Workforce Snohomish

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION POLICY

Policy Number: 1110 **Effective Date:** April 1, 2024

A. BACKGROUND

It is necessary for recipients, subrecipients and contractors to periodically collect personally identifiable information (PII) to verify, document, and enroll eligible customers into the programs managed by Workforce Snohomish. Loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of this information. With that in mind, it is imperative that proactive methods are implemented to ensure this critical, sensitive, personal information is protected at all times.

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.

Recipients, subrecipients and contractors must have their own internal controls and written documentation to maintain compliance with statutes, regulations, and terms of awards regarding PII. These must, at minimum, abide by the requirements outlined by WorkSource System Policy 1026 and this policy.

B. POLICY

Recipients, subrecipients and contractors shall take reasonable steps to ensure the safety of protected PII at all times per guidance in 2 CFR 200.3-e. See the appendix at the end of this document for a detailed description of PII. These steps shall include:

A. The limiting of access to PII data based on job requirements ("need to know justification").
B. Allowable methods of collecting, maintaining, storing, purging, and securely transmitting PII.
C. Ensuring that all devices where data containing PII is accessed and stored are secure.
D. Other access restrictions.

E. Staff training and education.
F. Strict adherence to the WFS data retention policy.
G. Reviewing and monitoring compliance with statutes, regulations and terms and conditions laid out in grant awards with respect to PII.
H. Steps that need to be taken in the event of a data incident or data breach.

METHODS

Limiting access to data and data that contains PII

Access to data that contains PII must be approved by a supervisor, with the staff person responsible for such data being made aware of the consequences in the event of loss of such data.

Allowable Methods for data collection/storage/purging and transfer

If capturing client data electronically, secure services, such as but not limited to ETO or CognitoForms, etc must be used. Any data collected, either electronically or by paper form must then be stored either within the system it was originally captured in or physically in a locked cabinet at either WFS or WorkSource Everett. Data containing protected PII, must not be collected or transmitted via standard email in an unencrypted format. If encrypted files are sent through email, the decryption key to the files must not be provided within the same email. Preferably, data containing PII should be transferred between agencies using a secure file transfer service.

Ensuring that all devices where data containing PII is accessed and stored are secure

All devices and servers used to access or store company and program data must be protected with a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module, such as BitLocker drive encryption or Apple File Vault 2, to secure the data contained in the device in the event of loss or theft. Devices must also be protected with a monitored Antivirus and Firewall application.

Access Restrictions

Customer PII must not be accessed or stored on an insecure wifi network. Guests to any recipient, subrecipient or contractor place of work must use an isolated guest wifi network. Open network ports will either be connected to the guest side of the network or remain disconnected entirely. Recipient, subrecipient and contractor staff must agree to limit access of company data that contains PII to company owned equipment only.

Staff Training

Recipient, subrecipient or contractor staff, as applicable, will be required to attend yearly training that covers the topic of data privacy and security awareness; staff “need to know” expectations in their official capacity having access to PPI; and consequences for careless or negligence, including unauthorized access to such records including corrective action, sanctions, dismissal and potential criminal penalties under the Privacy Act of 1974. . New employees must be given training upon hire Annual staff and new hire training must also include information on the recipient, subrecipient or contractors’ data breech reporting protocol or procedure that includes adherence with required reporting

timelines outlined in this policy.

Data Retention
WFS will perform an annual audit of all stored electronic and physical program data to determine what needs to be destroyed. The WFS data retention policy will be used to determine what data, if any, needs to be destroyed. Destruction of data will take place no more than once per calendar year, and for physical files, it will be done so using a secure data destruction service. See WFS Retention Policy 1150.

Recipients, subrecipients or contractors should adhere to the terms of their agreement or contract with WFS regarding retention of program data, including PII, for no less a period than those defined in WFS Retention Policy 1150. This includes transfer of records to WFS for secure storage. WFS may request a transfer of records at any time, upon receipt of which WFS will be responsible for the retention of said records.

