

# **WORKFORCE SOLUTIONS TEXOMA POLICIES & PROCEDURES**

## **CHAPTER 9 INFORMATION SECURITY SYSTEMS**

### **TABLE OF CONTENTS**

- 9.1 INTRODUCTION**
- 9.2 PURPOSE**
- 9.3 INFORMATION - DEFINITIONS**
- 9.4 AUTOMATION SUPPORT FOR BOARD, CONTRACTOR AND WORKFORCE CENTER PARTNER PERSONNEL**
  - 9.4.1 Board & Contractor Personnel**
  - 9.4.2 Workforce Center Partner Personnel**
- 9.5 CONFIDENTIALITY / SECURITY**
  - 9.5.1 Electronic Mail Confidentiality**
  - 9.5.2 Virus Protection**
- 9.6 AUTOMATION DEPARTMENT FUNCTION**
  - 9.6.1 Upgrade Existing Systems**
  - 9.6.2 Daily Procedures**
  - 9.6.3 Maintenance**
  - 9.6.4 Board, Contractor, TWC, and Partner Staff User Access**

## **9.7 AUTOMATION BACKUP PROCEDURES**

**9.7.1 Texoma CCMS / Grayson WFC Backup Procedures**

**9.7.2 WST Office Backup Procedures**

## **9.8 DATA INTEGRITY PROCEDURES**

## **9.9 DISASTER RECOVERY PROCEDURES**

## **9.10 SOFTWARE LICENSE AGREEMENTS**

## **9.11 COMPUTERIZED INFORMATION AND SYSTEMS ACCESS**

**9.11.1 Confidentiality of User IDs and Passwords**

**9.11.2 System Access Forms**

9.11.2.1 Original, Signed Forms

9.11.2.2 Supervisor-Only, Signed Forms

9.11.2.3 WST Automation Systems Access - Individual User  
Access Tracking Log

9.11.2.4 Acknowledgement of Receipt

9.11.2.5 TWC P-41 or P-41b41B Form

9.11.2.6 WORK//TEXAS Access

9.11.2.7 E-MAIL/Local Computer Security Acknowledgement

9.11.2.8 WST TWIST Privileges Request

9.11.2.9 Request for User Access to HHSC Systems

9.11.2.10 HHSC Enterprise Architecture & Security  
Management, Security and Privacy Agreement (SPA)

9.11.2.11 OAG – TWC User Information Form for Access to the  
Office of the Attorney General Child Support Division's  
(CSD) Portal

9.11.2.12 Child Care Local Application & BAPA Security Request

9.11.2.13 Automation System Access Termination

9.11.2.14 Common Access Forms

9.11.2.15 Systems Access Report for Other Agencies and  
Community Partners

**9.11.3 Granting User Access**

9.11.3.1 Types & Responsibilities of Users

9.11.3.1.1 Board, Contractor, TWC, and Partner  
Staff

9.11.3.1.2 Workforce Center Resource Room

9.11.3.2 Electronic Mail (E-Mail) Access

9.11.3.3 TWIST Access

9.11.3.4 WORK//TEXAS Access

9.11.3.5 TWC Mainframe RACF Access

9.11.3.6 Texas Department of Human Services Access

- 9.11.3.7 TIERS
- 9.11.3.8 Child Care Management System Access
  - 9.11.3.8.1 Local Application
  - 9.11.3.8.2 Budget and Payment Application (BAPA)
- 9.11.3.9 Users Outside the Workforce Solutions Texoma System

## **9.12 REPORTING INFORMATION SECURITY EQUIPMENT PROBLEMS**

- 9.12.1 **Serious Information Security Problems**
- 9.12.2 **Problems Involving Passwords / User IDs**
- 9.12.3 **Problems Involving Automation Equipment**

## **9.13 BOARD, CONTRACTOR, TWC, OR PARTNER STAFF USER ACCESS REVOCATION**

- 9.13.1 **Voluntary Separation**
- 9.13.2 **Involuntary Separation**

## **9.14 DATA SECURITY / AUTOMATION VIOLATIONS**

- 9.14.1 **WST Board, Contractor, TWC, or Partner Staff Security / Automation Violations**
- 9.14.2 **General Public Security / Automation Violations**

## **9.15 NETWORK / AUTOMATION SYSTEMS MONITORING**

- 9.15.1 **WST Board, Contractor, TWC, or Partner Staff Network/Automation Systems Monitoring**
- 9.15.2 **Workforce Center Customer / General Public Network/Automation Systems Monitoring**

## **9.16 RECORDS RETENTION**

## 9.1 INTRODUCTION:

Workforce Solutions Texoma (WST) has agreed to adopt and implement security guidelines and procedures to ensure WST automated systems will be used appropriately and that only authorized users will have access to confidential information in the performance of their assigned duties. Security measures utilized by the Board for the protection of the Texas Workforce Commission confidential data will conform, at a minimum, to the federal regulations contained in 20 CFR 603, and to the Texas Workforce Commission Systems Security Requirements.

## 9.2 PURPOSE

It is the policy of the WST that automated information, resources and technology under WST control are assets that require a degree of protection commensurate with their value. Measures will be taken to protect these assets against accidental or unauthorized disclosure, modification, or destruction, as well as to assure the security, reliability, integrity, and availability of information. This policy asserts the following:

- 1) Access to WST information resources (both internally and externally) must be strictly controlled.
- 2) Information that is Sensitive or Confidential must be protected from unauthorized access or modification.
- 3) Risks to information resources must be managed.
- 4) The integrity of data, its source, its destination, and processes applied to it must be assured.
- 5) In the event a disaster or catastrophe disables information processing and related telecommunication functions, the ability to continue critical WST services must be assured.
- 6) Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.
- 7) All individuals must be accountable for their actions relating to information and technology resources.
- 8) Information security programs must be responsive and adaptable to changing vulnerabilities and technologies affecting WST information resources.
- 9) Automation equipment and assets should be safeguarded against outside threats and maintained at high-quality standards.

It is the intent of the WST that protecting automated information assets is a priority. The scope of protection of automated information assets includes the following areas:

- 1) Physical protection of source documents, information processing facilities and equipment.
- 2) Maintenance of application and data integrity.
- 3) Assuring that automated information systems perform their critical functions correctly, in a timely manner, and under adequate controls.
- 4) Protection against unauthorized disclosure of information.
- 5) Assurance of the continued availability of reliable and critical information.

### **9.3 INFORMATION - DEFINITIONS**

Measures shall be taken to protect confidential and sensitive automated information against accidental or unauthorized disclosure, modification or destruction, as well as to assure the security, reliability, integrity and availability of information. Pursuant to the Texas Workforce Commission's Information Security Manual, definitions follow:

- 1) Confidential Information is information maintained that is exempt from disclosure under the provisions of the Texas Open Records Act or other state or federal law.
- 2) Sensitive Information is information that is maintained that requires special precautions, as determined by agency standards and risk management decisions, to assure its accuracy and integrity by utilizing error checking, verification procedures and/or access control to protect it from unauthorized modification or deletion.

## **9.4 AUTOMATION SUPPORT FOR BOARD, CONTRACTOR AND WORKFORCE CENTER (WFC) PARTNER PERSONNEL**

### **9.4.1 BOARD & CONTRACTOR PERSONNEL**

As contractor personnel are only authorized to use WST-owned computers and other automation equipment in the performance of WST business, the WST Technology Manager, in accordance with this policy, will provide automation support. Contractor personnel will strictly adhere to use of automation equipment for business-related purposes only and ensure the security and confidentiality of information contained in said systems.

