DATE: November 9, 2016

TO: South Bay One-Stop Business & Career Centers/Service Providers

SUBJECT: Directive No. 16-03
HANDLING AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

PURPOSE:

The purpose of this directive is to provide guidance to all SBWIB, Inc.'s staff and service providers on compliance with the requirements of acquiring, handling transmitting and protecting personally identifiable information (PII).

EFFECTIVE DATE:

This directive is effective on the date of issuance.

REFERENCE:

- **Department of Labor Training and Employment Guidance Letter (TEGL) No. 39-11**

BACKGROUND:

The U.S. Department of Labor Employment and Training Administration (DOLETA), Training and Employment Guidance Letter 39-11, issued June 28, 2012, and entitled "Guidance on the Handling and Protection of Personally Identifiable Information (PII)," requires that strong and effective measures be taken to mitigate the risks associated with the collection, storage, dissemination, and disposal of sensitive data, including PII.

As part of its grant activities, the South Bay Workforce Investment Board, Inc. have in their possession large quantities of PII and other sensitive information relating to their organization and staff; subcontractor and partner organization and 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

DEFINITIONS:

Based on the Office of Management and Budget (OMB) and DOLETA definitions, SBWIB defines PII and other sensitive information as follows;

- PII – 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 entitles under the Privacy Act.

- Protected PII and non-sensitive PII – the United States Department of Labor (DOL) has defined two types of PII: (1) Protected PII and (2) 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 accounts 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-mails 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.

    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 the individual. However, a name linked to 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 regulations require that PII and other sensitive information be protected. The SBWIB, Inc., South Bay One-Stop Business & Career Centers and WIOA service providers must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with Workforce Innovation Opportunity Act (WIOA) funds and must comply with all of the following:

- To ensure that such PII is not transmitted to unauthorized users, all 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.

- The SBWIB, Inc. and WIOA funded agencies must take the steps necessary to ensure the privacy of the PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure. All agencies must maintain such PII in accordance with the DOL Employment and Training Administration standards for information security described in this policy.

- WIOA funded agencies shall ensure that any PII used during the performance of their agreement with the SBWIB, Inc. has been obtained in conformity with applicable federal and state laws governing the confidentially of information.

- The WIOA funded agencies further acknowledge that all PII shall be stored in an area that is physically safe from access by unauthorized persons at all times. Accessing, processing, and storing of WIOA funded PII data on personally owned equipment, at off-site locations e.g., employee's home, and non-grantee managed IT services (e.g., Yahoo mail), is strictly prohibited.

- All WIOA funded 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.

- The WIOA requires that funded agencies have in place policies and procedures under which their employees and other personal 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/or criminal sanctions for noncompliance with statutory nondisclosure requirements.

- WIOA funded agencies must not extract information from data supplied by the CalJOBs / I-Train system for any purpose not stated in the contract agreement with the SBWIB, Inc.

- 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 agreement with the SBWIB, Inc.

- 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 using NIST validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.

- All WIOA funded agencies must permit city, state and federal staff to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the all interested parties are complying with the confidentiality requirements described in this policy.

- All WIOA funded agencies must retain data 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, all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

- If a WIOA funded employee fails to comply with PII requirements; as with any disciplinary actions, the particular facts and circumstances, including whether the breach was intentional, will be considered in taking appropriate action. Any action the SBWIB, Inc. takes must be consistent with the governing regulations on the protection of PII. Consequences will be balanced with the level responsibility and with type of PII involved. **The SBWIB, Inc. Chief Executive Officer may consider, but is not limited to the following disciplinary actions for failing to protect PII material: (1) written reprimand; (2) suspend system privileges; (3) suspend from duty; (4) remove the person from their current position; and (5) terminate employment.**

  Additionally, willful disclosure of PII may result in legal liability of the offender.

- If WIOA funded agency failure to comply with these requirements, or any improper use or disclosure of PII for an unauthorized purpose may result in the termination or suspension of the contract, or the imposition of special conditions or restrictions, or such other actions as the SBWIB, Inc. may deem necessary to protect the privacy of participants or the integrity of data.

PROCEDURE:

SBWIB, Inc. and WIOA funded agencies must ensure the security of PII and other sensitive information as follows:

- Before collecting PII or sensitive information from participants, the all interested parties must have participants sign releases acknowledging the use of PII for grant purposes only.

- Whenever possible, use of 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 the 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 or using a burn bag) 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.

ACTION:

All WIOA funded employees and agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII.

All WIOA funded employees and agencies are required to sign the attached ***Acknowledgement of Policy and Confidentiality Agreement.*** In addition, all participant enrolled into a WIOA program must sign the attached ***Authorization and Consent for Release of Information.***

If you have any questions regarding this directive, please contact the Compliance Manager or the IT Manager at (310) 970-7700.

Jan Vogel
Executive Director

Approved Executive Committee Minutes-11/9/2016

Atch