VIRGINIA CAREER WORKS

PIEDMONT REGION

Title:	Personal Identifying Information Policy	**Policy #:**	13
Effective Date:	July 16, 2020	**Revision Date:**	February 2, 2021

Purpose:

To establish the importance of protecting Personal Identifying Information (PII) within the workforce development system in Local Workforce Development Area 6.

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 transmitted via email or stored on CDs, DVDs, thumb drives, etc. 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 Virginia Career Works – Piedmont Region (VCW – Piedmont). Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations and non-grantee managed services is strictly prohibited.

The individual may agree in writing to release all or portions of their information and be provided the opportunity to indicate what information may and may not be shared. The consent may be modified or revoked by the individual at any time by providing written notice. Customer initials should be obtained to document customer designations and subsequent changes.

Instructions to Protect PII:

Before collecting PII or sensitive information, all participants in federal funded programs administered by the VCW – Piedmont must sign a disclosure and release to provide information regarding PII and authorizing the use of PII for purposes of the grant(s).

Whenever possible, ETA and VCCS recommend the use of unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record. WIOA uses the State ID, which is a system-generated number not related to the SSN. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. 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.

Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding, or using a burn bag) and securely deleting sensitive electronic PII.

Do not leave records containing PII open and unattended.

All documents containing PII shall be stored in locked cabinets when not in use.

Do not use any PII as identifiers on participant file folders

Piedmont Workforce Development Board (PWDB) 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.

PWDB 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).

Any breach or suspected breach involving the improper disclosure of PII is to be immediately reported to the OneStop Senior Management and Director, and the Executive Director of the PWDB.

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

Steps to Mitigate Data Security in the Charlottesville OneStop Center

- Secure password lengths that are only provided to the individual. In cases such as resource rooms these passwords are only provided to the staff managing the room.
- Administrator accounts for the computers are only provided / utilized by IT staff. End users and resource room managers are not provided with Administrative access.
- The computers are protected by Forticlient software. This software provides real-time protection from malware, and viruses. In addition to provides real-time URL filtering to aid in blocking access to dangerous sites.
- Remote access to the devices is limited to IT staff.
- Computers go to a locked screensaver after 20 minutes of inactivity.
- Company user accounts are monitored by Microsoft E3 and E5 protection monitoring tools.

Steps to Mitigate Data Security in the Culpeper and Orange OneStop Centers per the RGI network (Rappahannock Goodwill Industries)

- Password complexity requirements are enabled for all staff accounts. Password sharing and visibility is forbidden for all user accounts.
- In cases such as resource rooms - passwords are only provided to the staff managing the room.
- Administrator rights/accounts are strictly limited to IT staff. IT admin accounts require 2FA. End users and resource room managers have no administrative rights or access.
- Computers are protected by Microsoft Defender and TrendMicro Security Suite. These provide layers of protection from intrusion attempts, malware and viruses. TrendMicro includes browser security and URL filtering to prevent unsafe/inappropriate websites and content. RGI's Meraki networks also have URL filtering enabled globally.
- Remote access to computers is limited to IT staff.
- Computer monitor/displays blank at 10 minutes of inactivity, and PCs lock/sleep at 30 minutes of inactivity.
- User accounts and information are secured and monitored with Microsoft E3 licensing and Azure.

The Virginia Workforce Connection system is cloud-based and security Is managed by the State of Virginia.

112 Non-Disclosure/Confidentiality
Revision Date: 01/25/2005, 01/18/2018

The protection of confidential business, propriety and employee information and records is viral to the interests and the success of GIV. Such confidential information includes, but is not limited to:

- Customer list
- customer preferences
- financial information
- marketing strategies
- pending projects and proposals
- data processing and other computer data
- client information
- personnel information and data
- internal memos, emails, or meeting documents

Employees are prohibited from using, copying, or disclosing any such confidential information to any other person, employee, firm, corporation, or other entity, either during or subsequent to your employment, except as authorized in writing by the Chief Executive Officer and/or business segment authorized by the Chief Financial Officer "ONLY."

Employees must comply with GIV's Health Insurance Portability and Accountability Act (HIPAA) policies and procedures. The HIPAA policies and procedures reside with the HIPAA Privacy Officer.

Employees who improperly use or disclose trade secrets or confidential business information or employee information will be subject to disciplinary action, up to and including termination of employment and legal action, even if thy do not actually benefit from he disclosed information.

Additionally, all Goodwill WIOA staff are required to maintain the security of all participant records by keeping them in either a locked filing cabinet or in a filing cabinet within a locked office. Staff complete all WIOA mandated confidentiality agreements prior to the state WIOA unit providing staff access to the Virginia Workforce Connection system.