

 <p><b>Category:</b> Information Technology</p> <p><b>Policy applicable for:</b> Faculty/Staff/Student</p>	<p><i>Policy Title:</i> <b>Information Security Awareness and Education</b></p> <p><b>Effective Date:</b> 01/04/2008</p> <p><b>Prior Effective Date:</b> N/A</p> <p><b>Enabling Acts:</b> FCISA of 1987, ISO 27001/17799, COBIT, GLB, UC Policy, HIPAA, FERPA, PCI, Ohio Bulletin ITP-B.8, Ohio IT Bulletin ITB-2006.01</p>	<p><i>Policy Number:</i> <b>9.1.16</b></p> <p><b>Policy Owner:</b> Director, Information Security</p> <p><b>Responsible Office(s):</b> Information Security</p>
---	---	---

## Background

One of the best practices of information Security is to promote Information Security awareness to all individuals who have access to the information and systems of the enterprise for which it is responsible. Further, UC personnel should be educated and trained in various aspects of information Security to help inform how systems are run and how to develop and apply Information Security controls.

## Policy

Specific activities should be performed to promote Information Security awareness (the extent to which staff understand the importance of Information Security, the level of Information Security required by the organization and their individual Information Security responsibilities – and act accordingly) across the enterprise. These activities should be:

- endorsed by top management
- the responsibility of the UC Information Security group
- supported by a documented set of objectives
- delivered as part of an on-going Information Security awareness program
- kept up-to-date with current practices and requirements
- aimed at reducing the frequency and magnitude of incidents
- measurable

Information Security awareness should be promoted:

- to top management, business managers/users, faculty, IT staff and external personnel
- by providing Information Security education/training
- by supplying specialized Information Security awareness materials, such as brochures, reference cards, posters and intranet-based electronic documents

Faculty, Staff and students should be provided with guidance to help them understand:

- the meaning of Information Security (i.e. the protection of the confidentiality, integrity and availability of information)
- the importance of complying with Information Security policy and applying associated standards/procedures
- their personal responsibilities for Information Security

The effectiveness of Information Security awareness and education should be monitored by measuring:

- the level of Information Security awareness shown by faculty, staff and students
- the effectiveness of Information Security awareness and education activities by monitoring the frequency and attendance

Information Security-positive behavior should be encouraged by:

- making attendance at Information Security awareness training mandatory
- publicize Information Security successes throughout the organization

- linking Information Security to personal performance objectives/appraisals

Education/training should be given to provide staff with the skills they need to:

- assess Information Security requirements
- propose Information Security controls
- ensure that Information Security controls function effectively in the environments in which they are applied

Information Security education/training should be carried out to provide:

- systems development staff with the skills they need to design systems in a disciplined manner and develop Information Security controls
- IT staff with the skills they need to run computer installations and networks correctly and apply Information Security controls
- business users with the skills they need to use systems correctly and apply Information Security controls
- Information Security specialists with the skills they need to understand the business, run Information Security projects, communicate effectively, and perform specialist Information Security activities

**Audience:**

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

**Definitions:**

**Information Security Awareness:** A UC Information Security provided program that helps change organizational attitudes to realize the importance of Information Security and the adverse consequences of Information Security failure. Further, awareness reminds users of the importance of Information Security and the procedures to be followed.

**Information Security Education:** A UC Information Security provided program in which you will learn about Information Security.

**Procedure:**

<b>FCISA of 1987</b>	Federal Computer Information Security Act of 1987
<b>ISO 27001/17799</b>	International Standards Organization for Information Security
<b>COBIT 4.0</b>	ISACA Audit Controls Objective for IT
<b>GLB</b>	Gramm-Leach-Bliley Act
<b>UC Policy</b>	General Policy on the Use of Information Technology
<b>UC Policy</b>	Information Technology Management Policy
<b>UC Policy</b>	Information Security Policies
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>FERPA</b>	Family Educational Rights and Privacy Act
<b>PCI</b>	Payment Card Industry

<b>Ohio Bulletin ITP-B.8</b>	Security Education and Awareness
<b>Ohio IT Bulletin ITB-2006.01</b>	Security and Records Requests

**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.