September, 2008

Manhattan College Password Policy

Background, Rationale and Goal

Passwords are a key component of computer security for Manhattan College. They are the front line of protection for user accounts.

The weakest link in computer security efforts is your password. Although the College's Department of Computer Services spends a good deal of time protecting computers and servers against intruders, a big security hole is an easily-guessed password. Today, basic password-cracking programs can deduce a dictionary or name-based password in seconds.

A poorly chosen password could result in the compromise of the College's entire network.

Therefore, the rationale for this policy is to protect the College's systems, its data, the private and/or confidential information it maintains, its users and its users' data.

The goal of this policy is to establish a standard for creation of strong passwords, to protect those passwords, and to impose a frequency of change requirement.

Persons covered by this policy

All employees and all students are responsible for taking appropriate steps to select and secure their passwords.

Persons covered by this policy include all who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides on the College's systems, has access to JasperNet (the Manhattan College network) or stores information on the College's systems. Vendors, contractors and consultants that may be provided with occasional authorized access to College systems are also covered by this policy.

Password Policy

- All employees and students are required to use a strong password.

- For system administrators, all production or system-level passwords must be part of the InfoSec administered global password management database.

- Additionally, it is strongly recommended that all passwords be changed at least once every semester. The recommended change interval is every ninety (90) days. At this time, forced changes will not be implemented but it may be required at a later date.

- User accounts that have system-level privileges (e.g. system administrators) must have a unique password from all other accounts held by that user.

- Passwords must not be inserted into e-mail messages, other forms of electronic communication or otherwise communicated in a non-secure manner.

- Passwords must not be shared with anyone (e.g. roommates, research assistants, student workers in College offices

- All passwords must conform to the guidelines described below.

Password Guidelines

All persons covered by this policy should be aware of how to
select strong passwords as opposed to “poor” or “weak” passwords.

Do not use a poor or weak password. “Poor” or “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, characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words “Manhattan”, “Jasper”, or any derivation.
    - 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.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1 secret)

When you change your password, **you will be required to use a strong password** or the change will not be accepted. A “strong” password has the following characteristics:

- Contains both upper (A-Z) **and** lower case (a-z) characters

- **and** has numbers **and** punctuation characters:
    - 0-9

      OR
    - ! @ # $ % ^ & *( ) + | ~ - = \ ` { } [ ] : " ; ' < > ? /
- Is **at least eight alphanumeric characters** in length
- Is not a dictionary word in any language, slang, dialect, jargon, etc.
- Is not based on personal information, proper names of family, etc.

Password Protection

- Passwords should not be written down (e.g. on a "*Post-It*" note) and conspicuously posted somewhere or stored online.

- Users of the College's systems should create passwords that can be easily remembered. One way to do this might be to create a password based on a song title, affirmation, or other phrase e.g. the phrase might be: "This May Be One Way To Remember" and the password would then be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

- Do not use the same password for College accounts as for other non-College access (e.g. other Internet accounts, online banking, pension benefits, etc.). If your password is compromised, it could impact all systems using that same password.

- Do not share passwords with anyone, including administrative assistants or secretaries, roommates, etc. All passwords are to be treated as sensitive and confidential information.

Enforcement

Any employee or student found to have violated or circumvented this policy shall be deemed to be in violation of the Responsible Use of Computer Information and Services Policy of Manhattan College and may be subject to sanctions provided therein including the disabling of your account until it is secured.