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

IT Risk Assessment Policy: IT-17

PURPOSE:

IT risk assessments are designed to assess the security posture of a system or application with the purpose of management's awareness of the major security risks in the Sam Houston State University (SHSU) infrastructure and recommend mitigation plans of these risks.

The principal goal of our risk management process is to protect the University and its ability to perform its mission. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the University.

Risk assessments will be conducted annually and/or on an ad-hoc basis in response to specific events such as when major modifications are made to the system's environment or in response to a security incident or audit.

SCOPE:

The IT Risk Assessment Policy applies to all stakeholders involved in preserving the confidentiality, integrity, and availability of information resources. Stakeholders include, but are not limited to, information system owners, custodians, data owners, users, and information security personnel.

POLICY STATEMENT:

1. Appropriate security levels and data control requirements must be determined by information system owners for all information resources based on SHSU confidentiality, integrity, and availability requirements for the information, as well as its impact to SHSU's mission and legal requirements.

2. Information system owners and custodians are required to gather a broad range of data on information resources and potential threats. The data collection phases of the risk management process include an information technology asset inventory consisting of interconnected components, installation documentation, configuration baselines, network penetration tests, logs, patch histories and other vulnerability assessment data.

3. The Information Security Officer shall biennially commission risk assessments of the information resources that transmit, process, or store confidential SHSU information, and periodically for all other information systems. These risk assessments are to be completed by the information system owner and custodian.

4. The Information Security Officer shall review the results of the risk assessments and risk mitigations measures, technical controls, and procedural safeguards. The assessment may incorporate self-assessment questionnaires, vulnerability scans, scans for confidential information, and penetration testing. Findings and recommendations shall be provided to the information system owners and custodians of the information resources and shall also be presented to the President as appropriate. [TAC 202.73(a)(2)]

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, May, 2023
Next Review:	May, 2024