UNIVERSITY OF SOUTH DAKOTA

| | |
|---|---|
| **Policy Number:** | 5.008 |
| **Originating Office:** | Information Technology Services |
| **Responsible Executive:** | The Vice President for Administration and Technology |
| **Date Issued:** | 02/24/2011 |
| **Date Last Revised:** | 07/16/2018 |

# User Passwords

## Policy Contents

## I. REASON FOR THIS POLICY

Users of University *information systems* are assigned a unique identifier (ID) and password to prevent unauthorized access. Individuals who receive the benefits of a University ID must protect those credentials from unauthorized use or disclosure.

The purpose of this policy is to establish a standard for the creation of strong passwords and the protection of those passwords. This policy is also intended to comply with legal and regulatory standards; including, but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI-DSS)

**Policy last reviewed: July 11, 2018**

## II. STATEMENT OF POLICY

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

1. Individual users of University *information systems* must not share their credentials.
2. All passwords must meet the *Minimum Password Requirements*.
3. All *privileged accounts* must use multi-factor authentication (MFA) including, but not limited to, faculty and staff accounts. (effective July 2019)

4. *Repeated consecutive* failed attempts to authenticate will result in temporary disablement of the account. (effective July 2019)
5. A department and/or system administrator may implement a more restrictive policy on information systems where appropriate and necessary for the security of electronic information resources.
6. Information systems subject to laws and regulations, including but not limited to HIPAA and PCI, must adhere to additional password requirements as necessary.
7. Exceptions to this policy must be approved in writing by the Vice President for Administration and Technology.

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

**Minimum Password Requirements (effective July 2019):**

- Must be 8 or more characters in length
- Must not contain repeated characters such as aaaa1111
- Must not be a University username or email address
- Must not be a single dictionary word
- Must not be a password previously compromised as part of a security breach
- Must not match any of the 4 most recently used previous passwords

**Additional Password Requirements for Shared Credentials (requires approval, effective July 2019):**

- Must be 15 or more characters in length
- Must change at least once every 180 days

**Repeated Consecutive Failures:** For the purposes of this document, "repeated consecutive failures" is defined as 10 consecutive failures within 15 minutes.

Privileged Accounts: Accounts that provide access to protected information, including but not limited to HIPAA, FERPA, GLBA, and PCI. At a minimum, this definition includes all faculty and staff accounts.

## IV. PROCEDURES

**ITS Responsibilities**

- Store all passwords using a *strong hash* or *strong encryption*
- Transmit all passwords using *strong encryption*

**Students, Faculty, and Staff Responsibilities**

- **Never** share your password
- Change your password immediately if it is at risk for any reason, for example
  - You shared your password
  - You connected to an insecure wireless network
  - You have any reason to believe that your password is compromised
- Do not reuse the same password for multiple sites

**Recommendations**

- Use a password manager to store passwords, to make it easier to use a different password for every account
- Use a passphrase with 4 or more random dictionary words rather than a hard-to-remember password using a complex mix of letters, numbers, and special characters
  - A passphrase such as **correcthorsebatterystaple** is a better password than **$tr0nG3r**
  - You may use a separator if that helps you to remember the password, such as **correct:horse:battery:staple**

**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.

**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

National Institute of Standards and Technology, U.S. Department of Commerce, NIST SP 800-63B