BLACK HILLS STATE UNIVERSITY

Policy and Procedure Manual

SUBJECT: Multi-Factor Authentication for University Accounts

NUMBER: 7:3

Office/Contact: Network and Computer Services

1. Purpose

This policy establishes the University's standard for using multi-factor authentication (MFA), who is required to enroll in MFA, the policy for issuing bypass codes, and the distribution of hardware tokens.

2. Definitions

a. Multi-Factor Authentication (MFA): The three factors that prove identity to a system are something you are, something you have, and something you know. MFA requires at least two of the three factors during login.

b. Second Factor: An approved device that proves the individual has something in their possession is the second factor, and the individual's password (something they know) is the first factor.

c. Hardware Token: A small device that provides an alternative to using a smartphone or tablet as your second factor.

d. Bypass Codes: A short numerical code that can act as a second factor temporarily

3. Policy

i. Network Computer Services retains the ability to add or remove MFA protection to any application as needed to ensure the security of university accounts. At a minimum, the following systems will be protected:

1. Microsoft 365 applications, including email, OneDrive, and SharePoint.
2. South Dakota Board of Regents central applications that utilize a federated login, including D2L, SNAP, and Banner Self-Service

4. Procedure

a. All University employees, accepted students, and current students must enroll in MFA using either a smartphone, tablet, or hardware token as their second factor.

b. If an employee or student does not have access to their second-factor device, the individual can request a bypass code from the University's Help Desk. The Help Desk technician is required to verify the individual's identity by requesting their date of birth.

c. If an employee does not possess an approved second factor or does not consent to the use of their personal device, the employee's hiring department is responsible for purchasing a hardware token for the individual at a cost of approximately $20.

   i. If the individual leaves employment with the University, they are required to return the hardware token to the hiring department

   ii. If a hardware token is broken, lost, or stolen, the individual is responsible for replacing the token

d. In the case of an accepted or current student not possessing an approved second factor or not consenting to the use of their personal device, Network Computer Services will provide a hardware token for the individual at no cost to the student

   i. If the hardware token is broken, lost, or stolen, the individual is responsible for replacing it at a cost of about $20.

5. 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: Adopted by President on 2023/02/13; Reviewed 2024/12/03