



WORKFORCE INNOVATION AND OPPORTUNITY ACT (WIOA)

CONFIDENTIALITY

POLICY/PROCEDURES

Policy Number: Board Policy 6-2025-04-2

 New Policy

 X Revised

Date: June 4, 2025

Subject: Confidentiality of Customer Records and Personal Information

Michelle Burns

Michele Burns
Executive Director
CareerSource Okaloosa Walton

Board Approval

Michelle Crocker

Date: 06/10/2025

Michelle Crocker
Board Chair
CareerSource Okaloosa Walton

(Corrected typo on Page 8, 7/2/2025)



Workforce Innovation and Opportunity Act (WIOA)

Confidentiality of Customer Records and Personal Information

TABLE OF CONTENTS

	<u>Page</u>
PURPOSE	4
BACKGROUND	4
REFERENCES	5
 <u>PART I – POLICY PROVISIONS</u>	
A. EMPLOYMENT AND TRAINING ADMINISTRATION (ETA) GUIDANCE	5
B. REQUIREMENTS	6
C. RECOMMENDATIONS	7
 <u>PART II – CSOW GUIDANCE AND BEST PRACTICES</u>	
A. ONE-STOP SERVICE DELIVERY SYSTEM	8
B. RESOURCE ROOM	8
C. CAREER CENTER ORIENTATION	9
D. E-MAILS	9
E. CASE MANAGEMENT CONFIDENTIALITY TIPS	9

PART III – PUBLIC AND CONFIDENTIAL RECORDS

A. RECORDS MANAGEMENT AND CONFIDENTIALITY	9
B. COMPLIANCE AND MONITORING	10
C. POLICY REVIEW	10

PART IV – OTHER ADMINISTRATIVE FUNCTIONS

A. CONFIDENTIALITY	10
B. SUGGESTIONS FOR CHANGES OR WAIVER	10
C. ACTION REQUIRED	10
D. TRAINING HOURS	11

PART V. – KEY DEFINITIONS

A. DEFINITIONS	11
----------------	----



Workforce Innovation and Opportunity Act (WIOA)

Confidentiality

OF INTEREST TO

This policy applies to all CareerSource Okaloosa Walton employees, subrecipients, contractors, and partners engaged in the handling, storage, retention, and destruction of records and information created or maintained on behalf of CareerSource Okaloosa Walton.

SUBJECT

Confidentiality Of Customer Records and Personal Information

PURPOSE

This policy establishes the guidelines for the maintenance of personnel, client, and other official records of CareerSource Okaloosa Walton in compliance with federal, state, and local laws, including the Workforce Innovation and Opportunity Act (WIOA). It also outlines procedures for the handling and safeguarding of public and confidential records.

BACKGROUND

The Privacy Act of 1974 requires all government agencies -- federal, state and local -- that request Social Security numbers to provide a "disclosure" statement on the form. The statement explains if the customer is required to provide their Social Security number or if it is optional, how the SSN will be used, and under what statutory or other authority the number is requested

Employment and Training Administration (ETA) grantees may have in their possession large quantities of PII relating to their organization and staff, partner organizations individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files and other sources.

Federal agencies are required to take measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including Personally Identifiable Information (PII). As the grantor agency, ETA has provided Training and Employment Guidance Letter (TEGL)39-11 to grantees to notify them of the specific requirements to follow pertaining to the acquisition, handling, and transmission of PII.

In the course of conducting its operations, CareerSource Okaloosa Walton creates, receives, and maintains a wide range of records containing sensitive, confidential, and business-critical information. Proper retention and management of these records are essential to comply with legal and regulatory

requirements, support operational needs, and protect the privacy and confidentiality of individuals and entities associated with the organization. This policy establishes guidelines for secure storage, and appropriate disposal of records, while also ensuring that access to confidential information is restricted and safeguarded from unauthorized use or disclosure.

Rescinded Documents: 1. This policy replaces the Finance portion in the General Policies last updated September 2023. 2. Confidentiality #OS 001	1. Date / Revised: September 2023 2. March 1, 2002
---	--

REFERENCES

- Training And Employment Guidance Letter No. 39-11, Guidance on the Handling and Protection of Personally Identifiable Information (PII).
- Chapter 286, Florida Statutes, Public Business: Miscellaneous Provisions.
- Chapter 119, Florida Statutes, Public Records.
- Subrecipient Agreement, September 1, 2024.

