

 <p><b>Category:</b> Information Technology</p> <p><b>Policy applicable for:</b> Faculty/Staff/Student</p>	<p><i>Policy Title:</i></p> <p><b>Clean Desk Policy</b></p>	<p><i>Policy Number:</i></p> <p><b>9.1.7</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> ISO 27001/17799, COBIT 4.0, GLB, CSA of 1987, UC Policy, HIPAA, FERPA, PCI</p>	<p><b>Policy Owner:</b> Director, Information Security</p> <p><b>Responsible Office(s):</b> Information Security</p>

## Background

Detail.

## Policy

- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- Any UC Highly Restricted or UC Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing UC Highly Restricted or UC Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to UC Highly Restricted or UC Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing UC Highly Restricted or UC Sensitive information should be immediately removed from the printer.
- Upon disposal UC Highly Restricted and/or UC Sensitive documents should be shredded.

## Audience:

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

## Definitions:

**UC Highly Restricted or UC Sensitive Information:** Data protected under FERPA, GLB or HIPAA and/or data that has been classified UC Highly Restricted or UC Sensitive.

## Procedure:

<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>Computer Security Act of 1987</b>	DIR Practices for Protecting Information Resources Assets
<b>Computer Security Act of 1987</b>	DIR Standards Review and Recommendations Publications

<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

**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.