Introduction

Under the provisions of the Information Resources Management Act, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Audience

The TSSWCB Acceptable Use policy applies equally to all individuals granted access privileges to any TSSWCB Information Resources.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased administered, or otherwise under the custody and control of the TSSWCB are the property of the TSSWCB.

Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of the TSSWCB are not private and may be accessed by TSSWCB IS employees at any time without knowledge of the Information Resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

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 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.

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

User: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

Information Resources Acceptable Use Policy

- Users must report any weaknesses in TSSWCB computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on TSSWCB systems for which they do not have authorization or explicit consent.
- Users must not divulge Dialup or Dialback modem phone numbers to anyone.
- Users must not share their TSSWCB account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
- Users must not make unauthorized copies of copyrighted software.
- Users must not use non-standard shareware or freeware software without TSSWCB Information Resources management approval unless it is on the TSSWCB standard software list.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized TSSWCB user access to a TSSWCB resource; obtain extra resources beyond those allocated; circumvent TSSWCB computer security measures.
- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, TSSWCB users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on TSSWCB Information Resources.
- TSSWCB Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material which TSSWCB may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the TSSWCB official processes for dealing with academic ethical issues).
- Access to the Internet from a TSSWCB owned, home based, computer must adhere to all the same policies that apply to use from within TSSWCB facilities. Employees must not allow family members or other non-employees to access TSSWCB computer systems.
- Users must not otherwise engage in acts against the aims and purposes of the TSSWCB as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

Incidental Use

As a convenience to the TSSWCB user community, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to TSSWCB approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to the TSSWCB.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to the TSSWCB.
- Storage of personal email messages, voice messages, files and documents within the TSSWCB's Information Resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on TSSWCB Information Resources are owned by the TSSWCB, may be subject to open records requests, and may be accessed in accordance with this policy.

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**
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.
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.
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.
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.
21	All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IRM through IS reserves the right to remove any unlicensed software from any computer system.

Supporting Information, continued

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

Reference #	**Policy Standard detail**
22	The IRM through IS reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

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