The Workforce Connection, Inc.
Policy Title: **Handling and Protecting Personally Identifiable Information (PII)**

Approved: ***06/07/2016***
Effective: ***06/07/2016***
Status: ***Active***

Reference Number: 2016-200-07

Modifications: 06/07/2016
05-2017 Name Change
09/2021- DCEO policy modification

Purpose:
To define the policies and procedures for *Handling and Protecting Personally Identifiable Information* (PII).

References:
- OMB Memorandum M-07-16, Safeguarding Against and Responding to Breach of Personally Identifiable Information (II.A.c.2.j) (May 22, 2007)
- Privacy Act of 1974 - 5 U.S.C. § 552a
- U.S. Department of Labor Employment and Training Administration's Training and Employment Guidance Letter (TGEL) No. 39-11 (June 28, 2012)

Background:
Under the Workforce Innovation and Opportunity Act (WIOA) and Trade Assistance Act (TAA), staff obtains personal and confidential information from individuals as part of eligibility determination and continuation of services. WIOA, TAA, and other federal and state regulations governing information sharing stipulate implementation of confidentiality policies and procedures. It is the responsibility of all workforce professionals to protect the privacy of all applicants for program services, as well as the privacy of all participants receiving program services. The purpose of this policy is to describe the protections that must be in place to protect all personally identifiable information (PII) on applicants and participants including the requirements for the use, storage, and security of sensitive and confidential information, and the consequences for not adhering to these safeguards.

Definitions:
- *PII - Personally Identifiable Information* - 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. DOL has defined two types of PII:
    1. *Protected PII* - information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of 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.

    2. *Non-sensitive PII* - information that if disclosed, by itself, could not reasonably be expected to result in personal harm. It is stand-alone information not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include 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.

- *Sensitive Information* - Any unclassified information whose loss, use, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Federal programs, or privacy to which individuals are entitled under the Privacy Act of 1974.

  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

Handling and Protecting Personally Identifiable Information

1. Any staff who work directly with WIOA and TAA applicants and participants, or who handle or process PII about applicants or participants, must take steps to ensure that PII is processed in a manner that will protect the confidentiality of the records/documents, and that PII is not accessed, viewed, or used by either the general public, or unauthorized staff at partner organizations.
2. Federal and State law, regulations, and the USDOL policies require that PII and other sensitive information be protected. To ensure that PII and sensitive information is handled appropriately, service providers must:
   a. Ensure PII is not transmitted to unauthorized users, and all PII transmitted through email or stored electronically (e.g., DVD or thumb drive) is encrypted as outlined in the Requirements to Protect PII section of this policy.
   b. Take necessary steps to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure.
   c. Ensure that any PII used as part of the WIOA and TAA program administration has been obtained in conformity with applicable Federal and state laws governing confidentiality of information.
   d. Ensure that all PII obtained through the WIOA and TAA grants are stored in an area that is physically safe from Access by unauthorized persons at all times.
   e. Store PII only on secure work servers and Equipment that meet the standards of TEGL 39-11 and any updates to such standards provided by the USDOL. Storing PII on personally owned equipment, at off-site locations (e.g., employee's home), and on personal email accounts is prohibited.
   f. Advise all Local Area and/or provider staff who have access to sensitive/confidential/ proprietary/private data of the confidential nature of the information, the safeguards required to protect the information, and the civil and criminal sanctions for noncompliance with such safeguards.
   g. Implement policies and procedures regarding the handling of PII, including staff acknowledgement of 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 sanction for improper disclosure.

Under the TAA program, if staff discloses data to any unauthorized individual or entity, they may be guilty of a Class B misdemeanor in the State of Illinois and may be required to serve up to six (6) months in jail and pay a fine of up to $1,500 (see Illinois Unemployment Insurance Act (820 ILCS 405/1900, applicable to TAA through 20 CFR 618.852(b))).

Requirements to Protect Personally Identifiable Information

1. 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.

   a. Data may be downloaded to, or maintained on, mobile or portable devices only if the data are encrypted using National Institute of Standards and Technology (NIST) validated software products based on Federal Information Processing Standards (FIPS) 140-2 encryption.

   b. Wage data may only be accessed from secure locations or those off limits to the general public where Access is restricted to authorized employees or contractors, vendors, and delivery personnel who have a

business purpose for being there.
2. WIOA and TAA grantees and service providers should use unique identifiers for Participant tracking instead of the Social Security numbers (SSN). If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to an individual, such as using a truncated or masked SSN (e.g., last 4 digits only).
3. WIOA and TAA Grantee and service providers using an electronic system in addition to the Illinois Workforce Development System (IWDS) for Basic Career Services tracking or other registration processes must truncate or mask an individual's SSN in such systems.
4. WIOA and TAA grantees and service providers using paper applications containing SSNs must, at a minimum, enter the basic Intake information and the SSN in IWDS the day the information is received and destroy the paper application if feasible. If all eligibility information is not placed in IWDS that day, staff must mask the SSN on the paper application and store in a secure manner.
5. Documentation of SSNs (e.g., physical copy of social security card) shall not be obtained until such time WIOA eligibility is determined, the individual receives a WIOA Adult, Dislocated Worker, youth, or TAA program service which triggers participation in the program, and the individual becomes a participant.
6. When an individual becomes a participant, the service provider must attempt to obtain and verify the SSN for performance reporting purposes, but shall not deny access to the American Job Center's (in Illinois, called Illinois workNet® center) resource room or to WIOA or TAA program services if the individual does not disclose his or her SSN. If the individual refuses to provide an SSN, the Local Area will assign a temporary alternative identifying number. The individual will use this number for identification during subsequent visits to the Illinois workNet center or for program-funded activity tracking.
7. WIOA and TAA grantees and service providers should keep SSNs electronically in IWDS minimizing the use of paper files. If paper files are used or if the participant's SSN is listed on other forms of source documentation, the Service Provider must ensure that the SSN on the paper document has been masked (e.g., hiding original data with modified content with characters or other data).

