Section	**IS Security Policies**	05/01/05 -Effective 12/10/11 -Revised
Policy 2.00	**Change Management**	Information Services -Author

Introduction

The Information Resources infrastructure at the TSSWCB is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more 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 that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure

Purpose

The purpose of the Change Management Policy 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.

Audience

The TSSWCB Change Management Policy applies to all individuals that install, operate or maintain Information Resources.

Definitions

Information Resources (IR): 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.

Definitions, continued

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.

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. For mainframe applications Information Services is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

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.

Change:

- any implementation of new functionality
- any interruption of service
- any repair of existing functionality
- any removal of existing functionality

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability.

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

Change Management Policy

- Every change to a TSSWCB Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.
- 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 leader of the change management process.
- A Change Management Committee, appointed by IS Leadership, will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.
- A formal written change request must be submitted for all changes, both scheduled and unscheduled.
- All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change.
- The appointed leader of the Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backout plans, the timing of the change will negatively impact a key business process such as year end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
  - ❖ Date of submission and date of change
  - ❖ Owner and custodian contact information
  - ❖ Nature of the change
  - ❖ Indication of success or failure
- All TSSWCB information systems must comply with an Information Resources change management process that meets the standards outlined above.

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TSSWCB Information Resources access privileges, civil, and criminal prosecution.

Supporting Information

This Security Policy is supported by the following Security Policy Standards.

Reference # **Policy Standard detail**

12 The IR network is owned and controlled by IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.

14 The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

15 All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

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