

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i> Umbrella Information Security Policy</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</p>	<p><i>Policy Number:</i> 9.1.21</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
---	---	---

Background

The information assets of the University of Cincinnati (UC) must be available to the UC community, protected commensurate with their value, and must be administered in conformance with federal and state law.

Policy

UC will take reasonable steps to:

- Designate an Information Security Department to identify and assess the risks to non-public or business-critical information within the Institute and establish an Institute-wide information security plan. (GLB 314, GLB 314.4(a) + HIPAA 164.308(a)(1))
- Develop, publish, maintain, and enforce standards for lifecycle protection of UC information systems and supporting infrastructure in the areas of networking, computing, storage, human or device/application authentication, human or device/application access control, incident response, applications or information portals, electronic messaging, and encryption. (GLB 314.4(b & c)+ HIPAA - 164.308(a)(1,4,6,7), 164.310, 164.312(a,d,e))
- Develop, publish, maintain, and enforce guidelines and standards for UC workforce security related to the responsible use of information. (GLBA 314.4(b)(1) + HIPAA 164.308(a)(1-5))
- Provide Information Security Awareness training to authorized Institute users in the responsible use of information, applications, information systems, networks, and computing devices. (GLBA 314.4(b)(1) + HIPAA 164.308(a)(2-5))
- Develop, publish, maintain and enforce guidelines and standards which guide UC business associates and outsource partners in meeting UC's standards of lifecycle protection when handling UC information or supporting UC information systems and its supporting infrastructure. (GLB 314.4(d)(1-2) + HIPAA 164.308(b)(1)).
- Encourage the exchange of information security knowledge, including threats, risks, countermeasures, controls, and best practices both within and outside the University. (HIPAA 164.308(a)(5))
- Periodically evaluate the effectiveness of information security controls in technology and process. (GLB 314.4(c) + HIPAA 164.308(a)(8), 164.312(b))
- Provide for the confidentiality of Personally Identifiable Information (PII) in accordance with local, state and federal legislation. ((GLB 314.4(d)(1-2) + HIPAA 164.308(b)(1)+FERPA (20 U.S.C. § 1232g; 34 CFR Part 99)
- Perform a comprehensive risk assessment in regards to the safeguarding of restricted data. (GLB, HIPAA, PCI)

Audience:

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

Definitions:

Information Safeguards: Administrative, technical, and physical controls that support the confidentiality, integrity, availability, and authenticity of information.

Information systems and supporting infrastructure: Information in its hard copy and digital forms and the software, network, computers, tokens, and storage devices that support the use of information.

Lifecycle Protection: Information systems and supporting infrastructure have a lifecycle that begins with evaluation and selection, and advances through planning, development/acquisition, and operations through to disposal or retirement. Information Security safeguards are needed at all phases of the lifecycle.

Controls depend on the system, its capabilities, and expected usage, as well as anticipated threats against the information.

- Preventive controls include use of encryption, information integrity measures, security configuration, media reuse, use of antivirus, and physical protection
- Detective controls include network and information access monitoring, and intrusion detection (host based or network based), manual or automated review of security logs
- Corrective controls include recovery plans from handling isolated information safeguard failure incidents to business continuity plans.

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

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](#)

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.

DRAFT