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

Application Security Policy: IT-29

PURPOSE:

The purpose of the Application Security Policy is to avoid inadvertent release of confidential or sensitive information, minimize risks to users and the University, and ensure the availability of critical applications.

SHSU focuses its efforts on security applications that hold or utilize data sets containing student information/records, personally identifiable information such as social security numbers or credit card numbers, and other categories of data that are protected by federal or state laws or regulations. Ultimately, to ensure application availability and reliability, all applications must be secured regardless of the type of information they utilize.

SCOPE:

The Application Security Policy applies to applications developed by university staff as well as to those acquired from outside providers. All applications are subject to this policy regardless of whether the application is hosted on university equipment or elsewhere.

POLICY STATEMENT:

To keep risk to an acceptable level, SHSU shall ensure that the proper security controls will be implemented for each application. Data owners, custodians, system administrators, and application developers are expected to use their professional judgment in managing risks to the information, systems and applications they use and support. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the data processed by the system.

1. IT@Sam, individual departments, and contractors shall implement application security standards to have effective controls over systems they directly manage.

    a. If IT@Sam manages an environment or application, IT@Sam shall be responsible for implementing the application security controls.
    b. If a department manages an environment or application, that department shall be responsible for implementing the application security controls.
    c. If an outsourced contractor manages an SHSU environment or application for an individual department, the department must ensure that the contractor implements the application security controls.

d. University faculty and staff who engage any third-party hosting services (such as cloud services, SaaS, or managed hosting) for educational, research or approved purpose must:
    i. obtain prior approval from the Information Resources Manager or designee.
    ii. not entrust that provider with sensitive or confidential business data as defined in IT-06 Data Classification Policy.
    iii. Availability and support agreements (eg, 24X7, 8-5, Weekdays only) must be at a level commensurate with the applications expected availability and must be communicated to IT@Sam.

2. Applications installed or being changed should follow the standardized application lifecycle established by the IT@Sam Project Lifecycle.

3. Each individual user (whether a developer, administrator, or user) should have a unique set of credentials for accessing a computer application.

4. Authenticated users should have access to a computer application and should only be allowed to access the information they require (principle of least privilege).

5. Establishing and changing access for a user or group should be approved by the application's data owner.

6. Developers should follow best practices for creating secure applications with the intention being to minimize the impact of attacks.

7. Developers should not develop or test an application against production data sources.

8. Logs for the server, application and web services should be collected and maintained in a viewable format for a period of time specified by applicable state regulations.

9. Maintain a full inventory of all applications, to include authentication and authorization systems, the data classification and level of criticality for each application.

10. Document clear rules and processes for reviewing, removing, and granting authorizations.

11. Remove critical authorizations for access to applications for individuals who have left the university, transferred to another department, or assumed new job duties.

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