Mississippi Valley Workforce Development Board

Personally Identifiable Information (PII) Policy

Approved: December 20, 2021

Effective Date: December 20, 2021

Amended Date: N/A

A. Purpose

1. This policy applies to and provides guidance for Mississippi Valley Workforce Development Board (MVWDB) staff, contractor staff, grantees, sub-grantees, partner staff, and staff of any co-located partner in the workforce centers (collectively "Parties") involved in the handling and protecting of Personally Identifiable Information ("PII") as a result of WIOA activities in the Mississippi Valley Workforce Area (MVWA), including wage and education records, will protect PII in accordance with the law. FERPA (as amended), WIOA, and applicable Departmental regulations will be followed. As well as any governing guidelines including federal law, OMB guidance, United States Department of Labor, Employment and Training Administration policies (see Training and Employment Guidance Letter No. 39-11), as well as any relevant state and local requirements.

B. Overview

1. As part of its workforce development activities, Parties may have in their possession PII relating to their organization and staff, sub grantee and partner organizations and staff and individual program participants.
2. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files and other sources. Federal law, OMB guidance, federal, state, and local policies require that PII and other sensitive information be protected. To ensure compliance with these policies/regulations, PII and sensitive data developed, obtained, or otherwise associated with federal and state funding must be secured and protected at all times.
3. Per the MVWDB MOU the following apply:
   a. The collection, use, and disclosure of customer education records, and the PII contained therein, as defined under FERPA, shall comply with FERPA and applicable State privacy laws.
   b. All confidential data contained in the UI wage records must be protected in accordance with the requirements set forth in 20 CFR 603.
   c. All personal information contained in VR records must be protected in accordance with the requirements set forth in 34 CFR 361.38.
   d. Customer data may be shared with other programs, for those programs' purposes, within

the Iowa*WORKS* Center network only after written consent of the individual has been obtained, where required.

e. Customer data will be kept confidential, consistent with Federal and State privacy laws and regulations.

f. All data exchange activity will be conducted in machine readable format, such as HTML or PDF, for example, and in compliance with Section 508 of the Rehabilitation Act of 1973, as amended. 29 CFR 794(d).

C. Definitions

1. *Personally 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.
2. *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.
3. *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.
   a. 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:
      i. social security numbers (SSNs)
      ii. credit card numbers
      iii. bank account numbers
      iv. home telephone numbers
      v. ages
      vi. birthdates
      vii. marital status
      viii. spouse names
      ix. educational history
      x. biometric identifier (fingerprints, voiceprints, iris scans, etc.)
      xi. medical history
      xii. financial information
      xiii. computer passwords.
   b. 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:
      i. first and last names
      ii. e-mail addresses
      iii. business addresses

iv. business telephone numbers
v. general educational credentials
vi. gender
vii. or race.

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

4. To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email 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. This demonstrates why protecting the information of our program participants is so important.

D. Training and Policies

1. Parties' management shall ensure that all of their staff are trained in the use of PII upon hire and at least annually thereafter, including any training necessary to access the Iowa*WORKS* database system.
2. Each local program representative will sign an acknowledgement form that their staff have been provided training on confidentiality internally through their respective organization. Parties should have standard operating procedures in place to address the protection of PII.

E. Parties' Awareness and Acknowledgment

1. All Parties with access to PII 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 within the Federal and state laws.
2. All Parties who have access to PII are required to annually sign a PII Policy Acknowledgment Form (attached) acknowledging the confidential nature of the data and their responsibility to comply with safe and secure management of the data according to this policy and applicable law.
3. These forms shall be kept on file with the respective Parties' personnel files and shall be available for monitoring review at the request of the MVWDB.

F. Collection of PII

1. Before collecting PII or sensitive information from participants, parties shall ensure participants sign releases acknowledging the use of PII for program services only.
2. Whenever possible, parties shall use unique identifiers for participant tracking instead of SSNs.
3. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record.
4. Once the SSN is entered for performance tracking, the unique identifier should be used in place of the SSN for tracking purposes.
5. If SSNs must 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.

G. Ensure Privacy and Restriction of Use

1. All Parties 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 and must ensure that PII used during the performance of their duties has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.
2. Access to any PII shall be restricted to only those Parties who require it in their official capacity to perform duties in connection with the scope of their services.

H. Physical and Remote Access

1. All Parties shall ensure that all PII data obtained through their program services is stored in an area that is physically safe from access by unauthorized persons at all times and is managed with appropriate information technology (IT) services and designated locations.
2. Parties shall store paper documents containing PII in locked cabinets when not in use. 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.
3. 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.
4. To ensure that PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via email or stored on CDs, DVDs, thumb drives, etc., must be encrypted.
5. If special procedures are required to handle PII during the provision of mobile rapid response services, the one-stop operator shall develop and implement procedures to ensure compliance with this policy. The procedure will be reviewed as needed by the one stop operator and LWDB staff.
6. Parties shall never leave records containing PII open and unattended.

I. Use of Personal Mobile Devices

1. No employee may access Iowa Workforce Development (IWD) email through a personal mobile device without the approval from IWD and/or the MVWDB executive director.
2. If such approval to access the network and/or company email through a personal device is granted, the employee agrees to the following:
    a. All personal mobile devices must be password protected at all times.
    b. In order to protect PII, MVWDB/IWD retains the right to delete data and/or applications from any device that contains company information.
    c. Personal mobile devices will require the installation of various applications, as determined by IWD based on the mobile device.
3. Please note that in certain situations a device may be completely wiped in order to ensure that MVWDB/IWD can protect its interests.
    a. If given sufficient notice, MVWDB/IWD can work with the Parties to avoid such action.

b. If a Party's device has been compromised, lost, or stolen, such person shall reach out immediately to MVWDB/IWD.

J. Retention and Destruction

1. All PII data must be retained to satisfy all required record retention requirements. Thereafter, all PII data must be destroyed using appropriate methods for destroying sensitive PII in paper files (i.e., shredding) and securely deleting sensitive electronic PII.

K. Reporting

1. Parties shall immediately report any breach or suspected breach of PII to the MVWDB/IWD (in the case of electronic data) or to such Party's supervisor (in all other cases).

L. Related Information

1. TEGL 39-11

Equal Opportunity Programs/Employer
Auxiliary aids and services are available upon request for individuals with disabilities

Mississippi Valley Workforce Development Board

PII Policy Acknowledgment Form

I have reviewed and acknowledge understanding of the MVWDB 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 MVWA.

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 safeguarding of computer passwords and access to any/all computer information systems. I will not share my Iowa*WORKS* ID with or allow anyone to use my Iowa*WORKS* 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 MVWDB.

_____
Printed Name

_____
Signature

_____
Agency Name

_____
Date

Mississippi Valley Workforce Development Board

PII Policy Acknowledgment Form

Local program representative in signing this acknowledgement form confirm that their staff have been provided training on confidentiality internally through their respective organization and parties have standard operating procedures in place to address the protection of PII.

Our staff have reviewed and acknowledge understanding of the MVWDB 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.

Our agency further agrees 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 MVWA.

Access to software systems and files under our control containing PII will be limited to use in our responsibilities as authorized staff persons within the system. This includes the safeguarding of computer passwords and access to any/all computer information systems. No one will share their Iowa*WORKS* ID with or allow anyone to use their Iowa*WORKS* access. (Doing so will forfeit my access when applicable).

Our agency agrees to abide by regulations that govern the access, use and disposal of PII in accordance with WIOA and the MVWDB.

_____

Manager's Printed Name

_____

Manager's Signature

_____

Agency Name

_____

Date