

TEXAS WORKFORCE COMMISSION LETTER

ID/No:	WD 11-16
Date:	June 15, 2016
Keyword:	TWIST; WorkInTexas.com
Effective:	Immediately

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

From: Reagan Miller, Director, Workforce Development Division

Subject: ~~Access and Data Security for Workforce Applications in The Workforce Information System of Texas and WorkInTexas.com~~
Update

PURPOSE:

To provide Local Workforce Development Boards (Boards) **and other Texas Workforce Commission (TWC) grantees¹** with policy regarding computer-based automation security and providing other agencies and community partners with access **and connectivity** to **Workforce Applications (e.g., The Workforce Information System of Texas (TWIST) and WorkInTexas.com) that contain personally identifiable information (PII).**

This Workforce Development (WD) Letter provides Boards with updated information and guidance on:

- **protecting PII and other sensitive information from unauthorized disclosure; and**
- **the requirements of the National Institute of Standards and Technology (NIST) for moderate systems and, as applicable, cybersecurity and information security industry best practices.**

CHANGES TO WD LETTER 03-12, CHANGE 1:

New information in this WD Letter is indicated by:

- **a strikethrough of the original language, which indicates that language has been deleted; and**
- **bold typeface, which indicates new or clarifying language.**

¹ Grantees other than Boards that receive funds for Skills Development, Self-Sufficiency, Wagner-Peyser 7b, Apprenticeship, Workforce Innovation and Opportunity Act of 2014 statewide initiatives, Temporary Assistance for Needy Families statewide initiatives, and other statewide initiatives approved by TWC's three-member Commission.

BACKGROUND:

As Board partnerships expand, the Texas Workforce Commission (TWC) is providing policy to protect data security and **PII and other sensitive information** from unauthorized disclosure of information. The goal of data security is to prevent unauthorized access of files and records, and protect TWC's information from accidental or intentional destruction, disclosure, or misuse. **WD Letter 13-08, issued April 4, 2008, and entitled "Security of Personal Identity Data,"** provides Boards and other Commission grantees with information on ensuring the security and confidentiality of customers' personal identity data, such as Social Security numbers, addresses, phone numbers, and dates of birth.

WD Letter 13-13, issued April 2, 2013, and entitled "Handling and Protection of Personally Identifiable Information and Other Sensitive Information," provides Boards with information and guidance on PII and other sensitive information, specifically:

- TWC's definition of PII and other sensitive information;
- requirements for handling and protecting PII and other sensitive information; and
- recommended best practices.

PROCEDURES:

NLF: Boards must be aware that the term "Workforce Application" includes computer-based automated systems such as:

- TWIST; and
- WorkInTexas.com.

NLF: Boards must ensure that contractors protect customers' PII. TWC's Information Security strategy is to comply with NIST requirements for moderate systems and, as applicable, cybersecurity and information security industry best practices. The NIST standards are available online at NIST Special Publications: <http://csrc.nist.gov/publications/PubsSPs.html>.

Some NIST special publications that TWC uses for reference include the following:

- Cybersecurity Framework—
<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>
- NIST Special Publications 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations, as currently revised—
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- NIST SP800-53Ar4 Assessing Security and Privacy Controls in Federal Information Systems and Orgs—

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

- NIST Special Publication 800-88, Guidelines for Media Sanitization—<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>
- NIST SP800-122 Guide to Protecting The Confidentiality of Personally Identifiable Information (PII)—<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
- NIST SP800-27-RevA Engineering Principles for IT Security-A Baseline for Achieving Security—<http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>

Some industry resources that TWC uses for reference include the following:

- Information security management systems (ISO 27001)—<https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>; and
- Enterprise IT management (COBIT 5)—<https://cobitonline.isaca.org/>

NLF: Boards must:

- determine, assign, and secure **Workforce Application** ~~the WorkInTexas.com~~ and ~~TWIST~~ computer access codes required for Board staff, Workforce Solutions Office staff, workforce service provider staff, and staff from other agencies or community partners to perform assigned job duties, including changing or resetting users' local passwords and administering Resource Access Control Facility (RACF) security adds, changes, and deletes for users;
- ensure that users are aware of and comply with TWC's data security requirements;
- ensure that users understand that under no circumstances are user names, identification codes, passwords, or any other access security codes to be used by anyone other than the user to whom they are assigned and are not to be disclosed to anyone;
- ensure that users understand that they are responsible for any actions completed in **Workforce Applications** ~~WorkInTexas.com~~ and ~~TWIST~~ under the use of their access security codes;
- require that all users with access to **Workforce Applications** ~~WorkInTexas.com~~ and ~~TWIST~~ complete and annually sign the TWC Information Resources Usage Agreement, Form P-41, available on TWC's Intranet² at http://intra.twc.state.tx.us/intranet/gl/html/information_technology_forms.html
- maintain a signed copy of the most recent Form P-41 for each user per the Form P-41 instructions, available on TWC's Intranet at http://intra.twc.state.tx.us/intranet/gl/html/information_technology_forms.html; and
- **maintain a signed copy of the most recent Systems Access Report for Other Agencies and Community Partners, Form P-48, available on**

