

Section	IS Security Policies	05/01/05	-Effective
Policy 2.00	Computer Virus Detection	04/28/12	-Revised
		Information Services	-Author

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

The purpose of the Computer Virus Detection Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup.

Audience

The TSSWCB Computer Virus Detection 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.

Section	IS Security Policies	05/01/05	-Effective
Policy 2.00	Computer Virus Detection	04/28/12	-Revised
		Information Services	-Author

**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.

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

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

Trojan Horse: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network, using otherwise-unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is imilar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Server: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Security Incident: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

E-mail: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.

Section	IS Security Policies	05/01/05	-Effective
Policy 2.00	Computer Virus Detection	04/28/12	-Revised
		Information Services	-Author

Virus Detection Policy

- All workstations whether connected to the TSSWCB network, or standalone, must only use a TSSWCB IS approved virus protection software and configuration.
- If present, virus protection software must not be disabled or bypassed.
- If present, the settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- If present, the automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each file server attached to the TSSWCB network must only utilize TSSWCB IS approved virus protection.
- Each E-mail gateway must utilize TSSWCB IS approved e-mail virus protection software.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.

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	Computer Virus Detection	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.

- 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.

Section	IS Security Policies	05/01/05	-Effective
Policy 2.00	Computer Virus Detection	04/28/12	-Revised
		Information Services	-Author

Supporting Information, continued

This Security Policy is supported by the following Security Policy Standards

Reference # Policy Standard detail, continued

- 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.

 - 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