Procedure Statement

The purpose of this Procedure is to describe the requirements for developing and implementing new application software in the University.

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 provide a set of measures that will mitigate information security risks associated with system development and implementation of new application software. It applies to all individuals who use information resources.

Official Responsibilities and Procedure

1. For any new software application development requests or changes to existing internal applications, requests must be submitted through Information Technology Advisory Council (ITAC) and the CIO for review and approval. Systems or software that impact two or more department or qualifies for universal adoption require an ITAC recommendation.

2. Upon approval, Information Technology Services (ITS) is responsible for participating in system development projects. All projects should include a plan to address any applicable areas listed: 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. This methodology ensures that the software will be adequately documented and tested before it is deployed into an A&M-San Antonio production environment.

3. All production systems must have designated owners and custodians for the critical information they process. ITS must perform assessments of production systems to determine whether the controls employed are adequate.
4. All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. A designated access control administrator must be assigned for all production systems.

5. Where resources permit, there should be a separation between the production and test environments, if applicable.

---

**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)](#)
- [Texas Administrative Code (TAC) 202 as amended or supplemented](#)
- [Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education](#)
- TAMU System Policy [29.01 Information Resources](#)

---

**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.

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.

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.

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.

Test Environment – A testing environment is a setup of software and hardware on which testing is performed to verify functionality of newly built systems or software.

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

Vulnerability - A weakness or flaw in system security design, implementation, procedures or controls that can cause a violation of the system’s security policy or a security breach if exploited by an attacker.

Contact Office

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