Overview

Introduction

The Sam Houston State University (SHSU) Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of SHSU information technology resources.

The Information Security Program contains administrative, technical, and physical safeguards to protect university information technology resources. Measures shall be taken to protect these resources against accidental or unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Access to SHSU information technology resources shall be appropriately managed by the SHSU Information Security Program. Unauthorized modification, deletion, or disclosure of information technology resources can compromise the mission of SHSU, violate individual privacy rights, and possibly constitute a criminal act. (TAC §202.70).

This framework represents the basis of the institutional information security program and on the aggregate whole meets the objectives as articulated by TSUS Rule III, paragraph 19 and its associated guidelines. The SHSU Information Security Program and security standards are not intended to prevent or impede the authorized use of information technology resources as required to meet the university mission.

SHSU information technology resources may be limited or regulated by SHSU, as needed, to fulfill the primary mission of the university. Usage of SHSU information technology resources may be constrained as required to assure adequate capacity, optimal performance, and appropriate security of those resources.

Purpose

The purpose of the SHSU Information Security Program is to provide the university community with a description of the university strategic plan for achieving compliance with information security related laws and guidelines. Additionally the framework of this plan is designed to document the controls used to meet the information security program objectives by:

- Identifying system data owners, providing the data classification standard and identifying the category of its data.
- Reviewing all authorized users and their security access for each system.
- Providing security awareness training for all employees.
- Performing the risk assessment process and developing the risk mitigation plan.
- Reviewing and updating the disaster recovery plan.
- Reviewing current policies and training program.
- Creating a security effectiveness report to the president.
- Reviewing the current process and implement changes as necessary.

The Information Security Program process combines multiple security elements into a management framework that supports the objectives of confidentiality, integrity, and availability.