Password Protection Policy

Effective:
September 2, 2016

Purpose

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Montreat College's resources. All users, including contractors and vendors with access to Montreat College systems, are responsible for taking the appropriate steps to select and secure their password. 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

This policy applies to 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 Montreat College facility, has access to the Montreat College network, or stores any non-public Montreat College information.

Policy

Password Creation

- All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
- Users must not use the same password for Montreat College accounts as for other non-Montreat College access (for example, personal ISP account, option trading, benefits, etc.).
- Where possible users must not use the same password for various Montreat College access needs.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
- Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system. They must also be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

Password Change

- All system-level passwords (for example, root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (for example, email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- Password cracking or guessing may be performed on a periodic or random basis by Campus Technology or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the *Password Construction Guidelines*.

Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Montreat College information.
- Passwords must not be inserted into any form of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, “my family name”).
- Users must not share Montreat College passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Users must not write passwords down and store them anywhere in their office.
- Users must not store passwords in a file on a computer system or mobile device (phone, tablet, etc.) without encryption.
- Users must not use the “Remember Password” feature of applications (for example, web browsers).
- Any user suspecting that his or her password may have been compromised must report the incident to Campus Technology and change all passwords.

Passphrases

All of the rules that apply to passwords also apply to passphrases.

Policy Compliance

Compliance Measurement

Campus Technology will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Campus Technology in advance.

Non-Compliance

The responses for violation of this policy will include, but are not limited to, the following:

- Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
- Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.
- Loss of computer privileges: limitation or removal of computer privileges, either permanently or for a specified period of time.
- Restitution for damages: requiring reimbursement for the costs of repairs to or replacement of computer related material, equipment, hardware, software, data, and/or facilities, which reimbursement shall include, but not be limited to, the cost of additional time spent by college employees due to the violation.

In addition to the aforementioned, violators may be subject to disciplinary action – which may include suspension, expulsion, or termination – as may be prescribed by other rules, regulations, handbooks, procedures, or policies applicable to the violator. Furthermore, the violator may be subject to civil suits or ordinances, laws, statues, or regulations of the applicable local government, the State of North Carolina, or the United States of America.

Contact Information

Campus Technology
Phone: 828-669-8012 Ext. 3663
Email: support@montreat.edu

Revision History

Initial Draft: 08/09/2016
Revised: 08/18/2016
Revised: 09/02/2016