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

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 SHSU infrastructure and recommend mitigation plans of these risks.

The principal goal of a 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 SHSU Risk Assessment Policy applies to all stakeholders involved in preserving the confidentiality, integrity and availability of information technology resources. Stakeholders include, but are not limited to, SHSU administration, application administrators, system administrators, data owners, users, and information security personnel.

POLICY STATEMENT:

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

Information technology risk analysis and management processes require gathering a broad range of data on information technology assets and potential threats. The data collection phases of the risk management process include an information technology asset inventory consisting of server build documentation, network penetration tests, logs, patch histories and other vulnerability assessment tools for essential assets.

The ISO shall periodically (at least annually) complete or commission a risk assessment of the information resources considered essential to the university's critical mission and functions, and shall recommend, to the owners and custodians of these resources, appropriate risk mitigation 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 owners and custodians of the information assets and shall also be presented to the VPIT for sharing with the president as appropriate. [TAC 202.72(c)]

The key roles of personnel who are responsible for the protection of SHSU information technology resources and participate in the risk management/assessment process can be found in the SHSU Information Security Program at http://www.shsu.edu/~ucs_www/documents/Info_Sec_Program.pdf. Roles include Data Owner or designated representative(s), Data Custodian(s), Users, Information Security Officer (ISO), and Information Resources Manager.

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 19, 2012
Approved by: President's Cabinet, February 6, 2012
Next Review: November 1, 2015