


TEXAS WORKFORCE COMMISSION
Workforce Development Letter

ID/No:	WD 11-16, Change 1
Date:	August 21, 2024
Keywords:	Administration; WorkInTexas.com
Effective:	Immediately

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

From: 
Mary York, Director, Workforce Development Division

Subject: **Access and Data Security for Workforce Applications—Update**

PURPOSE:

The purpose of this WD Letter is to provide Local Workforce Development Boards (Boards) and other Texas Workforce Commission (TWC) grantees¹ with policy regarding computer-based automation security and the provision to other agencies and community partners with access and connectivity to Workforce Applications that contain Sensitive Personal Information (SPI).

This updated letter provides Boards with information and guidance on:

- protecting SPI and other confidential information from unauthorized disclosure;
- the requirements of the National Institute of Standards and Technology (NIST) for Moderate-Impact Information Systems and, as applicable, cybersecurity and information security industry best practices;
- Board requirements regarding workforce application access; and
- terminology and clarification relating to the implementation of WorkInTexas.com as TWC's workforce case management system.

RESCISSIONS:

WD Letter 11-16

BACKGROUND:

TWC is providing policy to protect SPI and other confidential information from unauthorized disclosure. 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.

¹ Grantees other than Boards that receive a TWC grant award.

WD Letter 02-18, Change 1, issued March 18, 2024, titled “Handling and Protection of Sensitive Personal Information and Other Confidential Information—Update,” provides Boards with information and guidance on SPI and other sensitive information, specifically:

- ensuring the security and confidentiality of customers’ SPI data;
- TWC’s definition of SPI and other confidential information;
- requirements for handling and protecting SPI and other sensitive confidential information; and
- recommended best practices.

PROCEDURES:

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

Local Flexibility (LF): This rating indicates that Boards 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.”

TWC Information Security Compliance

NLF: Boards must ensure contractors protect customers’ SPI. 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](#).

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

- [Cybersecurity Framework \(CSF\) 2.0](#)
- [NIST Special Publications 800-53r5 Security and Privacy Controls for Information Systems and Organizations, as currently revised](#)
- [NIST SP800-53Ar5 Assessing Security and Privacy Controls in Information Systems and Orgs](#)
- [NIST Special Publication 800-88r1, Guidelines for Media Sanitization](#)
- [NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#)
- [NIST SP800-160 Vol.1 Rev. 1 Engineering Trustworthy Secure Systems](#)

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

- [Information security management systems \(ISO 27001\)](#)
- [Enterprise IT management \(COBIT 5\)](#)

Workforce Application Access

NLF: Boards must:

- determine, assign, and secure computer access codes for Workforce Applications (which includes computer-based automated systems such as WorkInTexas.com)

required for Board staff, Workforce Solutions Office 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 users are aware of and comply with TWC's data security requirements;
- ensure users understand that under no circumstances are usernames, 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 users understand they are responsible for any actions completed in Workforce Applications under the use of their access security codes;
- require all users with access to Workforce Applications complete and sign the TWC Information Resources Usage Agreement, Form P-41, every two years, available on [TWC's Information Technology SharePoint](#);
- maintain a signed copy of the most recent Form P-41 for each user once signed via DocuSign; and
- maintain a signed copy of the most recent Systems Access Report for Other Agencies and Community Partners, Form P-48, available on [TWC's Intranet](#), when providing access to staff of other agencies or community partners.

NLF: When providing access to Workforce Applications, 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 Intranet at [TWC Information Security Manual](#).

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 (for example, participant information) is not republished or redistributed.

NLF: When requesting “Administrative” level permissions or access changes in WorkInTexas.com, Boards must ensure:

- the Board Executive Director approves before any changes can be implemented; and
- staff sends the approved request to the state office's WorkInTexas.com staff at wfsupportdesk@twc.texas.gov.

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

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 partner staff receives applicable training prior to granting edit access to Workforce Applications.

NLF: Boards must ensure appropriate staff who 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.

INQUIRIES:

Send inquiries regarding this WD Letter to wfpolicy.clarifications@twc.texas.gov.

ATTACHMENTS:

Attachment 1: Revisions to WD Letter 11-16 Shown in Track Changes

REFERENCES:

Texas Workforce Commission Information Security Standards and Guidelines
Agency Board Agreement (ABA) 2023 (et seq.), Section 2.4 – Privacy Awareness and
Training
Texas Workforce Commission Privacy Manual
WD Letter 02-18, Change 1, issued March 18, 2024, and titled “Handling Sensitive
Personal Information and Other Confidential Information—Update”