User Passwords

Policy Contents
I. Reason for this Policy.................................................................1
II. Statement of Policy ...............................................................1
III. Definitions ..............................................................................2
IV. Procedures ...............................................................................2
V. Related Documents, Forms and Tools ........................................3

I. REASON FOR THIS POLICY

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. The scope of this policy includes all individuals with a University account; including, but not limited to Faculty, Staff, Students and Affiliates.

Policy last reviewed 8/5/15 by CIO Management Team

II. STATEMENT OF POLICY

Passwords are an essential aspect of computer security, providing important front-line protection for electronic resources by preventing unauthorized access. Passwords help the University restrict unauthorized or inappropriate access to various resources at The University of South Dakota (USD) including, but not limited to user-level accounts, email accounts and documents stored in shared folders.

A poorly chosen password may result in the compromise of University systems, data or network. Therefore, all USD students, faculty and staff are responsible for taking the appropriate steps, as outlined below, to select appropriate passwords and protect them. Contractors and vendors with access to university systems are also required to observe these requirements.

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 (ITS) Department can require a more restrictive policy in protection of confidential data.

Any individual who violates this policy may lose computer or network access privileges and may be subject to disciplinary action in accordance with and subject to the SD Board of Regents’ Acceptable Use of Information Systems Policy (AUP) 7:1 and procedures, which may result in a range of sanctions up to and including suspension or dismissal for repeated or serious infractions.

### III. DEFINITIONS

**Strong Password:** A set of characters that is of sufficient length and complexity such that the password is not easily guessed or predictable. Strong passwords have these characteristics:

- Must have at least 8 characters
- Must contain at least one alphabetic and one non-alphabetic character
- Must contain at least one lowercase and one uppercase alphabetic character
- Must not be a University credential such as a username or email address
- Must not be dates or phone numbers
- Must not contain a word found in the dictionary
- Must not contain Social Security Numbers
- Must not be the name of a month preceded or followed by a number

### IV. PROCEDURES

**Password Composition**

Passwords are to be created following the guidelines found at http://www.usd.edu/technology/password-guidelines

**Password Aging**

- Passwords should be changed at least every 12 months, every 4 months is recommended.
- Passwords may not be changed more than once per day.

**Password Sharing**

- Sharing or allowing another person to use an individual account password is a violation of the Board of Regents’ Acceptable Use of Information Systems Policy (AUP) 7:1, unless the person is an information technology professional assisting you with a technical problem. Departmental account passwords should be shared only with appropriate
departmental personnel.

- Passwords must *never* be shared via e-mail, chat or other electronic written communication. The USD ITS department will *never* request a customer’s credentials by e-mail.

- Passwords may be shared via phone when necessary. However, users need to beware of “Phishing” or other social engineering scams where a user may have his or her password requested over the phone. University Information Technology personnel (i.e, Help Desk, IT Security Office, Desktop Support), as a best practice, do not normally request a user’s password over the phone.

- It is strongly recommended that passwords be changed after being shared as permitted in this section.

- Approval of the University's Information Technology Security Officer (ITSO) is required prior to sharing a password with a vendor (approval may be granted on a one-time or continuing basis), and this vendor access may require implementing the appropriate technology infrastructure to accommodate the access (depending on the circumstance and as determined by ITSO).

**Reporting a password compromise**

- Suspected compromises of passwords must be reported immediately to the ITS Help Desk at 677-6463 or toll free at 877-225-0027.

- The password in question should be changed immediately at [http://www.usd.edu/accounts/reset](http://www.usd.edu/accounts/reset).

**Password Auditing**

- ITS may require a more restrictive policy, such as stronger passwords, in some circumstances.

- ITS or its delegates may perform password assessments on a periodic or random basis. If a password is guessed or cracked during one of these assessments, the customer will be promptly notified and required to change their password. Again, the current password will NOT be sent or requested by e-mail from ITS.

**V. RELATED DOCUMENTS, FORMS AND TOOLS**

SD Board of Regents’ Acceptable Use of Information Systems Policy 7:1 - [https://www.sdbor.edu/policy/documents/7-1.pdf](https://www.sdbor.edu/policy/documents/7-1.pdf)