The University of the South

Password Management Policy

Purpose

The purpose of this policy is to establish a minimum expectation with respect to password management in order to protect data and the University's computer systems.

Scope

This policy applies to all users of computer systems of the University including faculty, staff, students, temporary workers, vendors and any other authorized users.

Responsible Party

The Associate Provost of the Library and Information Technology Services division of the University is responsible for maintaining this policy and may be contacted with any questions.

Definitions

Term	Definition
Active Directory username	Username used for access to most of the University's systems such as SSB, Sewanee-Secure Wi-Fi, Blackboard, Google Apps, desktop login and Active Directory.
NetID (also known as SSB Username and Active Directory Username)	Username used in most systems including SSB, active directory, blackboard, google apps.
Passphrase	A sequence of words or other text used to control access to a computer system (a Passphrase generally makes for a strong Password). For example, a passphrase might be "YeaSewaneesRight".
Password/PIN	A string of characters that allows access to a computer or system. For this policy, the terms Password and PIN can be used interchangeably.
Privileged	Accounts with elevated privileges in the system such as those with root or

Accounts	administrator level access.
SSB	Self-Service Banner which provides a person access to the University's main administrative software which includes student, financial aid, employee or other information.
SSB Username	Username used to access the Self-Service Banner system and also known as the NetID.
System Accounts	Accounts used for automated processes without user interaction or accounts used for device management.
User Accounts	Accounts used by individuals for accessing systems such as e-mail, self-service Banner and Internet Native Banner.

Policy

A combination of a personal user login ID for identification and a unique password for authentication will be required of all users before they are allowed access to the University's systems. The effectiveness of passwords to protect access to the institution's information directly depends on strong password construction and safe handling practices. Faculty, staff and students should protect their own data and University data by choosing quality passwords, practicing good password control and using recommended computer security practices.

1. Password Construction

- All users must construct strong passwords for access to all University networks and systems, using the following criteria where technically feasible:
    - Comprised of a passphrase of a minimum of 12 characters for user accounts and a minimum of 20 characters for system accounts;
    - Not be based on anything somebody else could easily guess or obtain, such as names, telephone numbers, dates of birth, pets, etc.;
    - Free of consecutive identical, all-numeric or all-alphabetic characters;
    - Passwords can't be reset to any of the 4 previous passwords.

2. Password Management – User and Privileged Accounts

The following requirements apply to user password management.

- Storage and Visibility
    - Passwords must not be stored in a manner which allows unauthorized access. For example, passwords can't be displayed in clear view.
    - Passwords will not be stored in a clear text file.
    - Passwords will not be sent via unencrypted email.
    - Passwords and user ids will not be sent in the same email.
- Changing Passwords
    - Users must change their passwords at least every 90 days.
    - Initial passwords and other passwords set by the Information Technology staff or helpdesk must be changed by the user at the first log-on.

3. Password Management – System Accounts

- System account password must be changed at least every 365 days.
- System passwords must be at least 20 characters in length.
- Vendor provided passwords must be changed upon installation.

Responsibilities

Each individual is responsible for protecting passwords for their accounts. All users of the University's computer systems should report to the Associate Provost for Library and Information Technology Services any of the following and the password can be changed immediately:

- Unauthorized password discovery or usage by another person;
- System compromise (unauthorized access to a system or account);
- Insecure transmission of a password;
- Accidental disclosure of a password to an unauthorized person; or
- Status changes for personnel with access to privileged and/or system accounts.

REVISION DATE: August 24, 2021