PART I – POLICY PROVISIONS

A. EMPLOYMENT AND TRAINING ADMINISTRATION (ETA) GUIDANCE

1. The Office of Manpower and Budget (OMB) **defines PII** as information that can be used to distinguish or trace an individual's identity either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual
2. The Department of Labor has **defined two types of PII - protected PII and non-sensitive PII**. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.
 - a. **Protected PII** is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.
 - b. *On the other hand, **non-sensitive PII** is information that if disclosed, by itself, could not reasonably be expected to result in personal harm.* Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. ***However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.***

3. To illustrate the connection between non-sensitive *PII* and protected PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. ***However, a name linked to a social security number, a date of birth, and mother's maiden name could result in identity theft.*** This demonstrates why protecting the information of our program participants is so important.
4. **Sensitive Information** is any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

B. REQUIREMENTS

1. Federal law, OMB Guidance, and ETA policies require that PII and other sensitive information be protected. ETA has determined that to ensure ETA compliance with Federal law and regulations, grantees must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with ETA funded grants.
2. Therefore, CareerSource Okaloosa Walton must comply with the following requirements:
 - a. To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. staff must not e-mail unencrypted sensitive PII to any entity.
 - b. ***Staff must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure.*** Staff must maintain such PII in accordance with the ETA standards for information security described in TEGl 39-11 and any updates to such standards provided by ETA.
 - c. Staff shall ensure that any PII used during the performance of their duties has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.
 - d. CareerSource Okaloosa Walton acknowledges that all PII data obtained through their ETA grant shall be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed using grantee issued equipment, managed information technology (IT) services, and designated locations approved by FloridaCommerce.
 - e. Accessing, processing, and storing of ETA grant PII data on personally owned equipment, at off-site locations e.g., employee's home, and non-grantee managed IT services, e.g., Yahoo mail, is strictly prohibited unless approved by FloridaCommerce.
 - f. Staff and other personnel who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and state laws.

Confidentiality of Customer Records and Personal Information
Board Policy 6-2025-04-2
June 4, 2025

- g. Grantees must have their policies and procedures in place under which grantee employees and other personnel, before being granted access to PII acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.
 - h. Grantees must not extract information from data supplied by ETA for any purpose not stated in the grant agreement.
 - i. Access to any PII created by the ETA grant must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.
 - j. All PII data must be processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal or any other means. Data may be downloaded to, or maintained on, mobile or portable devices only if the data are encrypted using NIST validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.
 - k. PII data obtained by the grantee through a request from ETA must not be disclosed to anyone but the individual requestor except as permitted by the Grant Officer.
 - l. Grantees must permit ETA to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the grantee is complying with the confidentiality requirements described above. In accordance with this responsibility, grantees must make records applicable to this Agreement available to authorized persons for the purpose of inspection, review, and/or audit.
 - m. Grantees must retain data received from ETA only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements, if any. Thereafter, the grantee agrees that all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.
3. A grantee's failure to comply with the requirements identified in TEGL 39-11, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the grant, or the imposition of special conditions or restrictions, or such other actions as the Grant Officer may deem necessary to protect the privacy of participants or the integrity of data.

C. RECOMMENDATIONS

- 1. Protected PII is the most sensitive information that you may encounter in the course of your grant work, and it is important that it stays protected. Grantees are required to protect PU when transmitting information but are also required to protect PII and sensitive information when collecting, storing and/or disposing of information as well.
- 2. Outlined below are some recommendations to help protect PII:

- a. Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only.
- b. Whenever possible, ETA recommends the use of unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN.
- c. Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding or using a burn bag) and securely deleting sensitive electronic PII.
- d. Do not leave records containing PII open and unattended.
- e. Store documents containing PII in locked cabinets when not in use.
- f. Immediately report any breach or suspected breach of PII to the FPO responsible for the grant, and to ETA. Information Security at ETA.CSIRT@dol.gov (202) 693-3444, and follow any instructions received from officials of the Department of Labor.

PART II – CSOW GUIDANCE AND BEST PRACTICES

A. ONE-STOP SERVICE DELIVERY SYSTEM

In the unique environment of the One-Stop Service Delivery System, customers encounter service providers representing many different community agencies and organizations. It is important that everyone in the One-Stop system be respectful of the customer's right NOT to be asked to share more personal information than is necessary or to have to repeat personal information repeatedly to different service providers. With that in mind, every effort should be made to develop and implement an integrated system of sharing basic and necessary information.

B. RESOURCE ROOM

- i. Resource Room staff must be aware that all discussions with customers occur in an open area affording little privacy. Staff must be cautious about talking loudly to customers and staff should never discuss customers in the resource room area. Private areas should be available for use for staff/customer discussion when it is appropriate.
- ii. Sign-in sheets ABSOLUTELY MUST NOT request or contain complete social security numbers. This is also true of workshop sign-in sheets or other documents on which customers are asked to provide written identifying information.
- iii. Sign-in sheets should require only information necessary for the purpose for which they are intended. Do not ask for address or telephone information unless it is essential to do so. In most

cases, such information should be obtained and maintained in a more secure environment than on a sign-in sheet that can be seen by anyone coming into the One Stop Center.

