



***HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.
POLICY***

ID NO.:	HWD 013-10 HWD 013-10-01 HWD 013-10-02	DATE ISSUED:	August 19, 2010 May 19, 2011 October 11, 2012
PROGRAM:	All	KEYWORD:	IT Security/Automation

Subject: Definition, acceptable use and limits on computer data, communications devices, hardware, and software.

Purpose: Workforce Solutions Heart of Texas Workforce information resources are assets that must be protected from unauthorized disclosure, modification, use, or destruction. Appropriate steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised.

References: Texas Workforce Commission Enterprise Information Security Standards and Guidelines and Texas Workforce Commission Information Technology User Reference guide, Texas Workforce Commission Workforce Development Letter (WD) 13-08

Discussion: Workforce Solutions Heart of Texas Workforce follows guidance prescribed by the Texas Workforce Commission for information technology and security.

This policy is crafted to not only provide general and specific guidelines but to increase the awareness of users to the potential risks associated with information technology.

Policy:

All users shall comply with the policies, standards, guidelines, and procedures as set forth in this policy.

1. The basis for this policy is the TWC Enterprise Security Policy. A copy has been attached to this policy.
2. Use of the TWC Information Technology User Reference guide where applies to local Boards
3. In addition to the standards and guidelines outlines in the TWC Enterprise Security Policy the Board has implemented the following in accordance with WD 13-08
 - Password Requirements

- User passwords must be at least 8 letters and numbers
 - Requirement of changing passwords every 60 days (with a 14 day notification) for WIT and individual workstation desktops
 - After three (3) failed attempts the user will be lockout and must notify IT staff for a reset
 - Do not share passwords, personal identification numbers, or any data or equipment used for authentication and identification purposes.
- **Physical and Electronic Security Controls**
 - Management may request staff access to TWIST, e-mail and/or other Workforce systems will be temporary discontinued when staff are out for an extended period of time, i.e. FMLA or other extended leave, leave of absence
 - Terminated staff accounts will be removed from the server after 60 days without a written request from upper management.
 - A written request, to include reason for access, from upper management must be submitted to IT staff for a supervisor to gain temporary access to another's staff member's account.
 - Customer information such as names and social security numbers will not be transmitted via instant messaging
 - Customer information containing social security numbers must not be transmitted via e-mail unless the information is password protected.
 - Client information on copiers or printers in unsecure areas must be retrieved immediately.
 - Documents that include personal identity data will be shredded.
 - Only authorized **staff** has access to customer files, Smart files, TWIST or other sensitive information. Temporary workers must be supervised at all times when working with customer information
 - Breaches in information security must be reported to upper management and the Board immediately
 - Client Information placed on disks, drives, etc must be password protected and kept secure at all times
 - Laptops and desktops must be secure at all times, password protected, and set to time out and lock at a prescribed time if not in use. Fifteen (15) minutes is the maximum time.
 - All computers will be powered down and turned off at the end of the workday, during lunch hours or when away from the desk for any extended period of time.

- o Confidential personal identity data will not be given out by telephone.

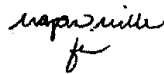
Aquanetta Brobston at 801 Washington Ave, Suite 700, Waco, TX 76701 or aquanetta.brobston@hotworkforce.com by noon on July 9, 2010.

Effective Date: August 19, 2010

TEXAS WORKFORCE COMMISSION LETTER

ID/No:	WD 13-08
Date:	April 1, 2008
Keyword:	Administration; All Programs; General
Effective:	Immediately

To: Local Workforce Development Board Executive Directors
Other Texas Workforce Commission Grantees
Commission Executive Offices
Integrated Service Area Managers



From: Laurence M. Jones, Director, Workforce Development Division

Subject: Security of Personal Identity Data

PURPOSE:

This WD Letter provides Local Workforce Development Boards (Boards) and other Texas Workforce Commission (Commission) grantees¹ with information on ensuring the security and confidentiality of customers' personal identity data, such as Social Security numbers, addresses, phone numbers, and date of birth.

BACKGROUND:

The acquisition of sensitive data, which can be sold or directly employed in criminal activity, is most frequently the aim of both system intrusion and computer theft. However, system access or the accessibility of electronic equipment that puts sensitive data at risk is only part of the problem, and responsibility for the security of such data does not rest solely with information technology staff. The unintentional actions or negligence of staff pose at least as great a risk, if not greater, than external attacks on system integrity.

PROCEDURES:

Boards, and other Commission grantees, must ensure the security and confidentiality of customers' personal identity data.

NLF

To that end, Boards, and other Commission grantees, must ensure steps are taken to keep confidential information secure, including the following:

NLF

¹ Grantees other than Boards that receive funds for Skills Development, Self-Sufficiency, Wagner-Peyser 7b, Apprenticeship, Workforce Investment Act statewide initiatives, Temporary Assistance for Needy Families statewide initiatives, and other statewide initiatives from the Commission.

Physical Security

- Limit access to sensitive printed materials.
- Use proper storage for materials that include personal identity data.
- When possible, shred documents that include personal identity data after use.
- Secure laptop computers when not in use.
- Do not leave documents that include personal identity data in plain view.

Electronic Security

- Do not share passwords, personal identification numbers, security tokens (e.g., smartcards), or any data or equipment used for authentication and identification purposes.
- Log off of computers when leaving them unattended, no matter for how short a time.
- Do not send any personal identity data in the subject or body of an e-mail; instead, save the data to a secure document using the password protection option and send the document as an attachment in a separate e-mail.
- Use password protection when saving personal identity data in a document that will be transported on a laptop computer or portable storage device.

Additionally, Boards, and other Commission grantees, must ensure that confidential personal identity data is not given out by telephone except to the customer whose data it is, and then only after the customer provides enough information to establish his or her identity.

NLF

INQUIRIES:

Direct inquiries regarding this WD Letter to wfpolicy.clarifications@twc.state.tx.us.

RESCISSIONS:

None

FLEXIBILITY RATINGS:

No Local Flexibility (NLF): This rating indicates that Boards, and other Commission grantees, must comply with the federal and state laws, rules, policies, and required procedures set forth in this WD Letter and have no local flexibility in determining whether and/or how to comply. All information with an NLF rating is indicated by “must” or “shall.”

Local Flexibility (LF): This rating indicates that Boards, and other Commission grantees, have local flexibility in determining whether and/or how to implement guidance or recommended practices set forth in this WD Letter. All information with an LF rating is indicated by “may” or “recommend.”