Sam Houston State University

Information Security Program

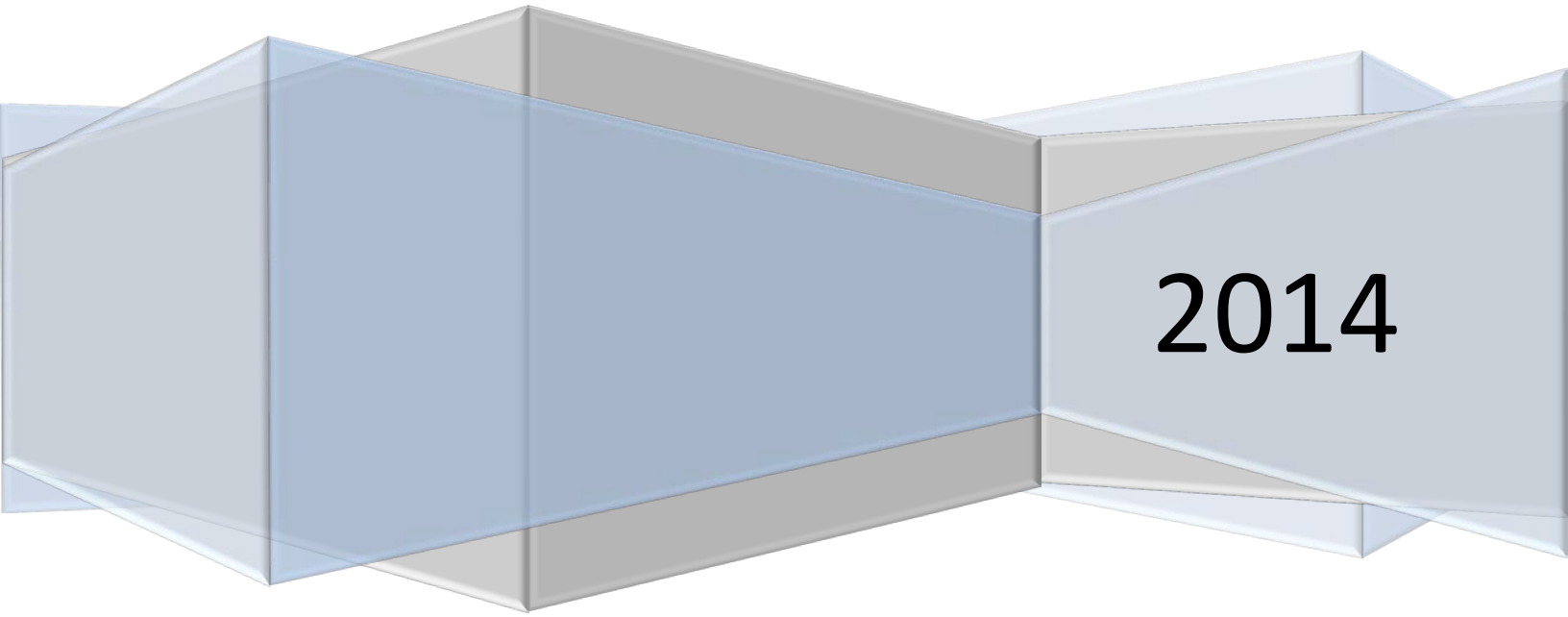

TABLE OF CONTENTS

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.

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.

SHSU Data Owners:

- Finance and Operations, VP Finance and Operations
- Student and Enrollment Management, VP Enrollment Management
- Academic Affairs, Associate Provost
- Banner General, Designated IRM

Data Custodian

Custodians of information technology resources, including third-party entities providing outsourced information technology resources services to state institutions of higher education shall:

- Implement the controls specified by the information owner(s);
- Provide physical, technical, and procedural safeguards for the information technology resources;
- Assist information owners in evaluating the cost-effectiveness of controls and monitoring; and
- Implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

SHSU Data Custodians:

- Graduate Admissions: Director of Projects
- Undergraduate Admissions: Director
- Purchasing: Director of Procurement and Business Services
- Budgeting: AVP Budget and Operations
- Student Records: Registrar
- Banner General: Director ERP Services
- Financial Aid: Director of Financial Aid
- Residence Life: Director of Residence Life
- Human Resources: Director of Human Resources
- Payroll: Manager
- Accounting, Cashier, Accounts Payable: Controller

Users

Users of information technology resources shall use the resources only for defined purposes and comply with established controls.

