Montgomery County Workforce Development Board

Clean Desk Policy

APPROVAL DATE: October 22, 2021

EFFECTIVE DATE: October 22, 2021

REVISED: Amended for Compliance and Accountability; July 16, 2021

REFERENCES: TEGL 39-11; 29 CFR Part §38.41 through §38.45, Part §38.54

PURPOSE: To provide guidance to 1) the Montgomery County WDB staff, 2) the Fiscal Agent for funds approved by the WDB, 3) One-Stop Operators, and 4) subcontracted Workforce Innovation and Opportunity Act (WIOA) programs (hereafter collectively referred to as *local WIOA administrative and service providers*) on compliance with the requirements of handling and protecting PII for customers who receive services funded with federal Department of Labor (DOL) Employment and Training (ETA) funds channeled to the local area directly or through the state.

BACKGROUND: The Montgomery County WDB must monitor subcontractors and vendors for data security and ensure all employees who handle PII sign a confidentiality agreement.

POLICY:

1. **Definitions:** OMB has defined two types of **PII: Protected PII** and **Non-sensitive PII**

   PII-- OMB Memorandum M-07-16, Safeguarding Against and Responding to Breach of Personally Identifiable Information (May 22, 2007) 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, use, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Federal programs, or privacy to which individuals are entitled under the Privacy Act of 1974.

   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.

   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.
   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.

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.

2. **Requirements:** Federal law, OMB Guidance, and Departmental and ETA polices require that PII and other sensitive information be protected. ETA has examined the ways its Local WIOA administrative and service providers, as stewards of Federal funds, handle PII and sensitive information and has determined that to ensure ETA compliance with Federal law and regulations, Local WIOA administrative and service providers must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with ETA funded grants.

   In addition to the requirement above, all Local WIOA administrative and service providers must also 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. Local WIOA administrative and service providers must not e-mail unencrypted sensitive PII to any entity, including ETA or contractors.

   - Local WIOA administrative and service providers 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. Local WIOA administrative and service providers must maintain such PII in accordance with the ETA standards for information security described in this TEGL and any updates to such standards provided to the grantee by ETA. Local WIOA administrative and service providers who wish to obtain more information on data security should contact their Federal Project Officer.

   - Local WIOA administrative and service providers shall ensure that any PII used during the performance of their grant has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

   - Local WIOA administrative and service providers shall ensure that any medical information that is collected or maintained must be kept under lock and separate from other personal information.

   - Local WIOA administrative and service providers further acknowledge that all PII data obtained through their ETA grant shall be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed using grantee issued equipment, managed information technology (IT) services, and designated locations approved by ETA. Accessing, processing, and storing of ETA grant 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 unless approved by ETA.

   - Grantee 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.

- Local WIOA administrative and service providers must have their policies and procedures in place under which grantee employees and other personnel, before being granted access to PII, 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.

- Local WIOA administrative and service providers must not extract information from data supplied by ETA for any purpose not stated in the grant agreement.

- Access to any PII created by the ETA grant must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

- 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.

- PII data obtained by the grantee through a request from ETA must not be disclosed to anyone but the individual requestor except as permitted by the Grant Officer.

- Local WIOA administrative and service providers must permit ETA to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the grantee is complying with the confidentiality requirements described above. In accordance with this responsibility, local WIOA administrative and service providers must make records applicable to this Agreement available to authorized persons for the purpose of inspection, review, and/or audit.

- Local WIOA administrative and service providers must retain data received from ETA 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.

3. **Recommendations.** Protected PII is the most sensitive information that you may encounter in the course of your grant work, and it is important that it stays protected. Local WIOA administrative and 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, ETA recommends the 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.

- Immediately report any breach or suspected breach of PII to the FPO responsible for the grant, and to ETA Information Security at ETA.CSIRT@dol.gov, (202) 693-3444, and follow any instructions received from officials of the Department of Labor.

4. **Monitoring, Compliance, and Accountability**: Questions regarding the MCWDB Clean Desk Policy and requirements have been added to all monitoring tools for all provider and employer contracts, including: Individual Training Accounts, On-the-Job Training and Cost Reimbursement contracts. The Montgomery County Commerce Department staff signs an Acknowledgement and Commitment to the Clean Desk Policy (see attached Acknowledgement), and ongoing monitoring by the Compliance Officer and staff is conducted within the Montgomery County Commerce Department and the PA CareerLink® office locations.

Authorized Signature: _____ **Date:**_____

Print Name and Title: _____

Acknowledgement of Receipt

I hereby acknowledge that I have received a copy of the Clean Desk Policy. I agree to read it thoroughly. I agree that if there is any policy or provision in this policy that I do not understand, I will seek clarification from the Executive Director. I understand that I am an "at will" employee and, as such, employment is not for any fixed period of time and may be terminated at the will of either party, with or without cause, and without prior notice. I am responsible for compliance with the policies and procedures contained in this document as well as any changes and/or modifications provided to me. I understand that all revisions are made a part of the policy and supersede all previous versions and/or revisions.

_____ _____

Employee Signature Date

_____

Please print name clearly