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

Identification/Authentication Policy: IT-22

PURPOSE:

The purpose of the Identification/Authentication Policy is to ensure the security and integrity of Sam Houston State University (SHSU) data and information resources by employing controls for securing user identification and authentication credentials. SHSU uses the three (3) basic authentication methods: something you know (i.e., a password), something you have (i.e., smart card, smart phone, hardware token, or ID), and something you are (i.e., fingerprint or other biometrics).

To ensure the security and integrity of SHSU data, identified users will securely authenticate to SHSU information resources and access only resources which they have been authorized to access.

If user identities are not properly authenticated, SHSU has no assurance that access to information resources is properly controlled. This policy mitigates the risk of unauthorized access of information, as well as establish user accountability and rules for access.

SCOPE:

The Identification/Authentication Policy applies to all SHSU information system owners and custodians as well as individuals granted access to SHSU information resources.

POLICY STATEMENT:

1. Identification and authentication shall use SHSU's Identity and Access Management system, which includes, but is not limited to, Single Sign-On and Multi-factor Authentication.

2. SHSU managers and supervisors have the responsibility of requesting access to information systems and approving user access privileges based upon their assigned duties, as well as notifying Data Owners and IT of the termination of access to information resources.

3. Prior to being granted access to SHSU information resources, the needs of the employee, contractor, vendor, guest, or volunteer shall be given ample consideration and authorization granted to allow access to SHSU information resources. Access should be granted according to the principle of least privilege as outlined in IT Administrator/Special Access Policy (IT-18).

4. SHSU accounts will have a unique identifier that is permanently associated with a single user. Once an identifier is assigned to a particular person, it is always associated with that person. It is not allowed to be reassigned to identify another person.

5. Use of the authentication service to identify oneself to an SHSU system constitutes an official identification of the user to the University, in the same way that presenting an ID

card does. Users will be held accountable for all actions of their accounts.

6. Regardless of the authentication method used, users must use only the authentication information that they have been authorized to use, i.e., must never identify themselves falsely as another person.

7. Users must keep their authentication information confidential, i.e., must not knowingly or negligently make it available for use by an unauthorized person. Anyone suspecting that their authentication information has been compromised must contact the Information Security Office immediately.

8. When using multi-factor authentication (MFA) with devices such as smartphones or hardware tokens for authentication into SHSU services, the user is responsible for the following:

    a. Notifying the IT Service Desk immediately if an MFA device is lost/stolen
    b. Replacement cost of an SHSU furnished MFA device.

9. Users must adhere to the requirements of the SHSU User Accounts Password Policy (IT-02).

10. SHSU information system owners and custodians shall be responsible for ensuring that authorization and account management processes are documented and that the appropriate people have been assigned the responsibility of creating and maintaining authorization records.

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, February 6, 2012
Reviewed by: Heather Thielemann, Information Resources Manager, June, 2023
Next Review: June, 2024