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

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 SHSU 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 that contain protected data. 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 protected 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 software/systems installed and utilized on SHSU information technology resources that contain confidential and/or protected data.

This policy does not apply to faculty or students developing and experimenting with software programs as part of an approved curriculum.

POLICY STATEMENT:

All software developed in-house that runs in a production environment shall be developed according to the IT@Sam Project Lifecycle and must adhere to the SHSU Application Security Policy (IT-29). At a minimum, this 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 for critical information. Additionally, this methodology ensures that projects match the strategic direction of the university and compliance with guidelines.

Where resources permit, there shall be a separation between the production, development, and test environments. This ensures that security is rigorously maintained for the production system, while the 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.

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

If an enterprise information system or component of that system is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of this policy and any special security requirements of the system. 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 IT@Sam Project Lifecycle and must adhere to the SHSU Application Security Policy (IT-29).

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 on production information systems and appropriate measures taken to address the risk associated with identified vulnerabilities.

IT@Sam Change Management procedures (IT-09) will be followed to review and approve a change before it is moved into production.

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

DEFINITIONS:

Change Management: The controlled identification and implementation of required changes within a business's information technology systems.

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.

Project Lifecycle: A series of activities which are necessary to fulfill project goals or objectives.

Risk Assessment: A systematic process of identifying, evaluating, and estimating the levels of risks involved in a process or system, their comparison against benchmarks or standards, determining appropriate ways to eliminate or control the hazard, and determining an acceptable level of risk.

System Development & Acquisition: An organization's ability to identify, acquire, install and maintain appropriate information technology systems. This includes the internal development of software applications or systems and the purchase of hardware, software or services from third parties.

Stakeholder: A person or group who has an interest in something and who is impacted by and cares about how it turns out.

Vulnerability Assessment: The process of identifying, quantifying, and prioritizing the vulnerabilities (weaknesses) in a system.

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 30 2015
Approved by: President's Cabinet, February 6, 2012
Next Review: November 1, 2016