Personally Identifiable Information (PII) and Personal, Private and Sensitive Information (PPSI) Policy
Effective Date: 12/04/2018

Introduction:
The Workforce Development Board of Rockland County (WDB-RC) is committed to ensuring a secure physical and electronic/digital environment which will protect customer's PII and PPSI. This applies to the collection, storage and/or disposal of PII/PPSI in any format (hard copy or electronic) including, but not limited to, computer-based information systems such as the One Stop Operating System (OSOS) case management system and the Re-Employment Operating System (REOS), hard copy documents, and digital media.

Action:
WDB-RC, local staff and service providers must follow this policy to reduce the risks associated with the collection, storage and dissemination customer's PII/PPSI:

All staff will acknowledge, by signing the disclosure, 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.

Accessing and Sharing of PII/PPSI

- Physical/Facility Security will be adequate to protect the facility and equipment from unauthorized physical access, tampering and theft.

- Safeguards/physical controls will be followed so that unauthorized users walking by an individual's work station cannot view confidential information on computer screens.
  For any unattended workstations:
  - Password "reminders" will not be visibly posted or taped to desk
  - User is logged off and/or workstation is locked
  - OSOS/REOS application cannot be left open
  - Email application cannot be left open
  - Unencrypted confidential information cannot be emailed
- Interviews/conversations will be conducted in a discreet manner.
- Confidential information on unattended desks cannot be left visible or unprotected.
- Customer files must be secured in a closed drawer or kept in a file cabinet.
- Documents containing confidential customer information must be kept in a secure, locked storage location.

- Staff will use OSOS ID numbers, not social security numbers in emails or other correspondence related to customers.
- Computer disks, DVDs, flash drives, and other electronic storage devices containing confidential information are to be encrypted.
- Paper documents with confidential information are to be shredded once they are no longer needed.
- Computer disks, DVDs, flash drives, and other electronic storage devices containing confidential information will be thoroughly and irretrievably destroyed or erased once the information is no longer needed.
- Access to any PII/PPSI related to programs funded by state or federal monies must be restricted to only those employees of the grant/contract recipient who need PII/PPSI in their official capacity to perform duties in connection with the scope of work in the grant/contract agreement.
- Local staff and service providers must not extract information from data supplied by their funding source for any purpose not stated in the grant/contract agreement.
- PII/PPSI data obtained by local staff or service providers as a result of a United States Department of Labor (USDOL) or NYSDOL request must not be disclosed to anyone but the requesting agency. Exceptions to this may be made only as permitted by the requesting agency (USDOL or NYSDOL).
- Members of the public seeking information under the Freedom of Information Law (FOIL) must be directed to the NYSDOL website and advised that they may file their FOIL request using the Electronic Request Form found at https://www.labor.ny.gov/secure/foilrequest.shtm.

Security Protocols related to OSOS and REOS

- Security Coordinators have been assigned to enforce data security requirements related to the use of OSOS/REOS for local staff, service providers who have been provided access to OSOS /REOS through the local area, NYSDOL staff, and non-federally funded partner staff in each Career Center.
  The Security Coordinators are:
  Rockland - MaryJean Marcisco (845) 627-4700
- Prior to gaining access to OSOS/REOS, local staff and service providers must comply with WDS TA #17-7; Use of One-Stop OSOS/REOS. Confidentiality agreements related to OSOS/REOS must be completed appropriately by all LWDB partners in order to gain access to these systems.
- Annually, local staff, service providers and other personnel who will have access to sensitive, confidential, proprietary, and/or private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and the fact that there are sanctions for noncompliance with such safeguards contained in Federal and State laws. To meet this requirement, all local staff, service providers and other personnel with access to OSOS and/or REOS data will take the online training, *Cornerstones of Confidentiality*. This training is accessible via the Statewide Learning Management System (SLMS)

Maintaining a Secure Environment

- To ensure that such PII/PPSI is not transmitted to unauthorized users, all PII/PPSI transmitted via email or stored on CDs, 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, and adhere to the New York State's Encryption Standard.

