

## TEXAS WORKFORCE COMMISSION LETTER

<b>ID/No:</b>	WD 13-13
<b>Date:</b>	April 2, 2013
<b>Keyword:</b>	Administration; All Programs; General
<b>Effective:</b>	Immediately

**To:** Local Workforce Development Board Executive Directors  
Agency Grantees  
Commission Executive Offices  
Integrated Service Area Managers

*Reagan Miller*

**From:** Reagan Miller, Director, Workforce Development Division

**Subject: Handling and Protection of Personally Identifiable Information and Other Sensitive Information**

---

### **PURPOSE:**

To provide Local Workforce Development Boards (Boards) and Texas Workforce Commission (TWC) Grantees (Agency Grantees)<sup>1</sup> with information and guidance on personally identifiable information (PII) and other sensitive information, specifically:

- requirements for their handling and protection; and
- recommended best practices.

### **BACKGROUND:**

The U.S. Department of Labor Employment and Training Administration (DOLETA), Training and Employment Guidance Letter 39-11, issued June 28, 2012, and entitled “Guidance on the Handling and Protection of Personally Identifiable Information (PII),” requires that strong and effective measures be taken to mitigate the risks associated with the collection, storage, dissemination, and disposal of sensitive data, including PII.

Based on the Office of Management and Budget (OMB) and DOLETA definitions, TWC defines PII and other sensitive information as follows:

- PII—information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII includes, but is not limited to, Social Security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birth dates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information, and computer passwords.

---

<sup>1</sup> TWC’s Integrity of the Texas Workforce System rule §802.2(1) defines *Agency Grantees* as “grantees that receive funding from the Agency, such as Skills Development Fund, Wagner-Peyser 7(b), and Workforce Investment Act (WIA) statewide, to provide workforce services.”

- Other sensitive information—any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of federally funded programs, or the privacy to which individuals are entitled under the Privacy Act of 1974, as amended (5 USC §552a). Essentially, it is stand-alone information not linked or closely associated with any PII, and includes information such as first and last names, e-mail addresses<sup>2</sup>, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as PII.

As part of their grant-funded activities, Boards and Agency Grantees have in their possession large quantities of PII and other sensitive information relating to their organization and staff; subcontractor and partner organizations and staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files, and other sources.

## **PROCEDURES:**

### **Handling and Protection of Personally Identifiable Information and Other Sensitive Information**

Boards and Agency Grantees must ensure the security of PII and other sensitive information as follows:

**NLF**

- Maintain PII and other sensitive information in accordance with the TWC standards for information security set forth in WD Letter 13-08, issued April 1, 2008, and entitled “Security of Personal Identity Data,” and any subsequent updates.
- Obtain PII in conformity with applicable federal and state laws governing confidentiality of information.
- Ensure PII and other sensitive information that is transmitted either by e-mail, or by mail stored on CDs, DVDs, thumb drives, etc., is encrypted using a Federal Information Processing Standards (FIPS) 140-2<sup>3</sup> compliant and National Institute of Standards and Technology (NIST) validated cryptographic module<sup>4</sup>.
- Ensure PII and other sensitive information is transmitted only to authorized users.
- Store PII and other sensitive information in an area that is physically safe from access by unauthorized persons at all times and process the data using Board- or Agency Grantee-issued equipment, managed information technology services, and approved designated locations.
- Prohibit accessing, processing, or storing of PII data on personally owned equipment and at off-site locations, unless explicitly permitted in the TWC Information Security Standards and Guidelines, available on the Intranet at [http://intra.twc.state.tx.us/intranet/its/docs/iris\\_standard.pdf](http://intra.twc.state.tx.us/intranet/its/docs/iris_standard.pdf).<sup>5</sup>

<sup>2</sup> Texas Government Code §552.137 provides that an e-mail address of a member of the public that is provided for the purpose of communicating electronically with a governmental body is confidential and not subject to disclosure under the Public Information Act.

<sup>3</sup> For more information on FIPS 140-2 standards and cryptographic modules, see FIPS PUB 140-2, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

<sup>4</sup> For examples of FIPS 140-2 certified options, see <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>.

<sup>5</sup> *The Intranet is not available to the general public.*

- Advise personnel who have access to sensitive, confidential, proprietary, or private data of the confidential nature of the information, the safeguards required to protect the information, and the civil and criminal sanctions for noncompliance with such safeguards in federal and state law.
- Establish policies and procedures under which personnel—before being granted access to PII and other sensitive information—acknowledge their understanding of the confidential nature of the information and the safeguards with which they must comply in its handling, as well as liability to civil and criminal sanctions for improper disclosure.
- Ensure that PII and other sensitive information is accessed only for the purposes set forth in the Agency-Board Agreement.
- Restrict access to PII and other sensitive information to only those employees who need it in the official performance of duties within the scope of work set forth in the Agency-Board Agreement.
- Process PII and other sensitive information in a manner that protects the confidentiality of the records and documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means. If data is downloaded to, or maintained on, mobile or portable devices, ensure that the data is encrypted using NIST-validated software products based on FIPS 140-2 encryption.
- Provide that PII and other sensitive information obtained through a request is not disclosed to anyone other than an individual or entity authorized by law to receive the information. Individuals authorized by law include, but are not limited to:
  - program staff with a need to know;
  - auditors;
  - state and fiscal monitors; and
  - persons or entities identified in a signed release from the participant.

