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

Identification/Authentication Policy: IT-22

PURPOSE:

The purpose of the Identification/Authentication Policy is to ensure the security and integrity of SHSU data and information technology resources by ensuring controls for securing user identification and authentication credentials. SHSU utilizes the three basic authentication methods: something you know (i.e., a password), something you have (i.e., smart card 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 technology 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 technology resources is properly controlled. This policy will mitigate 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 individuals granted access to SHSU information technology resources.

POLICY STATEMENT:

SHSU shall require that systems are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication (any or all of the basic authentication methods), and implementing access controls on SHSU information technology resources. Access control is provided at the firewall, network, operating system, and application levels.

SHSU managers/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@Sam of the termination of access to information technology resources.

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

SHSU accounts will have a unique identifier that is associated with a single user. Once an identifier is assigned to a particular person, it is always associated with that person. It is never subsequently reassigned to identify another person.

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. Security is everyone's responsibility, and everyone has a responsibility to protect their own "identity". Users will be held accountable for all actions of their accounts.

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. Additionally, 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 should contact the Information Security Office immediately.

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

SHSU Data Owners 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.

SHSU Data Owners may monitor related activities of individuals as a condition for continued access. At a minimum, SHSU Data Owners must review user access privileges annually.

DEFINITIONS:

Authentication Credentials: The verification of the identity of a user who wishes to access a system, commonly using a password in conjunction with a unique UserID.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Mitigate: The elimination or reduction of the frequency, magnitude, or severity of exposure to risks in order to minimize the potential impact of a threat.

Principle of Least Privilege: The practice of limiting user profile privileges on computers to only the information and resources that are necessary, based on users' job necessities.

Unauthorized Access: Access by a person who has not been given official permission or approval to access SHSU systems.

User Identification: A unique sequence of characters used to identify a user and allow access to a computer system or computer network.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by:	Mark C. Adams, Associate VP for Information Technology, January 30, 2015
Approved by:	President's Cabinet, February 6, 2012
Next Review:	November 1, 2016