WorkSource System Policies

Protecting Personally Identifiable Information (PII) Policy

POLICY #:	*ADM 3002, Rev. 3*
EFFECTIVE:	*April 26, 2024*
SUPERSEDES:	*Protecting Personal & Confidential Information Policy, Rev. 2, dated March 1, 2024*

PURPOSE:

This policy establishes the framework, minimum standards, and internal control requirements for safeguarding personally identifiable information (PII)[1] associated with individuals served through WorkForce Central, its subrecipients, and contractors.

The required annual staff "need-to-know" training was included in the Procedures section of this policy revision.

BACKGROUND:

Federal law, Office of Management and Budget (OMB), Department of Labor, Washington State, and other regulations and jurisdictions require implementation of proactive measures to ensure PII and other sensitive information is protected.

Services offered through WorkForce Central, its subrecipients, and contractors may require the collection of PII to verify, document and enroll eligible customers, and to administer and manage grants. Mishandling of PII can result in substantial harm to individuals including identity theft or other fraudulent use of this information. Therefore, it is imperative that proactive methods are implemented to ensure this critical and sensitive information is protected at all times.

POLICY:

WorkForce Central, its subrecipients, and contractors must abide by the protocols described in this policy to ensure the protection of PII. Failure to comply with the requirements of this policy,

[1] **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.

or any improper use or disclosure of PII for an unauthorized purpose may result in the termination or suspension of grant funds, or the imposition of special conditions or restrictions, or such other actions deemed necessary to protect the privacy of individuals served through our programs. The knowing misuse or unauthorized release of PII may result in a misdemeanor and a fine of up to $5,000 (Privacy Act of 1974).

Policy Requirement

WorkForce Central and its subrecipients and contractors must have an internal control structure and written policies that provide safeguards to protect PII, records, contracts, grant funds, equipment, sensitive information, tangible items, and other information that is readily or easily exchanged in the open market, or that grant funders or grant recipients consider to be sensitive. Reasonable measures must be taken and be consistent with applicable federal, state, local, and tribal laws regarding privacy and protection of confidential information.

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

- Allowable methods of collecting, maintaining, storing, purging, and securely transmitting PII
- Procedures staff must follow to ensure PII is protected at all times.
- Limitations, restrictions, and safeguards regarding removal of PII from offices, workstations, and remote work locations regardless of the form (paper files, electronic files, computer program, etc.)
- Restrictions for 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 that includes:
    - Required annual privacy and security awareness training
    - Staff "need to know" expectations in their official capacity having access to PII.
    - Consequences for carelessness or neglect, 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 regarding PII.
- Responsibilities and processes to follow when made aware of a breach[2], theft, or loss of PII, including notifying WorkForce Central of the security incident.

[2] **Breach:** Actual or suspected compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access and/or any similar occurrence where a person other than an authorized user accesses or potentially accesses PII, or an authorized user accesses or potentially accesses PII for other than authorized purposes.

- Appropriate steps to follow when notifying individuals of the breach, theft, or loss of their PII.

ESD Grants Only: Any unauthorized release, loss, or theft of PII related to grants funded through ESD, WorkForce Central and its subrecipients and contractors must immediately (within 24 hours) notify ESD at SystemPolicy@esd.wa.gov. Insert "PII Incident" in the subject line of the email. The following must be included in the email:

- Workforce Development Area (WDA)
- Reporting entity-WorkForce Central, subrecipient, contractor, or other contact information
- Date of incident
- Date of discovery (if different)
- Number and type of hard or electronic files/documents affected
- Description of the incident
- Initial determination of the level of incident:
    - Carelessness
    - Negligence
    - Fraud
    - Theft
    - Other
- Any other relevant information.

In response to the PII incident, ESD will take the following steps:

- Independently investigate and document the facts of the incident, including whether local internal controls and policies were followed.
- Notify WorkForce Central in writing of the requirement to develop and submit a corrective action plan, including the date by which the corrective action plan is due.
- Coordinate with appropriate entities, such as ESD's 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.
- Issue written notification to WorkForce Central when the corrective action(s) are completed to document formal closure of the matter.