### **9.4.2 WORKFORCE CENTER PARTNER PERSONNEL**

Workforce Center Partner personnel who are permanently housed in Texoma Workforce Centers are authorized to provide their own computers and automation equipment. However, if these computers and automation equipment are to be linked in any manner to Texoma systems, the technical support for said equipment will only be provided by the WST Technology Manager. No outside technology support will be allowed. Details of contractual arrangements for reimbursement of this support will be developed through appropriate parties in a separate contract or in the Shared Facilities Agreement. WFC Partner personnel will strictly adhere to ensuring the security and confidentiality of WST-related information contained in said systems and are required to sign all necessary forms relating to systems they access. Pursuant to WD 32-06, WST will notify TWC of any partner personnel given access to either TWIST or WIT systems.

## **9.5 CONFIDENTIALITY / SECURITY**

Confidential customer related information shall be accessible only to personnel who are authorized by the owner of the data and for purposes pertaining to customer's participation in workforce systems programs. Data containing any confidential information shall be readily identifiable and treated as such in its entirety

When confidential or sensitive information is received by another agency in connection with the transaction of official business, WST and Contractor staff will maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency.

By law, information obtained from the Texas Health and Human Services Commission (HHSC) is confidential. HHSC obtained information will only be used for purposes directly connected with programmatic functions. It is a criminal offense to release information obtained from HHSC for purposes other than those in conjunction with programmatic administration. The maximum punishment is one year in jail and/or \$3,000 fine (Human Resources Code Sec. 12.003).

WST, Contractor, TWC, and other partner agency staff who are authorized to use personal computers are responsible for the security of confidential or sensitive customer information contained in their system. Any staff authorized access to the Texas Workforce Information System of Texas (TWIST), the state JSMS system, or other state database systems, are responsible for the confidential or sensitive customer information contained therein. In order to retain the highest security standards for the protection of confidential or sensitive customer information, users will follow these guidelines:

- 1) Caution should always be used when printing confidential or sensitive information. Unless a printer is located in a secure area or there is someone at the printer to retrieve the information as it is printed, confidential information should not be printed.

- 2) Confidential information should be delivered directly to the individual it is intended for and not left on a desk or otherwise accessible to persons who are not authorized to see or use it.
- 3) Personal computers having access to local or area-wide networks, as terminals to the server, should never be left unattended while logged on to the network. In addition, users should not logon/login to a workstation and leave it unattended without logging off/out which means exiting from all systems, not physically turning off the computer. This also means that users should log off before leaving for the day. The network administrator and Contractor supervisory staff are responsible for monitoring users that remain logged on after normal business hours and notifying appropriate management of the violation.
- 4) Ensure that state and federal security and privacy requirements with respect to confidential or sensitive information is understood and enforced.
- 5) No personal computers or personal automation technology will be connected to WST systems.
- 6) Ensure that all WST-owned systems are used for business purposes only. No CPU's or installed applications are to be used for personal gain. In addition, systems are not to be used for games or contain any data or software that does not have an explicit business use.
- 7) Ensure that no alterations to hardware are undertaken. All requests for alterations to hardware must be submitted to the WST Technology Manager.
- 8) Ensure that no unauthorized software is installed on PCs. All requests for additional software installation must be submitted to the WST Technology Manager.
- 9) Ensure that personal passwords are protected and not released to other staff or individuals to ensure the integrity of the data entry process and system security. Users who are concerned that their password has been compromised have the responsibility to select a new password immediately. Staff granted access to computerized information and systems are responsible for all data entry and processing completed under his/her User ID. According to the TWC Agency Security Manual, it is a violation of the Texas Penal Code to use another person's User ID or password.

- 10) Ensure that activity conducted on the Internet or via e-mail is in accordance with the agency Internet and E-mail Policy as described in Sections 9.4.1, 9.11.3.2, and 9.11.3.5 of this policy.
- 11) All users are responsible for bringing any suspected security breaches to the attention of management staff in accordance with 9.14 of this policy.

### **9.5.1 ELECTRONIC MAIL CONFIDENTIALITY**

The content of electronic mail messages should be limited to WST official business. Pursuant to TWC Information Security Manual Section 6.2.1, Personal Use Exception, the use of electronic mail to coordinate lunch plans or other similar matters with fellow employees may reduce the amount of time spent on such activities, devote more time to job tasks, and enhance employee productivity. Therefore, incidental personal use of electronic mail systems will be allowed as long as such personal use does not interfere with the conduct of WST business or disrupt the work place. Under no circumstances will personal messages be sent through the TWC agency-wide network. Examples of permitted personal use of electronic mail systems include a message to a few employees regarding an employee luncheon or a retirement party for a co-worker. Examples of improper personal use of these systems that is not permitted include chain letters, advertising items for sale, or product advertising. In addition, transmission of any material in violation of local, state, and federal laws such as copyrighted material or material protected by trade secret is strictly prohibited.

All individuals granted access to the WST's electronic mail systems will assume responsibility for the content and dissemination of their messages. Electronic records constitute official records under the Open Records Act that may be available to the public. All e-mail sent or received is subject to inspection by the Board Technology Manager, Board Monitoring staff, and/or TWC staff at any time. Individuals should refrain from using e-mail for sensitive communications and should exercise caution when sending e-mail messages that include information about customers. Individuals should assume that their communication will be retained for a period of time either in electronic or hard copy form. Consequently, messages should be accurate, courteous, sent to only those selected personnel with a need to know, and authorized at an appropriate level. Abusive, harassing, bigoted, obscene, or profane messages are strictly prohibited as they not only reflect negatively on the individual and WST but may result in legal liability for both. Individuals shall not intrude on other communications by reading another person's electronic mail without a legitimate business need.

### **9.5.2 VIRUS PROTECTION**

CPU's and word processing systems are susceptible to becoming infected by computer viruses that can cause system malfunction and data loss. Strict adherence to the policies and procedures outlined herein will minimize this risk.

- 1) The WST Technology Manager has the responsibility of educating users about malicious software, the risks that it poses, virus symptoms and warning signs, how to use control measures, and procedures to protect themselves and the organization.
- 2) The WST Technology Manager will ensure that all WST-owned computer equipment will have the latest licensed anti-virus software installed to detect any virus threat to the system through e-mail, the disk drive, shared files, Internet usage, etc. In addition, patches for both Internet Explorer and Microsoft Outlook will be installed.
- 3) Control procedures will be initiated to run virus protection scans through the servers on all WST maintained computers and equipment.
- 4) Virus scanning software will be kept current. Each system will be set for automatic installation of updates as needed.
- 5) The WST Technology Manager will also institute procedures to monitor user and software activity to detect signs of attacks, to detect policy violations, and to monitor the overall effectiveness of policies, procedures and controls.
- 6) The WST Technology Manager will also keep up to date on potential virus threats and inform staff as needed.

## **9.6 AUTOMATION DEPARTMENT FUNCTION**

The primary function of the Automation Department at WST is the installation and support of automation and telephone services at the administrative offices, Texoma Workforce centers, and partner agencies, according to their individual contracts or Memorandum of Understanding (MOU) with the Board.

