IT Password Complexity Guidelines

Purpose

This guideline provides best practices for creating sufficiently secure passwords, and should be consulted when creating new passwords for Montclair State University Information Technology Division (MSU IT) resources. This document is considered a companion piece to the IT Password Protection Policy, therefore all policies contained therein must be consulted and followed.

Furthermore, this document is intended to supplement the campus Password Management policy and takes precedent in all cases where it raises the stated requirements of that policy for all passwords created and managed by MSU IT staff, contractors, and vendors.

Scope

The scope of this guideline 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 any MSU IT facility, has access to MSU IT resources, or stores any non-public MSU IT information. All users, including contractors and vendors with access to MSU IT systems, are responsible for taking the appropriate steps, as outlined below, to create their passwords. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, email accounts, appliances, network devices, and multi-function devices (printers, copiers, etc.)

Password Protection (Storage)

Passwords should never be written down or stored on-line. Since it's difficult for most people to memorize more than a few passwords, it is important to store your passwords securely using password management software. Please reference the IT Password Protection Policy for information regarding how to properly protect passwords.

Composition Guidelines

Passwords should be sufficiently strong and *unique,* and should meet the following complexity guidelines.

- Passwords should be longer than fifteen (15) characters. However, there is no suggested limit on the maximum length of a password, outside of any constraint imposed by an application or system. Think of the golden rule of passwords as, "the longer the stronger". (Longer passwords are more complex and harder to crack. It's all math.)
- Passwords should contain both upper and lower case characters (a-z, A-Z), at least one digit (0-9) and at least one special character (!$%^&*()_+|~-=\`{}[]:";'<>?,/))
- A space (" ") should be considered a valid character for passwords as it can increase the entropy and length of a password without sacrificing memorability.
- Passwords should never be a single word found in a dictionary (English or otherwise).
- Passwords should not include computer terms and names, names of family, pets, friends, co-workers, television characters.

- Passwords should not include birth dates or personal information such as addresses or phone numbers.
- Passwords should not include any references to Montclair State University, such as “MSU”, “Redhawk”, “Rocky”, “Montclair”, or building names such as “Dickson”, “Morehead”, etc.
- Passwords should avoid word and number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc
- Passwords should avoid any of the above spelled backwards or merely preceded or followed by a digit (e.g., secret1, 1secret).

Password Types

Generated Passwords

Passwords generated by software will have a higher level of entropy (uniqueness) than those created by a human. Most password management software includes a password generator. (Please reference the IT Password Protection Policy for a list of IT approved password managers.)

Passphrases

A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against *dictionary attacks*. A good passphrase is relatively long and contains a combination of upper and lower case letters and numeric and punctuation characters.

An example of a really good passphrase is something like: "1.After Years Of Waiting @_@ Nothing Came”.

Note that some password management programs generate random passphrases. However, if you are going to use a particular account password frequently, think of a song lyric, a line from a book, or any other phrase that complies with the above composition guidelines. This will make it easier to recall and type in the longer passphrase.

All of the composition rules above that apply to passwords apply to passphrases. Do not use any examples in this document as a password or passphrase.

Recommended Use

For system-level accounts (root, SYSTEM, Administrator, etc.) and non-interactive service accounts, a password generator should be used to meet the above requirements. Always store the password in the approved enterprise password repository if your department uses one (i.e. PAS) and in a password manager for your own use.

For privileged user-level accounts (<NetID>_loc, <NetID>_tech, etc.), use either method to create as strong (long) a password as possible. Always store in a password manager.

For user-level accounts (<NetID>, vendor web sites, etc.), consider passphrases for ease of recollection and entering and remember “the longer the stronger”. Always store in a password manager.