Appendix ZZ

MSUN Policy 1001.5

MONTANA STATE UNIVERSITY NORTHERN

Administrative Policy and Procedures Manual

Section 1000: Campus Policy

1001.5 Passwords

Effective: July 1, 2006

Overview

Passwords are an essential aspect of computer security, providing important front-line protection for electronic resources by preventing unauthorized access. A poorly chosen password may result in the compromise of Montana State University-Northern's systems, data or the entire campus network. Therefore, all MSU-Northern employees (including contractors and vendors with access to MSU-Northern systems) and students are required to use complex passwords and keep them secure.

A department and/or system administrator may implement a more restrictive policy on local systems where deemed appropriate or necessary for the security of electronic information resources. The Information Technology Services Office can require a more restrictive policy in protection of confidential data.

Purpose

The purpose of this policy is to establish a standard for the creation of complex passwords, the frequency with which they must be changed, and to educate users about the protection of those passwords.

Scope

This policy applies to all personnel

- who have or are responsible for an account or who have any form of access that supports or requires authentication on any system that resides at any MSU-Northern facility,
- who have access to the MSU-Northern network, and/or
- who store any non-public MSU-Northern information.

Policy

- All MSU-Northern domain passwords must be changed at least every 180 days.
- MSU-Northern passwords must not be inserted into email messages or other forms of electronic communication.
- All passwords must conform to the standards described below.

Password Construction Standards

Complex passwords requirements:

- Must be a minimum of 8 characters in length

- Must contain characters from ***three*** of the following four categories:
  - Uppercase characters (A through Z)
  - Lowercase characters (a through z)
  - Digits (0 through 9)
  - Non-alphanumeric characters (e.g. !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

Password Protection Standards
All passwords are to be treated as sensitive, confidential MSU-Northern information. Therefore:

- Do not use the same password for MSU-Northern accounts as for other non-Northern access (e.g., personal ISP account, non-Northern web email accounts, option trading, benefits, etc.). Where possible, don't use the same password for various MSU-Northern access needs. For example, select one password for email/domain access and a separate password for Banner.
- Do not share MSU-Northern passwords with anyone except Information Technology Services (ITS) technical personnel who are assisting you with a technical issue. You can verify the technician's identity by requesting to see their maroon and gold ITS photo ID (**not** their Northern ID). You are responsible for safeguarding your passwords.
- Do not display or conceal a password in your workspace
- Do not use the "Remember Password" feature of applications or websites.
- Do not store passwords in a file on **any** computer system (including Palm Pilots or similar devices) without encryption.
- If an account or password is suspected to have been compromised, report the incident to ITS and change all your passwords.

Password cracking or guessing may be performed on a periodic or random basis by MSU-Northern ITS. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Enforcement
Student violations of this policy will be handled by the Dean of Students, while employee violations will be referred to the individual's supervisor or the Dean of the College. Any employee found to have violated this policy may be subject to disciplinary action.

Montana State University-Northern • P.O. Box 7751 • Havre, MT 59501 • 800.662.6132
Copyright • Disclaimer • AA/EEO Statement • Online Privacy Statement