Procedure Statement

As Information Resources at Texas A&M University-San Antonio (A&M-San Antonio) expands and continuously become more complex it is important for a strong change management process to be in place.

Information resources may require planned upgrades or maintenance that call for system downtime or outages. Additionally, unplanned outage(s) may occur which result in upgrades or maintenance to information resources. Changes as a result of planned or unplanned maintenance are a critical part of providing technology support services for the University.

Reason for Procedure

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

The purpose of the implementation of this Procedure is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community.

This Procedure applies to all individuals who install, operate or maintain A&M-San Antonio information resources.

Official Responsibilities and Procedure

1. CHANGE MANAGEMENT PROTOCOLS:

   1.1 The following change management protocols apply to the department of ITS, as well as all campus departments. A change has a possibility of impacting normal operations on information resources. Items that are considered changes include, but are not limited to:
1.1.1 Installation or upgrades of server, networking, or security hardware or software, including patches and updates for the applications.

1.1.2 Modification of hardware or software that affects the operation of desktop computers connected to A&M-San Antonio’s network.

1.1.3 Modification of server, network, or security settings that affect access to ITS IR.

1.1.4 Modification or enhancements to the physical environment that supports ITS IR.

1.2 Specific tasks that should not be considered changes include:

1.2.1 Updates to operating systems,

1.2.2 Creation of new file shares or modification to permissions of existing shares,

1.2.3 Installation, activation, or removal of network cable drops, or

1.2.4 Creation, modification, or deletion of accounts and mailboxes.

2. CHANGE MANAGEMENT PROCEDURES:

2.1. All changes must be documented and submitted for approval prior to implementation. The following defines the procedure for documentation and approval:

2.1.1 The custodian requesting the change must fill out a Change Management Request email to obtain approvals.

2.1.2 Requestor will submit the email to the CIO and Directors for review. The CIO and Directors will work with necessary stakeholders ensure accuracy, completeness, and identify potential impacts. Change forms must be submitted a minimum of one full business day prior to the review date.

2.1.3 If appropriate, announcement messages should be distributed to users prior to the changes.

2.1.4 Changes to critical systems must be done in a test environment first, if available.

2.1.5 Once a change has been done, the Application Custodian needs to test the system in order to ensure the integrity of the system.

2.1.6 Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability that requires immediate attention.
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 the University 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.

Emergency Change – When an immediate response to imminent critical system failure is needed to prevent widespread service disruption.

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.

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.

**Scheduled Change** – A system modification accompanied by a formal notification received, reviewed, and approved by the review process in advance of the change being made.

**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.

**Unscheduled Change** – A system modification that fails to present notification to the formal process in advance of the change being made.

**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)