

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i> Information Security Emergency Response</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, PCI</p>	<p><i>Policy Number:</i> 9.1.11</p> <p>Policy Owner: VP and Chief Information Officer</p> <p>Responsible Office(s): Information Security</p>
---	--	---

Background

Establishment of an information emergency response process, supported by an emergency response team, which outlines actions to be taken in the event of a serious attack.

Policy

Creation of an emergency response process for dealing with serious attacks, supported by a pre-determined high-level information security emergency response team (ISERT), which includes a representative at the Director level or above.

Establishing a process for dealing with serious cyber attacks, which includes:

- a definition of an emergency situation
- a defined process allowing critical decisions to be made quickly
- clearly defined steps to be taken in emergency situations
- rehearsal of the process
- contact details for all key personnel (both internal and external)
- methods of dealing with third parties, such as the media

The process for dealing with serious attacks should include methods of:

- enabling support staff to react quickly should an emergency arise
- gaining approval for recommended actions within a critical timescale

The process for dealing with serious cyber attacks must ensure that, after an emergency has occurred:

- computers affected by the attack are cleaned
- the likelihood of further similar attacks is minimized
- security controls are reviewed
- a post mortem review is conducted

Audience:

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

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	Information Security Emergency Response Plan

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 - 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.