Information Security Officer (ISO)

Each institution of higher education head or his or her designated representative(s) shall designate an ISO to administer the University Information Security Program. The ISO shall report to executive management.

- It shall be the duty and responsibility of this individual to develop and recommend policies and establish procedures and practices, in cooperation with information owners and custodians, necessary to ensure the security of information technology resources assets against unauthorized or accidental modification, destruction, or disclosure.
- The ISO shall document and maintain an up-to-date Information Security Program. The Information Security Program shall be approved by the institution of higher education head or his or her designated representative(s).
- The ISO is responsible for monitoring the effectiveness of defined controls for mission critical information.
- The ISO shall report, at least annually, to the institution of higher education head or his or her designated representative(s) the status and effectiveness of information technology resources security controls.

- The ISO with the approval of the institution of higher education head or his or her designated representative may issue exceptions to information security requirements or controls. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.

Information Resources Manager (IRM)

The SHSU Information Resources Manager (IRM) is the duty of the Vice President for Information Technology (VPIT), also known as the Chief Information Officer (CIO), who is responsible to the State of Texas for management of the agency's information resources. The designation of an agency Information Resources Manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency.

Program Framework

This section defines the Information Security Program process that will ensure the continuity, performance and security of SHSU's information systems. This framework is based on the main objective of the information security program: confidentiality, integrity, and availability.

A review of SHSU's Information Security Program for compliance with required standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the Information Security Program (TAC§202.71(e).

The following processes will ensure that the appropriate safeguards are applied to SHSU's information systems and will continue to mature with the growing needs of the university's mission.

1. Establish Responsibility

At the beginning of each fiscal year, the assigned data owners and their selected data custodians will be reviewed by the IRM and the ISO per IT-05 Data Access Review Policy. The data owners will review/identify the related data stored on their system and identify the categories of data stored as confidential, protected or public according to the data classification standards in IT-06 Data Classification Policy. The data owners will then review the list of authorized users for each system and make the necessary changes using the least privileged model.

The IRM will review and approve information ownership and responsibilities to include personnel, equipment, hardware and software, as well as define information classification categories. (TAC§202.71(a)(b)).

2. Security Awareness Training

All employees with access to the SHSU information technology resources must participate in information security awareness training (IT-13 Technology Security Training Policy) (TAC§202.77). The training promotes awareness of:

- SHSU information security policies, standards, procedures, and guidelines.
- Potential threats against university protected data and information technology resources.
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information technology resources.

New employees will sign a non-disclosure agreement and will be provided individual access to the Information Security Awareness Training Program.

Employees are expected to complete the training within 30 days of receiving their access to the program, and then annually.

Department heads and university executive management are responsible for and will be provided status of training compliance.

3. Risk Assessment and Planning

Risk Planning

The principle reason for managing risk in an organization is to protect the mission and assets of the organization. Understanding risk, especially the magnitude of the risk, allows organizations to prioritize resources.

Security must be a consideration from the very beginning of any project at the university rather than something that is added later. A control review should be performed before implementation of information technology resources which store or handle confidential, sensitive, and/or protected information. This may include:

- A technical security evaluation to ensure appropriate safeguards are in place and operational.
- A risk assessment, including a review for regulatory, legal and policy compliance.
- A contingency plan, including the data recovery strategy.
- A review of on-going production procedures, including change controls and integrity checks.

