WS 18-17 Change 1
March 3, 2023
Information Security
Expires: Continuing

To: Workforce Solutions Service providers

From: Juliet Stipeche
Rebecca Neudecker
Kevin Rodney

Subject: Information Security Standards and Guidelines

Purpose

To update the guidelines for staff and users of Workforce Solutions information systems.

This issuance replaces Issuance WS 18-17 released on October 1, 2018.

Information Security

Workforce Solutions is the public workforce system for the Houston-Galveston 13-county region. In our work, we use several different information systems to collect and store data for and about our customers.

The information we store about our customers is confidential. Workforce Solutions staff must make sure they take all reasonable steps to ensure this confidentiality. Part of this responsibility includes understanding and adhering to Workforce Solutions Information Security Standards and Guidelines.

We will remove all access to Workforce Solutions information resources for any user who does not comply with our security policies and procedures described in this issuance and its attachments.

Usage Agreements

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 dated March 2, 2023. Staff will also sign agreements at hire and annually in October.

This agreement covers all Workforce Solutions information systems including but not limited to:

- Texas Workforce Commission (TWC) Mainframe/Intranet and E-mail
- Workforce Solutions E-mail
- The Workforce Information System of Texas (TWIST)
- Work-in-Texas.com (WIT)
- Financial Aid Communication System (FACS)
- Financial Aid Management System (FAMS)
- Child Care Management System (historical data)
- Data Management System(s)
- Texas Education Adult Management System (TEAMS)
- ***Restrictions on TikTok and other prohibited technologies***

There are separate agreements for the use of Texas Health and Human Services Commission information. Service providers should limit staff access to the Texas Health and Human Services Commission (HHSC) database to staff in supervisory positions or special designees.

Service providers are responsible for maintaining completed original Information Resources Usage Agreements, the certificates confirming staff completed the - TWC online trainings (see below), TWC complaint process online training for appropriate staff, and the Texas Health and Human Services Commission agreements (two forms), when appropriate.

Online Training

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

- Cyber Security Awareness
- Fraud Prevention and Detection
- Diversity, EEO, and Discrimination Prevention
- Human Trafficking
- KnowBe4

Equal Opportunity (EO) officers, office/contract managers, monitors, and navigators must also complete the following training module:

- Workforce Investment Act Discrimination Complaint Process

The service provider is responsible for maintaining certificates showing successful completion of these trainings. See attached guide for accessing these training modules and for printing certificates.

Staff must take and pass these training modules at hire and annually in October.

Access to TWC Mainframe (RACF)

The service provider or Office Local Information Security Officer (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. The service provider 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 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 Integrated Eligibility Redesign System (TIERS)

The service provider or Office LISO are responsible for requesting access to TIERS. If staff do not access TIERS within 90 days, access will be automatically suspended. If an account has been suspended, the LISO must submit a new User Access Request for HHSC Systems and the HHSC Computer Use Agreement.

Access to TEAMS

AEL service providers are responsible for requesting access to TEAMS. Staff needing access must complete the AEL Information Resources Usage Agreement and complete the online Family Educational Rights & Privacy Act (FERPA) training. Staff must access the TEAMS login page, complete the required fields and confirm the information provided by selecting "Submit." Next, they must 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.

Access to TWIST Web Reports and Ad Hoc Reports

TWIST Web Reports and Work-In-Texas Ad Hoc reports contain a significant amount of customers' personally identifiable information (PII). Workforce Solutions will give access to these reports on a case-by-case basis.

Local Information Security Officer (LISO)

Workforce Solutions service providers must have a primary and secondary Local Information Security Officer (LISO). The responsibilities for LISOs are detailed in Workforce Solutions Information Security Standards and Guidelines. A LISO must:

- Complete the RACF managers training modules

- Discuss the need for strict confidentiality of Workforce Solutions information sources with staff signing the Information Resources Usage Agreement.
- Provide each staff person with a copy of the Information Security Standards and Guidelines
- Update Workforce Solutions user database as appropriate and review the staff information on Workforce Solutions user database for accuracy monthly.
- Notify H-GAC on the same day when a staff person is no longer employed by Workforce Solutions service provider 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

Service providers must conduct Information Security reviews at locations where there is Personally Identifiable Information (PII), in physical or electronic format.

Service provider 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 Policies and Procedures 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 Policies and Procedures 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 Standards and Guidelines, at any stage, the review process begins again at the Daily Review level.

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

Action

1. Make sure that each staff member receives, reads, and understands Workforce Solutions Information Security Standards and Guidelines.

2. ***Make sure each staff member signs the new Information Resources Usage Agreement by Tuesday, March 7, 2023.***

3. Make sure each staff member signs an Information Resources Usage Agreement at hire and annually in October.

4. Make sure each staff member takes and passes the required training modules at hire and annually in October.

5. Update Workforce Solutions user database as appropriate.

6. Notify H-GAC's Workforce Security team (WorkforceSecurity@wrksolutions.com) no later than the same day staff leave employment.

7. Review and correct as necessary staff information in the Workforce Solutions user database by the 4th of each month.

Questions

Staff with questions about information security should speak to their supervisor or manager first. Direct questions to Workforce Security at WorkforceSecurity@wrksolutions.com.

Attachments

You can find these attachments at Information Security section at this link: Information Security and MIS

- Workforce Solutions Information Security Standards and Guidelines
- Information Resources Usage Agreement
  - Electronic
  - Hard copy
- Desk Aid for Required Information Security Training
- Workforce Solutions Information Security Review