

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i> Password Policy</p> <p>Effective Date: 01/06/2008</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> 9.1.23</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
---	--	---

Background

The purpose of this policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the University of Cincinnati user passwords.

Policy

- All passwords and passphrases, including initial passwords, must be constructed and implemented according to the following University of Cincinnati password policy:
 - Passwords must be changed every 180 days
 - Passwords must be a minimum length of 8
 - Passwords must be a combination of alpha and numeric characters
 - No more than 3 of these characters can be repeated in the password
 - Passwords must not be anything that can be easily tied back to the account owner such as: user name, social security number, UCID, nickname, relative's names, birth date, etc.
 - Passwords must not be word or acronym found in any dictionary
 - The same password cannot be used within a 5 password cycle period
 - No more than 4 characters from the existing password can be re-used in the new password you are creating
- In cases where developer or application passwords are used to automate systems, the passwords must be encrypted in storage and a different password/application ID should be used for each separate application.
- User account passwords must not be divulged to anyone.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with University of Cincinnati.
- System or Application Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users may not circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the University of Cincinnati Director of Information Security; such approval can be obtained by submission of a Risk Acceptance Form [http://www.uc.edu/infosec/documents/UC_InfoSec_F40_Risk_Acceptance_Form.pdf] In order for an exception to be approved there must be a procedure to change the passwords periodically.
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- UCit Helpdesk password change procedures must include the following:
 - ❖ Authenticate the user to the helpdesk before changing password
 - ❖ The user must be reminded to change their password at first login
- In the event passwords are found or discovered, the following steps must be taken:

- ❖ Take control of the passwords and protect them
- ❖ Report the discovery to the University of Cincinnati Help Desk at 556-4357.
- ❖ Transfer the passwords to an authorized person as directed by the University of Cincinnati Director of Information Security.

Guidelines:

- Passwords must contain a mix of upper- and lower-case characters and have at least 1 numeric character. Special characters should also be included in the password where the computing system permits. Examples of special characters are (!@#\$%^&* _+=~/~`';,;<>|).
- Passwords must not be easy to guess and you should not use:
 - ❖ Your username
 - ❖ Your ucid
 - ❖ Your name
 - ❖ Names of any of your family members
 - ❖ Your nickname
 - ❖ Your social security number
 - ❖ Your birthday
 - ❖ Your license plate number
 - ❖ Your pet's name
 - ❖ Your address
 - ❖ Your phone number
 - ❖ The name of your town or city
 - ❖ The name of your department
 - ❖ Street names
 - ❖ Makes or models of vehicles
 - ❖ Slang words
 - ❖ Obscenities
 - ❖ Technical terms
 - ❖ School names, school mascots, or school slogans
 - ❖ Information about you that is known or is easy to learn (favorite food, color, sport, etc.)
 - ❖ The reverse of any of the above
- You should not share your password with anyone
- You must treat your password as confidential information

Examples:

- Make the password difficult to guess but easy to remember.
- Combine short, unrelated words with numbers or special characters.
- Use a passphrase instead of a password. A passphrase is a sentence you can remember in which you take the first letter, or the 3rd letter, in order to create password. Example:
 - ❖ "I like to watch baseball games very much" would make a passphrase of "I!wBgvm1") and this would be a strong password
- Substitute numbers or special characters for letters. (But do not just substitute) For example:
 - ❖ **livefish** - is a bad password
 - ❖ **L1veF1sh** - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and it's substituted by 1's can be guessed
 - ❖ **I!v3f1Sh** - is far better, the capitalization and substitution of characters is not predictable.

Audience:

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

Definitions:

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

Strong Password: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.

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 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.

DRAFT