² The Intranet is not available to the general public.

TWC's Intranet

at [http://intra.twc.state.tx.us/intranet/gl/html/information technology for ms.html](http://intra.twc.state.tx.us/intranet/gl/html/information_technology_for_ms.html), when providing access to staff of other agencies or community partners.

NLF: Additionally, Boards must be aware that this reporting requirement does not apply to the access provided to Board staff, Workforce Solutions Office staff, workforce service provider staff, or Texas Veterans Commission (TVC) staff.

NLF: Boards must also be aware that Form P-41 applies to all TWC staff, Board staff, Workforce Solutions Office staff, workforce service provider staff, ~~Texas Veterans Commission (TVC) staff,~~ and staff from all other entities with access to **Workforce Applications** ~~WorkInTexas.com and TWIST.~~

NLF: When providing access to **Workforce Applications** ~~WorkInTexas.com and TWIST,~~ Boards must use a strict “need to know” standard for other agencies and community partners with a valid need, as determined by the Board and in accordance with the *Texas Workforce Commission Information Security Standards and Guidelines*, available on TWC's Intranet³ at http://intra.twc.state.tx.us/intranet/its/docs/iris_standard.pdf.

In TWIST, other agencies' and community partners' access to customer information is limited to “read only” or “edit,” as required to perform assigned duties previously agreed upon by the Board. In WorkInTexas.com, permissions are limited to “Staff Access” (which allows “View” of job seeker, employer, and staff information) and “Edit.” Permissions are determined by the specific, assigned duties previously agreed upon by the Board.

NLF: Boards must ensure that information obtained from Workforce Applications (e.g., participant information) is not republished or redistributed.

Boards must be aware that access to TWIST Web Reports is:

- ~~authorized only for Board staff, Workforce Solutions Office staff, workforce service provider staff, and TVC staff; and~~
- ~~not authorized for any other partners.~~

NLF: Boards must contact the state office's WorkInTexas.com staff at wfsupportdesk@twc.state.tx.us ~~workintexas.supportunit@twc.state.tx.us~~ when “State Role” access in WorkInTexas.com is requested or needed. Boards must receive authorization from the state office's WorkInTexas.com staff prior to granting State Role access.

NLF: Boards must monitor and evaluate access to **Workforce Applications** ~~WorkInTexas.com and TWIST,~~ and terminate or adjust other agencies' or community partners' access if their need is no longer valid.

³ The Intranet is not available to the general public.

NLF: Boards must consider their level of oversight and the partners’ supervisory authority over staff when determining whether access is required and what training must be provided.

NLF: Boards must ensure that partner staff receives applicable training prior to granting edit access to **Workforce Applications** ~~WorkInTexas.com~~ and TWIST.

NLF: Boards must ensure that appropriate staff that does not have access to the *Texas Workforce Commission Information Security Standards and Guidelines* is aware of TWC’s standards, procedures, and guidelines regarding information security, and that violations thereof may result in adverse disciplinary action and criminal prosecution.

~~Boards must submit basic information to their senior contract manager using the Systems Access Report for Other Agencies and Community Partners, Form P-48, available on TWC’s Intranet at http://intra.twc.state.tx.us/intranet/gl/html/information_technology_forms.html when providing access to staff of other agencies or community partners. Boards must be aware that this reporting requirement does not apply to the access provided to Board staff, Workforce Solutions Office staff, workforce service provider staff, and TVC staff.~~

INQUIRIES:

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

RECISSIONS:

WD Letter 03-12, Change 1

REFERENCES:

Texas Workforce Commission Information Security Standards and Guidelines
Master Board Contract, Section 2, Security Management

WD Letter 13-13, issued April 2, 2013, and entitled “Handling and Protection of Personally Identifiable Information and Other Sensitive Information”

WD Letter 13-08, issued April 4, 2008, and entitled “Security of Personal Identity Data”

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.”