

 <p><b>Category:</b> Information Technology</p> <p><b>Policy applicable for:</b> Faculty/Staff/Student</p>	<p><i>Policy Title:</i> <b>Privileged Access Policy</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, UC Policy, HIPAA, FERPA, PCI</p>	<p><i>Policy Number:</i> <b>9.1.14</b></p> <p><b>Policy Owner:</b> Director, Information Security</p> <p><b>Responsible Office(s):</b> Information Security</p>
---	---	---

## Background

Due to their high level of knowledge and access to sensitive systems, IT resources with Privileged or Administrative Access at the University of Cincinnati are in a unique position of trust and responsibility. It is important that these people be familiar with relevant UC policies and the requirements of UC, the government and the public.

## Policy

Review of policy:

- IT personnel in these roles must review the detail of UC policies regarding IT. The policies that must be reviewed are:
  - [General Policy on the Use of Information Technology](#)
  - [Information Technology Management Policy](#)
  - [Information Security Policies](#)

Annual acknowledgement of policy by those with privileged access:

- All IT personnel with privileged access are required to acknowledge on an annual basis that they have reviewed and that they accept the terms of the policies above.
- This acknowledgement is to be documented by signing the Privileged Access Agreement (PAA) available from UC Information Security at 558-ISec or [www.uc.edu/infosec](http://www.uc.edu/infosec) > Policies
- Once signed by the individuals, the forms are to be submitted to their manager for review and approval.
- The completed PAA form is to be submitted to the Department of Information Security for retention.
- Signed PAAs are to be retained by the Department of Information Security for a period of 5 years.

## Audience:

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

## Definitions:

**Privileged Access:** Access that allows an individual who can take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators or other such employees whose job duties require access to regulated data residing on a system or network. This data can be paper or electronic data. For the purposes of this policy, application and other developers are also considered privileged.

## 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>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](#)
- [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.