Capital Region Workforce Development Board

Securing & Protecting Personally Identifiable & Sensitive Information (PII & PPSI) Policy

Adopted 6/17/2022

PURPOSE

Establish a uniform policy to secure and protect PII and PPSI across the New York State Workforce Development System; and identify the related roles and responsibilities of Local Workforce Development Boards (LWDBs), Career Center and partner agency staff (hereafter called 'local staff'), and service providers.

POLICY

The Capital Region Workforce Development Board (CRWDB) local staff and service providers will ensure 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.

The Capital Region Workforce Development Board (CRWDB) and local staff and service providers will take measures to address the following topics to reduce the risks associated with the collection, storage and dissemination of Career Center customer's PII/PPSI:

A. Accessing and Sharing of PII/PPSI;

B. Security Protocols related to OSOS and REOS;

C. Maintaining a Secure Environment; and

D. Breaches of Confidentiality.

A. Accessing and Sharing PII/PPSI

1. Before being granted access to PII/PPSI, the CRWDB staff and service providers will have data confidentiality policies and procedures in place. Local staff and other personnel must acknowledge their understanding of such policies, including safeguards with which they must comply in their handling of PII/PPSI. It is important to note that improper disclosure may result in civil and criminal sanctions.
2. 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.
3. CRWDB local staff and service providers must not extract information from data supplied by their funding source for any purpose not stated in the grant or contract agreement.
4. PII/PPSI data obtained by CRWDB 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).
5. 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 on the Freedom of Information Law page.

B. Security Protocols related to OSOS and REOS

1. Security Coordinators: The CRWDB, Inc. and the New York State Department of Labor (NYSDOL) ensure Security Coordinators are in place to enforce data security requirements related to the use of OSOS and REOS for: CRWDB local staff, service providers who have been provided access to OSOS and REOS through the local area, NYSDOL staff, and non-federally funded partner staff in each Career Center (comprehensive, affiliate and specialized) in the local area. Their contact information must be readily available in the Career Center.
2. Prior to gaining access to the OSOS and/or REOS, CRWDB local staff and service providers will comply with Workforce Development System Technical Advisory (WDS TA) # 17-7: Use of One-Stop Operating System and Re-Employment Operating System (06/28/17). WDS TA #17-7 includes confidentiality agreements related to OSOS and REOS that must be completed appropriately by all LWDB partners in order to gain access to these systems.
3. Annual staff confidentiality training: CRWDB 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 CRWDB local staff, service providers and other personnel with access to OSOS and/or REOS data will take the online training, Cornerstones of Confidentiality, annually. This training is accessible via the Statewide Learning Management System (SLMS)

C. 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. CRWDB local staff and service providers must not e-mail unencrypted sensitive PII/PPSI to any entity.
3. 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 CRWDB, Inc. 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, 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 are 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. CRWDB 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.
7. Whenever possible, the OSOS ID number must 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. In addition, full SSNs should never be emailed, even when using encryption methods.
8. CRWDB local managers/supervisors will conduct and document an environmental assessment in all CRWDB Career Centers to determine whether local staff are maintaining a secure PII/PPSI environment (both physical and electronic/digital).
9. Records containing PII/PPSI, whether hard copy or electronic, may not be left open and unattended.

10. Hard copy documents containing PII/PPSI must be maintained in locked cabinets when not in use.
11. CRWDB 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.
12. 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. To ensure proper disposal, adhere to NYS Sanitization & Disposal Policy.
13. CRWDB and local 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.

D. 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. 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:
    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 CRWDB Executive Director immediately. The CRWDB Executive Director must immediately complete a New York State Security Breach Reporting Form.
3. The CRWDB 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.

REFERENCES

- TEGL 39-11, Guidance on the Handling and Protection of Personally Identifiable Information (PII): http://ows.doleta.gov/dmstree/tegl/tegl2k11/tegl_39-11.pdf
- New York State Information Technology Standard: Sanitization/Secure Disposal 6 (10/17/14) https://www.its.ny.gov/sites/default/files/documents/Enterprise_Sanitization_Secure_Disposal_Standard_v1.1.pdf
- Privacy Act of 1974: https://www.justice.gov/opcl/privacy-act-1974
- New York State Freedom of Information Law: http://www.dos.ny.gov/coog/freedomfaq.html
- New York State Breach Notification Act: https://its.ny.gov/breach-notification

FOR INQUIRIES

CRWDB Executive Director

CapitalRegionWDB@capreg.org