Authority

1 Texas Administrative Code (TAC) § 202
Texas State University System (TSUS) Rules and Regulations

Scope

This program applies equally to all individuals granted access privileges to any Sam Houston State University information technology resource, to include the following:

- Central and departmentally-managed university information technology resources.
- All users employed by SHSU, contractors, vendors, or any other person with access to SHSU’s information technology resources.
- Non-SHSU-owned computing devices that may store protected SHSU information.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, network resources owned or managed by SHSU. This includes third party service providers’ systems that access or store SHSU’s protected information.
- Auxiliary organizations, external businesses and organizations that use university information technology resources must operate those assets in conformity with the SHSU Information Security Program.

Information Security Roles and Responsibilities

The following distinctions among owner, custodian, and user responsibilities guide determination of the roles: (TAC §202.71(c)).

Data Owner

The owner or his or her designated representative(s) are responsible for and authorized to:

- Approve access and formally assign custody of information technology resources.
- Determine the asset’s value.
- Specify data control requirements and convey them to users and custodians.
- Specify appropriate controls, based on a risk assessment, to protect the state’s information technology resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information technology resources and services outsourced by the institution of higher education.
- Confirm that controls are in place to ensure the confidentiality, integrity, and availability of data and other assigned information technology resources.
- Assign custody of information technology resources and provide appropriate authority to implement security controls and procedures.
- Review access lists based on documented security risk management decisions.
- Approve, justify, document, and be accountable for exceptions to security controls. The information owner shall coordinate exceptions to security controls with the ISO or other person(s) designated by the state institution of higher education head.
- The information owner, with the concurrence of the institution of higher education head or his or her designated representative(s), is responsible for classifying business functional information.