Minnesota State Colleges and Universities
System Procedures
Chapter 5 – Administration

Guideline 5.23.1.1 Password Usage and Handling

Part 1. Purpose:

Subpart A. Where passwords are required, this system guideline identifies the standards for choosing and protecting passwords, and the system recommended practices to further enhance password privacy to protect Minnesota State Colleges and Universities (system) data and resources.

Subpart B. Passwords are one method used on system devices and systems to facilitate authentication. The security of system data is highly dependent upon the secrecy and characteristics of the password. Passwords are classified as not public data under the Minnesota Government Data Practices Act (MGDPA), per Minnesota State Statutes §13, and must be protected from unauthorized access. Compromised passwords can result in loss of data, denial of service, or attacks directed at Internet users from a compromised machine. Compromised passwords can also result in the inappropriate disclosure of not public data such as private student data, research participant data, and private employee data.

Subpart C. Nothing in this guideline shall be interpreted to expand, diminish or alter the academic freedom provided under Board policy, a system collective bargaining agreement, the terms of any charter establishing a system library as a community or public library, or the Board Policy 5.22, Acceptable Use of Computers and Information Technology Resources.

Part 2. Applicability. This guideline applies to all users of system information technology, whether or not the user is affiliated with the system, and to all uses of those resources, wherever located. This guideline establishes minimum requirements and colleges and universities may adopt additional conditions of use, consistent with this guideline and Board Policy 5.23, Security and Privacy of Information Resources, for information technology resources under their control. Those technologies that are not capable of supporting the characteristics described in this guideline, i.e. voicemail, are still subject to those characteristics that they are capable of supporting. The system is not responsible for any personal or unauthorized use of its resources, and security of data transmitted on its information technology resources cannot be guaranteed.

Part 3. Guidelines:

Subpart A. Password protection. Users must protect their passwords from unauthorized use and must not share passwords with others.

Subpart B. Strong Passwords. Users must use a password or passphrase that is a minimum of eight characters and must include a minimum combination of two character types and should include a combination of 3 character types such as: numbers, special characters, and lower and upper case letters.

Subpart C. Required changes. Passwords or passphrases must be changed at least every 180 days and should be changed at least every 90 days.

Subpart D. Lockout for Failed Attempts. System administrators should establish a standard for locking a user's account if the user fails to login to the system within a specified number of attempts. The lockout may be for a designated amount of time or until the account is administratively reset.

Subpart E. Password Administration. System administrators should enable password history, limiting the ability to re-use passwords.

Subpart F. Employee Role Change. When an employee changes position, including separation with the institution, access must be reviewed and updated. Access should be terminated immediately upon separation.

Subpart G. Service Accounts. Service accounts must use a password that is a minimum of twenty randomly generated characters and must include a combination of three character types such as: numbers, special characters, and lower and upper case letters.

a) **Periodic Changes.** Service account passwords must be changed at least annually.

b) **Employee Role Change.** Service account passwords must be changed immediately when an employee with access to a service account no longer needs access, such as when changing a job position or leaving the institution.

c) **Lockout for Failed Attempts.** A service account must lockout after no more than five (5) failed attempts. The lockout may be for a designated amount of time or until the account is manually unlocked.

Part 4. Definitions:

Subpart A. Institution. One of the separate entities, or having to do with an organizational entity as described under system.

Subpart B. May. A statement that is optional.

Subpart C. Minnesota Government Data Practices Act (MGDPA). Per Minnesota State Statutes §13, MGDPA regulates the collection, creation, maintenance and dissemination of government data in state agencies, statewide systems, and political subdivisions. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is a federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

Subpart D. Must. A statement that is required for a compliant implementation.

Subpart E. Must Not. A statement that is prohibited for a compliant implementation.

Subpart F. Not Public data. Data that is considered confidential, private, nonpublic or protected nonpublic data as defined in the MGDPA or any other relevant state or federal statute or system legal guideline.

Subpart G. Password/Passphrase. A sequence of characters, words or other text used to control access to a computer system, program or data.

Subpart H. Password history. A log of expired passwords, used primarily for automatic comparison with proposed new passwords. A password history is used to ensure that a user's proposed new passwords on a particular asset were not used in the recent past.

Subpart I. Should. A statement that is recommended but not required.

Subpart J. Should Not. A statement of practices that are not recommended but which may be followed.

Subpart K. System. Denotes the Minnesota State Colleges and Universities Board of Trustees, the system office, the state colleges and universities, and any part or combination thereof.

Subpart L. User. Any individual, including but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using system information resources, whether or not the user is affiliated with the system.

Part 5. Authority.

Subpart A. This standard derives authority from System Board Policy:

- 5.22 Acceptable Use of Computers and Information Technology Resources.
    - Procedure 5.22.1 Acceptable Use of Computers and Information Technology Resources
        - Part 4. Responsibilities of All Users,
        - Part 6. Security and Privacy, and
        - Part 8. College and University Policies and Procedures
- 5.23 Security and Privacy of Information Resources
        - Part 1. Policy Statement

Approval Date: 04/21/08,
Effective Date: 09/01/09,

Date and Subject of Revision:

1/25/12 – The Chancellor amends all current system procedures effective February 15, 2012, to change the term "Office of the Chancellor" to "system office" or similar term reflecting the grammatical context of the sentence.

12/21/11 - New Part 3, Subpart F Employee Role Change, and Subpart G Service Accounts were added.

01/21/09 - Part 4, technical change amended definition from "Public Data" to "Not Public Data."

01/14/09 - Revisions updated grammar and formatting, removed references to "MnSCU", removed unused definitions and clarified wording on definitions