Subject: Personal Identifiable Information Policy

Policy No: 2015-59
Effective Date: December 2, 2020
Revised: November 30, 2023

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.

Background:

The Benton-Franklin Workforce Development Council (BFWDC), staff, partner agencies, and subcontractors possess large quantities of 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. This policy outlines how to properly handle PII and the actions to be taken if a breach occurs.

The BFWDC is required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data, including PII.

Policy:

Federal law, OMB Guidance, and Departmental and Employment and Training Administration (ETA) policies require that personally identifiable information (PII) and other sensitive information be protected, and grantees must secure the transmission of PII and sensitive data developed, obtained, or otherwise associated with aforementioned funded grants.

A. PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, external drives, and devices 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. The BFWDC must not e-mail unencrypted sensitive PII to any entity.

C. The BFWDC 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. The BFWDC must maintain such PII in accordance with applicable laws.

E. Any PII must be obtained in conformity with applicable federal and state laws governing the confidentiality of information.

F. PII must be stored in an area that is always physically safe from access by unauthorized persons.

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

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

I. BFWDC personnel are required to complete annual privacy and security awareness training.

J. BFWDC 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.

K. Personnel must acknowledge their understanding of the confidential nature of

the data and the safeguards they must comply with in handling such data. 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;

L. The BFWDC may not extract information from data supplied by the Employment and Training Administration (ETA), Department of Labor (DOL), or the Employment Security Department (ESD) for any purpose not stated in the grant agreement.

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

N. 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.

O. Data containing PII may be downloaded to or maintained on mobile or portable devices only if the data is encrypted using NIST-validated software products based on FIPS 40-2 encryption. In addition, wage data may only be accessed from secure locations.

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

Q. Staff authorized to monitor, audit, and investigate may access records applicable during regular business hours.

R. The BFWDC will retain data for the period state and federal law requires. After that, the BFWDC will destroy the data, including degaussing magnetic tape files and securely deleting electronic data.

Disclosure of Data

A. Any breach or suspected breach of PII must immediately (within 24 hours) be reported to the Executive Director, Program Manager, or their designee.

B. Any grantee, including but not limited to BFWDC direct recipients, subrecipients, and contractors, must immediately (within 24 hours) notify the Benton-Franklin Workforce Development Council (BFWDC) Executive Director, or their designee of any release, loss, theft, or suspected unauthorized access of PII using “PII Incident” in the subject line.

Please include the following content:

- Workforce Development Area (WDA): Benton-Franklin 11
- Reporting Entity: BFWDC, subrecipient, contractor, other
- 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 the level of incident:
  - Carelessness
  - Negligence
  - Fraud
  - Theft
  - Other
- Any other relevant information

❖ In the event manager is not available, personnel are to report the theft or loss immediately to:

- DOL Computer Security Incident Response Capability (CSIRC): dolcsirc@dol.gov.

- Employment Security Department (ESD): SystemPolicy@esd.wa.gov.

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

Definitions:

Personally identifiable information (PII)
The Office of Management and Budget (OMB) defines PII as information that can be used to distinguish or trace an individual's identity alone or when combined with other personal or identifying information linked or linkable to a specific individual.

1. Any information that can be used to distinguish or trace an individual's identity, either alone or combined with other personal or identifying information 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 linked or linkable to an individual, such as medical, educational, financial, demographic, gender, race, and employment information. Images disclosing physical characteristics, photographic

images, fingerprints, retinal or iris scans, or voice signatures in any medium and from any source are also considered PII.

Sensitive Information
Any unclassified information whose loss, misuse, or unauthorized access to or modification could adversely affect the interest or the conduct of Federal programs or the privacy to which individuals are entitled under the Privacy Act.

Protected PII
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 or retinal scans, etc.), medical history, financial information and computer passwords.

Non-Sensitive PII
Information that, if disclosed, could not reasonably be expected to result in personal harm. It is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Non-sensitive PII includes first and last names, e-mail addresses, business addresses and phone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could be categorized as protected or sensitive 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