

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i> Information Security Forensic Investigation</p> <p>Effective Date: 01/04/2008</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 27001/17799, COBIT 4.0, GLB, UC Policy, HIPAA, FERPA</p>	<p><i>Policy Number:</i> 9.1.12</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
---	---	---

Background

A process should be established for dealing with incidents that require non-criminal forensic investigation. This policy is not meant to supersede any standards of best practice for criminal forensic investigations.

Policy

Establishing a process for dealing with incidents that require forensic investigation.

Documented standards/procedures for dealing with Information Security incidents at UC that may require forensic investigation, which cover:

- immediate preservation of evidence on discovery of an incident
- compliance with a published standard or code of practice for the recovery of admissible evidence
- maintenance of a log of evidence recovered and the investigation processes undertaken
- the need to seek legal advice where evidence is recovered
- notifying staff that actions may be monitored during the investigation

Evidence should be collected:

- in accordance with UC's policy for Information Technology Management
- as if criminal prosecution is pending
- with respect for all individuals' privacy and human rights
- from as many IT sources as possible (e.g. active, temporary and deleted files, e-mail or Internet usage, memory caches and network logs)
- from as many non-IT sources as possible (e.g. CCTV, building access logs and eye witness accounts)

During an investigation steps should be taken to:

- establish and document a chronological sequence of events
- log investigative actions
- demonstrate that appropriate evidence has been collected, preserved and that no one could have tampered with it
- secure target computer equipment
- analyze evidence in a controlled environment (e.g. using a copy or 'image' of the computer media to avoid corruption of the original)
- ensure that processes used to create and preserve evidence can be repeated by an independent third party
- limit information about an investigation to a few nominated individuals and ensure it is kept confidential
- obtain the involvement of the UC Police Department or the FBI immediately if it is determined a crime that is within their purview has been committed

Audience:

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

Definitions:

Forensic Investigation: The application of a broad spectrum of sciences, tools and techniques to answer questions of interest to the legal system.

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

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](#)

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