West Texas A&M UNIVERSITY™

The Division of Information Technology
University Information Security Standards

Information Security Standard – Change Management (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

The information resources infrastructure at West Texas A&M University is expanding and continuously becoming more complex. There are more people dependent on information resources being interconnected, upgraded and expanded (e.g., administrative systems and application programs). As the interdependency among information resources grows, the need for an effective change management process is essential.

From time to time, information resources require a service disruption for planned upgrades, maintenance or fine-tuning. Additionally, such activities may result in unplanned service disruptions. Managing these changes is a critical part of providing a robust and valuable information resource infrastructure.

The goal of change management is to ensure that the intended purpose of the change is successfully accomplished, while eliminating or minimizing any negative impact to the users of the resources as a result of the change. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact to the user community.

The West Texas A&M University Change Management Policy applies to all individuals that install, operate or maintain Information Resources.

2. Applicability

This information security standard applies to University systems storing or processing mission critical and/or confidential information.

The purpose of this information security standard is to provide a set of measures that will mitigate information security risks associated with Change Management. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202

- Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

3. Definitions

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

3.2 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.3 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.4 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

3.5 Custodian: The person (Information Security Administrators) responsible for implementing owner-defined controls and access to an information resource.

3.5 Change:

a. Any implementation of new functionality;
b. Any interruption of service;
c. Any repair of existing functionality; and,
d. Any removal of existing functionality.

3.6 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University 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 the University or department.

3.7 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

4. Procedures

A consistent process is to be used for the implementation of information resource changes. The degree to which change management activities and processes are employed is dependant on the projected inherent risk of the change (i.e., potential for unplanned disruption of service, corruption/loss of data, or disclosure of confidential information resulting from the change implementation). Where appropriate, the process should include: preparation, notification/awareness using the ALL email list, approval and documentation.

4.1 Every change to a West Texas A&M University information resource such as: operating systems, computing hardware, networks, and applications is subject to the change management policy and should follow the change management procedures, unless special circumstances exist.

4.2 All changes affecting computing environmental facilities (e.g. air conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the corresponding information technology department or the information resources manager (IRM).

4.3 A formal change request should be submitted for changes prior to changes being made. Change requests are to be submitted by using the information technology work order management system and must be approved, minimally, by information technology department manager. Additional approvals can be made by the information resources manager (IRM). Changes must be sufficiently prepared for to minimize outages.

4.4 Preparation includes:

(1) Review of previous similar changes and results in attempting to avoid any repetition of mistakes or negative impact

(2) The determination of the following:

(a) The best time/date for implementation (to minimize the impact to users);

(b) The net impact to other systems or impact to normal operation during and following the change implementation (inherent risk);

(c) The risk associated with the change implementation (to minimize the risk of disruption of service caused by the change); and,

(3) Ensuring that the changes do not negatively impact the overall system security

4.2 Notification/awareness includes a forum or notification process that informs users of changes planned for implementation. Typically, user notification may include e-mail in addition to an announcement posted on the web.

4.3 Approval and audit of application/software changes includes:

(1) Review of the code revision to be implemented, which shall be performed by someone other than the developer;

(2) Approval of the implementation of code revision performed by someone other than the developer; and,

(3) Review of logs for previous change implementations.

4.4 Documentation includes:

(1) Any issues identified during the preparation phase that

require special considerations or a revision to the implementation plan.

4.5 Change details for documentation include:

(1) Date/time of change;

(2) Expected duration or length of time required to implement the change;

(3) Nature of the change (a brief description of the net effect);

(4) Developer's name (when applicable) for the modification if newly developed or modified code is involved;

(5) Implementer's name of the modification;

(6) An indication of successful or unsuccessful completion of the change; and,

(7) An analysis and "lessons learned" (corrective/preventative actions) for changes that deviated unexpectedly from the plan, resulted in an unplanned disruption of service, corruption of data, or disclosure of confidential information

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer