# Policy

| SECTION: HUMAN RESOURCES | POLICY # | PAGE 1 OF 6 |
|---|---|---|
| TITLE: Handling and Protecting Personal Identifiable Information Policy | EFFECTIVE DATE: TBD | |
| APPROVED BY: | REPLACES: N/A | |

**PURPOSE:** The purpose of this policy is to communicate Worknet Pinellas, Inc dba CareerSource Pinellas commitment to properly handle and protect Personally Identifiable Information and other sensitive information and to describe all associated requirements that are necessary to ensure compliance with federal, state and local laws on this subject.

**BACKGROUND:**

**Department of Labor Guidance:**

On June 28, 2012 the USDOL issued TEGL 39-11 which provided guidance to direct grantees on compliance with requirements of handling and protecting personal identifiable information. The TEGL stated that "agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage and dissemination of sensitive data including personally identifiable information." Personal identifiable information is defined by the USDOL in this TEGL as information that can be used to distinguish or trace an individual's identity and could result in harm to the individual who name or identity is linked to that information. Examples include, but are not limited to, social security numbers, home telephone numbers, ages, birth dates, marital status, spouses or children's names, education history, medical information, financial information, computer passwords, and unemployment compensation claims. USDOL further defines sensitive information as "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."

**State of Florida Guidance:**

The personal identifying information of Temporary Cash Assistance (TCA) recipients (many times referred to as welfare clients) maintained by the Local area Workforce Boards is confidential and exempt from the Florida public records requirements pursuant to section 414.295, F.S. This includes information that identifies a recipient of TCA, a recipient's family or a recipient's household member. Information that identifies a

non-custodial parent is not specifically protected by State of Florida rules but shall be included as protected information by CareerSource.

Section 414.295, F.S., however, does allow for the disclosure of information within and among the partner agencies and their contracted service providers to conduct business related to TCA and other public assistance programs. The law also allows for the disclosure of protected TCA information for investigations related to the administration of Temporary Assistance for Needy Families (TANF) plan and programs. This information may also be shared to conduct business audits or investigations necessary to administer the TANF program(s).

As part of its workforce development and TANF responsibilities, CareerSource enters data, tracks participation, monitors performance and receipt of TANF funded services in various management information systems, such as the One-Stop Service Tracking (OSST) system. CareerSource also collects and has in its possession large quantities of personal identifiable information and sensitive information relating to its customers, both job seekers and employers, and staff. This information is found in customer electronic files, forms, reports, personnel files, job orders, etc. It is therefore incumbent upon CareerSource to develop policies and procedures to properly handle and protect this information.

**POLICY:** This policy is to protect the privacy of all personally identifiable information and sensitive information obtained from customers and/or other individuals through proper handling during collection, storage and dissemination and to protect such information from unauthorized disclosure. All personally identifiable information and sensitive information shall be protected through a combination of measures, including operational safeguards (policy and training), privacy-specific safeguards (procedures for collection and handling such information) and security controls (role-based access control, passwords, use of encrypted emails, etc.)

**APPLICABILITY:** This policy on the handling and protection of personally identifiable information and sensitive information applies to all CareerSource employees, DEO staff located in CareerSource offices, volunteers, interns, training vendors, program contractors and partners that have access to personally identifiable information and/or sensitive information of customers and employers that are or have received any level of services from CareerSource. Throughout this policy, wherever the word “staff” is used it shall mean all individuals listed under this section on “Applicability.”

**RESULTS OF FAILURE TO COMPLY WITH POLICY:** Failure of any individual listed above in “Applicability” to comply with this policy shall result in disciplinary action in accordance with the applicable Personnel Handbook. Failure by a partner agency that is located in a CareerSource facility, training vendor, or a program contractor to comply with this policy may result in termination of any MOU, agreement or contract.

**DEFINITIONS AND DETAILS:** It should be noted that this policy and the following details apply whether staff are working from their desk at the office or at another location. It is the staff’s responsibility and incumbent upon each staff as a custodian of public record data to ensure that any personally identifiable information and/or sensitive

customer information entrusted to them in the course of their work is kept secure and protected.

In general, CareerSource staff, DEO staff located in CareerSource facilities, volunteers, interns, program contractors, and training vendors that have access to personally identifiable information and/or sensitive information of customers and employers that have received or are receiving any level of services from CareerSource are not to

- Collect personally identifiable information and/or sensitive information without proper official authorization to do so.
- Access or review a family member or friend's information of any type within any MIS such as OSST, EFM, Florida MIS, Suntax, Project CONNECT or ATLAS system or access any information on any person or company not directly related to or required to complete assigned job responsibilities.
- Make copies of documents containing personally identifiable information and/or sensitive information unless authorized to do so and it is required to provide services.
- Disseminate or share personally identifiable information and/or sensitive information to others, including other staff, DEO staff located in CareerSource offices, volunteers, interns, program contractors, training vendors and/or partners, unless the release is authorized and there is an official need to know.
- Access, allow access to, and/or use any such information for personal intent or any purpose other than in performance of official CareerSource job duties.
- Place personally identifiable information and/or sensitive information on local drives, shared drives, e-mail folders, multi-access calendars, the CareerSource Intranet, Outlook or the Internet unless it is password protected and/or encrypted.
- Access, process, or store personally identifiable information and/or sensitive information of CareerSource customers and employers on personally owned equipment, a public website or bulletin board.

**A. Commitment to safeguard and properly handle personally identifiable information and/or sensitive information**

Individuals list under "Applicability" above shall commit to respect and safeguard any CareerSource customer's right to privacy by practicing and promoting confidentiality in gathering, recording, storing and/or sharing personally identifiable information and/or sensitive information.

This commitment shall be placed in writing; when a person is hired and annually thereafter, staff will be required to sign a statement of non-disclosure and confidentiality that acknowledges:

- their understanding of the importance of the proper handling and protection of personally identifiable information and/or sensitive information,

- the requirement that they comply with the proper handling and protection of personally identifiable information and/or sensitive information as described in this policy and any future modification of this policy,
- that they have been advised that they may be liable to civil and criminal sanctions for non-compliance,
- that they have been advised of potential for internal disciplinary action for non-compliance.

**B. Access to records containing personally identifiable information and/or sensitive information**

Staff do not all require the same level of access to personally identifiable information and/or sensitive information. The level of access required is determined by the individual's job responsibilities.

- Different levels of privilege/access may be authorized while the staff is working on a particular job, and then withdrawn if the level of access required changes.
- There must be a legitimate business reason or requirement to access a customer's personally identifiable information and/or sensitive information.
- Casual viewing of any individual's personally identifiable information and/or sensitive information, even data that is not confidential or otherwise included in this policy, constitutes misuse of access.
- Computer access is monitored and restricted based on job responsibility to protect personally identifiable information and/or sensitive information.
- Documents are not to be left where members of the general public may see or access them.
- In order to prevent unauthorized access, staff shall log off of all applications that provide access to personally identifiable information and/or sensitive information, or lock their computer when leaving their workstation. This is especially important during breaks and lunch. Unless there is a specific business need, all workstations should be shut down at the end of the workday.
- Staff shall not permit unauthorized access to any personally identifiable information and/or sensitive information in CareerSource's various information system(s) or other custodian records.

Staff should never leave their CareerSource issued laptop or mobile devices such as cellphone or PDA unattended and should always keep their electronic devices in a secure space or secured under lock and key when not in use. Staff should ensure password accountability standards apply to their portable and mobile devices.

**C. Password Accountability**

Regardless of the circumstances, an individual's password(s) gives access to CareerSource's electronic communication systems or the State systems such as OSST, EFM, etc. and must never be shared or revealed to anyone else. To do so exposes the staff to responsibility for actions the other person takes with the password, including the improper handling and protection of personally identifiable information and/or sensitive information. Staff are required to change their password when automatically notified by the MIS system or a minimum of every 90-days.

To prevent unauthorized parties from obtaining access to electronic communications, staff must choose passwords which are difficult to guess (for example, not a dictionary word, not a personal detail, and not a reflection of work activities).

**D. Release of personally identifiable information and/or sensitive information.**

Any requests for release of information shall be processed according to CareerSource's records management procedures. Records containing personally identifiable information and/or sensitive information may not be transferred or released from CareerSource to another agency, individual, the general public or the media without management approval. Care needs to be taken and the correct procedures followed to ensure that any personally identifiable information and/or sensitive information is not released to someone that may not treat the information in the same confidential manner as CareerSource.

Staff shall never give information, especially personally identifiable information and/or sensitive information, to the press or media. If asked, staff should politely decline any such requests and refer the individual to the CareerSource EEO Officer.

This restriction on the release of personally identifiable information and/or sensitive information applies to information in all formats, hard copies, electronic files, etc. as well as a verbal release or sharing of information in person or over the phone.

**E. Use of Email with personally identifiable information and/or sensitive information**

Staff should first review the need or requirement to transmit personally identifiable information and/or sensitive information in an outgoing email. If such information must be transmitted by email, staff should use identifiers such the OSST Customer ID, the EFM State ID, or other identifiers that do not use personally identifiable information and/or sensitive information whenever possible. In addition, staff must follow the guidelines and standards described below:

- The information must be adequately encrypted and password protected with NSIT encryption applied such as using the Barracuda Email filter available within MS Outlook if sent by email outside of CareerSource Pinellas.
- Double check that the correct email address(es) are being used and all recipients have an official "need to know" and authorization to access such information before sending.
- Double check the attachment to make sure the right encrypted document has been selected.

