Title: Protection of Personally Identifiable Information (PII)

Purpose: To provide a policy and guidance on handling and protection of Personal Identifiable Information as outlined in TEGL 39-11

Ratified: January 19, 2022

Background

As part of the WIOA grant activities, the American Job Center/One-Stop Career Center, as overseen by the Gloucester County WDB, may have in their possession large quantities of PII relating to the organization and staff; subgrantee and partner organizations and staff; and individual program participant. This information is generally found in personnel files, sub-recipient files, AOSOS (case management), and data sets. This policy relates to data privacy, security, and protecting the personally identifiable and sensitive information of all AJC/One-Stop Career Center customers.

WDB Responsibilities/Requirements

The Gloucester WDB is responsible for following the procedures outlined in TEGL 39-11 – protecting sensitive client information. The WDB and its sub-recipient grantees must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with WIOA funded grants.

- To ensure that PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) compliant and National Institue of Standards and Technology (NIST) validated cryptographic module.[1] Grantees must not e-mail unencrypted sensitive PII to an entity, including ETA or contractors.
- PII data obtained through AOSOS or from the participant or sub-recipient grantee will be ensured that the privacy and protection of the information from unauthorized disclosure.
- As part of this policy, customer/client information can only be released to partnering agencies (WIOA Title I, II, III, and IV) when the Universal Information Release Form is signed by the participant (see attachment).
- Grantees and staff acknowledge that all PII data obtained will be stored in an area that is physically safe from access by unauthorized persons at all times and the data will processed using grantee-issued equipment, and managed IT services (i.e. AOSOS, OMEGA, DocuSign, etc).
- Grantees must not extract information from data supplied by WDB for any purpose not stated in the agreement.
- Access to PII created by the WDB/WIOA/WFNJ grant must be restricted to only those employees of the grant recipient who need it in their official capacity to person duties in connection with the scope of work in the grant agreement.
- All PII data will be destroyed after satisfying Federal records retention.

Attachments (1) Training and Employment Guidance Letter NO. 39-11 (2) Universal Information Release Form

[1] Informatin of FIPS 140-2 standards and cryptographic models, grantees should refer to FIPS PUB 140-2 located online at: https://csrc.nest.gov/publications/fips/fips140-2/fibs1402.pdf