PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION POLICY and PROCEDURES

Revision 4 June 21, 2018

(6-18)

TABLE OF CONTENTS

1.00. GENERAL

1.00. **References:** USDOL TEGL 39-11, dated June 28, 2012; The Workforce Investment and Opportunity Act; The Privacy Act of 1974 as amended; WD Letter 13-08 dated April 1, 2008; WD Letter 13-13, dated April 2, 2013, and WD Letter 17-07 dated January 26, 2018

1.02. **Background:** Workforce customers have the right to control the use of their personal information and to expect that it will be protected from identity theft or other personal harm through indiscriminate use or release of this information. Workforce employees have the ethical and professional responsibility to protect this right consistent with the laws or regulations governing grants or programs. This manual outlines policy for handling and security of Personally Identifiable Information (PII) required by activities, grants, and programs administered by Workforce Solutions of Central Texas (WSCT). Changes and additions from previous policy are printed in red.

1.03**. Disclaimer:** Policies, procedures, and/or benefits summarized in this and all other WSCT policy and procedures manuals and policy letters are not contractual in nature. Workforce Solutions of Central Texas reserves the right to change, modify, add, or delete any policy at any time with or without prior employee or customer notification or approval.

2.00 KEY DEFINITIONS

2.01. **Personally Identifiable Information (PII)**: Information that can be used to distinguish or trace a person's identity, either alone or when combined with other personal or identifying information that can be linked to that person. This includes, but is not limited to:

- 2.01.01.Social Security Numbers (SSN), credit card numbers, bank account numbers, home phone numbers, age, birth dates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voice prints, iris scans, etc.) medical history, financial information, unemployment benefits information and status, and computer passwords.

- 2.01.02. Also included is information about persons with disabilities as relates to the disability itself and any information about the medical facts surrounding the disability.

2.02. **Sensitive Information:** Information whose loss, misuse, or unauthorized access to, or modification of, might adversely affect the interest or conduct of funded programs or the privacy to which persons are entitled. It is stand-alone and not necessarily linked or closely associated with PII but could have adverse consequences if released. Examples include, but are not limited to, first and last names, e-mail addresses, business addresses and phone numbers, general education credentials, past and current wage information, unemployment benefit information, and gender or race.

2.03. **Protected Sensitive Information:** Information gathered through the application and case management process not included above is generally considered to be sensitive and may be protected PII. This may include, but not limited to, photo-copies of ID or drivers' license, support services eligibility forms, names, and addresses of family members/friends.

3.00 WSCT CUSTOMER INFORMATION

3.01. **WSCT Disclosure Form:** To inform customers of their right to confidentiality and of the use and safeguarding of personal information, the WSCT Information Disclosure Form will be provided to, and signed by, the customer upon entry into a WSCT-administered grant, program, or activity where protected information is obtained from the individual.

3.02.**Exceptions:** PII is generally protected from indiscriminate release without customer approval and written release, however PII may be provided to appropriate authorities in the following situations regardless of customer wishes:

- 3.02.01. When information received by workforce staff indicates a clear and imminent danger to the customer or to others. In this case, the local Workforce Administrator will decide the action to be taken.

- 3.02.02.When requested by a court of law or others under process of law. All such requests for information will be referred immediately to the Central Texas Workforce Board open records contact person.

- 3.02.03. When requested by state, federal, or internal auditors, investigators, or monitors

- 3.02.04. When requested under the Open Records Act. These requests will be referred to the Central Texas Workforce Board open records contact person.

- 3.02.05. When required by first aid or safety personnel with a need for access during an emergency, medical information or information related to a customer disability may be provided.

3.03. **Filing, Storage, and Disposal of Information:** Customer information must be stored in a manner that ensures confidentiality. PII is normally found in a customer file stored locally and/or in a computer system such as TWIST, Work-in-Texas, etc.

- 3.03.01. Information subject to privacy, including information placed into TWIST or other computer systems shall not be placed or downloaded into unencrypted portable external storage devices such as smart phones, thumb drives, i-pads, home computers, or any other device where the information may be observed or stolen by unauthorized persons.

