

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i></p> <p>Directory Password Reset Policy</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></p> <p>9.1.13</p> <p>Policy Owner: VP and Chief Information Officer</p> <p>Responsible Office(s): Information Security</p>
---	---	--

Background

Policy

Automated password recovery/reset:

- UCit shall provide an automated password recovery/reset solution for any Central Directory system provided (i.e. Active Directory, Central Login Service)
- This system will operate in a manner and by processes approved by the Director of Information Security.
- The system should allow the user to select from a number of standard questions or to provide their own questions and to provide unique answers to those questions. These question/answer sets will be used for the purpose of verification of identity for both automated and manually assisted password resets.
- The password recovery solution should not rely on Social Security Number (SSN) or any portion thereof (Last 4).
- The password recovery solution should not rely on the M# or any portion thereof.
- UC organizations that provide systems for which a password is required, but is not kept in synch with a central UCit directory system should also consider providing an automated password recovery/reset solution for their application.

Assisted password recovery/reset:

- If the automated password recovery/reset solution provided by UCit is unavailable or fails, the user may then call the UC helpdesk to reset their password. The UC helpdesk may be reached at 513-556-HELP
- Any user requesting a password reset must verify their identity prior to having the reset completed.
- The user must confirm their identity by providing the answer to 3-4 confidential questions set up in the password recovery system.
- Verification is to be conducted by full time UCit help desk staff personnel only.

Audience:

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

Definitions:

Directory: A database of user information that allows for the central administration of account information. Directories allow a user to maintain their information or to change their password in one location have the change be immediately available to every application that uses the directory.

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
PCI	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.

DRAFT