C. CAREER CENTER ORIENTATION

During orientations or seminars in which customers may be sharing personal information with the group, the group facilitator needs to set the tone and the groundwork for an understanding that personal information shared in the group should be treated with appropriate sensitivity for privacy. Remember that staff set an example in this regard and should also be aware of potential liability concerns relating to their own discussions with each other regarding career center customers.

D. E-MAILS

Internal and external e-mail containing client information must be handled with utmost care. CareerSource Okaloosa Walton is subject to Florida's Sunshine Laws, therefore any written communication may become a matter of public record. Depending of the nature of the communications, when communicating by e-mail, use customer's initials, rather than names. If clarification is needed, do so via a telephone call or face-to-face conversation. **Do not include social security numbers in e-mails.**

E. CASE MANAGEMENT CONFIDENTIALITY TIPS

1. Customer files are confidential and should never be left in common areas or lying on desks where they can be seen by other customers. Records should be stored in proper filing cabinets. This is also true of other customer records such as log sheets or caseload printouts. Case managers need to be constantly aware of what types of information is visible in their offices that could be viewed by other customers.
2. Social security numbers should be found only in documents on which they are absolutely required and not open to the public. Lists or log sheets on which some identifying information is needed for cross reference purposes, a "last four protocol" should be used in lieu of full social security number.
3. Staff should not maintain unnecessary lists or documents containing social security numbers. Any such documents that are discarded must be shredded. Under no circumstances should staff discard un-shredded documents containing social security numbers.
4. Any request for records, either verbally, written, or by subpoena should be immediately brought to the attention of the Chief Operating Officer, Executive Director or Board staff so that proper handling procedures can be identified.

PART III – PUBLIC AND CONFIDENTIAL RECORDS

A. RECORDS MANAGEMENT AND CONFIDENTIALITY

1. CareerSource Okaloosa Walton ensures the confidentiality and secure storage of all employee and client records:

- a. Medical/disability-related records must be kept separate and confidential.
 - b. Access is limited to necessary management personnel and emergency responders.
 - c. Demographic and equal opportunity data must be used only for lawful and statistical purposes.
2. All public record and subpoena requests must be reviewed and approved by the Executive Director. The FloridaCommerce guidance shall be followed in all matters of confidentiality and public records access. All subrecipients, contractors, and partners must adhere to confidentiality standards via contract or Memoranda of Understanding (MOUs).

B. COMPLIANCE AND MONITORING

CareerSource Okaloosa Walton will regularly monitor record retention and confidentiality practices to ensure compliance with applicable laws and regulations. Subrecipients are required to follow this policy and will be monitored for adherence.

C. POLICY REVIEW

This policy shall be reviewed at least once every two years and updated as necessary to remain compliant with federal, state, and local requirements.

PART IV – OTHER ADMINISTRATIVE FUNCTIONS

A. CONFIDENTIALITY

All data collected as a result of this policy is for official use only, and should only be used in conducting official business. Refer to WFDB Policy Directive OS-001 for more information on the Board's confidentiality policy.

B. SUGGESTIONS FOR CHANGES OR WAIVER

1. Submit request for changes or waivers to this policy to the CareerSource Okaloosa Walton, 109 8th Avenue, Shalimar, Florida 32579, ATTN: Executive Director or Chief Operating Officer. Requests may also be e-mailed to:
 - a. The request for changes must include the suggested change and an explanation of how the change will improve the process.
 - b. Request for waivers must include names, effective dates, case notes relating to the waiver, dollar amounts, etc.; and any other documentation to support the request.

C. ACTION REQUIRED

CSOW staff in Okaloosa and Walton Counties engaged in administering WIOA programs will implement this Local Operating Procedure upon receipt.

D. TRAINING HOURS: One Hour.

PART V. - KEY DEFINITIONS

A. DEFINITIONS

1. **Public Records:** All documents created or received in connection with official business and subject to public inspection under Florida law.
2. **Confidential Records:** Information protected from public disclosure under Florida law, including but not limited to:
 - a. Social Security Numbers.
 - b. Medical Information and Claims.
 - c. Workers' Compensation Medical Records.
 - d. Discrimination Complaint Files (prior to final resolution).
 - e. Sealed Bids or Proposals (until notice of decision).
 - f. Identifying information in Temporary Cash Assistance records.