

 <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>Remote Authentication for Administrative Users</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, GLB, UC Policy, HIPAA, FERPA, PCI</p>	<p><i>Policy Number:</i></p> <p><b>9.1.15</b></p> <p><b>Policy Owner:</b> VP and Chief Information Officer</p> <p><b>Responsible Office(s):</b> Information Security</p>
---	--	--

## Background

There exist at the University of Cincinnati computer, network and system accounts that operate at a higher level of privilege than those granted to normal users.

These Privileged / Admin User Accounts are required for a variety of reasons, including the support or configuration of the associated technology. However, this extra level of access carries with it extra risk.

Holders of these special accounts must take extra steps to protect their admin user account(s).

## Policy

- Accounts with privileged access must be configured to either:
  - Not allow remote VPN connections
  - Allow remote connections only through a remote access server that requires two-factor authentication and a secure tunnel like VPN
- All personnel holding accounts with privileged access permitted to connect remotely must be provided with a VPN type of solution that requires two-factor authentication.
- Any person wishing to connect to UC systems using an account with privileged access must do so using strong (two factor) authentication.

## Audience:

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

## Definitions:

**Privileged Access:** Enables an individual to 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, staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network.

**Two-factor authentication:** To require 2 pieces of information in order to authenticate to a system. ① something that you know (like password, fingerprint or PIN) **and** ② something that you physically have (like a number from a smart card or a USB token that must be connected to the system).

## Procedure:

ISO 27001/17799	International Standards Organization for Information Security
COBIT 4.0	ISACA Audit Controls Objective

	for IT
<b>GLB</b>	Gramm-Leach-Bliley Act
<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 - 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.