- 3.03.02. PII and sensitive information contained in paper files shall be stored in a place that is physically safe from unauthorized access. Accessing, storing, and processing of PII data on private, personally-owned drives, computers, storage, or other devices and equipment, or at off-site locations is prohibited unless expressly permitted by TWC Information and Security Guidelines.

- 3.03.03. If permitted by TWC or in very isolated cases where it is absolutely necessary to download information into a storage device, employees may transfer information if the device is provided either by TWC or WSCT Information Technology (IT) and the device is protected with encryption installed by TWC or WSCT IT staff.

- 03.03.04. **Disposal:** Paper documents and files not being retained and containing PII and sensitive information will be disposed of by in-house shredding or use of a collection/disposal service that guarantees destruction of documents. Documents earmarked for destruction will not be placed in unsecure locations such as boxes or trash cans. PII and sensitive information contained in computers or other electronic devices will be deleted as applicable.

3.04. **Processing of Files or Documents Containing PII for Off-Site Movement:** It is essential that the security of files and documents containing PII be maintained.

- 3.04.01 **Key Definitions:**

  a. **Responsible Custodian:** The person who keeps the files, places information into them, and is responsible for them on a daily basis, usually a Case Manager or supervisor.

  b. **Containers:** Depending on the number, size, and types of files, the container may be envelopes or in the case of large quantities, a standard file box with a lid.

- 3.04.02. **Movement Requirements:** When files containing PII are moved off-site, the following applies:

  a. A written inventory of the contents (files) will be placed inside the container with the files.

  b. The inventory will include the names of the participants and/or other files in the box and the responsible custodian(s) of the files. Containers will be sealed using tape or other means. File boxes will be sealed to ensure that the lid is secure.

  c. Containers will be labeled on the outside indicating the contents (i.e.; WIOA files, Childcare, Etc.) and the name and location of the designated recipient.

  d. Files will be transported personally by a center employee and not sent via inter-office mail. This employee is responsible for the security of the containers until they are delivered to the designated recipient.

  e. During transit to the new location, the containers will not be placed or stored outside the custody of the delivering employee.

     1. Upon receipt of the files, the designated recipient will ensure that the files listed on the inventory are present and sign the inventory indicating that the contents have been received in their entirety.

2. A Workforce Technician in the office of the designated recipient may sign for the designated recipient in his/her absence. They will assume responsibility for the safe keeping and delivery of the container to the recipient.

3. Missing contents will be noted on the inventory and reported immediately to the supervisor of the responsible custodian who will take immediate action to recover the missing file(s).

4. Unrecoverable missing files will be reported by the supervisor to the responsible custodian's Center Administrator for further action.

3.05. **Release and Sharing of Information:** Most private information may be shared with entities that are authorized to receive this information and have an established need to know.

- 3.05.01. **Media Requests:** Information will not be released upon request from the media. All requests from news media will be referred, without comment, to the Workforce Board Executive Director. WSCT employees will not speak to media representatives on the behalf of WSCT without the express approval of the Executive Director of the Board.

- 3.05.02. **Sharing of Protected Information with Other Agencies and Entities:** A customer release form is provided for use as required. Customer release is generally not required if the requesting agency has access to computer files containing the information (such as TWIST or WIT).

  a. A release may not be required if information is requested by an outside agency such as Health and Human Services, Social Security, etc. that does not have access to the information on TWIST, WIT, etc., and the requested information is required for a customer's participation in, or compliance with, requirements for an activity or program of that entity. In this case a need to know must be established prior to release. Information will be limited to that required for the activity being covered. If in doubt, get a release from the customer. Do not volunteer or provide information that is not specifically asked for.

  b. In the case of schools or other training providers, a release is required.

  c. Information requested by other entities such as churches, commercial enterprises, non-profit service agencies, individuals, etc. will be referred to the open records contact person at the Board office.

- 3.05.03. **Unemployment Benefit Information (UI):** information about a customer's unemployment benefits is protected. WSCT employees shall not disclose UI related information or the fact that a person is receiving these benefits to any person or agency, even if released by the customer. Persons or agencies requesting UI information will be referred to the open records contact person at the Workforce Board.

