Manhattanville COLLEGE

Password Policy

Initiated Date:	4/3/13	Version Number: 1.0
Revision Date:	5/17/13	
OIT Contract:	Steve Handfinger	New Version Number: N/A

Introduction

Passwords are an important aspect of computer security. They are front line of protection for user accounts. A poorly chosen password may result in the compromise of Manhattanville College's entire network. As such all student, faculty, staff, contractors and vendors with access to Manhattanville College's network are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system, that resides at Manhattanville College.

Policy

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a bi-annual basis.
- All production system-level passwords must be part of the OIT staff administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every nine months. The recommended change interval is every four months.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

Passwords are used for various purposes at Manhattanville College. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and voicemail password, everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Simple substitutions of digits for letters. Zero for "o" (oh), numeral 1 (one) for l (ell)
- Bracketing the above with "#" or "!" or similar using non-alphanumeric characters.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long (9 is strongly recommended).
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Do not share passwords with anyone, including, spouse, friends, administrative assistants or secretaries. All passwords are to be treated as sensitive.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers

If someone demands a password, refer them to this document.

Do not use the "Remember Password" feature of applications. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system without encryption.
Change passwords at least once every nine months (except system-level passwords which must be changed bi-annually). The recommended change interval is every six months.

If an account or password is suspected to have been compromised, report the incident to Office of Information Technology staff member and change all passwords.

Changing Your Password

We encourage faculty, stuff and student to use the Self-Service Account Management, to manage your password. The URL is https://selfservice.mville.edu