- Local staff and service providers must not email unencrypted sensitive PII/PPSI to any entity.
- All PII/PPSI data obtained through grants/contracts funded with federal monies shall be stored in an area that is physically safe from access by unauthorized persons at all times. Such data may only be processed using equipment and services approved by the LWDB and NYSDOL.
- Accessing, processing, and storing of PII/PPSI data on personally owned equipment, including but not limited to laptops, tablets, portable devices and personal computers, at off-site locations and non-grantee managed Information Technology services (e.g. Yahoo mail), is strictly prohibited.
- All PII/PPSI 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 is encrypted using NIST validated software products based on FIPS 140-2 ENCRYPTION. In addition, wage data may only be accessed from secure locations and those accessing it must adhere to New York State's Encryption Standard.
- Local staff and service providers shall ensure that any PII/PPSI used during the performance of their grant/contract has been obtained in conformity with applicable Federal and State laws governing the confidentiality of information.
- Whenever possible, the OSOS ID number must be used for participant tracking instead of Social Security Numbers (SSNs). 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. In addition, full SSNs should never be emailed, even when using encryption methods.
- Two times each program year, Security Coordinators will conduct and document an environmental assessment in Career Centers to determine whether local staff is maintaining a secure PII/PPSI environment (both physical and electronic/digital) using the: Confidentiality – Environmental Assessment (Attachment A). The reports will be maintained by the Security Coordinators and kept on file for 3 years.
- Records containing PII/PPSI, whether hard copy or electronic, may not be left open and unattended.
- Hard copy documents containing PII/PPSI must be maintained in locked cabinets or drawers when not in use.
- Local staff and service providers must retain data received from USDOL funded grants only for the period of time required to use it for assessment and other purposes, or to satisfy applicable local/state/federal records retention requirements, if any. Thereafter, all data must be thoroughly and irretrievably destroyed.
- Appropriate methods must be used for destroying sensitive PII/PPSI in paper files (e.g., shredding) and securely deleting sensitive electronic PII/PPSI. PII/PPSI must be thoroughly and irretrievably destroyed.

- Partners will permit NYSDOL and/or USDOL to make onsite inspections during regular business hours in order to conduct audits and/or other investigations to ensure compliance with confidentiality requirements, provided reasonable notice is given. Partners will also make records available to NYSDOL and/or USDOL and/or their authorized designees for the purpose of inspection, review and/or audit.

Breaches of Confidentiality

- A breach or suspected breach of confidentiality must be reported to the Security Coordinators immediately. The Security Coordinators must immediately complete a New York State Security Breach Reporting Form and shall email to Infosec.IT@labor.ny.gov and OSOS.WDTD@labor.ny.gov. A breach of confidentiality is an event that compromises or potentially compromises the confidentiality of an individual's or group of individuals' PII/PPSI. A breach may include the loss of control, unauthorized disclosure, unauthorized acquisition, unauthorized access, misuse or unauthorized modification of PII/PPSI or similar situations, whether physical or electronic. Some examples include but are not limited to:
    - Computers, laptops, CDs, or disks containing a customer's PII/PPSI are missing or stolen.
    - An individual's PII/PPSI is revealed to a third party without a valid consent to do so on file.
    - A customer receives another customer's mail that lists the customer's name, address, and SSN.
    - Department records containing an individual's PII/PPSI are downloaded or copied.
    - An electronic device is infected or potentially infected with a virus or worm.
    - Discussion of PII/PPSI is overheard by an unauthorized individual.

Key Definitions

Digital Media is digitized content (text, graphics, audio, and video) that can be transmitted over the internet or computer networks.

Environmental Assessments are reviews of physical and electronic/digital space where PII/PPSI is used and/or stored during normal business activities to determine if such information is properly protected/secured.

PII is 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.

PPSI is any unclassified information whose loss, use, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of State or Federal programs, or privacy to which individuals are entitled under the Privacy Act of 1974 or constitute an unwarranted invasion of personal privacy under the New York State Freedom of Information Law.

PERSONALLY IDENTIFIABLE INFORMATION(PII)/PERSONAL PRIVATE AND SENSITIVE INFORMATION (PPSI)

Sign Off Form

I have reviewed and acknowledged the WDB PII/PPSI Policy and agree that all necessary steps will be taken to ensure the privacy and confidential nature of all PII/PPSI to protect such information from unauthorized disclosure.

I further agree that all PII/PPSI will be stored in an area that is physically safe from access by unauthorized persons at all times, and be managed with appropriate information technology (IT) services and designated locations. Access to any PII/PPSI through program and grant activity will be restricted to only those individuals who need access in their official capacity to perform duties in connection with the scope of work.

Printed Name

Signature

Agency Name

Date