Section	**IS Security Policies**	05/01/2005	-Effective
		04/28/2012	-Revised
Policy 2.00	**Physical Access**	Information Services	-Author

Introduction

Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Resources facilities is extremely important to an overall security program.

Purpose

The purpose of the TSSWCB Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

Audience

The TSSWCB Physical Access Policy applies to all individuals within the TSSWCB's enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources Security, and data owners.

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.

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

Physical Access Policy

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Resources restricted facilities must be managed.
- All IR facilities must be physically protected in proportion to the criticality or importance of their function at the TSSWCB.
- Access to Information Resources facilities must be granted only to TSSWCB support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting access to Information Resources facilities must include the approval of the person responsible for the facility.
- Requests for access must come from the applicable TSSWCB data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.
- Cards and/or keys must not have identifying information other than a return mail address.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within the TSSWCB or are separated from their relationship with the TSSWCB
- Visitors must be escorted in card/key access controlled areas of Information Resources facilities.
- The person responsible for the Information Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

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.
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.
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management.

Supporting Information, continued

This Security Policy is supported by the following Security Policy Standards

Reference #	Policy Standard detail
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.
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.
9	On termination of the relationship with the agency users must surrender all property and IR managed by the agency. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.
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.

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