The WST Technology Manager will serve as the designated point of contact for the Texas Workforce Commission and the Health and Human Services Commission on security matters. A back-up contact will also be designated. The names of the local Security Administrator(s) will be provided to the Texas Health and Human Services Commission and the Texas Workforce Commission along with the names of local users, as required. The Technology Manager, or designee, is responsible for granting

computer or systems access pursuant to 9.11 Computerized Information and Systems Access of this policy.

For the purposes of this document, it shall be understood that job duties delegated to the WST Technology Manager can also be performed by anyone designated by the Technology Manager. Therefore, for the purposes of this document, the definition of the WST Technology Manager is understood to be "WST Technology Manager, or designee."

Additional functions are outlined below and are not all-inclusive and may be modified by management as the need arises.

### **9.6.1 UPGRADE EXISTING SYSTEMS**

The WST Technology Manager is responsible for recommending and implementing cost saving measures in both automation and telephone services for all Board and Workforce Center functions. Recommendations will be made to the Board Director and purchased as funds allow. Hardware and software procurement and acquisition will be accomplished in accordance with the WST Procurement (WST P&P Ch 2) and Fiscal Accounting System (WST P&P Ch 1) Policies and Procedures. The WST Technology Manager's expertise may be utilized to prepare technical purchase requisition specifications as needed.

### **9.6.2 DAILY PROCEDURES**

The WST Technology Manager is responsible for ensuring on a daily basis that all automated systems are functional and accessible to Board and contractor staff. The following is a daily list of operations that will be completed by the WST Technology Manager:

- 1) Ensure the backup was done overnight. Please refer to "Automation Backup Procedures," Section 9.7.
- 2) Ensure the network is operational and all servers are running.
- 3) Ensure that the routers are working properly.
- 4) Ensure latest virus definition files have been updated.
  - a) Right click on McAfee Anti-Virus logo and check for latest definition files.
  - b) Ensure downloads have been deployed on the servers/workstations using automated procedures.

### **9.6.3 MAINTENANCE**

The WST Technology Manager is responsible for the maintenance and care of all technology equipment. The following maintenance activities will be performed on an "as needed" basis:

- 1) Installation of hardware and upgrades.
- 2) Installation of software and upgrades.
- 3) Monitoring of hardware performance in an effort to anticipate problems.
- 4) Relocation of automation equipment.
- 5) Working with appropriate vendors to resolve hardware/software problems.
- 6) Perform any other routine maintenance as needed to automation equipment to ensure good working order.
- 7) Provide WST, Contractor, and partner agency staff with necessary training to perform routine maintenance on personal computer equipment.
- 8) Assist WST staff in inventory tracking, monitoring, and tagging.

#### **9.6.4 BOARD, CONTRACTOR, TWC, AND PARTNER STAFF USER ACCESS**

The WST Technology Manager is responsible for requesting access from TWC and assigning computer access required to access TWC and other systems. See 9.11.2 below for information related to systems access and required paperwork.

### **9.7 AUTOMATION BACKUP PROCEDURES**

Backups are performed nightly for the following areas/programs:

- 1) WST administrative departments.
- 2) Contractors and the programs they operate.

#### **9.7.1 TEXOMA CCS / GRAYSON WFC BACKUP PROCEDURES**

- 1) Servers are located at 2415 S. Austin Blvd, Denison, TX, in the Computer Room. Outlying offices in Bonham and Gainesville are

mapped to the Grayson WFC server. Staff in these offices saves all pertinent data to the Grayson WFC server for back-up purposes.

- 2) Server name is "Texoma" and type is a Dell PowerEdge 6400.
- 3) A full, automated backup of all data files is performed nightly.
- 4) The daily backup log generated by Backup Exec. is checked to ensure the success of the backup.
- 5) The back-up tapes are rotated on a five-day back-up cycle.
- 6) After backup is confirmed, backup tape is removed from drive and appropriate tape is inserted for the current nightly backup.
  - b) On Fridays, tape backup is archived off-site to the Board Offices and placed in the fireproof strong box located in the Technology Manager's office.
  - c) Adaptec software is used to copy the following folders on the Grayson WFC Server:
    - (1) Forms Folder
    - (2) Policies and Procedures
    - (3) Workers Folder
    - (4) CCS Folder under the SYS Directory

### **9.7.2 WST OFFICE BACKUP PROCEDURES**

- 1) Server is located at 5904 Texoma Parkway, Sherman, TX, in the Server Room.
- 2) Server name is "Texoma 25" and it is a Dell PowerEdge 6400.
- 3) A full, automated backup of all data files is performed nightly.
- 4) The daily backup log generated by Backup Exec. is checked to ensure the success of the backup.
- 5) The tapes are rotated on a five-day backup cycle.
- 6) After backup is confirmed, backup tape is removed from drive and appropriate tape is inserted for the current nightly backup.

- 7) On Fridays, tape backup is archived off-site at the Denison Workforce Center and placed in the fireproof safe located in the Computer Room.

## **9.8 DATA INTEGRITY PROCEDURES**

In order to maintain data integrity, the WST Technology Manager will follow the following procedures:

- 1) All data in the Computer Rooms in the form of tape or in the servers are not accessible to the general public or unauthorized personnel.
- 2) All data that is taken off-site is immediately stored in a fireproof strongbox or safe.
- 3) Only authorized personnel are allowed in the Computer Rooms. The Computer Room at the Grayson WFC will remain locked when Technology Manager or designee is not present. Authorized personnel include the Technology Manager, or designee. In the event both are unavailable, systems support staff working for WST will have access to the servers in order to serve as backup.
- 4) Both Share and NTFS level security is implemented in order to prevent system misuse.

## **9.9 DISASTER RECOVERY PROCEDURES**

The WST Disaster Recovery procedures are to be enacted in the event of a natural disaster to the Board's automated information systems. Data and software essential to the continued operation of critical agency functions is backed up. See section 9.7 for backup details. The security controls over the backup resources will be as stringent as the protection required of the primary resources.

WST Computer Users must determine the criticality of data stored on the system and based upon its criticality rating, take appropriate measures to ensure its protection through backup procedures. Servers will be backed up on a daily scheduled basis, but this will not provide for a backup of data contained on users' hard drives. All data being maintained on users' respective systems or data that has been saved to floppy disks will not be protected in the event of a natural disaster. If the data is critical to everyday operations, adequate backup should be scheduled as a routine part of operations. Backups are automatic for information stored on all Servers. Any information contained on users' hard drives or on disks must be transferred nightly to the shared drive in order for back-up operation to function.

## **9.10 SOFTWARE LICENSE AGREEMENTS**

The WST Technology Manager will ensure that software license agreements are strictly adhered to at all times. Proprietary software will not be duplicated, modified, or used on more than one personal computer except as expressly provided for in the manufacturer's license agreement. In order to keep software costs to a minimum, and whenever possible, bulk license agreements will be purchased. In addition, no unlicensed software or freeware may be loaded on any WST equipment without prior approval or authorization.

In accordance with WST Policy & Procedures Chapter 4, Property, all software purchased in excess of \$5,000 will be tagged with a WST Inventory number. The WST Technology Manager will be responsible for ensuring proper storage of WST software disks and licenses in the Board Electrical Room.

## **9.11 COMPUTERIZED INFORMATION AND SYSTEMS ACCESS**

Board, Contractor, TWC, and partner staff managers are responsible for ensuring that access to computerized information and systems is allocated to staff in a manner that is limited to information required to complete assigned job tasks. Management staff should be aware of the responsibilities of the job assigned to each employee and the authority needed by that employee to access the proper computerized information to complete said job assignments. Management staff is responsible for ensuring paperwork is completed correctly, requesting access and terminating access of staff to computerized information and systems and forwarding same to the WST Technology Manager to request or terminate access. Once the Technology Manager is assured that paperwork is completed properly, he/she will either grant or terminate access and forward required paperwork to TWC to request or terminate access, depending on the system access required.

