Section	**IS Security Policies**	05/01/2005	-Effective
		12/10/2011	-Revised
Policy 2.00	**Network Configuration Security**	Information Services	-Author

Introduction

The TSSWCB network infrastructure is provided as a central utility for all users of TSSWCB Information Resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the TSSWCB Network Configuration Security Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of TSSWCB information.

Audience

The TSSWCB Network Configuration Security Policy applies equally to all individuals with access to any TSSWCB Information Resource.

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 assistants (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.

Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency's information resources. The designation of an agency 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.

Definitions, continued

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

Information Services (IS): The name of the agency department responsible for computers, networking and data management.

Network Configuration Security Practice Standards

- TSSWCB Information Services owns and is responsible for the TSSWCB network infrastructure and will continue to manage further developments and enhancements to this infrastructure
- To provide a consistent TSSWCB network infrastructure capable of exploiting new networking developments, all cabling must be installed by TSSWCB IS or an approved contractor.
- All network connected equipment must be configured to a specification approved by TSSWCB IS.
- All hardware connected to the TSSWCB network is subject to TSSWCB IS management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of TSSWCB IS.
- The TSSWCB network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by TSSWCB IS.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by TSSWCB IS.
- All connections of the network infrastructure to external third party networks is the responsibility of TSSWCB IS. This includes connections to external telephone networks.
- TSSWCB IS Firewalls must be installed and configured following the TSSWCB Firewall Implementation Standard documentation.
- The use of departmental firewalls is not permitted without the written authorization from TSSWCB IS.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the TSSWCB network without TSSWCB IS approval.
- Users must not install network hardware or software that provides network services without TSSWCB IS approval.
- Users are not permitted to alter network hardware in any way.

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.
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.
19	IR computer systems and/or associated equipment used for agency business that is conducted and managed outside of agency control must meet contractual requirements and be subject to monitoring.
20	External access to and from IR must meet appropriate published agency security guidelines.

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