- Set the following warning in the email signature block for all outgoing emails: "This email may contain information subject to the Privacy Act of 1974 and is "For Official Use Only." Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

**F. Use of a printer, copier or fax with personally identifiable information and/or sensitive information**

If a staff must print, copy or transmit personally identifiable information and/or sensitive information through use of a printer, copier or fax machine, staff must

- Verify the printer/fax location prior to sending a document containing personally identifiable information and/or sensitive information.
- Set up and turn on "Locked Print" when sending any document containing personally identifiable information and/or sensitive information to the printer/copier; this will ensure the document does not print until the staff enters his/her password and selects print.
- Avoid use of a fax to transmit documents containing personally identifiable information and/or sensitive information whenever possible. If such information must be faxed, staff must validate the fax number prior to transmitting documents with personally identifiable information and/or sensitive information. Staff should also ensure the receiving fax machine is secured or attendant staff is standing by on the receiving end of the fax. Do not fax personally identifiable information and/or sensitive information to unattended fax machines.

**G. Storage and eventual destruction of records**

Records containing personally identifiable information and/or sensitive information must be correctly stored in a securely locked cabinet or securely locked room and eventually destroyed (in line with legal requirements and the CareerSource Records Management policy) by authorized personnel.

- All records must be stored in a secure, safe area where there is no access by unauthorized persons and limited possibility of damage by pests, vermin or environmental factors.
- Records may be stored only in authorized locations within the building.
- If hard copies of personally identifiable information and/or sensitive information must be transported, it must be done in a safe and confidential manner ensuring that access is only given to authorized staff.
- Records containing personally identifiable information and/or sensitive information should never be stored in a staffs' car or residence.
- Any records or paperwork containing personally identifiable information and/or sensitive information that is no longer needed (for example, the paperwork has been scanned into the CareerSource ATLAS system) shall be placed in the locked bins for shredding.

**H. Medical records and records of domestic violence are subject to HIPAA Act of 1996**

Medical records, disability-related information and information on domestic violence from applicants, registrants, eligible applicants/registrants, participants, terminees, employees, and applicants for employment must be stored in a manner that ensures confidentiality, and must be used only for the purposes of record-keeping and reporting; determining eligibility, where appropriate, for WIOA Title I-financially assisted programs or activities; determining the extent to which the recipient is operating its WIOA Title I-financially assisted program or activity in a nondiscriminatory manner; determining services that must be provided; or other use authorized by law. This information must be stored separately from all other information about a particular individual, and treated as confidential medical or domestic violence records.

Access to customer related disability information, medical information or domestic violence information shall be limited. A separate file containing this information (medical information form, medical documentation, assessment of domestic violence, safety plan, contacts with medical personnel or domestic violence providers, etc.) will be scanned into ATLAS separately and labeled "medical or domestic violence information). MIS will e-file this information into a separate folder/document and then restrict access to the file. No hard copies of the disability-related, medical information or domestic violence information will be kept by any staff.

**I. Reporting a violation of this policy**

It is the individual staff's responsibility to immediately report if he/she has committed a breach of or violated this Policy. Additionally, given the potential harm that CareerSource may suffer with the release of any personally identifiable information and/or sensitive information, all employees are required to report any suspected violation(s) of this policy.

If a staff is asked to divulge personally identifiable information and/or sensitive information about a customer by a person who has no authority to request this, the staff should report the matter to his/her supervisor immediately.

If a staff hears another person discussing personally identifiable information and/or sensitive information in an inappropriate way (e.g., chatting to a colleague in the office or lunchroom, telling friends in a social setting), the staff is required to report the matter to his/her supervisor immediately.

**J. Handling the disclosure of any personally identifiable information and/or sensitive information**

Management will determine how this region will respond to any incident of the disclosure of personally identifiable information and/or sensitive information. Consideration shall be given to determining when and how agencies and individuals should be notified, when and if a breach should be reported publicly, and what future actions should be taken to eliminate the possibility of the same breach in the future, if possible.

**ACTION STEPS REQUIRED:**
Following are the action steps each CareerSource employee, DEO staff located in a CareerSource facility, volunteer, intern, training vendor, program contractors and partners must take.

1. Each individual must review this policy directive. If the individual has a question about anything contained herein, it is his/her responsibility to immediately bring the question to the attention of his/her supervisor. If not resolved, the supervisor will contact the individual named under "Inquiries" below.
2. CareerSource contract managers and appropriate Directors shall provide this policy and any subsequent revisions to all partner agencies located in a CareerSource facility, program contractors and training vendors and require that each submit a letter stating that this policy was provided to all appropriate staff and that they shall abide by this policy.
3. It is the responsibility of each individual to immediately report any breach of this policy to their Director or to the attention of the individual shown under "Inquiries" below.
4. Each supervisor, manager, and director is responsible for informing employees of this policy.
5. Each individual must replace previous policies associated with personal Identifying Information with this policy reissuance.

**POLICY AMENDMENTS OR REVOCATION:**
Notwithstanding any of the foregoing, CareerSource reserves the right to revise or revoke this policy at any time.

This policy is written to establish local procedures and is not intended to supersede any applicable laws or regulations. Failure of CareerSource to adhere strictly to the steps outlined within this policy shall not be construed as a violation of any administrative procedures.

**INQUIRIES:**
Any question about this policy should be directed to the CareerSource HR Business Partner.