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

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 the internet.
- To educate individuals who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

Audience

The TSSWCB Internet Use Policy applies equally to all individuals granted access to any TSSWCB Information Resource with the capacity to access the internet, the intranet, or both.

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.

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.

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

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present "information super highway."

Intranet: A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contain links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape, Navigator, and Microsoft Internet Explorer.

Vendor: someone who exchanges goods or services for money.

Ownership

Electronic files created, sent, received, or stored on computers 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.

Internet and Intranet Usage Policy

- Software for browsing the Internet is provided to authorized users for business and research use only.
- All software used to access the Internet must be part of the TSSWCB standard software suite or approved by the ISO. This software must incorporate all vendor provided security patches.
- All sites accessed must comply with the TSSWCB Acceptable Use Policies.
- All user activity on TSSWCB Information Resources assets is subject to logging and review.
- Content on all TSSWCB Web sites must comply with the TSSWCB Acceptable Use Policies.
- No offensive or harassing material may be made available via TSSWCB Web sites.
- No personal commercial advertising may be made available via TSSWCB Web sites.
- TSSWCB internet access may not be used for personal gain or non-TSSWCB personal solicitations.
- No TSSWCB data will be made available via TSSWCB Web sites without ensuring that the material is available to only authorized individuals or groups.
- All sensitive TSSWCB material transmitted over external network must be encrypted.
- Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

Incidental Use

- Incidental personal use of Internet access is restricted to TSSWCB approved users.
- 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 liability for, or embarrassment to, the TSSWCB.
- Storage of personal files and documents within the TSSWCB's Information Resources should be nominal, and not be included with files backed up using TSSWCB systems..
- All files and documents – including personal files and documents – 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.
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.

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