- 3.05.04. **Wage Records**: Persons allowed to release WSCT wage information are limited to those designated by the Chief Operating Officer. Persons requesting their personal wage records must do so in person at the center and be referred only to the designated staff. Designated staff will ensure that positive identification is made of the person prior to accessing TWC wage records. The printed information will be handed directly to the person and will not be phoned, faxed, mailed, or e-mailed. Other persons or agencies requesting wage information will be directed to the open records contact person at the Workforce Board.

3.06. No WSCT form or sign-in/attendance sheet will request or display the customer's complete social security number or other PII unless it is required by a grant or activity. Forms may include the last 4 digits of the social security number or, in some cases the TWIST ID. This does not apply to eligibility, TWIST, TWC, or other agency forms that may require the entire number.

4.00 PHYSICAL SECURITY OF PROTECTED INFORMATION

4.01. Any customer and administrative paper files and documents kept in WSCT offices will be secured when Case Managers or other responsible staff is out of the office/cubicle or location where the files are located. Employees will ensure that the office door is closed and, if possible, locked. If there is no door or it cannot be locked, the files must be off the desk and secured. The best practice is to have a clean desk when departing for the day, especially in a cubicle environment.

4.02. When the office/cubicle is occupied, files or documents shall not be in plain view except when the customer is present or the employee is working with a file.

4.03. PII and sensitive information should be retained only for the period of time prescribed by law or agency rules, or while needed for official purposes.

4.04. Any employee suspecting a compromise of PII shall report same to their Supervisor immediately who will report it to the Workforce Administrator and the Chief Operating Officer.

5.00 ELECTRONIC SECURITY

5.01. Electronic security of PII includes all information contained in computers, e-mails, Fax, and all other electronic storage/communications devices.

5.02. Unoccupied office/cubicle computers, to include laptops, will be secured either by locking (control-alt-delete, click on lock computer), logging off, or shutting down the computer. Portable storage devices will not be left on a desk or in plain sight.

5.03. Employee computer and software passwords, PIN's, security smartcards, thumb-drives, or any other data or equipment used for customer authentication or identification purposes, encrypted or not, will not be shared with others. The exception is WSCT Information Technology staff when it is necessary to troubleshoot or fix problems.

5.04: Use of laptops with PII stored in them is **prohibited** in off-premises wireless “hot spots” or networks (Starbucks, hotels, etc.). It is permissible to access the WSCT network off-premises using existing secure VPN means installed by WSCT IT staff provided the information is not visible to others. In this case the rules pertaining to office use apply.

5.05. PII shall not be sent by electronic means that is not controlled by WSCT or by state or federal agencies. PII data transmitted in TWIST or other state-hosted information systems is considered secure. Communication of data through WSCT internally-hosted electronic means is considered secure. Unless it is encrypted, e-mail to external sources is not secure.

5.06. PII data will not be transmitted via telephone except to and from the known and identified customer to whom it applies.

5.07. **Loss or Theft of Removable Media:** Loss or theft of removable media (servers, computers, drives, etc.) containing TWC data will be reported to the Chief Operating Officer and the Board Executive Director or designee who will promptly inform TWC of the loss. Official reports from local authorities will also be forwarded to TWC.

6.00 FORMER STAFF

6.01. Supervisors and Workforce Administrators of WSCT and other partner agencies located within WSCT controlled premises will promptly report to IT any employee under their supervision who exits WSCT or who has a change/denial in access status to the Central Texas Workforce electronic system. This shall be done by submitting the Move-Add-Change form to the WSCT IT department.

6.02. **Departures:** Action concerning voluntary departures will be taken so as to delete the user ID from the WSCT system by the end of the workday following departure. Those whose departure is not voluntary (suspension or dismissal) shall have their user ID deleted immediately. On the day of departure or day of denial of access, a completed and signed IS Request Form will be scanned to PCsupport@workforcelink.com. Do not send the form to an individual IT staff person or by FAX or inter-office mail.