VIRGINIA CAREER WORKS

NEW RIVER | MOUNT ROGERS REGION

POLICY

TITLE:	Personal Identifying Information	PROGRAM:	Adult/DLW/Youth
EFFECTIVE DATE:	10/01/2020	REVISIONS:	

Purpose:
To establish the importance of protecting Personal Identifying Information (PII) within the workforce development system in Local Workforce Development Area 2.

Reference:
DOL TEGL 39-11
VWL 19-05

Definitions:
Personal Identifying Information (PII) – PII is defined as 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.

Sensitive Information – any classified 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.

Protected PII and non-sensitive PII – the Department of Labor has defined two types of PII, Protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

- Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, Social Security Number (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifies (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

- Non-sensitive PII, on the other hand, is information that if disclosed, by it, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not likely or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, email addresses, business addresses, business telephone numbers, general education credentials, gender or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected of sensitive PII.

Policy:
All PII and other sensitive data are to be saved using at least password protection. Information saved on mobile devices (flash drives, external hard, etc.) must be encrypted. If a file must be shared via email, the file must be encrypted. Any participant information that is transmitted or stored on the above named devices should not include Social Security Numbers (SSNs) or Date of Birth. Information concerning a participant should include only State ID, User Name or User ID from the Virginia Workforce Connection (VaWC) when provided as part of a data correction or related VaWC transaction.

All PII used during the performance of the grant will be obtained in conformity with applicable Federal and State laws governing the confidentiality of information.

All PII data obtained through federal funded programs 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 grantee/sub grantee issued equipment, managed information technology (IT) services, and designated locations approved by the New River/Mount Rogers Workforce Development Board. Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations and non- grantee managed services is strictly prohibited.

NR/MR WDB staff and Program Operator employees and other personnel who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and state law.

NR/MR WDB staff and Program Operator employees must not extract information from federally funded programs for any purpose not stated in the grant agreement, contract, and/or memorandum of understanding (MOU).

In the event that NR/MR WDB staff or Program Operator employees suspects, discovers or is notified of a data security incident or potential breach of security relating to personal information, the New River/Mount Rogers Workforce Development Board shall as soon as possible, but no later than twenty four (24) hours from the incident, notify the WIOA Title I Administrator and Grant Recipient. The notification shall include the following:

1. Approximate date of the incident;
2. Description of cause of the security event and how it was discovered;
3. Number of individuals affected and type of PII involved; and
4. Steps taken/to be taken to remedy the event.

The NR/MR WDB will also comply with notification requirements in 18.2-186.6 of the Code of Virginia.

All participants in federal funded programs administered by the New River/Mount Rogers Workforce Development Board must sign a disclosure and release to provide information regarding PII and authorizing the use of PII for purposes of the grant(s).

NR/MR WDB staff and Program Operators should refer to Virginia Workforce Letter #19-05 for additional definitions and clarification on PII.