Sullivan County LWDA
August 2018

Policy: ***Securing and protecting Personally Identifiable Information (PII) and Personal, Private and Sensitive Information (PPSI)***

Purpose: To ensure a secure physical and electronic/digital environment that will protect customer 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 OSOS and REOS, hard copy documents and digital media.

This policy applies to all local staff and service providers of the Sullivan County Workforce Area.

Action:

Accessing and Sharing PII/PPSI

1. Access to any PII/PPSI related to programs funded by state or federal monies is restricted to only those staff who implement the programs and who need the PII/PPSI in order to perform their job in connection with the program.
2. Staff and/or service providers cannot extract information for purposes other than those outlined in their job duties and program responsibilities.
3. PPI/PPSI data obtained by local staff or contracted service providers as a result of a USDOL or NYSDOL request can only be disclosed to the requesting agency.
4. Members of the public seeking information under the Freedom of Information Law (FOIL) must follow Sullivan County FOIL procedures and put the request in writing to County FOIL Officer, Michelle Huck, Sullivan County Government Center, 100 North Street, Monticello, NY 12701.

Security Protocols related to OSOS and REOS

1. Security Coordinators: The Center for Workforce Development Director is the Security Coordinator for the local area and the NYSDOL coordinator for the region is the Associate Business Services representative. All requests for access to OSOS and/or REOS must go through these coordinators.
2. Prior to getting access to OSOS and/or REOS staff must complete the requirements of TA #17-7 including the Individual Access Agreement for OSOS and REOS, the *Cornerstones of Confidentiality* and , if applicable, the interagency Agreements for OSOS and /or REOS.
3. The online training , *Cornerstones of Confidentiality*, must be must be taken annually by all local staff and service providers who have access to sensitive client data and must be advised of potential sanctions for violations of this requirement. The training is available through the Statewide Learning Management System (SLMS).

Maintaining a Secure Environment

1. To ensure that such PII/PPSI is not transmitted to unauthorized users, all PII/PPSI transmitted via e-mail 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. For more information, visit http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

2. Local staff and service providers may not e-mail unencrypted sensitive PII/PPSI.

3. All PPI/PSSI data must be stored in a secure area that cannot be accessed by unauthorized persons. Data may only be processed on equipment approved by the LWDB and NYSDOL.

4. 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.

5. 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.

6. Local staff and service providers shall ensure that any PII/PPSI used during the performance of their job has been obtained in conformity with applicable Federal and State laws governing the confidentiality of information.

7. Whenever possible, the OSOS ID number will be used for participant tracking instead of Social Security Numbers (SSN). 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 (last 4 numbers). In addition, full SSNs should never be emailed, even when using encryption methods.

8. Two times each program year, the Director and Center Supervisor(s) will conduct and document an environmental assessment in the Career Center to determine whether staff are maintaining a secure PII/PPSI environment (both physical and electronic/digital). Completed forms must be maintained by the Security Coordinator for three years.

9. All participant records containing PII/PPSI whether hard copy or electronic, may not be left open and unattended.

10. All participant records and/or documents containing PII/PPSI must be maintained in cloaked cabinets when not in use.

11. 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 following County policy and procedures.

12. Partners will permit NYSDOL and /or USDOL to make onsite inspections in order to conduct audits and/or investigations to ensure compliance, provided reasonable notice is given. Partners will make all relevant records available for NYSDOL/USDOL and/or their authorized designee for inspection, review and/or audit.

Breaches of Confidentiality

1. A breach of confidentiality is an event that compromises or potentially compromises the confidentiality of an individual's or group of individuals' PII/PPSI. This 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:

a. Computers, laptops, CDs, or disks containing a customer's PII/PPSI are missing or stolen;

b. An individual's PII/PPSI is revealed to a third party without a valid consent to do so on file;

c. A customer receives another customer's mail that lists the customer's name, address, and SSN;

d. Department records containing an individual's PII/PPSI are downloaded or copied;

e. An electronic device is infected or potentially infected with a virus or worm; or

f. Discussion of PII/PPSI is overheard by an unauthorized individual.

2. A breach or suspected breach of confidentiality must be reported to the Career Center Supervisor immediately. The Career Center Supervisor must immediately complete a New York State Security Breach Reporting Form. This form shall be emailed to infoSec.IT@labor.ny.gov and OSOS.WDTD@labor.ny.gov, copying appropriate local area Security Coordinators.

3. The Career Center supervisor, local staff and/or service providers will comply with NYSDOL instructions; must cooperate with any investigation commenced by NYSDOL regarding the breach or suspected breach; and are responsible for complying with any corrective action required by NYSDOL to address the breach.

4. All breaches are required to be reported in compliance with the New York State Breach Notification Act. The New York State Information Security Breach and Notification Act is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law.

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.*