

**BLACK HILLS STATE UNIVERSITY**  
**Policy and Procedure Manual**

SUBJECT: Password Requirements

NUMBER: 7:2

---

Office/Contact: Network and Computer Services

Source: SDBOR Policies 7:1 and 7:4

Link: <https://www.sdbor.edu/policy/documents/7-1.pdf>;<https://www.sdbor.edu/policy/documents/7-4.pdf>

---

1. Purpose

This policy establishes the University's standard for creation of strong passwords and the protection of those passwords.

2. Definitions

- a. Compromise - made vulnerable (as to attack or misuse) by unauthorized access, revelation, or exposure

3. Policy

- a. Passwords have no expiration date
- b. Passwords must be changed if under suspicion of compromise or if the password has been compromised.
- c. All passwords must be strong passwords, as defined below.
- d. General Password Construction Standards
  - i. Strong passwords contain the following characteristics:
    - 1. Contain at least three (3) of the four (4) following character classes:
      - a. Lower case characters
      - b. Upper case characters
      - c. Numbers
      - d. Special characters (e.g., !@#\$%^&\*()\_+= etc.)

2. Passwords must contain fifteen (15) or more alphanumeric characters
- ii. Weak passwords contain the following characteristics:
  1. Less than fifteen (15) characters
  2. Common usage words such as:
    - a. Names of family, pets, friends, co-workers, etc.
    - b. Birthdays and other personal information
    - c. Letter or number patterns (e.g., qwerty, 12345, etc.)
- e. Password Protection Standards
  - i. Passwords shall not be shared with anyone. Sharing or allowing another individual to use an account password is a violation of SDBOR Policy 7.1 and University Policy 7:5, (Acceptable Use Policy). All passwords are to be treated as sensitive, confidential information.
    1. Network and Computer Services, as a function of operation, may ask users for their passwords for technical support services. These instances do not violate SDBOR Policy 7:1 or University Policy 7:5.
    2. Network and Computer Services will not send or request a password by email, and individuals should not respond to such requests.
  - ii. Passwords must never be written down or stored electronically without the use of encryption.
  - iii. Passwords must not be revealed in email, chat, or other electronic communication.
  - iv. Passwords must not be revealed on questionnaires or security forms.
  - v. Vendor password sharing must be approved by Network and Computer Services.
  - vi. Network and Computer Services may require more restrictive policy standards as circumstances require.
  - vii. If someone demands a password, individuals should refer them to this policy and direct them to Network and Computer Services.

- f. If an account or password compromise is suspected, incidents must be immediately reported to Network and Computer Services.
  
4. Responsible Administrator  
The Vice President for Finance and Administration, or designee, is responsible for the annual and ad hoc review of this policy and its procedures. The University President is responsible for formal policy approval.

SOURCE: Approved by President Laurie Nichols on 1/12/2022.