Risk Assessment

SHSU performs annual assessments of its information risks and vulnerabilities (IT-17 Risk Assessment Policy). Risk assessments may be aimed at particular types of information, areas of the organization, or technologies. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of university controls. Risk assessments shall:

- assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
- evaluate the sufficiency of existing policies, procedures, information systems, internal controls and security practices, in addition to other safeguards in place to control risks;

- be classified and updated based on the inherent risk. Risk and frequency will be ranked 'high', 'medium', or 'low' based on TAC§202.72 criteria;
- design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of state and federal laws;
- monitor the effectiveness of those safeguards;
- analyze data collected to identify control objectives, risk exposures, mitigation strategies and action plans for addressing each risk with timelines; and
- support the annual report to the president and substantiate any changes to the information security program that may be needed as a result of evaluating the information collected.

4. Disaster Recovery/Business Continuity Plan

IT@Sam is responsible for developing and maintaining a Disaster preparedness/ Recovery/ Business Continuity Plan designed to address the operational restoration of SHSU's critical computer processing capability. This plan identifies the strategy to recover centrally administered data storage, programs, and processing capability in the event of a disaster. The plan identifies the minimum acceptable recovery configuration, which must be available for SHSU to resume the minimum required levels of essential services. The plan is located in strategic areas and available to all Computer Services personnel through a shared network resource. The plan contains proprietary and confidential information, is not intended for public distribution, and will not be published on the Web in its entirety. (TAC§202.74 and Texas Government Code 552.139) (Texas Government Code, Sec. 552.139)

The IT@Sam Disaster Preparedness/Recovery Plan described above does not address the needs of individual departments beyond the restoration of access to their critical centrally administered applications. All major university divisions/departments develop individual plans for protecting their information resource assets and operating capability. Each departmental plan will address losses ranging from minor temporary outages to catastrophic.

5. Annual Review

At the end of each fiscal year, the Information Security Officer (ISO) will review the risk assessment results, Security Awareness Training Program, Information Security User Guide, Information Security Program and all SHSU IT Policies.

The ISO and IRM will report the status and effectiveness of SHSU's information security controls and will present recommended revisions and improvements based on the information collected. The report will include:

- Description and/or narrative of any security incident that resulted in a significant impact to the university.
- Status of the Risk Assessments noting any significant changes.
- Status of the Vulnerability Assessments noting any major findings and corrections.
- Status of the IT Policy review.
- Status of the IT Security Awareness Training Program.
- Anticipated changes in the next fiscal year.

Compliance References

SHSU's information security practices must comply with a variety of federal and state laws, and SHSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver's license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

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 to the use of institutional information technology resources are listed below.

To avoid breaches of any law, regulation, contractual obligation, or institutional policy, information technology resources will be regularly tested and audited to assure adherence with both external and internal standards.

Students, faculty and staff are responsible for understanding and observing these and all other applicable policies, regulations and laws in connection with their use of the institution's information technology resources.

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act of 2002 (FISMA)
- Texas Administrative Code, Title 1, Subchapter 203
- Texas Administrative Code, Title 5, Subtitle A, Chapter 552
- Texas Penal Code, Chapter 33, Computer Crimes
- Texas Penal Code, § 37.10, Tampering with Governmental Record
- United States Code, Title 18, § 1030, Computer Fraud and Related Activity of 1986
- Copyright Act of 1976
- Digital Millennium Copyright Act October 20, 1998
- Electronic Communications Privacy Act of 1986
- The Information Resources Management Act (IRM) TGC, Title 10, Subtitle B, 2054.075(b)
- Computer Software Rental Amendments Act of 1990
- ISO/IEC 27002:2005 standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

Failure to Comply (Enforcement)

Consistent with SHSU policies, the ISO is authorized by the President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the University community.

Administrators must ensure that measures are taken within their department to comply with this policy and its related standards, guidelines and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by

the ISO. Approved requests will be reviewed annually to determine if an exception is still warranted.

