Section	**IS Security Policies**	05/01/05	-Effective
		04/28/12	-Revised
Policy 2.00	**Portable Computing Security**	Information Services	-Author

Introduction

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

Purpose

The purpose of the TSSWCB Portable Computing Security Policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of TSSWCB information.

Audience

The TSSWCB Portable Computing Security Policy apply equally to all individuals that utilize Portable Computing devices and access 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.

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.

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from IR. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell phones.

Portable Computing Policy

- Only TSSWCB-approved portable computing devices may be used to access TSSWCB Information Resources.
- Portable computing devices must be password protected.
- TSSWCB data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive TSSWCB data must be encrypted using approved encryption techniques.
- TSSWCB data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- Non TSSWCB computer systems that require network connectivity must conform to TSSWCB IS Standards and must be approved by the TSSWCB ISO.
- Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

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.
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.
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.
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.
12	The IR network is owned and controlled by IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
20	External access to and from IR must meet appropriate published agency security guidelines

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