Washington State
WorkSource System Policy

Policy Number: 1026

Policy Title: Safeguarding Personally Identifiable Information (PII)

Effective Date: November 30, 2023

1. Purpose:

This policy establishes the framework, minimum standards, and internal control requirements for safeguarding enrollees' personally identifiable information (PII) that align with federal Workforce Innovation and Opportunity Act (WIOA) law, regulation, and guidance.

2. Background:

It is necessary to periodically collect personally identifiable information (PII) in order to verify, document, and enroll eligible customers into WIOA Title I and Wagner-Peyser Act programs and to administer and manage those programs and grants. Loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of this information. Because both direct recipients of federal funds and Local Workforce Development Board (LWDB) staff, subrecipients, and contractors may have access to individuals' PII, it is imperative that proactive methods are implemented to ensure this critical, sensitive, personal information is protected at all times.

3. Policy:

a. All grantees of U.S. Department of Labor (DOL) funds including the Washington Employment Security Department (ESD), LWDBs, recipients, subrecipients and contractors, must have an internal control structure and written policies in place that provide safeguards to protect personally identifiable information, records, contract, grant funds, equipment, sensitive information, tangible items, and other information that is readily or easily exchanged in the open market, or that DOL, ESD, and the recipient or subrecipient consider to be sensitive.

   Per guidance and standards in 2 CFR 200.303, grantees, including but not limited to, ESD, LWDBs, recipients, subrecipients, and contractors shall take reasonable measures to safeguard protected PII and other information the Federal awarding agency or pass-through entity designates as sensitive consistent with applicable Federal, State, local, and tribal laws regarding privacy and responsibility over confidentiality.

   At a minimum, internal controls and written policies must address:

   - Allowable methods of collecting, maintaining, storing, purging, and securely transmitting PII
   - Steps to be taken by staff at all times to ensure privacy of personal information;

- Limits, restrictions, and safeguards regarding removal of such information from offices, workstations, and remote work locations regardless of the form (paper files, electronic files, computer program, etc.);
- Restrictions regarding accessing or storing customer PII on personally owned employee devices or equipment and non-secure public internet connections or those not managed by grantee IT services;
- Staff training and education content including:
  - requirement to complete annual privacy and security awareness training,
  - staff "need to know" expectations in their official capacity having access to PII;
  - consequences for carelessness or negligence, including unauthorized access to such records including corrective action, sanctions, dismissal, and potential criminal penalties under the Privacy Act of 1974;
- Description of methods to evaluate and monitor compliance with statutes, regulations, and terms and conditions of Federal awards with regard to PII;
- Responsibilities and next steps should the contractor or subrecipient become aware of a breach, theft, or loss of PII, including immediately notifying LWDB of the security incident; and
- Appropriate steps to be taken regarding communicating the breach with affected individuals.

b. Any grantee, including but not limited to, direct recipients, LWDBs, recipients, subrecipients, and contractors must immediately (within 24 hours) notify the ESD at SystemPolicy@esd.wa.gov of any release, loss, theft, or suspected unauthorized access of PII using **"PII Incident"** in the subject line. For those grants managed by ESD, in addition to notifying SystemPolicy@esd.wa.gov, grant managers must follow ESD HR Policy 0031-1.

   Please include the following content:

   - Workforce Development Area (WDA)
   - Reporting Entity-LWDB, subrecipient, contractor, other and contact information
   - Date of Incident
   - Date of Discovery (if different)
   - Number of files breached or affected
   - Type of Issue:
     - Hard copy files or information
     - Electronic files or information
   - Description of the incident
   - Initial Determination of level of incident:
     - Carelessness
     - Negligence
     - Fraud
     - Theft
     - Other
   - Any other relevant information
   - If staff member is also an ESD employee, please refer to ESD HR Policy 0031-1-Security Breach Notification;
   - If a Social Security Administration (SSA) related data breach/security incident, include **"SSA"** in the title;

- If ESD equipment loss or theft is involved, ESD staff must complete a Security Incident Report

c. ESD must take the following steps in response to a PII incident:

1. Independently investigate and document the facts of the incident, including whether or not local internal controls and policies were followed;
2. Notify the LWDB, ESD program manager, or direct recipient, in writing, of the requirement to develop and submit a corrective action plan, including the date by which the corrective action plan is due;
3. Coordinate with appropriate entities, such as the Workforce Monitoring Unit, Grants Management Office, and Policy Unit, to review and, when satisfied, approve the corrective action plan, and ensure that the action step(s) are satisfactorily implemented by the date(s) identified in the plan;
4. Issue written notification to the LWDB, ESD program manager, or direct recipient when the corrective action(s) are completed to document formal closure of the matter.

4. Definitions:

Personally identifiable information (PII) -

1. Any 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. Examples include, but are not limited to name, address, phone number, email address, social security number, passport number, driver's license or state identification card information, date and place of birth, mother's maiden name, or biometric records; and
2. Any other information that is linked or linkable to an individual such as medical, educational, financial, demographic, gender, race, and employment information. Images disclosing physical characteristics, photographic image, fingerprints, retinal scans, or voice signature in any medium and from any source, are also considered PII.

Breach - Actual or suspected compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access and/or any similar occurrence where:

1. A person other than an authorized user accesses or potentially accesses PII, or
2. An authorized user accesses or potentially accesses PII for other than authorized purposes.

Security incident - A set of events that have been examined and determined to indicate a violation of security policy or an adverse effect on the security status of one or more systems within an organization or entity.

5. References:

- Training and Employment Guidance Letter (TEGL) 39-11
- 20 CFR 683.220
- 2 CFR 200.303
- Guidance on the Protection of Personal Identifiable Information | U.S. Department of Labor (dol.gov)
- RCW 19.255

6. Supersedes:

None

7. **Website**:

   Workforce Professionals Center

8. **Action**:

   Local Workforce Development Boards and their contractors, as well as ESD Administrators, must distribute this policy broadly throughout the system to ensure that WorkSource System staff are familiar with its content and requirements.

9. **Attachments**:

   None

Direct Inquiries To:

Employment System Administration and Policy
Employment System Policy and Integrity Division
Employment Security Department
P.O. Box 9046
Olympia, WA 98507-9046
SystemPolicy@esd.wa.gov