Staff granted access to computerized information and systems are responsible for all data entry and processing completed under his/her User ID. Therefore, staff are responsible for ensuring confidentiality of User ID's and passwords. According to the TWC Agency Security Manual, it is a violation of the Texas Penal Code to use another person's User ID or password.

### **9.11.1 CONFIDENTIALITY OF USER IDS AND PASSWORDS**

Once staff privileges for access to systems have been granted locally or by TWC, the WST Technology Manager will ensure that all necessary hardware and software is installed on user's computer. Once local or TWC approval is received, users will initially receive technical assistance, user ID, and a temporary password from the WST Technology Manager to log onto approved systems. After initial access, staff will be required to create their own, personalized password that must remain confidential. This password is not to be shared with any other individual. If users are concerned that their password has been compromised, a new password should be selected immediately. For additional

information on Confidentiality and Security requirements, see 9.5 of this policy. For information on violations of this policy, please see 9.14.

### **9.11.2 SYSTEM ACCESS FORMS**

WST Technology Manager will be responsible for determining and obtaining security for computer access codes for all users to perform assigned job duties. Board, Contractor, TWC, and partner staff will be required to sign all TWC required paperwork for each respective system/function that is needed to perform each job and forward it to the Technology Manager prior to access being granted. Required, paperwork will be maintained by the Technology Manager. The *CC Automation Security Awareness Training Certificate* may be transmitted electronically since it does not require signatures. All other required forms may be submitted in the following format:

#### **9.11.2.1 ORIGINAL, SIGNED FORMS**

The following original, staff and/or supervisor signed forms, are required to be forwarded to WST:

- a) P-41 TWC Information Security Agreement / P-41B TWC Information Security Agreement for Board Users and Other Users
- b) WST E-Mail/Local Computer Security Acknowledgement
- c) Acknowledgement of Receipt
- d) Security and Privacy Agreement (SPA) from TA Bulletin #135, Attachment 2
- e) Request for User Access to HHSC Systems from TA Bulletin #135, Attachment 4

#### **9.11.2.2 SUPERVISOR-ONLY, SIGNED FORMS**

The following forms requiring supervisor/management-only signatures can be e-mailed with supervisor/management name typed in signature location:

- a) *WST WorkInTexas Access Request*
- b) *WST TWIST Privileges Request*
- c) *CC Local Application Access Request*
- d) *CC BAPA Security Access Request*
- e) *Request for User Access to HHSC Systems*
- f) *Goldmine Access Request*
- g) *WST Automation Systems Access Termination*

Once approval is granted for access, the WST Technology Manager will be responsible for installing all required hardware and software on computers for each appropriate system. The WST Technology Manager is also responsible for

terminating access to technology systems, as requested. Required paperwork is as follows:

### **9.11.2.3 WST AUTOMATION SYSTEMS ACCESS – INDIVIDUAL USER ACCESS TRACKING LOG**

Prior to granting access to any systems, WST must receive an *Individual User Access Tracking Log*. Contractor staff will designate the systems for which Contractor, TWC, and partner staff are requesting access by completing checkboxes in the first column of this form. WST Technology Manager will ensure the completion of the form for WST staff.

This form also identifies the forms required for access to E-Mail, Mainframe RACF System, TWIST, Work<sup>in</sup>Texas, TAMENU, CEI, TIERS, Goldmine, the Child Care Local Application and the Child Care Budget & Payment Applications (BAPA) systems and provides a tracking mechanism for WST Technology Manager to note dates access was granted and/or revoked and by whom. WST Technology Manager will ensure this tracking log, along with each system's required forms, is placed in a file maintained for each individual granted access to any system identified above.

### **9.11.2.4 ACKNOWLEDGEMENT OF RECEIPT**

Board, Contractor, TWC, and partner staff requesting access to any TWC information or automated systems, must sign an *Acknowledgement of Receipt*, pursuant to WD 05-01. This *Acknowledgement of Receipt* verifies that users have read and agree to comply with the Texas Workforce Commission's Information Security Policy and Provisions, Ch 6, of the TWC Security Manual, located on the TWC Intranet at:

<http://intra.twc.state.tx.us/intranet/dp/html/smtoc.html>.

This *Acknowledgement* must be forwarded within 5 working days after employee has been notified of applicable User IDs to the WST Technology Manager who will maintain the original form in a secure location. Said form requires user's signature, printed name and date. This form is required for all Board, Contractor, TWC, and partner staff requesting access to any WST systems.

### **9.11.2.5 TWC P-41 or P-41B**

Any user requesting WST automation equipment and access, including, but not limited to, personal computers, laptops, Internet, E-Mail, Mainframe RACF Systems (TPTX1), THHSC, and TWIST, will be required to complete a *TWC Form P-41 or P-41B (TWC Information System Security Agreement)*. This form is required pursuant to TWC WD 32-06 and the Local Board Master Contract, Section 2, Security Management. It will be completed upon initial request for access as well as updated at-

least on an annual basis. The purpose of the *P-41 or P-41B* is to provide a written acknowledgement that users have received, read, and understand TWC's security policies and procedures and agree to accept personal responsibility for their equipment and information security/confidentiality. Said form requires user's, supervisor's and Information Security Manager's (WST Technology Manager's) signatures and dates. Form *P-41* is issued for different types of users, as follows:

- 1) *Form P-41* is for TWC Employees.
- 2) *Form P-41B* is for WST, Contractor, and Partner Agency Users.

*Again, please note the P-41 is required to be completed on an annual basis.*

#### **9.11.2.6 WORK//MTEXAS ACCESS**

Board, Contractor, TWC, and partner staff who require access to WORK//MTEXAS are required to complete the *WST WORKINTEXAS Access* form. Said form must include Supervisor's signature and date, and the WST Technology Manager's signature and dates entered in CCS System and when user was notified. See 9.11.3, Granting User Access, below for procedures to obtain access.

#### **9.11.2.7 E-MAIL / LOCAL COMPUTER SECURITY ACKNOWLEDGEMENT**

Board, Contractor, TWC, and partner staff who require access to Workforce Texoma/TWC CPUs and E-Mail Systems are required to complete the *E-Mail/Local Computer Security Acknowledgement*. Said form must include user's initials witnessed by user's supervisor initials, and user's and supervisor's signatures and dates. See 9.11.3, Granting User Access, below for procedures to obtain access.

#### **9.11.2.8 WST TWIST PRIVILEGES REQUEST**

Board, Contractor, TWC, and partner staff who require access to the TWC TWIST System are required to complete the *WST TWIST Privileges Request*. Said form must include Supervisor's and WST System Administrator's signatures and dates. See 9.11.3, Granting User Access, below for procedures to obtain access.

#### **9.11.2.9 REQUEST FOR USER ACCESS TO HHSC SYSTEMS**

Board, Contractor, TWC, and partner staff who require access to the Texas Health and Human Services (THHSC) Mainframe (SAVERR, TAMENU, Attorney General, TIERS, Client Eligibility Inquiry (CEI), and TVCC) are required to complete the *Request for User Access to HHSC Systems Form* pursuant to TA Bulletin #135. Said form must include user's supervisor's signature and date, and the WST System Administrator's (WST Technology Manager's) signature and date. In order to receive HHSC access, this form must be accompanied by a completed *Security and Privacy Agreement (SPA) Form*. See 9.11.3, Granting User Access, below and TA Bulletin #135 for procedures to obtain access.

