

## Information & Technology Services Secure Password Standard

### **Overview**

- Passwords are an important aspect of computer security. Passwords are the primary method used to verify the identity of a network user and the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire computer network. MnSCU System Guidelines as well as the Payment Card Industry Data Security Standard require that passwords be configured securely. As such, all passwords that are managed by Information & Technology Services (including those of faculty, staff, students, contractors and vendors with access to ITS systems) will be configured and secured using the standard described below.

### **Scope**

- This standard applies to all user passwords that are managed by Information & Technology Services.
- This standard applies to all machine-level and service account passwords controlled by Information & Technology Services.
- This standard also applies to SNMP community strings used on devices that are controlled by Information & Technology Services.

### **Standard**

- All passwords must be protected from unauthorized access. Users are discouraged from writing down passwords in easily viewable locations, such as under keyboards, on monitors, or in a desk drawer.
- Passwords must not be reused. Where possible, systems will be configured to prevent the reuse of old passwords.
- Passwords must be at least 8 characters long.
- Passwords must include a combination of 3 character types such as numbers, special characters, lower case letters, or upper case letters.
- Password must be changed every 180 days.

### **Additional Authority**

- MnSCU System Guideline 5.23.1.3, Guideline for Password Usage and Handling, defines minimum standards for setting and protecting passwords.
- Minnesota Government Data Practices Act (MGDPA) defines passwords as Not-public data which must be protected from unauthorized access.
- Payment Card Industry (PCI) Data Security Standard (DSS) Section 8.

## ***Exceptions***

- MnSCU System Guideline 5.23.1.3 requires each college or university to have a process in place for documenting exceptions from the System Guideline.
- Exceptions to this standard can be granted by the Vice President of Information & Technology Services or the Vice President's designee.
- Any exceptions to the MnSCU System Guideline or the Information & Technology Systems Password Standard will be documented in this document.
- Current Exceptions:
  - Any password that cannot be configured to comply with these requirements due to limitations in the software is exempted from those requirements that it cannot comply with.
  - The Personal Identification Number (PIN) used for voice mail systems need not comply with password complexity rules and need not be changed.
  - IT Service account passwords that are applied to limited-access accounts and consist of at least 16 randomly-generated characters are exempted from the requirement to change passwords every 180 days.

## ***Effective and Review Date:***

- These password requirements take effect on January 1, 2009.
- This document will be reviewed on July 1, 2009 and every two years after that.