Bay Consortium Workforce Development Board

Policy Number:	**19-01**
Effective Date:	**February 6, 2019**
Revised Date:	**February 5, 2020**
Title:	**WIOA Personally Identifiable Information (PII) Policy**

PURPOSE

The purpose of this policy is to provide guidance on compliance with the requirements of handling and protecting personally identifiable information (PII).

REFERENCES

- U. S. Department of Labor (DOL), Employment and Training Administration (ETA), Training and Employment Guidance Letter (TEGL) 39-11, Guidance on the Handling and Protection of Personally Identifiable Information (PII) (June 28, 2012)
- VWL 19-05

POLICY and PROCEDURES

As part of their WIOA activities, BCWDB WIOA funded contractors (including WIOA service providers) may have in their possession large quantities of PII relating to their organization and staff; partner organizations and their staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files and other sources. All parties in possession of PII are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of PII.

Federal regulations require that PII and other sensitive information be protected. All WIOA funded agencies (including WIOA service providers) must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with WIOA funds and must comply with all of the following:

- Ensure PII is not transmitted to unauthorized users and all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted.
- Take the necessary steps to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure.
- Ensure that any PII is obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

- Acknowledge that all PII data shall be stored in an area that is physically safe from access by unauthorized persons at all times. Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations (i.e. employee's home, personal email), is strictly prohibited unless approved by ETA.
- Ensure all employees and other personnel who will have access to sensitive, confidential, proprietary, and/or private data (1) are advised of the confidential nature of the information and of the safeguards required to protect the information; and (2) are advised that, per Federal and state laws, civil and criminal sanctions may be imposed for noncompliance.
- Have in place policies and procedures under which all employees and other personnel acknowledge (1) their understanding of the confidential nature of the data; (2) the requirements with which they are required to comply when handling such data; and (3) that they may be liable to civil and/or criminal sanctions for noncompliance with statutory nondisclosure requirements.
- Must not extract information from data supplied by the VAWC system for any purpose not stated in the contract with the BCWDB.
- Access to any PII must be restricted to only those employees who need it in their official capacity to perform duties in connection with the scope of work in the grant or agreement with the BCWDB.
- 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. Data may be downloaded to, or maintained on mobile or portable devices only if the data are encrypted.
- Must permit the BCWDB, Federal and or state staff to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the WIOA funded agency is complying with the confidentiality requirements described in this policy.
- Must retain data received only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements, if any. Thereafter, the grantee agrees that all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.
- Protected PII is the most sensitive information encountered in the course of grant work, and it is important that it stays protected. WIOA service providers are required to protect PII when transmitting information, but are also required to protect PII and sensitive information when collecting, storing and/or disposing of information as well.

  Outlined below are some recommendations to help protect PII:

- Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only.
- Whenever possible, use unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN.

- Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding) and securely deleting sensitive electronic PII.
- Do not leave records containing PII open and unattended
- Store documents containing PII in locked cabinets when not in use.
- Immediately report any breach or suspected breach of PII to the BCWDB.

DATA BREACH

In the event that a BCWDB or contracted WIOA service provider suspects, discovers, or is notified of a data security incident or potential breach of security relating to personal information, the BCWDB shall as soon as possible, but no later than twenty-four (24) hours from the incident, notify the WIOA Title I Administrator and Grant Recipient. The WIOA Title I Administrator will notify the DOLETA Federal Project Officer assigned to Virginia about data security incident or potential breach. Timely notice (within 24 hours) of a breach will be provided to Bay Consortium Workforce Development Board members and Chief Local Elected Officials.

- The notification shall include the following:
- Approximate date of the incident;
- Description of cause of the security event and how it was discovered;
- Number of individuals affected and the type of PII involved;
- Steps taken/to be taken to remedy the event.

The BCWDB or contracted WIOA Service provider shall also comply with notification requirements outlined in §18.2-186.6. of the Code of Virginia.

WIOA Title I Administrator
Academic and Workforce Programs Virginia Community College System
300 Arboretum Place, Suite 200
Richmond, VA 23236
Telephone: (804) 819-5387
Fax: (804) 786-8430
Email: wioa@vccs.edu

DEFINITIONS

For purposes of this policy, following are definitions of terms related to PII.

- PII – 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.
- Sensitive Information – any unclassified information whose loss, misuse, or unauthorized access to or modification of 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 and non-sensitive PII - DOL 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.

    1. 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.

    2. 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. For example, 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.