#### **9.11.2.10 HHSC ENTERPRISE ARCHITECTURE & SECURITY MANAGEMENT, SECURITY AND PRIVACY AGREEMENT (SPA)**

Board, Contractor, TWC, and partner staff who require access to the THHSC Mainframe (SAVERR, TAMENU, Attorney General, TIERS, CEI, and TVCC) are required to complete the *HHSC Security and Privacy Agreement (SPA) Form* pursuant to TA Bulletin #135. Said form must include user's signature, printed name, and date. In order to receive HHSC access, this form must be accompanied by a completed *Request for User Access to HHSC Systems*. See 9.11.3, Granting User Access, below for procedures to obtain access.

#### **9.11.2.11 OAG – TWC USER INFORMATION FORM FOR ACCESS TO THE OFFICE OF THE ATTORNEY GENERAL CHILD SUPPORT DIVISION'S (CSD) PORTAL**

Board, Contractor, TWC, and partner staff who require access to the Office of the Attorney General for child support inquiries are required to complete the *TWC User Information Form for Access to the Office of the Attorney General Child Support Division's (CSD) Portal*. Said form must include user's supervisor approval. The WST Technology Manager will e-mail or fax said form to TWC who will grant access to the OAG Child Support Portal. See 9.11.3, Granting User Access, below for procedures to obtain access.

#### **9.11.2.12 CHILD CARE LOCAL APPLICATION & BAPA - SECURITY REQUEST**

Board, Contractor, TWC, and partner staff who require access to the TWC Child Care Local Application and/or BAPA System are required to complete the *Child Care Local Application & BAPA Security Request*. Said form must include user's supervisor signature and date, and the WST Technology Manager's signature and dates entered in CCS System and when user was

notified. See 9.11.3, Granting User Access, below for procedures to obtain access.

### **9.11.2.13 AUTOMATION SYSTEM ACCESS TERMINATION**

In the event of a user's voluntary or involuntary termination from employment, Management staff is required to completed *Automation Systems Access Termination* and forward it to the WST Technology Manager as soon as employment is terminated.. The *Systems Access Termination* may also be used to remove a user from access to any system. Said form requires signature of user's supervisor and date. WST Technology Manager will ensure access to all automation systems is terminated within 24 hours of termination date.

### **9.11.2.14 COMMON ACCESS FORMS**

Several forms were created and are required in order to access multiple systems. These forms include:

- a) *WST Automation Systems Access – Individual User Access Tracking Log* (9.11.2.3);
- b) *Acknowledgement of Receipt* (9.11.2.4);
- b) *TWC P-41 and P-41B Form* (9.11.2.5); and
- c) *WST E-Mail/Local Computer Security Acknowledgement Form* (9.11.2.7).

These forms are required for users who need access to WST systems and equipment and must be received by WST prior to granting access to any systems and equipment. See 9.11.2 for information as to which forms provide access to each particular system.

### **9.11.2.15 SYSTEMS ACCESS REPORT FOR OTHER AGENCIES AND COMMUNITY PARTNERS**

Pursuant to WD 32-06, WST will ensure that TWC is notified of all outside agency and workforce center partners who are granted access to TWIST and/or Work//Texas by completing the Systems Access Report for Other Agencies and Community Partners and forwarding same to WST's assigned TWC Contract Manager.

## **9.11.3 GRANTING USER ACCESS**

WST Technology Manager will be responsible for obtaining user access for all approved staff that submits a completed request. WST reserves the right to grant or revoke access based on user's job duties and monitoring of data

information for appropriateness to perform job function. All requests must have supervisory approval. Pursuant to WD 32-06, WST will ensure appropriate training is given to any partner staff receiving edit access to customer reporting systems. Procedures for obtaining/granting access are specialized for each system:

### **9.11.3.1 TYPES & RESPONSIBILITIES OF USERS**

#### **9.11.3.1.1 BOARD, CONTRACTOR, TWC, AND PARTNER STAFF**

Access to the Internet through WST for Board, Contractor, TWC, and Partner Staff is for the purposes of appropriate job-related activities. Files and applications from outside WST sources, such as the Internet, are subject to the security requirements contained herein. Software may not be downloaded and installed on local computers or networks without prior authorization of the WST Technology Manager. For information on violations of this policy, see Data Security / Automation Violations, Section 9.14 below.

Internet access is granted locally. The WST Technology Manager will ensure Board, Contractor, TWC, and partner staff who require Internet access for work-related activities are granted said access upon completion and forwarding of a *WST E-Mail/Local Computer Security Acknowledgement*, an *Acknowledgement of Receipt*, and appropriate *P-41 or P-41B Form*.

#### **9.11.3.1.2 WORKFORCE CENTER RESOURCE ROOM**

Access to the Internet through WST Workforce Center by customers using the Resource Room equipment, will solely be used for the purpose of appropriate job-search activities. The WST Technology Manager will ensure computers in all WST Workforce Center Resource Rooms are equipped with Internet Access to allow customers to conduct job-search related business. For information on violations of this policy, see Data Security / Automation Violations, Section 9.14 below.

### **9.11.3.2 ELECTRONIC MAIL (E-MAIL) ACCESS**

WST uses the TWC system for E-Mail purposes. All Board, Contractor, TWC, and partner staff who are granted access to use the e-mail system need to be aware that all e-mail sent or received is the sole property of

the Texas Workforce Commission and the State of Texas and is, therefore, subject to inspection by TWC staff at any time. In addition, the WST reserves the right to monitor and inspect any e-mail transmissions at any time. All e-mail transmissions should be work-related, and all confidentiality standards apply. Refer to 9.5.1, Electronic Mail Confidentiality, of this policy for additional information.

Requests for e-mail access are forwarded to TWC for approval. Using the approved TWC spreadsheet, the WST Technology Manager will request access to the TWC e-mail system for authorized Board, Contractor, TWC, and partner staff who require e-mail for work-related purposes upon being forwarded the following forms:

- a) *WST Automation Systems Access – Individual User Access Tracking Log*
- b) *TWC P-41 or P-41B*
- c) *E-Mail/Local Computer Security Acknowledgement.*

The *Acknowledgement of Receipt* must be completed and forwarded to the WST Technology Manager within 5 days of accesses being granted.

The WST Technology Manager will retain original request forms and liaison with user to ensure logon identification and technical assistance is provided to gain entry into the system.

### **9.11.3.3 TWIST ACCESS**

The Workforce Information System of Texas (TWIST) is an automated system created and maintained by the TWC. Its purpose is to gather, track, and report customer data for individuals enrolled in the State of Texas workforce-related programs.

TWIST access is granted locally. TWIST access will be granted to only the sections necessary for the user to perform essential job duties and individuals will be limited to “read only” or “edit” as required to perform those job duties. Pursuant to WD 32-06, TWIST Web Reports access will not be granted to Workforce Center partner staff. All Board, Contractor, TWC, and partner staff who require access for job-related purposes will be granted specific data entry rights in the TWIST system upon completion and forwarding to the WST Technology Manager the following forms:

- a) *WST Automation Systems Access – Individual User Access Tracking Log*
- b) *P-41 or 41B*
- c) *E-Mail/Local Computer Security Acknowledgement*

d) *TWIST Functional Area Privileges Request.*

The *Acknowledgement of Receipt* must be completed and forwarded to the WST Technology Manager within 5 days of accesses being granted.

