WS 16-13
October 14, 2016
Information Security
Expires: Continuing

To: Workforce Solutions Contractors

From: Mike Temple
David Baggerly

Subject: Information Security Standards and Guidelines

Purpose

Transmit updates and revisions to Workforce Solutions Information Security Standards and Guidelines, Desk Aides, and forms. This issuance replaces Issuance WS 14-10.

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 members 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 October 2016. This is done at hire and annually in October.

This agreement covers the following information systems:

- Texas Workforce Commission Mainframe/Intranet and E-mail
- Workforce Solutions E-mail
- TWIST
- Work-in-Texas.com
- Financial Aid Communication System (FACS)
- Financial Aid Management System (FAMS)
- Child Care Automated Attendance (CCAA)
- Child Care Management System (historical data).
- Data Management System(s)

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.

Contractors are responsible for maintaining completed original Information Resources Usage Agreement, the certificates confirming staff completed the three TWC online trainings, TWC complaint process online training for appropriate staff, and the Texas Health and Human Services Commission agreements (two forms) when appropriate.

Online Training

All Workforce Solutions Information Systems users must complete these three Texas Workforce Commission's training modules:

- IT Security Awareness
- Fraud Prevention and Detection
- Diversity, EEO, and Discrimination Prevention

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

- Workforce Investment Act Discrimination Complaint Process

The contractor is responsible for maintaining the 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)

Contractor or Office LISO are 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 TIERS

Contractor 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, LISO must submit a new User Access Request for HHSC Systems and the HHSC Computer Use Agreement.

Access to 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.

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 restrict access to these reports and access will be given on a case by case basis.

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 Standards and Guidelines. 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 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 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.

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 an Information Resources Usage Agreement at hire and annually in October. For 2016, staff should sign the Information Resources Usage Agreement no later than November 4, 2016.

3. Make sure each staff member takes and passes the required training modules at hire and annually in October. For 2016, complete the required training modules no later than November 4, 2016.

4. Update Workforce Solutions user database as appropriate.

5. Notify H-GAC's Workforce Security team (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 4th of each month.

7. Provide Workforce Security with a complete list of current LISO (name, telephone number and email address) for each location by Friday, October 28, 2016.

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
- HHSC Request for User Access Form
- HHSC Security and Privacy Agreement Form
- Desk Aid for Required Information Security Training
- Workforce Solutions Information Security Review