



PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION POLICY

Policy Number: 1110

Effective Date: May 1, 2017

A. BACKGROUND

In order to provide services to job seekers and other WorkSource System customers, Workforce Snohomish staff, subrecipients, contractors and partner must collect and store a wide variety of protected personally identifiable information (PII). Workforce Snohomish is committed to assuring the appropriate use and protection of PII from unauthorized use or disclosure.

B. POLICY

Although a Workforce Snohomish, subrecipient, contractor or partner staff may be authorized to access confidential data, these staff may access the data only in connection with the performance of their official duties.

Confidential PII records include entire record systems, specific records or individually identifiable data that are not subject to public disclosure under Workforce Snohomish's Public Records Policy, and may include all documents, file content, computer files, letters, and other notations of records or data.

Documents that contain PII (participants' or family members') social security numbers, driver's license, birth certificates, I-9 documents, TANF/FSUP, etc., must be stored in a confidential, locked file cabinet which is only accessible by appropriate staff, kept separate from the working files. The working file may not contain any PII documents.

Computers that have access to customer data must be locked when not in use and anytime a staff person is away from their workstation.

All staff with access to on-line systems containing PII must follow the procedures set out by the administering agency. Electronic information and data is subject to all the requirements of this policy.

C. DEFINITIONS:

- **Protected Personally Identifiable Information (PII)** - The Office of Management and Budget defines as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal identifying information that is linked or linkable to a specific individual. Examples of protected PPI include but are not limited to social security numbers (SSN), credit card numbers, bank account numbers, ages, birthdates, medical history, financial history and computer passwords.

References:

- TEGL 39-11 Handling and Protection of Personally Identifiable Information
- 2 CFR 200.79, Personally Identifiable Information
- [WorkSource System Policy 5403: Records Retention and Public Access](#)

Supersedes:

N/A

Attachments:

N/A