Procedure Statement

Application development security measures must be taken throughout an application’s life cycle in order to build more secure and robust applications. When a web application’s design begins, it is essential to apply threat risk modeling; otherwise, resources, time and money will be consumed on useless controls that fail to focus on the real risks.

Reason for Procedure

This Procedure applies to all users of Texas A&M University-San Antonio (A&M-San Antonio) information resources.

The purpose of the implementation of this Procedure is to serve as a framework for developing, deploying and maintaining secure applications.

This Procedure is intended for all developers, security testers and system architects developing and/or administering applications to process A&M-San Antonio data.

Official Responsibilities and Procedure

1. Information Technology Services (ITS) should be notified or involved in any work related to the development or deployment of applications at A&M-San Antonio.

2. The ISO must always have a full inventory of all web applications.

3. ITS must ensure that a security risk assessment of the system is performed prior to moving the application to production. The application owner is responsible for resolving all security related risks and vulnerabilities prior to ITS certifying the application as ready for production.

4. Security scans must be performed at least annually after deployment in order to identify vulnerabilities.
Non-Compliance

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to A&M-San Antonio information resources, civil, and/or criminal prosecution.

Related Rules

DIR Practices for Protecting Information Resources Assets

Family Educational Rights and Privacy Act (FERPA)

Gramm Leach Bliley Act (GLB Act)

Health Insurance Portability and Accountability Act (HIPAA)

TAMU System Policy 29.01 Information Resources

Texas Administrative Code (TAC) 202 as amended or supplemented

Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education

Definitions

Accounts - Information Resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

Application Custodian – The guardian or caretaker of the application; the person(s) charged with implementing the controls specified by the owner of the application. This custodian is responsible for any errors or application updates. Application custodians are responsible for testing the functionality of the application after any major change performed by either the application custodian or system custodian.

Change – Any implementation of new functionality, any interruption of service, any repair of existing functionality, and/or any removal of existing functionality.
Change Management – The process of controlling modifications to hardware, software, firmware, and documentation to ensure that information resources are protected against improper modification before, during and after system implementation.

Confidential Information - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

Custodian - Guardian or caretaker (the holder of data). The agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

Incident Report – A formal reporting of a known information technology related incident. This is performed by completing the associated ITS form.

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resources Manager (IRM) - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.

Information Security Officer (ISO) - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

Information Technology Services (ITS) – The designated name for the central information technology department for the university.

ISAAC (Information Security Awareness Assessment and Compliance) - A web-based system used to assess the security posture of information systems and measure compliance with the Information Security Standards.

Logon ID - A unique account name that is required as the first step in logging into a secure information resource. A logon ID typically must be associated with a user password to obtain access to the information resource.

Mission Critical Information - Information that is defined by A&M-San Antonio or information resource owner to be essential to the continued performance of the mission of A&M-San Antonio or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of A&M-San Antonio or department.
**Owner** - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

**Production System** - The hardware, software, physical, procedural and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

**System Custodian** – Guardian or caretaker of the operating system and physical hardware; the person(s) charged with implementing the controls specified by the owner of the system. This custodian is responsible for operating system updates and assisting the Application Custodian with any testing or major changes to the system.

**User** - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner’s procedures and rules.

---

**Contact Office**

Finance and Administration, Information Technology Services (210) 784-4357 (HELP)