

**TEXAS WORKFORCE COMMISSION LETTER**

<b>ID/No:</b>	WD 13-08
<b>Date:</b>	April 1, 2008
<b>Keyword:</b>	Administration; All Programs; General
<b>Effective:</b>	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) grantees<sup>1</sup> 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

---

<sup>1</sup> 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](mailto: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.”