Catawba Regional
Council of Governments

CATAWBA WIOA LOCAL INSTRUCTION PY23-20

TO:	Grantee
SUBJECT:	Confidentiality of EO records and PII Data
ISSUANCE DATE:	January 17, 2024
EFFECTIVE DATE:	January 17, 2024
EXPIRATION DATE:	Indefinite

Purpose: To provide local guidance on handling of confidential Equal Opportunity (EO) records and Personally Identifiable Information (PII).

Background: PII is the information that can be used to uniquely identify, contact, or locate specific individuals. Examples of PII elements include: name, address, date of birth, race, gender, and familial status. In accordance with 29 CFR S 38.41, each recipient must collect and record the race/ethnicity, sex, age, and where known, disability status, of every applicant, registrant, participant, terminee, applicant for employment, and employee. Beginning on January 3, 2019, each recipient/subrecipient must also record the limited English proficiency and preferred language of each applicant, registrant, participant, and terminee.

Policy: Working with and protecting PII is an essential part of every job function. EO and PII information must be stored in a manner that ensures confidentiality and is used only for the purposes of recordkeeping and reporting; determining eligibility, where appropriate, for WIOA Title I financially assisted programs or activities; determining the extent to which the recipient is operating its WIOA Title I financially assisted program or activity in a nondiscriminatory manner; or other use authorized by law.

Any medical or disability-related information obtained about a particular individual, including information that could lead to the disclosure of a disability, must be collected on separate forms. This information must be maintained in one or more separate files, whether in hard copy, electronic, or both, apart from any other information about the individual, and treated as confidential. Both electronic and hard copy files must be locked or otherwise secured (for example, through password protection).

Persons in the following categories may be informed about an individual's disability or medical condition and have access to the information in related files under the following listed circumstances:

- Program staff who are responsible for documenting eligibility, where disability is an eligibility criterion for a program or activity.
- First aid and safety personnel who need access to underlying documentation related to a participants' medical conditions in an emergency; and,
- State and federal government officials are engaged in enforcing WIOA and its nondiscrimination and EO regulations.

PII handling

Physical PII

- All locations where sensitive data is stored should be secured physically. Office spaces, storage closets, and file cabinets should all be locked with a key possessed only by authorized staff members.
- PII should not be left plainly visible on desks, printers, or fax machines. Printed documents with PII should never be freely accessible and/or unattended.
- A cover sheet should always be used when transmitting PII via fax.

Electronic PII

- PII must only be used and stored on equipment approved by the Grantee or Grantor
- All computers must be running operating systems and antivirus software that are approved by the grantee or grantor and are up to date.
- Never use your personal email or other accounts to transmit PII.

Employees who have access to PII are prohibited from:

- Publicly displaying or otherwise unlawfully disclosing any person's PII.
- Using PII as a primary account number or printing PII on any identification badge, membership card, permit, or license.
- Mailing documents containing PII where the number is visible on or from the outside of the envelope or packaging.
- Including more than four sequential digits of a social security number
- Transmitting PII over the internet or computer system network unless the connection is secure
- Require an individual to use or transmit all or more than 4 sequential digits of his or her SSN to gain access to internet website or a computer system or network
- Utilizing SSN as passwords for access to computer systems.

When SSNs or any other PII are visible on any documents, staff should ensure the information is marked with a black marker and is not visible before uploading documents in SCWOS. No social security cards are to be uploaded in SCWOS. When utilizing Eligibility Explorer, staff needs to review all uploaded documents for PII information and delete any confidential information.

Supervisors, managers, and other necessary personnel may be informed regarding restrictions on the activities of individuals with disabilities and regarding reasonable accommodations for such individuals.

Effective security is a team effort involving the participation and support of every individual who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

If you have any questions or comments, please call Amanda Baker at 803-327-9041.

Amanda Baker

Amanda Baker
WIOA Administrator