NORTHWEST WORKFORCE COUNCIL

Policy:	**Personally Identifiable Information**
Number:	**WIOA 01-43, Rev 1**
Effective:	**October 15, 2020**

Last Revised: March 6, 2024

BACKGROUND: The Northwest Workforce council, staff, partner agencies and subcontractors have access to large quantities of Personally Identifiable Information (PII) relating to the organization, staff, applicants and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files, the MIS and financial databases and other sources.

The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. NWC is required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. This policy outlines how NWC staff shall properly handle and protect PII and the actions that will be taken if a breach has occurred. In addition, NWC will require that subrecipients and contractors adequately protect the PII of individuals who may access the services the contractors provide through the NWC contract.

DEFINITIONS: The Office of Management and Budget (OMB) defines PII as 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.

The Department of Labor has defined two types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

A. Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

B. Non-sensitive PII, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

C. To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number, a date of birth, and

mother's maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

POLICY: Federal law, OMB Guidance, Departmental, and Employment and Training Administration (ETA) polices require that PII and other sensitive information be protected.

A. PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module.

B. NWC must not e-mail unencrypted sensitive PII to any entity.

C. NWC must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure.

D. Any PII must be obtained and maintained in accordance with applicable Federal and state laws governing the confidentiality of information.

E. PII must be stored in an area that is physically safe from access by unauthorized persons at all times.

F. Data containing PII will be processed using NWC issued equipment that is managed by the approved information technology (IT) services vendor. Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations e.g., employee's home, and non-NWC managed IT services, e.g., Yahoo mail, is strictly prohibited.

G. NWC employees and other personnel who will have access to sensitive/confidential/proprietary/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 and state laws.

H. NWC will orient new employees and other personnel on the policies and procedures in place regarding confidential information before any individual is granted access to PII.

I. Personnel must 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.

J. NWC may not extract information from data supplied by the Employment and Training Administration (ETA) or the Employment Security Department (ESD) for any purpose not stated in the grant agreement.

K. Access to any PII must be restricted to only those NWC employees who need it in their official capacity to perform duties.

L. 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.

M. Data containing PII may be downloaded to, or maintained on, mobile or portable devices only if the data are encrypted using NIST validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.

N. PII data obtained by NWC through a request from ETA or ESD must not be disclosed to anyone but the individual requestor except as permitted by law.

O. Staff authorized to conduct monitoring, auditing and investigations may access applicable records during regular business hours.

P. NWC will retain data for the period of time required by state and federal law. Thereafter, NWC will destroy the data including the degaussing of magnetic tape files and deletion of electronic data.

Q. NWC will conduct required annual staff training and education with curricula that includes 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.

In addition to input from staff at each annual training described above, NWC will monitor for compliance of its PII policy, by including an agenda item on each of its regular Leadership Team meetings for review and discussion of effectiveness of the policy. Any concerns raised or noted will be immediately problem solved for solutions.

Responsibilities and Next Steps After Suspected or Actual Breach, Theft or Loss of PII

NWC Staff or included contractor must immediately notify the NWC Executive Director of the suspected breach, including any release, loss, theft, or suspected unauthorized access of PII. NWC will then, as soon as feasible, notify ESD of any breach involving unauthorized access at SystemPolicy@esd.wa.gov using **"PII Incident"** in the subject line and shall 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

For those grants managed by ESD, in addition to notifying SystemPolicy@esd.wa.gov, grant managers must follow ESD HR Policy 0031-1.

Violation of Policy

Unauthorized disclosure of PII or other sensitive or confidential information can subject the disclosing employee and NWC to civil and criminal liability under the Privacy Act of 1974. Disclosure of this information is grounds for immediate disciplinary action up to and including termination of employment.

References:

- Training and Employment Guidance Letter (TEGL) 39-11
- State WorkSource System Policy 1026, Safeguarding Personally Identifiable Information (PII)
- 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