Title: File and Information Maintenance Policy	**Related Forms:** Yes
Effective Date: 1/27/2017	**Revised Date:** 9/22/2022

Purpose
To protect confidentiality of all private and personal information and maintain files in an organized and relevant manner.

References
- VWL #14-02 Guidance on the Handling and Protection of Personally Identifiable Information
- Privacy Protection Act of 1980
- VWL #16-03 Standardized Participant File Format
- VWL #16-03 Attachment A, Standardized Participant File Format
- VWL #19-05 Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- 29 CFR Part 37
- VWL #11-03 Record Retention
- VWL #14-09 Timely Data Entry
- TEGL 39-11 Guidance on the Handling and Protection of Personally Identifiable Information
- VWL #20-06 WIOA Participant Activity Code Definitions, Projected Durations & Use Projection Limitations
- VWL #20-07 Change 2 Virginia Workforce Connection System of Record & Electronic Case Files

Policy
The Greater Roanoke Workforce Development Board (GRWDB) is committed to protecting personally identifiable information (PII) and other confidential information. Signed consent forms must be obtained for an individual to authorize the release of personal information. Additionally, the GRWDB will follow all state guidelines and guidance regarding file format for WIOA programs.

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

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 identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

Non-sensitive PII is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is standalone 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, e-mail 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 or sensitive PII.

Procedure

All WIOA customers must be advised of this policy. All GRWDB Staff and Service Provider staff are required to sign a confidentiality pledge which specifies that the individual is aware of the priority placed on confidentiality and the customer's right to privacy. The pledge will also include an understanding that when/if their role terminates/changes, all PII obtained that is no longer required for job duties must be surrendered to the GRWDB at that time. In projects for feedback, performance or other statistical goals, results may only be reported as group data, no individual results may be reported. This same policy holds true for collection of market opinion surveys, panel or focus group findings and research of satisfaction among other customer groups.

Prior to collection of PII or sensitive personal information:

- Individuals shall be notified that such information will only be used for purposes of service under the WIOA-funded grant program and its attendant regulations. As part of the WIOA program application individuals shall sign a release acknowledging such.
- Individuals shall also be notified that with written consent, such information may be shared with other partner organizations for purposes of referral and potential coordination of services beyond WIOA.
- The individual may agree in writing to release all or portions of their information and be provided the opportunity to indicate what information may or may not be shared. The individual may also indicate if there are specific organization(s) to which their information 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.

Written consent for release of information will remain in effect from the date of signature for 3 years allowing for the training period and follow up to occur. The customer will be advised of this policy at the time of the signing of the release form. If the customer objects to signing due to the 3-year timeframe, an adjustment in timeframe may be made by GRWDB staff. The consent form will state that the participant's information may be used for reporting purposes because of federal regulations associated with the benefit of federal funds and that the participant's personal information will remain confidential.

To protect PII once collected, the following guidelines must be followed:

- PII of WIOA participants shall not be transmitted by email or stored on CDs, DVDs, thumb drives etc. unless it can be encrypted using federally approved standards. Only the GRWDB may grant such permission with advance written approval and, at the time of the request, will convey the necessary standards to be followed.
- PII and sensitive data will only be retained and destroyed in accordance with state guidance.

- No PII or sensitive information will be used for any purpose other than necessary under WIOA. Any information collected for customer service or continuous improvement efforts will be aggregated, reported anonymously without any connection to an individual.
- When/if there is a change in Service Provider/WIOA Staff, all PII that has been collected by that staff person/provider must be surrendered to the GRWDB in order to transfer it to the new provider/staff.

Files should be documented properly for all activities with clients. For example, if Staff Assisted Job Search is provided, a copy of the job listing or flyer for the job fair that client was referred to should be placed in file to substantiate action. Each activity should have documentation to explain and show how the activity was provided. Additionally, any & all barriers that are identified should be addressed within each client's IEP (Individualized Employment Plan). For example, if an individual is identified as being basic skills deficient, that barrier should be identified within the IEP with steps and actions to eliminate or mitigate that barrier.

All files and other work-related records shall only be in possession of staff as needed for their specific job duties. Access to any PII must be restricted to only those employees funded by WIOA Title I that need it in their official capacity to perform duties in connection with the scope of work in the grant agreement, contract, or MOU. When/if any individual is no longer in need of any files or records for the duties of their job, all records & files must be returned to GRWDB staff. Formal documentation of the return or surrender of records may be required. Records and files may include, but are not limited to, program participant files, access to electronic records, access to work-related software programs, work phone and/or phone information (i.e.: texts, pictures, etc.), and emails.

Data Breach
Failure to comply with the requirements included in this policy and any guidance referenced above, or any improper use or disclosure of PII for an unauthorized purpose, may result in termination or suspension of the employee, contract or memorandum of understanding, or the imposition of special conditions or restrictions, such as the GRWDB may deem necessary to protect the privacy of participants or the integrity of data.

In the event that the GRWDB or contracted service provider suspects, discovers, or is notified of a data security incident or potential breach of security relating to PII, the GRWDB 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 WIOA Title I Administrator will notify the DOLETA Federal Project Officer assigned to Virginia about the data security incident or potential breach. It is also recommended that timely notice of a breach is provided to local workforce development board members and chief local elected officials.

The notification shall include the following:

- Approximate date of the incident
- Description of cause of the security event and how it was discovered
- Number of individuals affected and the type of PII involved
- Steps taken/to be taken to remedy the event

The GRWDB and/or contracted service provider shall also comply with notification requirements outlined in §18.2-186.6. of the Code of Virginia.

Electronic Case Management

The Virginia Workforce Connection (VaWC) will be the only system of record utilized for electronic case records for WIOA Title I programs. Documents uploaded to VaWC must be in PDF format, as it allows a document to retain its pagination, formatting, and fonts. All local staff will follow guidance from the Virginia Community College System (VCCS) regarding electronic case files. The local area will utilize Adobe PDF and DocuSign for electronic signatures, only. Meetings and document inspection will be provided electronically using Zoom. Case-related electronic documents must be stored within the VaWC. Backup copies of documentation may not be stored on any computer's desktop or hard drive. Documentation of participant expenses (i.e.: invoices, supportive services, training contracts, etc.) must all be uploaded into VaWC as documentation as well as all applicable eligibility documentation.