



WINDHAM SCHOOL  
DISTRICT

**NUMBER:** SD-10.13 (rev. 1)  
**DATE:** March 10, 2011  
**PAGE:** 1 of 7  
**SUPERSEDES:** OP-10.13  
March 24, 2008

# **SUPERINTENDENT DIRECTIVE**

---

**SUBJECT:** INFORMATION RESOURCES SECURITY

**AUTHORITY:** WBP-03.02, “Windham School District Superintendent Responsibilities and Authority”

References: Public Information Act, Chapter 552, Texas Government Code; TDCJ Executive Directive (ED)-15.08, “TDCJ Information Resources Security”

**APPLICABILITY:** Windham School District (WSD)

**POLICY:**

Information resources residing within the WSD are strategic assets belonging to the people of Texas. Measures shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification, or destruction, as well as assure the availability, integrity, utility, authenticity, and confidentiality of information.

**DEFINITIONS:**

“Access” means to interact with or otherwise make use of information resources.

“Confidential Information” is information maintained by WSD that is exempt from disclosure under the provisions of the Texas Public Information Act or other state or federal law.

“Information Resources” are any and all computer printouts, online display devices, magnetic/optical or other 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, thin-client devices, personal digital assistants, pagers, distributed processing systems, network attached and computer controlled equipment, telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, they are 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 Security Officer” (ISO) is the individual responsible for administering the information security functions within the WSD. The ISO is the internal and external point of contact for all information security matters.

“Information Security Program” refers to the element(s), structure, objective(s), and resources that make up the functions required to ensure the security of WSD information resources.

“Internet” is a global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and educational entities.

“Intranet” refers to the internal Texas Department of Criminal Justice (TDCJ) and WSD networks that provide services within the organizations similar to those provided by the Internet outside the organizations.

“Network” refers to all data transport networks used primarily to interconnect computers and networks of computers for the purpose of transporting data, allowing interoperation of computer applications on more than one computer system, and providing access to data.

“Owner” is a person responsible for a business function, for determining program controls, and for determining the need for access for use.

“Restricted Information” is information maintained by WSD that requires special precautions to assure its accuracy and integrity by utilizing error checking, verification procedures, and/or access control to protect it from unauthorized modification or deletion. Restricted information may be either public or confidential and requires a higher than normal assurance of accuracy and completeness.

“Security Incident” is an event which results in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.

“User” is an individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner’s procedures and rules.

## **PROCEDURES:**

### I. General

- A. Information concerning a person, system, or asset of the WSD which is obtained while performing employee duties is to be held in the strictest confidence and may not be disclosed except as required by law or job duties.
- B. Access to the Internet from mobile WSD owned computers shall adhere to all the

same policies that apply to use from within WSD facilities. Employees shall not allow family members or other non-employees to access WSD computer systems.

- C. Personally owned computers shall not be used to access WSD systems without the approval of the director of the Division of Information Technology or designee. Such access shall be granted only if the personally owned computers are equipped with personally owned and up-to-date antivirus and firewall software. WSD data shall not be saved to personal computer devices.
- D. USB connected devices (e.g. flash/thumb drives, portable hard drives, card readers, cameras, WiFi adapters, web cams, and HUBS) shall not be used on, or to access, WSD systems without the approval of the director of the Division of Information Technology or designee. In general, the WSD shall provide these devices with an appropriate business case and funding source.
- E. The integrity of electronic data, which includes its source, its destination, and the processes applied to it, must be assured. Changes to the format and integrity of electronic data shall be made only by the WSD Division of Information Technology (DoIT) and/or the TDCJ Information Technology Division (ITD) staff.
- F. Computer hard drives and portable media (e.g., tapes, USB drives, floppy disks, and CDs) shall be forwarded to the DoIT for destruction when they are no longer needed.
- G. Only DoIT or TDCJ/ITD staff shall monitor or modify equipment, systems, and network traffic.

## II. Protection of Equipment and Materials

WSD information resources are vital assets and must be protected against environmental and business disruptions.

- A. Confidential or restricted information, when handled or processed by terminals, communication switches, network components, tapes, disks, diskettes, and paper outside the central computer room, shall receive the level of protection necessary to ensure its integrity and confidentiality.
- B. Laptops and portable media (e.g., tapes, thumb/flash drives, USB hard drives, floppy disks, and CDs) are highly susceptible to theft and loss. Employees shall use security measures, including physical and data encryption, when sensitive information is present, to ensure that WSD resources are protected.
- C. Servers, thin-client devices, computers, portable media, and other related materials shall be appropriately secured to prevent vandalism, theft, and unauthorized use/operation.