Maintenance and Custody of Records with PII

1. The Office of Employment and Training (OET) requires grantees to maintain records related to the management and administration of the grant sufficient to:
a. Supply information for required monitoring and reporting;
b. Ensure adequate tracking of funding; and
c. Ensure lawful expenditures of funding.

2. All PII shall be stored in a secure environment physically located in the continental United States with Access limited to the least number of staff.
3. User Equipment containing data (servers, routers, hubs, etc.) are to be maintained in secure spaces or those off limits to the general public where access is restricted to authorized employees or contractors, vendors, and delivery personnel who have a business purpose for being there.
4. Individuals who are not employees or contractors may not be present in these spaces unless escorted by authorized personnel.
5. Users shall not leave workstations unattended while accessing the data. Technical or logical controls should be utilized, such as locking the computer or automatic screensavers, so as not to expose the data to unauthorized personnel/passersby.
6. Paper documents containing PII information must be stored securely in locked offices, rooms, cabinets, and/or desks.
7. OET may require the transfer of certain records from the Grantee or service provider if the organization is no longer able to maintain custody of those records.

Retention and Destruction of Records with PII

1. OET requires that records must be retained and stored in a manner that will preserve their integrity and admissibility as evidence in any audit or other proceedings. The burden of production and authentication of the records is the responsibility of the custodian of the records.

2. Electronic Retention of records, including the use of cloud-based storage systems, is allowable, assuming the electronic storage meets all other retention requirements outlined in WIOA, TAA, Uniform Administrative Requirements, WIOA regulations, OET data sharing requirements, and this policy manual.
3. Grantees are to retain records for a period of at least three (3) years after submittal of the final closeout Expenditure report for that funding period to comply with 2 CFR 200.334, unless a different retention period is specified in 2 CFR 200.334, 44 Ill. Admin. Code 7000.430(a) and (b), the applicable Notice of Funding Opportunity (NOFO), or grant agreement. If any litigation, claim, or audit is started before the expiration of the retention period, the records must be retained until all litigation, claims, or audit exceptions involving the records have been resolved and final action taken. Thereafter, the Grantee agrees that all data will be destroyed.
4. WIOA and TAA grantees and service providers must use appropriate methods for destroying sensitive PII in paper files and securely deleting sensitive electronic PII. 4.
5. Acceptable destruction methods for various types of media include:
   a. Paper documents containing sensitive or confidential information (PII/SSN) must be shredded for disposal and are prohibited from being disposed of in the office trash. A contract with a recycling firm to recycle sensitive or confidential documents is acceptable, provided the contract ensures that the confidentiality of the PII will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.
   b. If PII has been stored on server or workstation data hard drives, similar media (e.g. floppies, USB flash drives, portable hard disks, or similar disks), optical discs (e.g., CDs, DVDs, Blu-ray) or magnetic tape , the user shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s) (e.g., by incineration of the disc(s), shredding the discs, or completely defacing the readable surface with a coarse abrasive).

Monitoring of Protection of Personally Identifiable Information

1. TWC will conduct oversight of the implementation of the WIOA Adult, Dislocated Worker, and youth and TAA programs to ensure that participants are eligible for enrolled programs and documentation supporting the eligibility are contained in the case files. The procedures for protecting PII must also be monitored by the local area.
2. Service providers must permit TWC to make on-site inspections during regular business hours for the purpose of conducting monitoring reviews, audits and/or other investigations to assure compliance with the confidentiality requirements. In accordance with this responsibility, services providers must make records available to authorized persons for the purpose of inspection, review, and/or audit.
3. TWC will make available to OET any reports, records, plans, or any other data that is required to be submitted by law, regulation, or policy, or upon official request for as long as the records are retained.

Security Breach Reporting

1. In the event of an unauthorized Access to unauthorized disclosure of, loss of, damage to or inability to account for any PII (a breach), WIOA Grantee and service providers must promptly:
   a. Report such breach to DCEO by telephone with immediate written confirmation sent by email describing in the detail any accessed materials and identifying any individual(s) who may have been involved in such breach;
   b. Take all actions necessary and reasonably requested by DCEO to stop, limit or minimize the breach;
   c. Restore and/or retrieve, as applicable and return all PII that was lost, damaged, accessed, copied, or removed;
   d. Cooperate in all reasonable respects to minimize the damage resulting from the breach;
   e. Provide any notice to Illinois residents as required by 815 ILCS 530/10 or applicable federal law, in consultation with DCEO; and
   f. Cooperate in the preparation of any report related to the breach that DCEO may need to present to any governmental body.
2. Any perceived or suspected breach of PII either electronically or by other means shall be reported

immediately following the procedures outlined in the Incident Reporting section of the policy manual.
3. WIOA and TAA grantees and service providers are required to follow any instructions provided by OET or DOL regarding addressing the breach of PII.

Action Required: This information should be disseminated to all The Workforce Connection, Inc. staff, fiscal agent staff, program service providers, partner agencies, sub-awardees, and contractors.

Inquiries: Questions regarding this policy should be directed to The Workforce Connection, Inc. Executive Director

Effective Date: Immediately