Protection of Personally Identifiable Information (PPII)

POLICY

It is the policy of AJCC to protect personally identifiable information (PII) and other confidential and/or sensitive customer information. This policy and related procedures outline the process for transporting hard-copy PII between AJCC's various office locations. This policy applies to all AJCC staff and AJCC sub-recipient staff.

PROCEDURES

AJCC recognizes the need to maintain the confidentiality of PII. When any hard-copy PII or other confidential and/or sensitive customer information is being transported between AJCC's various office locations, this information must be locked in a secure container provided by AJCC administration.

- Prior to departing from one location to another, all hard-copy PII or other confidential and/or sensitive customer information being transported must be placed in the secure container and locked before leaving the facility.
- The container will remain locked until the staff person arrives at the next location.
- In the event that an AJCC or sub-recipient staff person is no longer employed by the recipient staff person is no longer employed by the organization, the combination lock on the secure container will be reset.

REFERENCE:

U. S. Department of Labor (DOL), Employment and Training Administration (ETA), Training and Employment Guidance Letter (TEGL) 39-11, Guidance on the Handling and Protection of Personally Identifiable Information (PII) (June 28, 2012).

Federal regulations require that PII and other sensitive information be protected. All WIOA funded agencies (including WIOA service providers) must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with WIOA funds and must comply with all of the following:

- To ensure that such PII is not transmitted to unauthorized users and all PII and other sensitive data transmitted via e-mail or stored on Compact Discs (CDs), Digital versatile discs (DVDs), thumb drives, etc., must be encrypted.
- Grantees must maintain such PII in accordance with the ETA standards for information security described in this TEGL and any updates to such standards provided to the grantee by ETA.
- Grantees shall ensure that any PII used during the performance of their grant has been obtained in conformity with applicable federal and state laws.
- Grantees further acknowledge that ll 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 ant that the data will be processed using grantee issued equipment, managed information technology (IT) services and designated location approved byt ETA. Accessing, processing, and storing of TTA grant PII on personally owned equipment, at off-site locations (e.g., employee's home), and non-grantee managed IT services, (e.g., Yahoo, G- Mail), is strictly prohibited unless approved by ETA.
- Grantee employees and other personnel who have access to sensitive/

confidential/propriety/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 state laws.

- 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.
- Grantee must not extract information from data supplies by ETA for any purpose no stated in the grant agreement.
- Access to any PII created by the ETA 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.
- 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.
- PII data obtained by the grantee through a request from ETA must not be disclosed to anyone but the individual requestor.
- Grantee must permit ETA to make onsite inspections to assure that the grantee is complying with the confidentiality requirements described above. Grantee must make records applicable to this Agreement available to authorized persons for the purpose of inspection, review, and/or audit.
- Grantees must retain data received from ETA only for the period of time required. Thereafter, the grantee agrees that all data will be destroyed.