

 <p>Category: Information Technology</p> <p>Policy applicable for: UC Data Center Staff and Management</p>	<p><i>Policy Title:</i> Data Center – Visitor Tours</p> <p>Effective Date: 10/04/2008</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 27001/17799, COBIT 4.0, HIPAA, FERPA, GLB</p>	<p><i>Policy Number:</i> 9.1.25</p> <p>Policy Owner: UC CIO</p> <p>Responsible Office(s): UC Information Security</p>
---	--	--

Background

The purpose of this policy is to raise awareness of physical security measures that need to be followed when conducting tours of data center facilities in the university. It is designed to provide procedures as to how tours should be carried out, ensuring the application of control procedures as preventive measures against any human threat to resources and sensitive information of the data centers.

Policy

- The visitor in charge of the visiting group entering the university data center should sign a non-disclosure agreement before entering the facility. This person is responsible for ensuring that the group members understand the confidentiality required. The data center manager should keep a copy of the NDA on file for 3 years.
- The data center should have authorized staff members physically present as an escort to monitor the visitors touring the data center. This monitoring should be in effect throughout the duration of the tour.
- Authorized staff members should be aware that any physical contact to the computer systems and its components by unauthorized individuals, regardless of the visitors being either university employees or outsiders of the university, is strictly prohibited.
- There should be a ratio of one authorized staff member in attendance for every five visitors at the time of the visit.
- Any electronic devices that can take pictures, videos, or transfer data using portable media is strictly prohibited. These devices should be left in private vehicles or at home and should be removed before entering the data center facilities.

Audience:

This policy applies to the UCit Data Center.

Definitions:

Data Center: A centralized warehouse for the storage, management, and dissemination of data and information organized around a particular organization such as the university. The facility houses computer systems and related equipment, including the data library.

Procedure:

ISO 27001/17799	International Standards Organization for Information Security
COBIT 4.0	ISACA Audit Controls Objective for IT
HIPAA	Health Insurance Portability and Accountability Act
FERPA	Family Educational Rights and

	Privacy Act
GLB	Gramm-Leach-Bliley Act

Related links:

- [International Standards Organization 17799:2005](#)
- [Control Objectives for IT](#)
- [Health Insurance Portability and Accountability Act](#)
- [The Family Educational Rights and Privacy Act](#)
- [Gramm-Leach-Bliley Act](#)

Phone Contacts:

UC Information Security	8-ISEC
Director, Information Security	6-9177
UC Office of the CIO	6-2228

Disciplinary Actions:

Violation of this policy may result in revocation of network access for the effected system(s). Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants and dismissal for interns and volunteers. Additionally, individuals are subject to loss of University of Cincinnati Information Resources, access privileges, civil, and in some cases criminal prosecution.