PASSAIC COUNTY WORKFORCE DEVELOPMENT BOARD

Subject: WIOA Title I Personally Identifiable (Pll) and Sensitive Information

Effective Date: 05/08/26

PURPOSE

The purpose of this policy is to adopt requirements for the local workforce development area and partners regarding the handling and protection of Personally Identifiable Information (PII). The policy aligns with federal guidance from the U.S. Department of Labor, specifically TEGL 39-11 and the NJDOL NJWIN 6-15 to ensure the privacy and security of individual data within the workforce system

POLICY

The Workforce Development Board adopts and implements the following Federal and State of New Jersey NJDOL policies.

Personally Identifiable Information (PII) and Sensitive Information Policy

The WIOA Personally Identifiable Information (Pll) Policy establishes guidelines for ensuring the confidentiality, integrity, and security of personal information collected from program participants and stakeholders. Compliance with the federal TEGL 39-11 and the NJDOL NJWIN 6-15 are the standard for local PII policy, focusing on the safe handling and storage of sensitive data. Training and Employment Guidance Letter (TEGL) 39-11, issued by the U.S. Department of Labor (DOL), is the federal foundational guidance for handling and protecting Personally Identifiable Information (PII) within the public workforce system. It establishes the security standards that state and local agencies must follow to manage sensitive participant data.

Provisions of TEGL 39-11

- Definition of PII: It distinguishes between Protected PII (high risk of harm if leaked, such as SSNs, bank accounts, and birth dates) and Non-sensitive PII (lower risk, such as names or business emails).
- Mandatory Safeguards: Grantees are required by the WDB to 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
    - Access Control: Access to PII must be limited to authorized personnel who "need to know" to perform their specific job duties.

    - Data will be processed using grantee issued equipment, managed information technology (IT) services, and designated locations approved by ETA.
    - Encryption: All sensitive data transmitted via email or stored on portable media (CDs, thumb drives) must be encrypted using FIPS 140-2 compliant modules.
    - Physical Security: Paper records must be stored in locked cabinets and destroyed using secure methods like shredding.
    - Grantees are required to 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 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.

- Before collecting Pll or sensitive information from participants, have participants sign releases acknowledging the use of Pll for grant purposes only.
- Use appropriate methods for destroying sensitive Pll in paper files (i.e., shredding or using a burn bag) and securely deleting sensitive electronic Pll.
- Acknowledgment Requirements: Grantee employees must sign written acknowledgments of the confidential nature of the data and the potential civil/criminal penalties for improper disclosure before being granted access.
- Breach Reporting: Any suspected or confirmed breach of PII must be reported immediately to the DOL Employment and Training Administration (ETA) or the appropriate administrative entity.

Requirements of NJWIN 6-15

The NJDOL is responsible the security and confidentiality of information contained within a number of manual and automated workforce development system databases used at the local AJC/One-Stops including, but not limited to, America's One-Stop Operating System (AOSOS). It is the responsibility of the NJDOL protect the computing resources (data, information, software and hardware) under its management from unauthorized access, use, modification, disclosure, copying and destruction. AJC/One-Stop partners are responsible to comply with NJWIN 6-15, the state-level adoption of TEGL 39-11. While the

TEGL provides the broad federal framework, the following NJWIN requirements apply to New Jersey's local boards and the America's One-Stop Operating System (AOSOS).

- PII Policy Implementation: Local Workforce Development Boards (LWDBs) must have written policies and procedures to protect PII stored in or obtained from the America's One-Stop Operating System (AOSOS).
- Handling Sensitive Data: Social Security Numbers (SSNs) should be truncated or replaced with unique identifiers for tracking purposes. Locally developed forms must not require the recording of full SSNs.
- Storage and Disposal: Records containing PII must be kept in locked cabinets when not in use and destroyed using secure methods like shredding and securely deleting sensitive electronic Pll.
- Monitoring and Compliance: LWDBs are responsible for monitoring their providers to ensure they comply with these privacy standards. Noncompliance is subject to corrective action by the NJDOL.
- Information Sharing: These policies must be shared with all partners, contractors, and providers who have access to customer data.

WDB Procedures for Securing PII and Sensitive Information

PII Policy Declaration (WDB staff, partners, fiscal agents, contractors, and providers who have access to customer data)

I _____ (print name) understand that if I am provided access to any workforce development system database (for example, an AOSOS logon ID and password) I am responsible for all system transactions performed under that logon ID.

I recognize that the information stored in and available through any workforce development system used in the conduct of my duties in the State's One-Stop Career Centers and/or partner agencies has been given by its sources with an explicit or implicit condition of confidentiality, and that all the information was provided solely for the purpose of facilitating the provision of needed services to clients of the New Jersey One-Stop Career Centers and partner agencies (herein after called the "One-Stop Career Center system").

If given access to any workforce development system and its information, I agree that:

I will use the information provided ONLY:

a. To assess the needs of clients of the One-Stop Career Center system for services through the New Jersey One-Stop Career system and its partners;

b. To develop an employability plan;

c. To schedule, and, if appropriate, obligate available funds to pay for, services specifically designed to assist the client in obtaining and retaining employment;

d. To develop operational reports or evaluate program performance as authorized under federal or state law

I will NOT divulge system IDs and passwords to any other person, including, but not limited to, any client and/or fellow employee of this or any other agency, with the exception of the duly constituted administrator(s) of the automated system within the Department of Labor and Workforce Development.

I WILL NOT, under ANY circumstances, extract record or duplicate information from any workforce development system including, but not limited to AOSOS, on my behalf or on behalf of any other, for personal or non-One-Stop Career Center system business reasons.