PROCEDURES:

1. **Collecting, Maintaining, Storing, Purging and Transmitting PII**

a. Customer PII must not be accessed or stored on personally owned devices or equipment or when using non-secure public internet.
b. PII must not be communicated via email or stored on a CD, DVD, thumb drive, etc. unless the device is encrypted.
c. Customer information must only be communicated through agency approved technology and services.
d. Social security numbers must not be delivered via email. In the event this occurs, the email must be immediately deleted and subsequently deleted from the "Deleted Items" folder.
e. Access to PII must be restricted to only authorized personnel who need the information to perform duties in connection with the scope of work in the applicable grant agreement.
f. Staff must be discreet when verbally communicating personal and confidential information and ensure the receiver(s) are authorized to receive the information. See **e.**, above.
g. WorkForce Central, its subrecipients and contractors must have policies and procedures that require employees and other personnel, prior to being granted access to PII, to 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.
h. Personal and confidential information must be stored in a secure location at all times.
i. Records containing PII must not be left open and unattended (e.g., copies left unattended on workstations or print jobs left unattended on a copy machine or printer).
j. Personal and confidential information must not be tossed into regular trash or recycle bins. Use appropriate methods for destroying sensitive PII in paper files (e.g., shredding) and securely deleting sensitive electronic PII upon completion of the applicable record retention schedule.
k. Removing PII from offices, workstations, and remote work locations, whether in paper or electronic form, should only occur on rare occasions. Strong security measures must be in place when transporting personal and confidential information (e.g., keep in a locked trunk of vehicle rather than the back seat).
l. Archive boxes must be clearly marked as containing personal and confidential information.
m. WorkForce Central, its subrecipients and contractors must permit authorized federal, state, and local personnel to make onsite inspections during regular

business hours for the purpose of conducting audits or other investigations to ensure compliance with confidentiality requirements described in this policy.

n. Medical and Disability Information: If collection of medical and disability is necessary, follow guidelines in ESD WorkSource Information Notice (WIN) 0023, (current and future iterations) – Management of Medical and Disability Related Information located on the Workforce Professionals Center Policy, State Guidance-WorkSource Information Notice (WIN) page.

o. Authorization to Share Confidential Information and Records: In accordance with federal and state law, individuals applying for WIOA Title I or other federally funded services must be provided an opportunity to submit written authorization allowing the service provider to share their personal and confidential information and records among partners of the WorkSource One-Stop system. The Authorization to Share Confidential Information and Records form informs the individual that their information may be shared among the WorkSource One-stop partners solely for the purpose of delivering WorkSource employment and training services, further disclosure is strictly prohibited, and if the individual requests their personal and confidential information not be shared among the WorkSource One-Stop partners, this request will not affect their eligibility for program services [RCW 50.13.060(10)(b)(i)]. Customers applying for WIOA Title I services must sign and date the Authorization to Share Confidential Information and Records form attesting they have read and understand how their information will be shared and protected.

2. Notifying Impacted Individuals

a. Any person or business that conducts business in Washington state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of Washington state whose personal information was or is reasonably believed to have been acquired by an unauthorized person and the personal information was not secured. Notice is not required if a breach of the security of the system is not reasonably likely to subject consumers to a risk of harm.

b. Notification to impacted individuals must be made in the most expedient time possible, without unreasonable delay, and no more than 30 calendar days after the breach was discovered, unless the delays is at the request of law enforcement, or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

c. Further procedures for informing impacted individuals are described in RCW 19.255.010.

3. **Staff training:** WorkForce Central and it subrecipients must provide an annual "privacy and security awareness" training for staff that includes a review of this policy with an emphasis on:
    a. Staff "need to know" expectations in their official capacity having access to PII.
    b. Consequences for carelessness or neglect, including unauthorized access to such records including corrective action, sanctions, dismissal, and potential criminal penalties under the Privacy Act of 1974.
4. Monitoring Requirements
    a. Through its annual monitoring questionnaire, WorkForce Central ensures subrecipient compliance with PII requirements.

REFERENCES

- Public Law 113-128, Workforce Innovation and Opportunity Act of 2014
- Privacy Act of 1974
- Social Security Act
- 20 CFR 683.220
- 2 CFR 200.303(e)
- RCW 42.56 – Public Records Act
- RCW 50.13 – Records and Information, Privacy and Confidentiality
- Governor's Executive order 00-03-Public Records Privacy Protections
- TEGL 39-11-Guidance on Handling and Protection of Personally Identifiable Information
- ESD WIN 0023, Rev. 2-Management of Medical and Disability Related Information
- ESD Policy 1026 – Safeguarding Personally Identifiable Information (PII)