

---

## INFORMATION TECHNOLOGY SERVICES POLICY

---

### **Name of Policy**    **Password Policy**

---

#### **1. Purpose**

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

#### **2. Scope**

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

#### **3. Definitions**

**Strong Password** – A set of alphanumeric characters that is of sufficient length and complexity to make brute-force cracking methods infeasible.

#### **4. Policy Statement**

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 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 also are expected 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 Department can require a more restrictive policy in protection of confidential data.

##### **4.1 Password Composition**

Passwords created by users of University systems, and on systems where technology makes it possible, should conform to the following guidelines:

4.1.1 Must be at least eight characters

4.1.2 Must include a combination of the following:

4.1.2.1 Upper-case characters (A-Z)

4.1.2.2 Lower-case characters (a-z)

4.1.2.3 One or more numerals (0-9) or special characters (i.e. \* & % \$)

4.1.3 Must **not** be:

- 4.1.3.1 The user's login name
- 4.1.3.2 The reverse of the name
- 4.1.3.3 All numbers or all letters
- 4.1.3.4 Dictionary words
- 4.1.3.5 Generally available personal information (names of family, etc.)

These provisions will be enforced electronically whenever possible.

#### 4.2 Password Aging

- 4.2.1 Passwords should be changed annually. Once a semester (Fall and Spring) is recommended.
- 4.2.2 Passwords may not be changed more than once per day
- 4.2.3 Re-use of any of the accounts four prior passwords is not permitted

#### 4.3 Password Protection

- 4.3.1 Passwords should be treated as confidential university information
- 4.3.2 Passwords should never be included in email messages or other forms of electronic communication.

#### 4.4 Password Sharing

- 4.4.1 Sharing or allowing another person to use an individual account password is a violation of the Board of Regents' Acceptable Use Policy (AUP), 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.
- 4.4.2 Passwords should never be shared via e-mail, chat or other electronic written communication.  
The USD ITS department will never request a customer's user-name or password by e-mail.
- 4.4.3 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.
- 4.4.4 It is strongly recommended that passwords be changed after being shared as permitted in this section.
- 4.4.5 Approval of the University's IT Security Officer 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)

#### 4.5 Reporting a password compromise

- 4.5.1 Suspected compromises of passwords must be reported immediately to the ITS Help Desk at 677-6463 or toll free at 877-225-0027.
- 4.5.2 The password in question should be changed immediately at <https://www.usd.edu/accounts/reset>.

#### 4.6 Password Auditing

- 4.6.1 ITS may require a more restrictive policy, such as stronger passwords, in some circumstances
- 4.6.2 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

### 5. Consequences

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 Policy [http://www.usd.edu/its/policies/SDBOR\\_AUP\\_rev061504.pdf](http://www.usd.edu/its/policies/SDBOR_AUP_rev061504.pdf) and procedures, which may result in a range of sanctions up to and including suspension or dismissal for repeated or serious infractions.

### 6. Revision History

| Date       | Change           | Made By       |
|------------|------------------|---------------|
| 04/22/2008 | Approved Version | Steve Weidner |