Sam Houston State University
A Member of The Texas State University System
Information Technology

Password Policy: IT-02

PURPOSE:

This policy establishes guidelines and requirements for creating and managing passwords within Sam Houston State University (SHSU) information resources to help protect sensitive information, prevent unauthorized access, and reduce the risk of data breaches or malicious activities.

Information system custodians will ensure passwords are secured using industry best practices.

SCOPE:

The SHSU Password Policy applies to all user passwords and all other authenticators used in SHSU information resources.

POLICY STATEMENT:

General Requirements

1. Passwords must be unique. SHSU username and password should not be used for external services (e.g., LinkedIn, Facebook, or Twitter).
2. Passwords must not be reused following password resets.
3. Passwords must not be easy to guess and never be set to those obtained from previous, known breaches, commonly used passwords, dictionary words, repetitive or sequential characters (e.g., 'aaaaaa', '1234abcd'), or context-specific words (including the name of the application or service, or derivatives thereof).
4. Passwords should not be easily accessible to others (e.g., posted on monitors, under keyboards).
5. Passwords must be encrypted when stored.
6. Passwords for individual user accounts should never be shared with anyone, including family, supervisors, co-workers, and IT personnel.

Security Incidents

1. If you know or suspect that your account has been compromised, you must change your password immediately to a new and unique value and contact the Service Desk for further guidance and assistance.
2. If IT suspects that your account or password has been compromised, IT may take appropriate actions such as changing your password or disabling your account. The IT Service Desk should be contacted for assistance.

Information Systems (Systems) and Information System Custodians (Custodians)

1. Custodians must prevent or take steps to reduce the exposure of any clear text, unencrypted account passwords that SHSU applications, systems, or other services have received for purposes of authentication.
2. Custodians must never request that passwords be transmitted unencrypted. Of particular importance is that passwords never be sent via email.
3. Custodians must change vendor-supplied and other default passwords used in a system prior to first use.
4. To the extent practicable, all Systems that require users to authenticate their identities should be configured to leverage Single-Sign On (SSO) systems maintained by IT.
5. Systems must require passwords to reauthenticate a locked device or session.
6. Systems must enforce the maximum available setting for password history.
7. Systems must allow for password changes through self-service means by each account owner.
8. Systems that store passwords for verifications must do so by using a combination of strong encryption and a "One-way function", a cryptographic technique known as hashing, that makes it difficult to determine the actual passwords from the stored information.
9. Systems must incorporate one (1) of the following standards:
    a. Modern Authentication System Standards:
        i. Passwords must have a minimum length of fifteen (15) characters.

            It is strongly recommended that passwords contain a mix of upper case, lower case, and numeric characters or special characters (!@#%^&*+=?/~';:,<>|\).
        ii. Passwords must be changed at least once every four (4) years.
        iii. Multi-factor authentication must be enabled on all user accounts.
    b. Legacy Authentication System Standards:
        i. Passwords must have a minimum length of eight (8) characters.
        ii. Passwords must contain a mix of upper case, lower case and numeric characters or special characters (!@#%^&*+=?/~';:,<>|\).
        iii. Passwords must be changed at least once every ninety (90) days.

Detailed information and instructions for password management can be found on the SHSU website in the New Employee Technology Orientation training booklet. https://www.shsu.edu/dept/it@sam/documents/New+Employee+Technology+Orientation.pdf

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02

Approved by: President's Cabinet, June 2023

Reviewed by: Heather Thielemann, Information Resources Manager, June, 2023

Next Review: June, 2024