SHSU reserves the right to temporarily or permanently suspend, block, or restrict access to university information technology resources, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of SHSU information technology resources; to protect SHSU from liability; or to enforce this policy and its related standards and practices.

Failure to adhere to the provisions of this policy statement or the appropriate use policy statement may result in:

- suspension or loss of access to institutional information technology resources
- appropriate disciplinary action under existing procedures applicable to students, faculty and staff, and
- civil or criminal prosecution

Potential violations will be investigated in a manner consistent with applicable laws and regulations, and SHSU policies, standards, guidelines and practices TAC§202.77.

The VPIT or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate university officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Third-party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to SHSU.

Appeals of university actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for SHSU students and employees.

Obtaining a Policy Exemption

Exemptions to policies are granted on a case-by-case basis and must be reviewed and approved by the university designated IRM. The IRM will mandate the documentation and additional administrative approvals required for consideration of each policy exemption request. TAC§202.71(c)(1)(H) and (d)(5).

Definitions

Contains an alphabetized listing of both common and specific terms that are used in this Information Security Program.

Availability – Ensuring that information systems and the necessary data are available for use when they are needed.

Business Continuity Plan - A plan to ensure that the essential business functions of the organization are able to continue (or re-start) in the event of unforeseen circumstances. The BCP will identify the critical people (roles / functions), information, systems and other infrastructure, e.g. telephones, which are required to enable the business to operate. A detailed plan will be laid out and, if called upon, should be executed to assure minimum additional disruption.

Confidentiality – Assurance that information is shared only among authorized persons or organizations.

Data Custodian – The person responsible for overseeing and implementing physical, technical, and procedural safeguards specified by the data owner.

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

Disaster Recovery Plan - The plan that is activated when there is an emergency which ensures that health and safety come first followed by damage limitation. Having contained the impact of the disaster, and having ensured that the situation is under control e.g. through the Emergency Services, then the Business Continuity Plan will be activated.

Information Resources Manager (IRM) – Officer responsible to the State of Texas to manage SHSU information technology resources.

Information Security – The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information Security Officer (ISO) – Officer designated to administer the university Information Security Program.

Information Security Program – Program that contains administrative, technical, and physical safeguards to protect information technology resources.

Integrity – Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Mitigate – The effort to reduce loss by making a deficiency less severe and lessening the impact of potential damages.

Remediate – The act or process of correcting a fault or deficiency.

Risk – The likelihood that something bad will happen that causes harm to, or loss of, an information asset.

Risk Assessment – A systematic process of evaluating the potential risks that may be involved in the use of the SHSU information technology resources.

Security Incident - A security incident is a computer, network, or paper based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

Threat – Anything that has the potential to cause harm.

User – Person responsible for viewing, amending and updating the content of the SHSU information assets.

Vulnerability – A weakness that could be used to endanger or cause harm to an information asset.

Vulnerability Assessment - the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Appendix A – Presidential Approval of Information Security Program

Sam Houston State University
Memorandum

To:	Dr. Dana L. Gibson President	Date:	June 10, 2014
From:	Mark Adams Chief Information Officer	Subject:	Information Security Program Presidential Approval

---

This memorandum requests formal approval of the updated Information Security Program. (ver 2014-03-31).

Background

Based on the 2009 Texas State University System Rules (TSUS) Audit Findings verifying compliance with the TSUS Rules and Regulations and the Texas Administrative Code (TAC 202) Subchapter C, the Information Security Program developed in 2012 (ver 2012-08-30) was updated. The updated document was reviewed and approved by the Information Security Officer and Information Resource Manager and forwarded to the President for approval.

Approval

I approve the Information Security Program (copy attached) which provides a general framework for Information Security and assures our compliance with the Texas State University System Rules and Regulations and TAC 202 Subchapter C.

Signed _____ Date 6/11/14

Dana Gibson, President