

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

Introduction

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

Purpose

The purpose of the Software Licensing Policy is to establish the rules for licensed software use on TSSWCB Information Resources.

Audience

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

Vendor: someone who exchanges goods or services for money.

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

Software Licensing Policy

- The TSSWCB provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
- Third party copyrighted information or software, that the TSSWCB does not have specific approval to store and/or use, must not be stored on TSSWCB systems or networks. Systems administrators will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).
- Third party software in the possession of the TSSWCB must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

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.

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

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.

- 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.

- 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.

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