- D. Precautions shall be taken to prevent damage by fire, flood, power surge, or other external sources through utilization of proper safety measures, careful selection/designation of equipment/material locations, and limitation of user/visitor access.
- E. Offenders shall not be permitted access to servers, terminals, or work stations in WSD administrative or unit offices. Offender clerks shall be permitted to work only on stand-alone computers or networked computer terminals that are specifically designated for use by offenders. Electronic and media transfer of data or files between the file server(s) and computers used by offender clerks shall be prohibited unless the transfer is made by, or under the direct supervision of, DoIT staff.
- F. Terminals and workstations shall not be left unattended when employees are signed on to the network.
- G. All equipment that is connected to the WSD Internet/Intranet shall be protected by approved virus-scanning software with a current virus database.

H. Identification/Authentication

Employees shall take all necessary steps to prevent unauthorized access to confidential/restricted information.

1. Information resources shall contain authentication controls that comply with WSD procedures.
2. Information resources which use passwords shall be based on industry best practices, password usage, and documented WSD rules.
3. Each user of information resources shall be assigned a unique identifier/password, except for situations where risk analysis demonstrates no need for individual accountability of users. Requests for exceptions must be approved by the director of the Division of Information Technology or designee.
4. User identification shall be authenticated before the user is granted access.
5. The following policies protect user identification and passwords:
  - a. When a user receives access to information resources, a user identification and a temporary password are assigned in order to sign on for the first time only. The assigned password shall be changed immediately upon login. Passwords must be a minimum of eight characters in length, including one digit.
  - b. Users shall not share their WSD accounts, passwords, personal

identification numbers, identification cards, or similar information or devices used for identification and authorization purposes.

- c. Users may change passwords at any time, but shall do so at least every 30 days. If the user suspects the password has been compromised, the password shall be changed immediately and the DoIT shall be notified.
- d. A user's access shall be appropriately modified or removed when the user's employment or job responsibilities change.
- e. A user's access authorization may be removed if the user is absent from work for more than three consecutive work days for disciplinary reasons or for any reason, as determined by the superintendent.
- f. Contact the DoIT Help Desk at (936) 291-5268 for a temporary password if needed (e.g., forgotten).

### III. Information Security Program

- A. The superintendent shall designate an ISO to administer the WSD Information Security Program. It shall be the duty and responsibility of the ISO to:
  - 1. Develop and implement policies and establish procedures and practices, in cooperation with owners and custodians, necessary to ensure the security of information resource assets against unauthorized or accidental modification, destruction, or disclosure;
  - 2. Monitor the effectiveness of the program;
  - 3. Report security incidents as outlined in section IV of this policy; and
  - 4. Report the status and effectiveness of information resources security controls to the superintendent on an annual basis.
- B. Users shall report any weaknesses in WSD computer security or any incidents of possible misuse to the ISO. Reports shall be made by sending an e-mail to the DoIT Help Desk at [helpdesk@wsdtx.org](mailto:helpdesk@wsdtx.org) or calling (936) 291-5268.

### IV. Security Incidents

- A. Security incidents shall be promptly investigated and documented.
- B. Security incidents shall be reported to the appropriate outside organization (e.g., TDCJ) if there is a substantial likelihood that such incidents may impact the outside organization's information resources and networks or if criminal activity is

suspected. Further, suspected criminal activity not involving outside organizations shall be reported to the TDCJ Office of Inspector General. Reports shall include, but not be limited to:

1. Description of the incident to include:
  - a. Discovery of a virus or intrusion;
  - b. Unwanted disruption or denial of service;
  - c. Unauthorized use of a system for the processing or storage of data; and
  - d. Changes made to system hardware, firmware, data, or software without the consent of the director of the Division of Information Technology or designee;
2. Time elapsed between initial detection of the incident and containment of the security breach or full restoration of adversely affected functions, whichever is later;
3. Description of the WSD response to the incident; and
4. Estimated total cost incurred by the WSD in containing the security incident or restoring adversely affected functions.

V. Emergency Actions/Business Continuity

- A. Information systems data shall be backed up daily and stored off site in a secure, environmentally safe, locked facility accessible only to authorized representatives. Off-site storage shall be on WSD/TDCJ controlled property, or other such property and/or service specifically designed to accept and store data.
- B. Information resources shall be protected from environmental and other hazards. Employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.
- C. The DoIT shall develop business continuity and disaster recovery plans in support of WSD plans. The plans shall:
  1. Ensure that critical WSD functions are restored as quickly as possible;
  2. Ensure that alternate facility, staff, and other resource needs are identified and available when needed;
  3. Contain instructions for plan implementation;

4. Ensure that appropriate checklists are developed to handle various possible contingencies; and
5. Ensure that annual tests are conducted.

\* Signature on file

Debbie Roberts, Superintendent  
Windham School District