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

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:

Federal and State regulations and policies require local Workforce Boards to implement policies and procedures minimize identify theft of personal identification and other sensitive information of customers served through programs.

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

Policy/Procedures:

Administrative staff and service providers must not e-mail unencrypted sensitive PII to any entity. To ensure PII and other sensitive data is not transmitted to unauthorized users, transmit via e-mail or store on CDs, DVDs, thumb drives, etc., using encrypted files that are Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

In addition to the above requirement, local administrators and service providers must comply with all of the following:

- All PII data obtained through federal or state funded grants/contracts/sub-awards 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 information technology (IT) services at designated locations approved by NIWA. Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations, e.g., employee's home, and non-grantee managed IT services, is strictly prohibited unless approved by the local workforce board.

- Employees and other personnel who will have access to sensitive/confidential or 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 by Federal and state laws.

- Administrators and service providers must acknowledge their understanding of the confidential nature of the data, safeguards, and compliance in handling of sensitive data and that they may be liable to civil and criminal sanctions for improper disclosure.

- Administrators and service providers must not extract information from data supplied by any funding source for any purpose not stated in the grant, contract or sub-award agreement.

- Access to any PII created by federal or state grant, contract or sub-award agreement must be restricted to only those employees of the grant, contract, or sub-award agreement recipient who need it in their official capacity to perform duties in connection with the scope of work.

- All PII data must be processed in a manner that protects confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving 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. NOTE: wage data may only be accessed from secure locations.

- PII data obtained by administrators or service providers through a request from their funder must not be disclosed to anyone but the individual requestor except as permitted by the grant, contract, or sub-award agreement provider.

- Administrators and service providers must make records applicable to Federal/State grants, contracts, and sub-awards available to authorized persons for the purpose of inspection, review, and/or audit.

- Administrators and service providers will retain data received from ETA-funded grants only for the period of time required to use it for assessment and other purposes, or to satisfy applicable local/ state/ Federal records retention requirements, if any.

Failure to comply with requirements identified in this Policy, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination, suspension, or restrictions of the grant, contract, or sub-award, as deemed necessary to protect the privacy of participants or the integrity of data.

Procedures to protect PII:

- Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only.

- When possible, use unique identifiers for participant tracking instead of SSNs. 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.

- Destroy sensitive PII in paper files by depositing in locked shredding bins and securely deleting sensitive electronic PII.

- Do not leave records containing PII open and unattended.

- Store documents containing PII in locked cabinets when not in use.

Reporting a Breach: Any breach or suspected breach of PII will immediately be reported to the funding source administrator responsible for the grant, contract or sub-award. This individual will investigate the breach and, when necessary, report it to State personnel and DOL (Randy Boschutle or Tim Golemo, Illinois Department of Commerce and Economic Development Office of Employment and Training randy.boschulte@illinois.gov-217/558-4755 or tim.bolemo@illinois.gov 217/558-2418) and ETA Information Security at ETA.CSIRT@dol.gov, 202-693-3444). Staff will follow any instructions received from officials of the State or Department of Labor

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