

Policy Statement

Title:	Minimum Password Standards
Effective Date:	February 5, 2008
Responsible Officer:	Assistant Vice Chancellor / CIO
Responsible Office:	iCIT
Last Reviewed:	February 5, 2008
Version:	003 (FINAL version as adopted)

Policy Statement

1. Account holders must protect the confidentiality of their passwords and use strong passwords that cannot easily be guessed or otherwise compromised.

Reason for Policy

1. The purpose of this policy is to provide guidance to account holders regarding passwords in order to protect individual and University information and resources.
2. Access to and protection of University information resources should be consistent with the mission of the University. Since the majority of University information resources are accessed via username and password, passwords must be strong and confidential.

Policy Requirements

1. Net-ID passwords must meet the following minimum standards:
 - a. Passwords must be at least eight (8) characters long.
 - b. Passwords must contain at least one (1) character from each of the following categories:
 - i. Upper case letters (A-Z)
 - ii. Lower case letters (a-z)
 - iii. Numeric digits (0-9)
 - c. Passwords must not contain a series of 3+ recurring characters (e.g. “aaa” or “999”)
 - d. Passwords must not resemble the Net-ID or name of the account holder.
 - e. Passwords must not be any of the account’s four (4) prior passwords.
2. Account holders must change their Net-ID password at least once every 180 days.
 - a. Account holders may change their password at any time. It is not necessary to wait for expiration.
3. Non Net-ID passwords (such as local system passwords) must meet or exceed the Net-ID Minimum Password Standards.
4. Passwords used to access sensitive systems and/or data must meet appropriate standards for those particular systems and/or data.

Related Policy Information

1. The University reserves the right to:
 - a. Suspend account holders' access to preserve the confidentiality, integrity and availability of the University's network, systems or information
 - b. Periodically audit passwords for compliance
2. Consequences for non-compliant passwords include:
 - a. Attempts to create or change a password to one that does not meet the Minimum Password Standards will result in rejection of the change to the password.
 - b. Accounts with expired passwords will be denied access by participating systems.

Scope and Exclusions

1. All account holders must adhere to the Minimum Passwords Standards for all systems and applications that come into contact with University resources.
2. All devices and systems connected to the University network must require passwords meeting the Minimum Password Standards and, if possible, technically enforce them.
 - a. If a system cannot meet the Minimum Password Standards, the system must be protected by other means, such as, but not limited to, a dedicated firewall, limited network access or multi-factor authentication.

Contact Information

Office / Unit Name	Contact Name, Title	Phone	Email
iCIT / CIO Office	Elena Pokot, CIO	Ext. 5088	icit-office@uww.edu
iCIT Security Office	Christian Schreiber, IT Policy and Security Officer	Ext. 7792	security@uww.edu
iCIT HelpDesk	Lisa Rowland, HelpDesk Manager	Ext. HELP (4357)	helpdesk@uww.edu

Definitions

Word	Definition
Account Holder	Faculty, staff, students and other authorized users (as defined by the Network Infrastructure Use Policy) who have been issued a UW-Whitewater Net-ID.

Responsibilities

Area of Responsibility	Responsibility
iCIT	Implements the technical infrastructure that enables and enforces the Minimum Password Standards.
iCIT Security Office	Facilitates the development of policies, and develops procedures and guidelines which manage password usage and practices.
Account Holders	Account holders must protect their Net-ID passwords by: <ul style="list-style-type: none">• Not divulging password information to any other entity.• Not leaving password information unprotected (such as writing passwords down and leaving in an unsecured area).• Not using a password based on a dictionary word or other easily-guessed word.

History

Date	Revision(s)
June 13, 2006	Original policy approved by UTC
February 5, 2008	Revised policy approved by Executive Tier committee <ul style="list-style-type: none">• Updated format to new policy template• Updated minimum standards to require 8 characters and combination of upper case, lower case, and numeric characters• Added requirement prohibiting series of 3+ sequential characters• Added requirement that passwords not resemble Net-ID or name of account holder• Added consequences for non-compliance to Related Policy Information• Defined policy scope• Added exclusion for systems that cannot meet minimum standards• Added contact information• Defined account holders• Defined responsibilities