- I will handle all information contained in REPORTS summarizing or based on data contained in workforce development system database with exactly the same strict observance of security and confidentiality as the original data.
- I will provide participants with a release to sign acknowledging that Pll will only be used for grant purposes.
- I will follow the procedure for using unique identifiers in place of Pll.
- I will follow the procedure for the storage of both electronic communication and hard copies of Pll information.
- I will NOT copy or duplicate any data provided through workforce development system database except for use for the purposes stated above within the One-Stop Career Center of which I am an employee, or its partner agencies.
- I will NOT verbally or in writing communicate information received through Workforce development system databases to any person other than employees of the One-Stop Career Center which employs me, or its partner agencies, and to these ONLY for the purposes explicitly stated above.
- I WILL log out from any workforce development system application and or database whenever I temporarily leave my computer monitor.

I understand that provision to me of any workforce development system username and password in no way places an obligation upon the New Jersey Department of Labor and Workforce Development to maintain, repair or replace the hardware or software which I will use to access the system.

I understand that the New Jersey Department of Labor and Workforce Development will neither defray the cost of nor charge a cost for Internet access service or line usage incurred incident to my accessing workforce development system(s) unless agreed to in a formal contract or memorandum of understanding between partner agencies.

I understand that a username and a password for access to the workforce development system(s) and their data, if provided to me, are not an inherent right of mine by virtue of my employment position or of any other factor, and that they are provided only for the purposes stated above and are provided conditional upon my strict observance of the security and confidentiality procedures prescribed above.

I understand that, in the event that I fail to observe any of the above-stated security and confidentiality procedures, any and all levels of access to the workforce development system(s) may be denied to me. Other disciplinary action is possible. Serious breaches of security may also result in criminal action against the involved individual(s).

I understand that any and all levels of access to workforce development system(s) may be denied to me at any time at the discretion of the duly appointed administrators of the workforce development system(s) in the New Jersey Department of Labor and Workforce Development and/or the Passaic County Workforce Development Board.

Staff Signature and Date:_____

The WDB procedure for handling PII and Sensitive Information

Managing PII (Personally Identifiable Information) requires a "lock and key" approach, whether the data is on a screen or a sheet of paper.

Electronic Communication

- Encryption: Never send PII in the body of an email or as an unencrypted attachment. Use end-to-end encrypted platforms or password-protected files (sending the password via a different channel).
- Access Control: Store files on WDB approved secure centralized servers or cloud drives. Only employees who "need to know" should have access.

- Storage Limits: Avoid saving PII on local desktops or unencrypted USB drives. Use auto-delete policies for emails and temporary folders after a set period.
- Multi-Factor Authentication (MFA): Ensure any system housing electronic PII requires MFA for entry.

Hard Copies

- Clean Desk Policy: Do not leave documents containing PII on desks, printers, or in unlocked bins. If you aren't looking at it, it should be put away.
- Physical Security: Store papers in locked filing cabinets located in restricted-access rooms.
- Controlled Printing: Use "follow-me" printing where a user must scan a badge or enter a PIN at the device to release the document.
- Secure Disposal: Never throw PII in a regular trash or recycling bin. Use cross-cut shredders or locked "secure shred" consoles for professional destruction.

For Both

- Inventory: Keep a data map of where PII lives so you can purge it once the legal retention period ends.
- Labeling: Mark sensitive files (digital or physical) as "Confidential" or "Contains PII" to alert handlers of the risk.

Acknowledgement: I acknowledge that I have read the procedure for handling PII and Sensitive Information and my use of my PII has been discussed with me by my manager.

Signature and Date_____

Passaic County Workforce Development Board Personally Identifiable Information (PII) Participant Release Form

Funding Agency: Passaic County Workforce Development Board

Notice of Collection: As part of the WIOA intake and eligibility process, we are required to collect certain PII, including Social Security Numbers, Date of Birth, Financial Records.

Confidentiality Commitment: We will take all necessary steps to ensure the privacy of your PII and protect it from unauthorized disclosure. Your data will be stored in a secure area with access restricted to staff members directly involved in this program.

Restricted Use: Your information will be used for grant purposes only, including federal reporting, program evaluation, and auditing. It will not be released to any other party without your additional written consent unless required by law.

Acknowledgement: I acknowledge that the use of my PII has been discussed with me. I understand that my information is being collected and will be used strictly for the grant purposes stated above.

Participant Signature: _____ Date: _____
Staff Signature: _____ Date: _____

Passaic County WDB procedure for using unique identifiers in place of Pll

The Workforce Development Board procedures for the Workforce Innovation and Opportunity Act (WIOA) mandates use of unique identifiers (such as Case IDs or State IDs) for tracking participants to minimize the exposure of Personally Identifiable Information (PII), especially Social Security Numbers (SSNs).

Procedure for Unique Identifiers

- Initial Collection Only: SSNs may be collected during initial intake for eligibility verification and federal performance tracking.
- Linking Records: Once the SSN is entered into the system of record, a system-generated unique identifier (e.g., State ID, User ID, or Application Number) is linked to the participant's record.
- Replacement in Documentation: Staff must use this unique identifier instead of the SSN for all subsequent participant tracking, including:
    - Training or contract documents.
    - Case management reports and routine tracking logs.
    - External communications with partners or vendors.
- Folder Labeling: PII must never be used as identifiers on participant physical file folders.

POLICY REVISIONS

The WDB Workforce Innovation and Opportunity Act (WIOA) policies are reviewed amended annually by the WDB to remain in compliance with all federal mandates and state-level policy changes issued by the New Jersey Department of Labor and Workforce Development. Partners will be notified of any policy revisions.