

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i> Information Security Records</p> <p>Effective Date: 01/04/2008</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 27001/17799, COBIT, GLB, UC Policy, HIPAA, FERPA, PCI, OB IT Policy, Ohio Revised Code Section 149.433, Ohio Administrative Code 123:3- 1-01</p>	<p><i>Policy Number:</i> 9.1.17</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
---	--	---

Background

Policy

The following items have been identified as Information Security records:

- Any Information Security investigation, either closed or ongoing.
 - Any investigative notes from Information Security investigations.
- Any police or law enforcement agency information.
- Results of vulnerability assessments.
- Results of penetration tests.
- Any record containing a password.

- Lock protected records and computer media in drawers or filing cabinets.
- Physically secure laptops and desktops with Security cables.
- Secure your workstation before walking away.
- Do not divulge any information that may be considered protected without checking first with the Director of Information Security.

Audience:

This policy applies to all organizations and individuals associated with the University of Cincinnati.

Definitions:

Information Security Records: Information which, if released, could jeopardize the Information Security of the university.

Procedure:

ISO 27001/17799	International Standards Organization for Information Security
COBIT 4.0	ISACA Audit Controls Objective for IT
GLB	Gramm-Leach-Bliley Act
UC Policy	General Policy on the Use of Information Technology
UC Policy	Information Technology Management Policy
UC Policy	Information Security Policies

HIPAA	Health Insurance Portability and Accountability Act
FERPA	Family Educational Rights and Privacy Act
PCI	Payment Card Industry
Ohio IT Policy ITP-B.1	Information Security Framework
Ohio Revised Code Section 149.433	Exempting Security and Infrastructure Records
Ohio Administrative Code 123:3-1-01	Use of Electronic Signatures and Records

Related links:

- [International Standards Organization 17799:2005](#)
- [Control Objectives for IT](#)
- [Gramm-Leach-Bliley Act](#)
- [UC Policy - General Policy on the Use of Information Technology](#)
- [UC Policy - Information Technology Management Policy](#)
- [UC Policy - Information Security Policies](#)
- [Health Insurance Portability and Accountability Act](#)
- [The Family Educational Rights and Privacy Act](#)
- [Payment Card Industry](#)
- [Ohio Bulletin ITP-B.8](#)
- [Ohio IT Bulletin ITB-2006.01](#)

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.