29.01.03.H0.05 Change Management

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

The Information Resources infrastructure at Texas A&M University-Texarkana (TAMUT) is expanding and continuously becoming more complex. There are more people dependent on the network, computers, and application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential. From time to time, each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur which may result in upgrades, maintenance or fine-tuning. Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

Reason for Procedure

The purpose 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 and to increase the value of Information Resources. This procedure applies to all individuals who install, operate or maintain TAMUT Information Resources.

Definitions

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.

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

Incident Report: Form that must be completed when an emergency change occurs.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, 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, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes 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.

Information Technology: The name of the TAMUT department responsible for computers, networking and data management.

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 program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Scheduled Change: 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: Failure to present notification to the formal process in advance of the change being made.

Procedures and Responsibilities

1. THE FOLLOWING CHANGE MANAGEMENT PROTOCOLS APPLY TO THE DEPARTMENT OF INFORMATION TECHNOLOGY, AS WELL AS ALL CAMPUS DEPARTMENTS. INFORMATION TECHNOLOGY HIGHLY RECOMMENDS THAT ALL DEPARTMENTS ADOPT THESE INDUSTRY BEST PRACTICES RELATED TO IT CHANGE MANAGEMENT IN THEIR RESPECTIVE AREAS. A CHANGE IS DEFINED AS A MODIFICATION TO THE HARDWARE, SOFTWARE, AND DOCUMENTATION MANAGED BY

INFORMATION TECHNOLOGY THAT HAS A REASONABLE POSSIBILITY OF IMPACTING NORMAL OPERATIONS ON THOSE RESOURCES. ITEMS THAT ARE CONSIDERED CHANGES INCLUDE, BUT ARE NOT LIMITED TO:

1.1 Installation or upgrades of server, networking, or security hardware or software, including patches and interim fixes for the applications.

1.2 Modification of hardware or software that affects the operation of desktop computers connected to the TAMUT network.

1.3 Modification of server, network, or security settings that affect access to IT IR.

1.4 Modification or enhancements to the physical environment that supports IT IR.

1.5 Specific tasks that should not be considered changes include:

1.5.1 updates to Operating Systems,

1.5.2 creation of new file shares or modification to permissions of existing shares,

1.5.3 installation, activation, or removal of network cable drops, or

1.5.4 creation, modification, or deletion of accounts and mailboxes.

2. CHANGE MANAGEMENT PROCEDURES

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

2.1 The custodian requesting the change must fill out the Change Management Request form to obtain approval.

2.2 He/she will submit the form to his/her supervisor or manager for review. The manager will ensure accuracy and completeness. Change forms must be submitted to the supervisor or manager a minimum of one full business day prior to the review date.

2.3 All changes must be forwarded to the Associate Vice President for Information Technology/CIO and Information Security Officer at itsecurity@TAMUT.edu.

2.4 Changes to critical systems must be done in a test environment first.

2.5 Once a major change has been done, the Application Custodian needs to do a formal testing procedure to the system in order to ensure the integrity of the system.

2.6 Announcement messages must be distributed to users prior to the change. The supervisor or manager should prepare this announcement, and the director/supervisor for that area will be responsible for posting the announcement. Typically, user notification may include an email or a posted message on the university website.

2.7 It may occasionally be necessary to implement emergency changes which will be documented. Any changes that are planned within a period of 12 hours or less will be documented as emergency changes. An Incident Report must be completed for these changes.

2.8 A Systems' Incident Report form must be filled out for any unplanned incident on the systems (i.e. power outages).

2.9 All changes affecting computing environmental facilities (i.e. air-conditioning, water, heat, plumbing, electricity and alarms) need to be planned with the CIO or ISO.

2.10 A formal written change request must be submitted for all changes.

2.11 Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability.

2.12 All TAMUT information systems must comply with an Information Resources change management process that meets the standards outlined above.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Information Security Officer, 903-886-5425