



<b>WS 17-14 Change 2</b>
<b>Release Date: October 15, 2024</b>
<b>Effective Date: October 15, 2024</b>
<b>Expires: Continuing</b>

To: All Service Providers

From: Juliet Stipeche  
Kristi Rangel  
Russell Tomlin  
Kevin Rodney

Subject: Information Security Standards and Guidelines - Change 2

---

## **PURPOSE**

This policy outlines updated procedures for managing and protecting Workforce Solutions' Sensitive Personal Information (SPI) and other confidential information. Updates apply to the Information Security Standards and Guidelines, Desk Aids, and related forms. *The new FNS Civil Rights Training module must be completed by November 15, 2024*, while all other required trainings are due annually by the end of October.

## **RECISSIONS**

WS 17-14 Information System Standards and Guidelines, Released September 30, 2024

## **BACKGROUND**

Workforce Solutions collects and stores sensitive personal and confidential data about customers in various information systems. This policy ensures staff understand and adhere to information security standards to protect this data.

## **POLICY**

Any user of Workforce Solutions information systems and all staff must execute the **Information Resources Usage Agreement** and acknowledge in writing that they received, read, and understood Workforce Solutions Information Security Standards and Guidelines. There are separate agreements for use of Texas Health and Human Services Commission information. Contractors should limit staff access to the Texas Health and Human Services Commission database to staff in supervisory positions or special designees.

### **Online Training**

All users of Workforce Solutions information systems must complete the Texas Workforce Commission's training modules and Workforce email training:

- Cybersecurity Awareness

Workforce Solutions Issuance 17-14 Information Security Standards & Guidelines, Change 2  
October 15, 2024—Page 1

- o Staff [Cybersecurity Awareness](#)
- o TWC Staff [Cybersecurity Awareness](#)
- [Fraud Awareness Training](#)
- [Diversity, EEO, and Discrimination Prevention](#)
- [Human Trafficking](#)
- [FNS Civil Rights Training](#)
- [KnowBe4](#)

EO officers, office/ contract managers, monitors, and navigators must also complete this Texas Workforce Commission’s training module:

- [WIOA Discrimination Complaint Process](#)

All contractors are responsible for maintaining the certificates showing successful completion of these trainings. Staff must take and pass these training modules at hire and annually in October.

### **Access to TWC Mainframe (RACF)**

Contractor or Office LISO is responsible for adding and deleting access to the TWC Mainframe. If staff do not access RACF within 90 days, access will be automatically revoked. If staff do not access RACF within 180 days, access will be automatically deleted. Contractor or Office LISO are also responsible for resetting passwords for their staff.

Note: Staff do not need access to the TWC Mainframe to complete the two TWC online training modules required at hire and annually thereafter. The LISO must limit access to the TWC Mainframe to staff who need access to perform their job.

### **Access to Texas Educating Adult Management System (TEAMS )**

AEL contractors are responsible for requesting access to TEAMS. Staff needing access to TEAMS must complete the AEL Information Resources Usage Agreement and complete the online [Family Educational Rights & Privacy Act \(FERPA\)](#) training. Staff must then go the [TEAMS](#) login page, complete the required fields and confirm the information provided by selecting “Submit”. Then submit the AEL Information Resources Usage Agreement and the Family Educational Rights & Privacy Act certificate along with an approval message from the Designated Director to [TEAMS Technical Assistance](#).

### **Local Information Security Officer (LISO)**

Each contractor and each Workforce Solutions funded location must have staff assigned as a primary and a secondary Local Information Security Officer (LISO). The responsibilities for LISO’s are detailed in Workforce Solutions Information Security Guide. In summary, the LISO must:

- Complete the RACF Managers Training Modules before managing RACF rights for her location.
- Discuss the need for strict confidentiality of Workforce Solutions information sources with each staff person signing the Information Resources Usage Agreement.
- Provide each staff person with a copy of – Information Security Standards and Guidelines.
- Update Workforce Solutions user database as appropriate.

- Review the information of staff members on the Workforce Solutions user database for accuracy monthly.
- Notify H-GAC no later than the same day if a staff person is no longer employed by Workforce Solutions contractor or if job duties change resulting in changes to access to information systems.
- Manage TWC Mainframe/Intranet access for staff – add, delete, change passwords. Staff selected as LISO, primary and backup, must complete RACF Management training before having management access to their location.

### **Monitoring Information Security**

Contractors must conduct Information Security reviews at each location where there is Personally Identifiable Information (PII), in physical or electronic format.

Contractor must conduct these reviews using the Information Security Review Document according to this schedule;

- Daily Reviews – Authorized staff will conduct daily reviews. If the daily reviews for the location do not reveal violation of Information Security Policy and Guide for twenty consecutive business days, reviews for that location will step to weekly reviews.
- Weekly Reviews – Authorized staff will conduct weekly reviews. If the weekly reviews for the location do not reveal violation of Information Security Policy and Guide for thirteen consecutive weeks, reviews for that location will step to monthly reviews.
- Monthly Reviews - Authorized staff will conduct monthly reviews.

If a reviewer identifies a violation of Information Security Guide, at any stage, the review process begins again at the Daily Review level.

The contractor must designate staff to maintain a log showing the outcome of the required reviews for each location. Each location must maintain the review documents for that location.

The contractor will educate and counsel staff, or take other appropriate actions, at locations where there are violations of the Information Security Standards and Guidelines.

### **ACTIONS**

1. All contractors must ensure each staff receives, reads, and understands Workforce Solutions Information Security Standards and Guidelines.
2. Make sure each staff member signs an Information Resources Usage Agreement at hire and annually in October.
3. Make sure each staff member takes and passes the required training modules at hire and annually.
4. Update Workforce Solutions user database as appropriate.

5. Notify H-GAC's Workforce Security team ([WorkforceSecurity@wrksolutions.com](mailto:WorkforceSecurity@wrksolutions.com)) no later than the same day staff leave employment.
6. Review and correct as necessary staff information in the Workforce Solutions user database by the 4<sup>th</sup> of each month.
7. Maintain and provide Workforce Security with a complete list of current LISO (name, telephone number and email address) for each location.

## REFERENCES

- [WD 11-16, Change 1](#), Access and Data Security for Workforce Applications Update
- [WD 17-07, Change 2](#), Storage and Use of Disability-Related and Medical Information—Update 04/16/2024, Handling Sensitive Personal Information and Other Confidential Information—Update
- [WD 02-18, Change 1](#), Handling Sensitive Personal Information and Other Confidential Information—Update

## ATTACHMENTS

- [Workforce Solutions Information Security Standards and Guidelines](#)
- [Desk Aid Workforce Security Training](#)
- [Information Resources Usage Agreement](#)
- [Code of Conduct](#)
- [Fraud, Waste, Theft and Abuse](#)
- [FNS Civil Rights Training](#)
- [EO Acknowledgement](#)
- [HHSC TIERS Access and Security Role Assignment Request Form](#)
- [HHSC Information Security Acceptable Use Agreement Form](#)

## QUESTIONS

Staff should first ask questions of their managers or supervisors. Direct questions for Board staff to [Workforcepolicy@wrksolutions.net](mailto:Workforcepolicy@wrksolutions.net).