Network Password Policy

Purpose

Dakota State University (DSU) has established a formal policy regarding network user passwords. The purpose is to protect the networks, devices, and information at the university as well as to be in compliance with the Payment Card Industry Data Security Standards (PCI-DSS).

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of password changes.

Audience

This policy applies to all individuals with a University network account; including, but not limited to faculty, staff, students and affiliates.

Policy

DSU requires the use of strong passwords for our network systems. Passwords must contain characters from three of the following five categories:

- English uppercase characters (A-Z)
- English lowercase characters (a-z)
- Base 10 digits (0-9)
- Non-alphanumeric ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase.

The minimum password length is eight characters.

Passwords must not contain the user's entire username or full name.

Default passwords must be changed before a user is allowed access to a system.

Passwords must be changed every 180 days.

A user must use 8 new passwords before an old password can be used.

DSU users may not knowingly share their passwords with others. This includes, but is not limited to, the following restrictions:

- DSU users may not share their passwords with other DSU employees or students. (The exception is ITS employees that work on staff or student computers. Users are strongly encouraged to change their password after work is completed on their computer).
- DSU users may not share their passwords with friends, family members, or significant others.
- DSU users may not knowingly use their DSU email address and password, nor their DSU username and password, as the credentials to access third-party online services (e.g. Facebook, Google, Twitter, or any other third-party website or service.

DSU users may not share their passwords with others through negligent or careless behavior. This includes, but is not limited to, the following restrictions:

- DSU users may not send their passwords by e-mail.
- DSU users may not post their passwords in any public area, or any area that is easily accessible by others (e.g. a Post-It note stuck to the monitor, the bottom of the keyboard, in an unlocked desk drawer, etc.)

Enforcement

Users found in violation of this policy may be denied access to the DSU network. DSU will immediately disable and reset the password for any DSU user whose password has been shared with others, or reasonable evidence exists that it may have been shared. Also, DSU will notify the supervisor of the employee of the password violation.

Related Policies

SD Board of Regents' Acceptable Use of Information Systems Policy 7:1
SD Board of Regents' Security of Information Technology Systems Policy 7:4
DSU Computing Privileges Policy

Revision History

This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DSU's needs and goals.

Revision Date	**Reviewed by**
2014-03-14	Security Policy Committee