The WST Technology Manager will retain original request forms and liaison with user to ensure logon identification and technical assistance is provided to gain entry into the system.

#### **9.11.3.4 WORK//MTEXAS**

WORK//MTEXAS is a live Internet based system and access is granted locally. WORK//MTEXAS access permission levels are limited to "Staff Access" which allows staff to 'View' job seeker, employer, and staff information, and "Edit" which allows staff to change information in WORK//MTEXAS. Permissions in WORK//MTEXAS are to be granted according to the specific, assigned job duties for said staff/partners. All Board, Contractor, TWC, and partner staff who require access for business-related purposes will be granted access to the WORK//MTEXAS systems upon completion and forwarding to the WST Technology Manager the following forms:

- a) *WST Automation Systems Access – Individual User Access Tracking Log*
- b) *P-41*
- c) *E-Mail/Local Computer Security Acknowledgement.*

The *Acknowledgement of Receipt* must be completed and forwarded to the WST Technology Manager within 5 days of accesses being granted.

The WST Technology Manager will retain original request forms and liaison with user to ensure logon identification and technical assistance is provided to gain entry into the system.

#### **9.11.3.5 TWC MAINFRAME RACF ACCESS**

Mainframe RACF access to utilize the TWC Intranet and the Job Search Matching System (JSMS) will be granted to staff to assist job seeker and employer customers in employment-related activities.

TWC Mainframe RACF access is granted locally. All Board, Contractor, TWC, and partner staff who require access for business-related purposes will be granted access to the TWC Mainframe RACF systems upon

completion and forwarding to the WST Technology Manager the following forms:

- a) *WST Automation Systems Access – Individual User Access Tracking Log*
- b) *P-41 or 41B*
- c) *E-Mail/Local Computer Security Acknowledgement.*

The *Acknowledgement of Receipt* must be completed and forwarded to the WST Technology Manager within 5 days of accesses being granted.

The WST Technology Manager will retain original request forms and liaison with user to ensure logon identification and technical assistance is provided to gain entry into the system.

### **9.11.3.6 TEXAS DEPARTMENT OF HUMAN SERVICES ACCESS**

HHSC systems access, (SAVERR, TAMENU, Attorney General, TIERS, CEI, and TVCC systems) will be requested for staff who have a business-related need for those systems to assist customers in their job-search or child-care needs.

HHSC access is granted through request to TWC by the WST Technology Manager upon receipt of completed forms:

- a) *WST Automation Systems Access – Individual User Access Tracking Log*
- b) *P-41 or 41B*
- c) *E-Mail/Local Computer Security Acknowledgement*
- d) *Security and Privacy Agreement (SPA)*
- e) *Request for User Access to HHSC Systems*

The *Acknowledgement of Receipt* must be completed and forwarded to the WST Technology Manager within 5 days of accesses being granted.

The WST Technology Manager will retain original request forms and liaison with user to ensure logon identification and technical assistance is provided to gain entry into the system.

### **9.11.3.7 TIERS**

HHSC systems access, for TIERS will be requested for staff who have a business-related need for those systems to assist customers in their job-search or child-care needs.

HHSC access is granted through request to TWC by the WST Technology Manager upon receipt of the following completed forms:

- a) *WST Automation Systems Access – Individual User Access Tracking Log*
- b) *P-41 or 41B*
- c) *E-Mail/Local Computer Security Acknowledgement*
- d) *Security and Privacy Agreement (SPA)*
- e) *Request for User Access to HHSC Systems*

The *Acknowledgement of Receipt* must be completed and forwarded to the WST Technology Manager within 5 days of accesses being granted.

The WST Technology Manager will retain original request forms and liaison with user to ensure logon identification and technical assistance is provided to gain entry into the system.

### **9.11.3.8 CHILD CARE MANAGEMENT SYSTEM ACCESS**

#### **9.11.3.8.1 LOCAL APPLICATION**

The TWC Child Care System Local Application contains all childcare customer, provider, and claim information. Access to the Child Care Local Application system is granted locally. The WST Child Care Program Manager will grant appropriate data entry rights to staff who have a business-related need for this system upon receipt of the following completed forms:

- a) *WST Automation Systems Access – Individual User Access Tracking Log*
- b) *P-41 or 41B*
- c) *E-Mail/Local Computer Security Acknowledgement*
- d) *Child Care Local Application & BAPA Security Request*

The *Acknowledgement of Receipt* must be completed and forwarded to the WST Technology Manager within 5 days of accesses being granted.

The WST Child Care Program Manager will serve as liaison with user to ensure logon identification and technical assistance is provided to gain entry into the system. The WST Technology Manager will retain original request forms.

#### **9.11.3.8.2 BUDGET AND PAYMENT APPLICATION**

## **(BAPA)**

The Child Care System Budget and Payment Application System (BAPA) contains all financial information connected with billing and payment of childcare services.

BAPA access is granted by TWC. The WST Child Care Program Manager will request appropriate data entry rights for staff who have a business-related need for this system upon receipt of the following completed forms:

- a) *WST Automation Systems Access – Individual User Access Tracking Log*
- b) *P-41 or 41B*
- c) *E-Mail/Local Computer Security Acknowledgement*
- d) *Child Care Local Application & BAPA Security Request*

The *Acknowledgement of Receipt* must be completed and forwarded to the WST Technology Manager within 5 days of accesses being granted.

The WST Child Care Program Manager will serve as liaison with user to ensure logon identification and technical assistance is provided to gain entry into the system. The WST Technology Manager will retain original request forms.

### **9.11.3.9 USERS OUTSIDE THE WORKFORCE SOLUTIONS TEXOMA SYSTEM**

#### **9.11.3.9.1 DEFINITION OF “OUTSIDE USER”**

For the purpose of this policy, “Outside User” is defined as anyone not employed by the Texoma Workforce Development Board, or the Board’s One Stop Contractor. This includes “System” Partners as defined in the Texoma Workforce Development Board Fee for Services Policy.

#### **9.11.3.9.2 DEFINITION OF THE WORKFORCE SOLUTIONS TEXOMA TECHNOLOGY NETWORK**

The Workforce Solutions Technology Network includes all:

- Desktop Personal Computers,
- Laptop Personal Computers,
- Printers,
- Electronic Projectors,
- Local Area Network (LAN), or
- Servers

### **9.11.3.9.3 USE OF WORKFORCE SOLUTIONS TEXOMA TECHNOLOGY EQUIPMENT**

Workforce Solutions Texoma maintains up-to-date technology equipment and offers the use of that equipment to individuals and organizations who are working in one or more of the Workforce Solutions Texoma Workforce Centers.

In order to receive permission to use Workforce Solutions Texoma Technology Equipment, Outside Users must:

- Complete the Workforce Solutions Texoma Room / Equipment Usage Agreement and indicate they are requesting access,
- Complete a Workforce Solutions Texoma Technology Access Request for Users Outside the Workforce Solutions Texoma System indicating what type of access they will need, and
- Provide at least 24 hours advance notice.

