UNIVERSITY OF SOUTH DAKOTA

Policy Number: 5.007
Originating Office: Information Technology Services
Responsible Executive: Chief Information Officer
Date Issued: 1/26/2011
Date Last Revised: 2/11/2025

Faculty & Staff User Accounts

Policy Contents

I. REASON FOR THIS POLICY

The University of South Dakota must protect its information technology (IT) resources including its private and sensitive data by requiring the use of electronic identifiers (username and password) to control access. This policy will be evaluated on an annual basis to ensure its adequacy and relevancy regarding The University of South Dakota's needs and goals.

II. STATEMENT OF POLICY

Most university business is completed via electronic resources. Access to email, calendars, university-owned computers, network file shares, time sheets, and online resources require use of a username and password.

USD requires all faculty and staff to have electronic identifiers (username and password) to gain access to the resources necessary for them to complete their job duties and to protect these resources from unauthorized use.

Access may be granted to various university resources and South Dakota Board of Regents (SDBOR) resources. Permissions granted to these resources are based upon the role of the employee.

University-assigned email addresses are an official means of communication for university employees. Employees who forward their email from their official University email to an external address do so at their own risk. ITS is not responsible for mail forwarding settings, and the Service Desk will not provide support for unofficial email services.

Sharing or disclosing individual account credentials, including usernames and passwords, is strictly prohibited. Never request, obtain, or attempt to use another individual's credentials. Unauthorized sharing or solicitation of account credentials may result in security risks and unauthorized access and may result in disciplinary action.

III. DEFINITIONS

Banner: Human Resources, Finance and Student Information System.

USD Account: Username and password needed to access USD specific resources.

EPAF: Electronic Personnel Action Form

IV. PROCEDURES

Eligibility Requirements:

- Have officially accepted a position through the Human Resources office.
- Payroll documents have been completed and submitted by the hiring department, including the EPAF, and entered into Banner by Human Resources.
- The timing of the creation of the accounts can be found in the 'Account Lifecycles and Priorities' knowledge article referenced below in Section V.

Creation of USD Accounts:

- USD accounts for faculty and staff are automatically created when the above Eligibility Requirements are met.

Responsibilities:

- Account Owner:
    - Adhere to the guidelines set forth in the South Dakota Board of Regents policy Acceptable Use of Information Technology Systems.
    - Adhere to the guidelines in the Information Security and Data Responsibilities policy.
    - Never disclose your account credentials, including usernames and passwords, to any individual, system, or third party.
    - Use approved authentication mechanisms such as multi-factor authentication (MFA), to securely access university systems and services.

- Human Resources:
    - Establish processes for hiring and terminating employees in Banner.
    - Document procedures and provide training to the campus community.
    - Ensure Banner data is accurate and entered correctly.
- Hiring Department:
    - Notify HR in a timely manner when a new employee is hired or ending employment.
    - Follow established processes for updating Banner, including the submission of EPAFs.
- Information Technology Services:
    - Creating and removing accounts
    - Maintaining availability of resources

Account Removal:

- Accounts will be removed:
    - After the employee no longer has an active position with the university
    - If there are job-related performance issues as determined by HR
- The timing of the removal of the accounts can be found in the *Account Lifecycles and Priorities* knowledge article referenced below in Section V.

Extensions:

- All extended access to accounts beyond the normal account removal timeframe must be approved by Human Resources.
- Extension requests must be submitted to the Service Desk at least three working days prior to account removal.
- ITS cannot guarantee extension requests received less than three working days prior to account removal. ITS will make every effort to accommodate these extension requests.
- If approved, the standard extension will be for thirty (30) days.

V. RELATED DOCUMENTS, FORMS AND TOOLS

SDBOR Acceptable Use of Information Technology Systems Policy 7.1

USD Information Security and Data Responsibilities Policy 5.003

Account Lifecycles and Priorities – Coyote One Stop Knowledge Base

SDBOR IT Security Policy for Employees Leaving the BOR System 7.2