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

System Development & Acquisition Policy: IT-08

PURPOSE:

The purpose of the System Development & Acquisition Policy is to ensure that security is an integral part of Sam Houston State University (SHSU and/or University) system planning and management, and the business processes associated with those systems.

It is important that the procedures for new and changed systems integrate information security requirements into the software life cycle of information systems. The security requirements must identify controls that are needed to ensure confidentiality, integrity, and availability. These controls must be appropriate, cost-effective, and mitigate risks that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of the data. This is true regardless of whether the systems are purchased, used from community or open-source collaborations, or developed by SHSU.

SCOPE:

The System Development & Acquisition Policy applies to all information resources acquired or developed by SHSU.

POLICY STATEMENT:

1. All software developed in-house that runs in a production environment shall be developed according to the Information Technology Project Lifecycle and must adhere to the SHSU Application Security Policy (IT-29). At a minimum, the Project Lifecycle Plan shall address the areas of stakeholder identification and involvement; preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. The requirement for such methodology ensures the software will be adequately documented and tested before it is used. Additionally, this methodology ensures that projects match the strategic direction of the University and are in compliance with guidelines.

2. Where resources permit, there shall be a separation between the production, User Acceptance Testing (UAT) development, and development environments. This ensures that security is rigorously maintained for the production system, while the UAT development and test environments can maximize productivity with fewer security restrictions. Testing should not be performed using production systems due to the threat to its confidentiality and/or integrity.

3. All applicable systems shall have designated owners and custodians. Information Technology shall perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

4. When an information system or component of that system that processes confidential information is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of the University and any special security requirements of the system. Information system custodians must deliver this documentation to the Information Security and Compliance Office for review. The vendor must allow testing of the system's security controls by SHSU, if needed. All acquired software that runs on production systems shall be subject to the Information Technology Project Lifecycle and must adhere to the SHSU Application Security Policy (IT-29).

5. An assessment of the system's security controls and a vulnerability assessment must be performed on all new information systems or systems undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed by vendors for third-party information systems and by Information Security and Compliance Office for locally managed information systems. Information system custodians must take appropriate measures to address the risks associated with identified vulnerabilities.

6. Information Technology Change Management procedures (IT-09) must be followed to review and approve a change before it is moved into production.

7. Opportunities for misuse of information must be appropriately minimized or prevented with risk assessments, monitoring and logs, and end-user awareness and training on preventive strategies.

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, April 17, 2023
Reviewed by: Heather Thielemann, Information Resources Manager, April, 2023
Next Review: April, 2024