

| | | | |
|-------------|-----------------------------|----------------------|------------|
| Section | IS Security Policies | 05/01/05 | -Effective |
| Policy 2.00 | Vendor Access | 04/28/12 | -Revised |
| | | Information Services | -Author |

Introduction

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors, they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to the TSSWCB.

Purpose

The purpose of the TSSWCB Vendor Access Policy is to establish the rules for vendor access to TSSWCB Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of TSSWCB information.

Audience

The TSSWCB Vendor Access Policy applies to all individuals that are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

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.

Vendor: someone who exchanges goods or services for money.

| | | | |
|-------------|-----------------------------|----------------------|------------|
| Section | IS Security Policies | 05/01/05 | -Effective |
| Policy 2.00 | Vendor Access | 04/28/12 | -Revised |
| | | Information Services | -Author |

Vendor Access Policy

- Vendors must comply with all applicable TSSWCB policies, practice standards and agreements, including, but not limited to:
 - ❖ Safety Policies
 - ❖ Privacy Policies
 - ❖ Security Policies
 - ❖ Auditing Policies
 - ❖ Software Licensing Policies
 - ❖ Acceptable Use Policies
- Vendor agreements and contracts must specify:
 - ❖ The TSSWCB information the vendor should have access to
 - ❖ How TSSWCB information is to be protected by the vendor
 - ❖ Acceptable methods for the return, destruction or disposal of TSSWCB information in the vendor's possession at the end of the contract
 - ❖ The Vendor must only use TSSWCB information and Information Resources for the purpose of the business agreement
 - ❖ Any other TSSWCB information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- The TSSWCB will provide an IS point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each vendor must provide the TSSWCB with a list of all employees working on the contract.
- Each vendor employee with access to TSSWCB sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate TSSWCB personnel.
- If vendor management is involved in TSSWCB security incident management the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable TSSWCB change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate TSSWCB management.

| | | | |
|-------------|-----------------------------|----------------------|------------|
| Section | IS Security Policies | 05/01/05 | -Effective |
| Policy 2.00 | Vendor Access | 04/28/12 | -Revised |
| | | Information Services | -Author |

Vendor Access Policy, continued

- All vendor maintenance equipment on the TSSWCB network that connects to the outside world via the network, telephone line, or leased line, and all TSSWCB IR vendor accounts will remain disabled except when in use for authorized maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the TSSWCB Password Practice Standard and Admin/Special Access Practice Standard. Vendor's major work activities must be entered into a log and available to TSSWCB management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to the TSSWCB or destroyed within 24 hours.
- Upon termination of contract or at the request of the TSSWCB, the vendor will return or destroy all TSSWCB information and provide written certification of that return or destruction within 24 hours.
- Upon termination of contract or at the request of the TSSWCB, the vendor must surrender all TSSWCB Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized TSSWCB management.
- Vendors are required to comply with all State and TSSWCB auditing requirements, including the auditing of the vendor's work.

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 | Vendor Access | 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.

- 2** Security awareness of personnel must be continually emphasized, reinforced, updated and validated.

- 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.

- 4** Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department 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.

- 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.

| | | | |
|-------------|-----------------------------|----------------------|------------|
| Section | IS Security Policies | 05/01/05 | -Effective |
| Policy 2.00 | Vendor Access | 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

- 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.
- 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.
- 17** All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the agency is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

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