Compliance
WFS pre-award process encompasses review and identification of any data or special data handling and reporting requirements with regard to PII. This information is subsequently highlighted and made accessible to staff and as applicable subrecipients. WFS staff (leadership, program and operations) maintain oversight and monitor compliance with statutes, regulations and terms and conditions of Federal Awards. Initial review and subsequent evaluation of Federal awards encompasses PPI. As modifications are made to Federal award agreements, including changes in statutes, regulations and terms and conditions, a briefing is issued to support staff and subrecipient compliance with new or changed requirements of the award. Evaluation of these changes or modifications are incorporated into monitoring of program/grant award activities.

Recipients, subrecipients and contractors are required to monitor compliance with statutes, regulations, and the terms and conditions of their awards at regular intervals.

Initial Actions After a Breach is Detected
Determine and address the source of the breach immediately to prevent any further data loss. Depending on the type of breach, actions taken may include changing locks or access codes, to suspending online accounts. Depending on the scope of the incident, legal counsel may be sought to advise on federal and state laws.

Incident Reporting
Recipients, subrecipients and contractors must have their own processes in place for incident reporting. In addition to those processes, any release, loss, theft, or unauthorized access of data containing PII, whether it be classified as a data Incident or Breach, must be reported to the Workforce Snohomish senior leadership team using the WFS data incident reporting form (https://www.cognitoforms.com/WorkforceSnohomish1/DataIncidentReportingForm) or via email senior-lt@workforcesnohomish.org within 12 hours of the Incident/Breach (See Appendix for the definition of a Data Security Incident versus a Data Security Breach). If submitting an incident report via email, the subject line of the email must read "**PII Incident.**" The WFS senior leadership team shall, upon receiving such a message, notify

ESD at SystemPolicy@esd.wa.gov or other funding entity as applicable, immediately of the data Incident/Breach. The information that needs to be supplied with any such incident report is as follows: (this data will be captured when using the WFS incident reporting form noted above)

- **Workforce Development Area (WDA) #4**
- Reporting entity-LWDB, subrecipient, contractor, other
- Reporting entity 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

Once the data incident report has been filed, the WFS Communications department will be tasked with notifying all parties affected including the Local Workforce Development Board either by mail or other preferred communication method. Key details of the data incident must not be withheld as these details may help consumers protect themselves and their information. Importantly, however, information that might put consumers at further risk must not be shared publicly.

In accordance with RCW 19.255.010, this notification is to include 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.

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 delay 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.

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

C. DEFINITIONS:

Personally Identifiable Information (PII)

Washington state law, RCW 19.255.005, defines the following data as PII and any breach involving this data should be handled as described in this policy.

First name or first initial, and last name in **combination with** any one or more of the following data elements:

A. Social security number
B. Driver's license or Washington ID card number
C. Account or credit/debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
D. Full date of birth
E. Private key (password) that is unique to an individual and is used to authenticate or sign an electronic record
F. Student, military or password identification number
G. Health insurance policy or ID number
H. Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or
    a. Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;
    b. Username or email address in combination with a password or security questions and answers that would permit access to an online account; and
    c. Any of the data elements or any combination of the data elements described in (A-G) without the consumer's first name or first initial and last name if:
        i. Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and
        ii. The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Data Security Incident

A “Data Security Incident” or “Incident” shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources.

Common examples of Data Security Incidents include, but are not limited to, any of the following:

- Successful attempts to gain unauthorized access to a system or Staff or Client PII regardless of where such information is located
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of Confidential Information or PII
- Changes to system hardware, firmware, or software characteristics without the recipient, subrecipient or contractor’s knowledge, instruction, or consent
- Loss or theft of equipment where Confidential Information or PII is stored
- Unforeseen circumstances such as a fire or flood that could lead to the loss or misuse of Confidential Information or PII
- Human error involving the loss or mistaken transmission of Confidential Information or PII
- Hacking, social engineering, phishing or other subversive attacks where information is obtained by deceitful practice

Data Security Breach

A “Data Security Breach” or “Breach” is any Incident where recipients, subrecipients or contractors cannot put in place controls or act to reasonably prevent the misuse of Confidential Information or PII. A Breach is also an incident where data has been misused.

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.

References:

- TEGL 39-11 Handling and Protection of Personally Identifiable Information
- WorkSource System Policy 5403: Records Retention and Public Access
- Washington State WorkSource System Policy 1026
- 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
- 2 CFR 200.79, Personally Identifiable Information

Supersedes:

N/A

Attachments:

N/A