Disclosure of PII and other sensitive information also is authorized when required by court order and in response to a subpoena by a governmental entity with subpoena authority. (If not accompanied by a court order or a signed written authorization from the individual, refer subpoenas from attorneys representing civil litigants to the Board's or Agency Grantee's attorney to determine objections.)
- Retain PII and other sensitive information only for the period of time required to use it for assessment and other official purposes, or to satisfy applicable federal or state records retention requirements, if any. Where appropriate, destroy PII, including degaussing magnetic tape files and deleting electronic data.
- Safeguard records containing PII and other sensitive information by never leaving them open and unattended.
- Immediately report any breach or suspected breach of PII or other sensitive information to TWC's Chief Information Security Officer at [CISO@twc.state.tx.us](mailto:CISO@twc.state.tx.us).

Boards and Agency Grantees must be aware that failure to comply with these requirements, or failure to take appropriate action to prevent any improper use or disclosure of PII and other sensitive information for an unauthorized purpose, is subject to sanctions or other actions as deemed necessary by TWC, up to and including termination of contracts and recoupment of funds or criminal or civil prosecution. Boards and Agency Grantees must hold individuals accountable who improperly use or disclose PII and other sensitive information for unauthorized purposes.

NLF

### **Recommended Best Practices**

It is recommended that Boards and Agency Grantees follow these procedures to ensure the security of PII and other sensitive information:

LF

- Before collecting PII or other sensitive information from customers, have them sign release forms acknowledging its use, disclosing the entities that will have access to it, and notifying them that in certain circumstances the proper, secure release of their information will be necessary.
- Whenever possible, use unique identifiers such as WorkInTexas.com or The Workforce Information System of Texas (TWIST) identification numbers for participant tracking instead of SSNs. While SSNs can initially be required for performance tracking purposes, a unique identifier can later be linked to each individual's record. Once the SSN is entered for performance tracking, the unique identifier can be used in place of the SSN for tracking purposes. If SSNs are used for tracking purposes, ensure that they are stored or displayed in a way that disassociates them from particular individuals, using a truncated SSN or an alternate number such as a TWIST or WorkInTexas.com ID.
- Use appropriate methods for destroying PII and other sensitive information in paper files (e.g., shredding or using a burn bag); securely delete electronic PII and other sensitive information; and ensure that contracts with disposal facilities clearly state that confidentiality of records is required throughout the disposal process.<sup>6</sup>
- If feasible, store documents containing PII and other sensitive information in locked cabinets when the documents are not in use.
- Create procedures to document chain of custody when documents are removed from storage premises.
- Follow the TWC Information Security Standards and Guidelines to ensure the security of PII and other sensitive information.

### **INQUIRIES:**

Direct inquiries regarding this WD Letter to [wfpolicy.clarifications@twc.state.tx.us](mailto:wfpolicy.clarifications@twc.state.tx.us).

### **RESCISSIONS:**

None

---

<sup>6</sup> For more information on destruction of PII and other sensitive information, see Draft NIST Special Publication 800-88 Revision 1, [http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800\\_88\\_r1\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf).

---

**REFERENCE:**

- Privacy Act of 1974, as amended (5 USC §552a)
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), available at <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>
- U.S. Department of Labor Employment and Training Administration, Training and Employment Guidance Letter 39-11, issued June 28, 2012, and entitled “Guidance on the Handling and Protection of Personally Identifiable Information (PII),” [http://wdr.doleta.gov/directives/attach/TEGL/TEGL\\_39\\_11\\_Acc.pdf](http://wdr.doleta.gov/directives/attach/TEGL/TEGL_39_11_Acc.pdf)
- Federal Information Processing Standards Publication 140-2
- Texas Government Code §552.137
- WD Letter 13-08, issued April 4, 2008, and entitled “Security of Personal Identity Data”
- Texas Workforce Commission Information Security Standards and Guidelines, [https://intra.twc.state.tx.us/intranet/its/docs/iris\\_standard.pdf](https://intra.twc.state.tx.us/intranet/its/docs/iris_standard.pdf)

**FLEXIBILITY RATINGS:**

**No Local Flexibility (NLF):** This rating indicates that Boards and Agency 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 Agency 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.”