Ohio HB104</p>	<p><i>Policy Number:</i> <b>9.1.1</b></p> <p><b>Policy Owner:</b> VP and CIO</p> <p><b>Responsible Office(s):</b> Information Security</p>
---	--	--

## Background

The University of Cincinnati uses a variety of data in support of its teaching, research and outreach missions. These data are valued resources that the university should protect. In addition, Federal and State laws require that the University of Cincinnati must limit access to certain categories of data to protect the privacy of employees, students, subjects, and patients. (See Related Links section: Summary of Applicable Laws)

## Policy

The purpose of this policy and suite of accompanying resources is to help ensure the protection of the university's restricted 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." It applies regardless of the place of storage and whether used for administration, research, teaching or other purposes.

This policy describes the actions necessary to secure and protect University-owned data defined as **restricted** and **controlled data**. (See Related Links section: Data Classification for full definitions and examples.) **Controlled Data**, such as proprietary data, graded papers, etc. must also be protected and stored securely. Some data, such as Social Security Numbers, Personal Health and Financial Data need to be handled with the utmost care and must be protected to the greatest possible extent. This latter category of data is defined as **Restricted Data**.

The responsibility of protecting these data is shared by everyone that uses, stores, or comes in contact with such data. (See Related Links section: Minimum Safeguards) Here we differentiate between **Data Trustees, Stewards, Custodians, and Users**. (See Related Links section: Roles and Responsibilities) **Data Trustees** are defined as university administrators at the vice-presidential level who bear the ultimate responsibility for ensuring the protection of the data stored by those in their reporting area. **Data stewards** are defined as university employees who have direct operational-level responsibility for information management. **Data custodians** are defined as computer system administrators responsible for the operation and management of systems and servers which store or provide access to institutional data. Broadly, the **Trustees** are responsible for determining the detailed policies; the **Stewards** determine the procedures needed to implement the policies, and the **Custodians** implement the procedures. Jointly they are responsible for identifying and implementing safeguards for Restricted and Controlled Data. Many university activities cross management line; for such activities that involve access to, or

storage of, University data, the policies must be coordinated by all **Trustees, Stewards,** and **Custodians** involved.

The **Users** also share a responsibility for safeguarding University data. They do so by ensuring that they follow the relevant policies and by providing data access only to authorized individuals. University community members must report actual or suspected criminal activity associated with any such incident to University Police or, if off campus, other appropriate law enforcement agencies. In addition, any breach, loss, or unauthorized exposure of Restricted Data shall be immediately reported to the unit head and the University's Information Security Department via e-mail at [infosec@uc.edu](mailto:infosec@uc.edu). The University's Director of Information Security will then take the appropriate actions to comply with local, state, and federal law.

## **Related Links**

**Minimum Safeguards**

**Data Classification and Data Types**

**Risk Acceptance Form**

**Roles and Responsibilities**

**Summary of Applicable Laws**