1.0 Purpose

This policy describes the University's requirements for acceptable password selection and maintenance. It provides guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password.

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Passwords must therefore follow the policy guidelines listed below.

2.0 Scope

This policy applies to anyone accessing systems that hold or transmit Montclair State University data. Systems include, but are not limited to: personal computers, laptops, Montclair State-issued cell phones, and small factor computing devices (e.g., tablets, USB memory keys, electronic organizers), as well as Montclair State electronic services, systems and servers. This policy covers departmental resources as well as resources managed centrally.

3.0 Policy

All passwords (e.g., email, web, desktop computer, laptop, mobile device, etc.) should be strong passwords and should follow the guidelines below. In general, a password's strength will increase with length, complexity and frequency of changes.
Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

Central and departmental account managers, data trustees, and security and/or system administrators are expected to set a good example through a consistent practice of sound security procedures.

1. All passwords must meet the following guidelines, except where technically infeasible:

   - Must contain at least eight (8) alphanumeric characters.
   - Must contain at least two (2) non-alphabetic characters and least three (3) alphabetic characters.
   - At least one (1) alphabetic character must be upper-case and at least one (1) must be lower-case.
   - Passwords cannot consist of a single word in any dictionary, language, slang, dialect, jargon, etc.
   - Passwords cannot consist of easily guessed or obtained personal information, names of family members, pets, etc.
   - Passphrases consisting of three or more dictionary words joined by non-alphabetic characters are acceptable. The words chosen should have some identifiable relationship for the user to help them remember the passphrase without the need to write it down. An example of such a passphrase might be: Summer2013#Beach_Party!

2. To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must never be used as a user ID or a password.

3. All passwords are considered **Private** information and should be handled according to the University's Safeguarding Sensitive and Confidential Information Policy. As such they should never be written down or stored on-line unless adequately secured.
4. Passwords should not be inserted into email messages or other forms of electronic communication.

5. The same password should not be used for access needs external to Montclair State (e.g., online banking, benefits, etc.).

6. It is recommended that passwords be changed at least every six months. Passwords for various systems and applications may have an “aging” feature that mandates a password change after a certain number of days or months after the last password change. Users are required to abide by any University password aging policies.

7. Passwords should not be shared with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of the Information Technology Division and must have a primary responsible contact person. Shared passwords used to protect network devices require a designated individual to be responsible for the maintenance of those passwords, and that individual will ensure that only appropriately authorized employees have access to the passwords.

8. If a password is suspected of being compromised, it should be changed immediately and the incident reported to the University Help Desk.

9. Password cracking or guessing may be performed on a periodic or random basis by IT Security or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

3.1 Client device (desktop/laptop) Administrator Passwords

In addition to the general password guidelines listed above in Section 3.0, the following apply to desktop administrator passwords, except where technically and/or administratively infeasible:

1. Admin passwords for client devices must be changed at least every six months.
2. Where technically and administratively feasible, attempts to guess a password should be automatically limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.

3. Failed attempts should be logged, unless such action results in the display of a failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities or compromises should be immediately reported to the University Help Desk.

3.2 Server Administrator Passwords

In addition to the general password guidelines listed above in Section 3.0, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

1. Passwords for servers must be changed as related personnel changes occur.

2. If an account or password is suspected to have been compromised, the incident must be reported to IT Security and potentially affected passwords must be changed immediately.

3. Attempts to guess a password should be limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.

4. Uniform responses should be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimizes clues that could result from hacker attacks.

5. Failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities such as suspected attacks should be reported to the University Help Desk.

6. Owners of departmental servers that are connected to the campus network must provide central IT with the ‘administrator’ or ‘root’ password to the device, or an account with equivalent privileges. This account will be used only by full-time IT security personnel to ensure the security and integrity of the device via routine, coordinated system scans or other non-intrusive mechanisms.
no circumstances will IT use the administrator/root account to manage the
departmental device or perform any activity that would potentially compromise its
intended functionality or expected performance. (See Network Connectivity Policy)

NOTE: Log files should never contain password information.

4.0 Related Policies and Links

Account Management Policy
Network Connectivity Policy
Safeguarding Sensitive and Confidential Information Policy

Revision History

rev 1.0 11/13/13 Initial release