Workforce Development Board Mid-Ohio Valley **Policy #24**

Subject: **Securing Personally Identifiable Information (PII)**

Effective Date: May 1, 2017

Purpose: To address the security of Personally Identifiable Information (PII), both sensitive and non-sensitive, for services offered through Title I of the Workforce Innovation and Opportunity Act.

References: TEGL No. 39-11; Federal Information and Security Management Act (Title III of the E-Government Act 2002); OMB M-06-15, and M-06-19; Executive Order 13402; Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99

Background: The Workforce Innovation and Opportunity Act requires that recipients of WIOA Title I funds provide Personally Identifiable Information (PII) to access WIOA services. Federal law, OMB guidance, federal, state and local policies require that PII and other sensitive information be protected.

Policy: All WDB-MOV staff, contractor staff, grantees, sub-grantees, partner staff, and any other individuals or groups involved in the handling of personally identifiable information as a result of WIOA will protect PII in accordance with the law.

WDB-MOV staff, contractor staff, grantees, sub-grantees, employees and any other individuals or groups involved in the receipt, handling, and/or protecting of PII and sensitive data developed, obtained or otherwise associated with grantee funding MUST:

> Annually (by July 1), sign a disclosure acknowledging the confidential nature of the data and agree to comply with safe and secure management of the data in accordance with federal and state requirements. (These disclosures must be kept on file with the contractor for monitoring review at the request of the WDB-MOV.)

The following definitions will be applied to Personally identifiable information in the region:

DEFINITIONS

Personal Identifiable Information (PII): 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: 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.

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 educational credentials, gender or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

Standard Operating Procedures will be developed to address the specifics required for the protection of PII

- when in use
- storage of
- in transport
- final disposal of

PII should only be accessible by staff who need it in an official capacity to perform their responsibilities under WIOA. Staff must not extract information from data sources for personal use/reasons.

PII will be processed so as to protect the confidentiality of the record/documents and to prevent unauthorized access.

PII will be retained for the required period of time per ETA guidelines, then destroyed.

Action: The Workforce WV/One Stop Center shall have staff who provide services under Title I of the Workforce Innovation and Opportunity Act sign a release annually acknowledging their use of PII for grant purposes only and of their intent to protect all PII from unauthorized users. All partners, contractors etc., will be notified of this policy.

As part of the WIOA orientation applicants/participants will be asked to sign an authorization to release information to listed parties, which may be revoked by the participant through written request.

Contractors/partners/grantees should have standard operating procedures in place to address the protection of PII.

Expiration Date: Effective until rescinded or modified by the Workforce Development Board Mid-Ohio Valley.

Approved:	October 28, 2016	LEO/WDB
	April 28, 2017	LEO's/Board

Personally Identifiable Information Acknowledgment

I have reviewed and acknowledge understanding of the WDB-MOV "Securing Personally Identifiable Information" Policy and agree that all necessary steps will be taken to ensure the privacy and confidential nature of all personally identifiable information (PII) to protect the PII from unauthorized disclosure.

I further agree that all personally identifiable information will be stored in an area that is physically safe from access by unauthorized persons, and will be managed with appropriate information technology (IT) services at all times.

All collection and use of any information, systems or records that contain personally identifiable information (PII) will be limited to purposes that support the programs and activities conducted with WIOA funding through the One Stop system in the WDB-MOV.

Access to software systems and files under my control containing PII will be limited to use in my responsibilities as an authorized staff person within the system. This includes the safe-guarding of computer passwords and access to any/all computer information systems. I will not share my MACC ID with, or allow anyone to use my MACC access. (Doing so will cause me to forfeit my access).

I agree to abide by regulations that govern the access, use and disposal of PII in accordance with WIOA and the WDB-MOV.

_____
Printed Name

_____
Signature

_____
Agency Name

_____
Date