### **9.11.3.9.4 DEFINITION OF ACCESS TO THE WORKFORCE SOLUTIONS TEXOMA TECHNOLOGY NETWORK**

Access Includes:

- Attaching a laptop computer of any kind, not owned and controlled by Workforce Solutions Texoma to the Workforce Solutions Local Area Network (LAN) by means of a network cable, or a wireless network connection, or
- Inserting a temporary storage device of any kind including floppy discs, compact discs (CD's), portable flash drives, or any other portable memory storage device into any Workforce Solutions Texoma Desktop or Laptop Personal Computer.

### **9.11.3.9.5 RECEIVING PERMISSION TO ACCESS THE WORKFORCE SOLUTIONS TEXOMA TECHNOLOGY NETWORK**

Workforce Solutions Texoma prefers Outside Users utilize technology equipment already in place, however outside equipment may be used with proper prior permission. In order to receive permission to attach outside equipment or access the Workforce Solutions Texoma Technology Network, Outside Users must:

- Complete the Workforce Solutions Texoma Room / Equipment Usage Agreement and indicate they are requesting access,
- Complete a Workforce Solutions Texoma Technology Access Request for Users Outside the Workforce Solutions Texoma System indicating what type of access they will need,

- Provide at least 24 hours advance notice, and
- Allow Workforce Solutions Texoma Information Technology Personnel to inspect any outside laptop computer or external storage device, or software, including performing virus scan and other diagnostic tests to prevent damage to the Workforce Solutions Texoma Network.

Upon completion of a virus scan and/or other diagnostic tests, Workforce Solutions Texoma Information Technology Personnel will provide written notification regarding whether permission for the equipment, storage device, or software to be attached to the Workforce Solutions Texoma Technology Network is granted or denied.

Attaching laptop computers to Workforce Solutions Texoma's computer network or projectors, or loading outside software or applications on Workforce Solutions Texoma's network will be done only by Workforce Solutions Texoma personnel

#### **9.11.3.9.6 REPEATED ACCESS TO THE WORKFORCE SOLUTIONS TEXOMA TECHNOLOGY NETWORK**

Each occurrence of access to the Workforce Solutions Technology Network will be treated separately. Once connected to the Workforce Solutions Texoma Technology Network, if any equipment, storage device, or software is disconnected, it must be submitted to the Workforce Solutions Information Technology Staff for thorough virus scan and diagnostic testing before being re-connected.

#### **9.11.3.9.7 ACCESSING THE WORKFORCE SOLUTIONS TEXOMA TECHNOLOGY NETWORK WITHOUT PERMISSION**

Attaching any type of equipment, storage device, or software to any Workforce Solutions Texoma desktop or laptop computer or network, without the express written consent of Workforce Solutions Texoma Information Technology personnel will constitute a violation of this policy and may result in organizational, civil, or criminal action and/or the termination of my relationship, or the relationship of my organization, with Workforce Solutions Texoma including permanent exclusion from the Workforce Solutions Texoma Technology System.

#### **9.11.3.9.8 LIABILITY**

Outside users are liable for any damages caused to Workforce Solutions Texoma Technology Equipment or Network, including, but not limited to:

- Damage to any computer, printer, projector, or other piece of equipment due to misuse, neglect, malicious intent, or negligence during their use of said equipment, or
- Damage to any part of Workforce Solutions Texoma's Local Area Network including equipment or files due to misuse, neglect, malicious intent or negligence during their use of said network. All outside users of Workforce Solutions Texoma Technology Equipment or Network must be informed of this policy in writing and must sign acknowledging their receipt, understanding of, and agreement with, this policy prior to being granted permission to use Workforce Solutions Texoma Technology Equipment or Network.

## **9.12 REPORTING INFORMATION SECURITY EQUIPMENT PROBLEMS**

### **9.12.1 SERIOUS INFORMATION SECURITY PROBLEMS**

Any user that discovers a possible information security problem should immediately notify their supervisor/manager, who will immediately notify the WST Technology Manager or designee by phone call if the problem involves a security threat to the system. See WST 9.4 and 9.5. Some instances where these types of problems may occur involve users accessing restricted computer functions/systems without proper authorization or potential virus threats. The WST Technology Manager will act on these issues immediately in order to protect WST and TWC systems from further exposure/risk.

### **9.12.2 PROBLEMS INVOLVING PASSWORDS / USER IDS**

Users who forget their passwords, have a password that is expired, or whose User ID has been revoked, should immediately contact their supervisor/manager. The supervisor/manager will then e-mail the WST Technology Manager or designee with notification of issue. If possible, the problem will be resolved at the local level, i.e., re-setting a TWIST password. If the problem cannot be resolved at the local level, the Technology Manager will notify TWC to resolve the problem. Information concerning problem resolution will be communicated back to the user/supervisor/manager via e-mail.

### **9.12.3 PROBLEMS INVOLVING AUTOMATION EQUIPMENT**

Users will report problems involving CPUs or other computer equipment (printer, monitor, keyboard, mouse, hardware, or software), by completing the *Workforce Texoma Technology Problem Report*. This form will be forwarded to the Denison WFC Director or designee who will log in the request and then forward said request to the WST Technology Manager, with a copy of the request being sent to the WST Administrative Assistant. The Administrative Assistant will log in the

problem. After the Technology Manager resolves the issue, he or his designee will notify the WFC Director or designee.

### 9.13 BOARD, CONTRACTOR, TWC, OR PARTNER STAFF USER ACCESS REVOCATION

WST reserves the right to revoke access based on user job duties and monitoring of data information for appropriateness to job function.

#### 9.13.1 VOLUNTARY SEPARATION

If a Board, Contractor, TWC, or partner staff resigns or retires, supervisory staff is responsible for notifying the Board Technology Manager, or designated alternate as noted in the charts below, within one business day by submission of a completed *Automation Systems Access Termination*. Access to all systems must be terminated within 24 hours of staff separation. Automation Systems Access will be terminated by completing and submitting the Automation Systems Access Termination form to the following:

WORKFORCE CENTER CONTRACTOR, PARTNER, AND TWC STAFF			
	Primary	1st Back-Up	2nd Back-Up
WorkInTexas	IWS Systems Support Spec	IWS BSU Team Lead	IWS Performance Analyst
E-Mail	WST Technology Mngr	WST IT Specialist	WST QA Mngr
CC Local Application	WST CC Program Mngr	WST Technology Mngr	WST Admin Asst
Mainframe RACF System	IWS Systems Support Spec	IWS Performance Analyst	IWS BSU Team Lead
TA MENU	WST Technology Mngr	WST IT Specialist	WST QA Mngr
CC BAPA	WST Technology Mngr	WST IT Specialist	WST QA Mngr
CEI	WST Technology Mngr	WST IT Specialist	WST QA Mngr
OAG Portal	WST CC Program Mngr	WST Technology Mngr	WST Admin Asst
TIERS	WST Technology Mngr	WST IT Specialist	WST QA Mngr
TWIST	WST Admin Asst	WST Technology Mngr	WST IT Specialist

WORKFORCE SOLUTIONS TEXOMA BOARD STAFF			
	Primary	1st Back-Up	2nd Back-Up
WorkInTexas	WST Technology Mngr	WST IT Specialist	WST QA Mngr
E-Mail	WST Technology Mngr	WST IT Specialist	WST QA Mngr
CC Local Application	WST CC Program Mngr	WST Technology Mngr	WST Admin Asst
Mainframe RACF System	WST Technology Mngr	IWS Performance Analyst	IWS Systems Support Spec
TA MENU	WST Technology Mngr	IWS IT Specialist	WST QA Mngr
CC BAPA	WST Technology Mngr	IWS IT Specialist	WST QA Mngr
CEI	WST Technology Mngr	IWS IT Specialist	WST QA Mngr

OAG Portal	WST CC Program Mngr	WST Technology Mngr	WST Admin Asst
TIERS	WST Technology Mngr	IWS IT Specialist	WST QA Mngr
TWIST	WST Admin Asst	WST Technology Mngr	WST IT Specialist

### 9.13.2 INVOLUNTARY SEPARATION

If Board, Contractor, TWC, or partner staff is involuntarily separated, i.e., suspension or discharge, the supervisor will notify WST Technology Manager, or designee as noted in the charts in 9.13.1 above, that same day by telephone so that the user access can be revoked immediately. This action will be followed up by submission of a written *Automation Systems Access Termination* within 24 hours to the WST Technology Manager.

