COASTAL COUNTIES WORKFORCE, INC.
Your partner in business development and economic prosperity...

Subject:	Personally Identifiable Information (PII) Policy for CCWI
Purpose:	To transmit Area 4's policy on PII
Statutory Authority:	Workforce Innovation and Opportunity Act (WIOA), H.R. 803, 113th Cong., (2013-2014): (38) (final regulation TBD)
Action:	CCWI staff is required to adhere to all policies and guidelines set forth in the policy below.
Effective Date:	September 10, 2015
Revision Date(s):	N/A
Expiration Date:	Indefinite

Personally Identifiable Information (PII) and Sensitive Information Policy Statement

As a general practice, Coastal Counties Workforce, Inc. does not obtain or hold personally identifiable information; solely the service provider preserves such information. However, in the event that information is shared and/or stored in CCWI offices, all rules/guidance as outlined in TEGL No. 39-11 will be applied as appropriate.

Per TEGL 39-11, PII is defined "as information that can be used to distinguish or trace an individual's identify, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual."[1]

Sensitive Information is defined as "any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act."[2]

For CCWI, the service provider, and its staff, in any instance when PII or sensitive information is obtained the receiver will ensure compliance with Federal law and regulations and the following provisions shall apply:

- All PII obtained will be protected from unauthorized disclosure

[1] U.S. Department of Labor. Employment and Training Administration Advisory System. Advisory: Training and Employment Guidance Letter No. 30-11. Washington D.C. (June 28, 2012), http://wdr.doleta.gov/directives/attach/TEGL/TEGL_39_11_Acc.pdf. August 20, 2015.

[2] Ibid.

- Any PPI used during the performance of the grant has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information
- All policies and procedures are in place under which all employees acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply
- Staff will not extract information for any purpose not stated in the grant agreement
- Any PII created by the grant must be restricted to only those employees who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement
- PII data requested by ETA must not be disclosed to anyone but the individual requestor except as permitted by the Grant Officer
- ETA and Maine Department of Labor (MDOL), as applicable, will be allowed to make onsite inspections during regular business hours for the purpose of conducting other investigations to assure that CCWI and the service provider is complying with confidentiality requirements
- CCWI will retain data received from ETA only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements, if any

Additionally, the service provider and its staff will adhere to the following provisions:

- 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) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. The service provider will not e-mail unencrypted sensitive PII to any entity
- All PII data obtained shall be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed using service provider issued equipment, managed information technology (IT) services, and designated locations approved by CCWI. Accessing, processing, and storing of ETA grant PII data on personally owned equipment, at off-site locations e.g., employee's home, and non-service provider managed IT services, e.g., Yahoo mail, is strictly prohibited unless approved by the ETA.
- All employees will be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil sanctions for noncompliance with such safeguards that are contained in Federal and state laws
  All PII will 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 devises 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 a secure location.

LWIB Approved: September 10, 2015