Section	**IS Security Policies**	05/01/05	-Effective
		04/28/12	-Revised
Policy 2.00	Security Training	Information Services	-Author

Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific, training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

Purpose

The purpose of the Security Training Policy is to describe the requirements for ensure each user of TSSWCB Information Resources is receives adequate training on computer security issues.

Audience

The TSSWCB Security Training Policy applies equally to all individuals that use any TSSWCB 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 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 Services (IS): The name of the agency department responsible for computers, networking and data management.

Security Training Policy

- All users must sign an acknowledgement stating they have read and understand TSSWCB requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect TSSWCB information resources.
- IS must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

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**
2	Security awareness of personnel must be continually emphasized, reinforced, updated and validated
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.

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