## 9.14 DATA SECURITY / AUTOMATION VIOLATIONS

The Board agrees to notify the Texas Workforce Commission immediately if a security violation is detected that involves one of their systems/data, or if the Board has any reason to suspect that the security or integrity of the Texas Workforce Commission or the Health and Human Services Commission data has been or may be compromised in any way. WST also reserves the right to revoke access based on user job duties and monitoring of data information for appropriateness to job function.

The Board will immediately remove access authorization from one or more individuals at any time a security violation occurs. Written notice of removal of access authorization for any individual connected to TWC systems will be submitted to TWC Commission within 10 working days.

Additionally, as directed by WIT Project Team's System Functionality Letter (6/26/09), staff should take all appropriate measures to protect job seeker identity information. This is absolutely essential for maintaining the integrity of system data as WIT interfaces and exchanges data with at least two other systems (UI and TWIST). With the advent of single sign-on and the new UI Auto-Registration feature, staff must be extremely conscientious about verifying that the job seeker requesting a password reset is the same job seeker represented in the account identified in WorkInTexas.com. When attempting to locate or identify a job seeker in WIT, staff should always verify as much information (full spelling of customer's name, date of birth, complete address, phone number, SSN, work experience and education) as possible before acting on any requested changes, updates, or password resets.

### 9.14.1 WST BOARD, CONTRACTOR, TWC, OR PARTNER STAFF SECURITY / AUTOMATION VIOLATIONS

WST automation equipment is to be used for business purposes only, pursuant to 9.5, Confidentiality/Security section of this policy. No automation equipment will be used for personal purposes. No equipment will be used to display pornographic or other sexually oriented material. WST reserves the right to

revoke access based on user job duties and monitoring of data information for appropriateness to job function. In addition, WST Board, Contractor, TWC, or partner staff who are proven to have violated any part of the WST Information Security Systems Policies and Procedures may be faced with disciplinary action, up to and including termination from employment and/or legal action.

#### **9.14.2 GENERAL PUBLIC SECURITY / AUTOMATION VIOLATIONS**

The general public has access to WST automation equipment for job search activities in Resource Rooms provided at all WST Workforce Centers. Automation equipment may consist of personal computers, printers, telephones, fax machines, or copiers. All equipment provided for use in the Resource Rooms is to be used strictly for job search activities. No equipment will be used for personal or individual's private business-related activities. No equipment will be used to display pornographic or other sexually oriented material. In addition, use of computer equipment to access any information over the Internet that is not job-search related is strictly prohibited. Board, Contractor, TWC, or partner staff that observe individuals using WST automated equipment for purposes other than for job-search activities should report same to Workforce Center management staff immediately. Individuals committing such violations will be warned that equipment is to be used for job search activities, and if non-authorized activities continue, the individuals will be asked to leave the Workforce Center. It will be up to Workforce Center management staff to make a determination as to how long said individuals will be restricted from use of equipment.

### **9.15 NETWORK/AUTOMATION SYSTEMS MONITORING**

WST Technology Manager will ensure Network monitoring occurs to ensure data integrity, optimize traffic on the Wide Area Network (WAN), prevent unauthorized downloads, and to prevent unauthorized use of software and equipment. Network monitoring is currently performed through use of several different software packages including:

- a. Red-Hand
- b. Net-Op School

The WST Technology Manager will ensure software is properly installed and provide training to appropriate Board and/or contractor staff to operate network/automation systems monitoring. Routine checks will be performed in the following manner:

#### **9.15.1 WST BOARD, CONTRACTOR, TWC, OR PARTNER STAFF NETWORK / AUTOMATION SYSTEMS MONITORING**

WST Technology Manager has the responsibility of monitoring all WST Board, Contractor, TWC, or partner staff who has access to network/automation systems, software, and equipment. This monitoring will be performed during routine maintenance of equipment, when a potential violation is reported, or when a Manager has cause to suspect that a violation has occurred. Staff will report automation systems violations immediately to management staff who will, in turn, report same to the WST Technology Manager and Executive Director. Once it has been determined that policy violations have occurred, the Executive Director will work with the Workforce Center's Director or supervisory entity to suggest what disciplinary action will be taken.

### **9.15.2 WORKFORCE CENTER CUSTOMER / GENERAL PUBLIC NETWORK / AUTOMATION SYSTEMS MONITORING**

The Workforce Center Contractor is responsible for monitoring customer, general public technology, and equipment usage in all Workforce Center Resource Rooms. The WST Technology Manager will provide training to designated staff to ensure ease-of-use of software to conduct this monitoring. The Workforce Center Contractor will develop procedures that will detail the appropriate chain of command and procedures for reporting any unauthorized use of equipment or software violations. Monitoring of Resource Room equipment and software will occur on a random basis throughout the time frame Resource Rooms are in operation. The Workforce Center Systems Director, or designee, has the right to ask any individual to leave the premises in the event of automation systems violations. In addition, the Workforce Center Contractor will ensure that signs will be posted in all Resource Rooms advising customers that equipment is to be used for the purpose of job search activities only, that activities may be monitored, and individuals who are in violation of this policy may be asked to vacate the premises and/or be restricted from computer access.

### **9.16 RECORDS RETENTION**

WST will ensure that systems access records and associated forms, including the yearly required *P-41* or *P-41B* forms, are maintained for each person granted access for at least three years after the forms' dates.

#### **References:**

Texas Workforce Commission's Security Manual Located at:

<http://intra.twc.state.tx.us/intranet/dp/html/smtoc.html>

Texas Workforce Commission Federal Regulations 20 CFR 603

WD Letter 02-01, Dated February 1, 2001

WD Letter 05-01, Dated February 22, 2001

WD Letter 01-04, Dated January 26, 2004

WD Letter 09-04, Dated February 2, 2004

WD 32-06 – dated May 22, 2006 - Access and Security in The Workforce Information

System of Texas and WorkInTexas.com  
TA Bulletin #135, Dated November 8, 2006  
Texas Open Records Act  
Human Resources Code Sec. 12.003

WD Letter 19-07, Dated March 7, 2007

[WorkInTexas.com Project Team System Functionality Letter, 6/9/09](#)

WST Automation/Computer Access Forms

- Acknowledgement of Receipt 3.07
- CC Local Application/BAPA Request 1.05
- E-Mail.Local Computer Acknowledgement 10.04
- HHSC Systems Access Form 11.06
- Individual User Access Tracking Log 1.05
- P-41 TWC Information Resources Usage Agreement 10.07
- Systems Access Termination Form 2.08
- TWC OAG Portal Access Request Form
- TWIST Privileges Request Form 1.06
- WorkInTexas Access Form 1.06