| | | | |
|---|---|---|---|
| Section | **IS Security Policies** | 05/01/2005 | -Effective |
| | | 12/10/2011 | -Revised |
| Policy 2.00 | **Network Access 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 ‘active equipment’, continues to develop with sufficient flexibility to meet TSSWCB 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 Access Security Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of TSSWCB information.

## Audience

The TSSWCB Network Access Security Policy apply 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 Access Policy

- Users are permitted to use only those network addresses issued to them by TSSWCB IS.
- Remote users may connect to TSSWCB Information Resources only through an ISP and using protocols approved by the TSSWCB.
- Users inside the TSSWCB firewall may not be connected to the TSSWCB network at the same time a modem is being used to connect to an external network.
- 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.
- Non TSSWCB computer systems that require network connectivity must conform to TSSWCB IS Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, TSSWCB users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the TSSWCB network infrastructure.
- 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 |
|---|---|
| 1 | IR Security controls must not be bypassed or disabled. |
| 3 | All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management. |
| 5 | Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service. |
| 6 | The use of IR must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management. |
| 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