SECTION 9 – PRIVACY, CONFIDENTIALITY, AND RECORDS PROTECTION

9.1 Purpose

This section establishes uniform standards for the protection, confidentiality, storage, transmission, and destruction of personally identifiable information (PII) and participant records for all workforce programs administered or overseen by the New River/Mount Rogers Workforce Development Board.

The purpose of this section is to:

- Protect participant privacy
- Safeguard sensitive information
- Prevent unauthorized disclosure of participant data
- Ensure compliance with federal and state confidentiality requirements
- Support audit, monitoring, and oversight requirements

These standards are established in accordance with:

- Workforce Innovation and Opportunity Act (WIOA)
- Training and Employment Guidance Letter (TEGL) 39-11 – Safeguarding Personally Identifiable Information
- Virginia Works Letter (VWL) 19-05 Change 1 – Information Security Requirements
- Applicable federal and state privacy and nondiscrimination regulations

All staff, contractors, subrecipients, service providers, and partners with access to participant information must comply with the requirements established in this section.

9.2 Definitions of Personally Identifiable Information

Personally Identifiable Information (PII) refers to any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information.

Sensitive PII

Sensitive PII includes information that, if disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Examples include:

• Social Security numbers
• Date of birth
• Driver's license or state identification numbers
• Passport numbers
• Financial account information
• Medical or disability information
• Personal identification numbers
• Wage records or tax information

Sensitive PII requires the highest level of protection and must be stored and transmitted using secure methods.

Non-Sensitive PII

Non-Sensitive PII includes information that can identify an individual but generally presents lower risk if disclosed.

Examples include:

• Name
• Address
• Telephone number
• Email address
• Education history
• Employment history

Even non-sensitive PII must be handled in accordance with confidentiality requirements.

9.3 Confidentiality Requirements

Participant information shall:

• Be used solely for authorized program purposes
• Not be disclosed without legal authority
• Not be shared with unauthorized individuals
• Be discussed only in private settings
• Be transmitted securely

Access to participant records shall be limited to staff whose job responsibilities require such access.

9.4 Electronic Data Security

Electronic systems containing participant data must:

- Utilize password-protected access
- Employ role-based access controls
- Require secure authentication
- Be maintained on secure networks
- Be protected by current security software

Staff shall not:

- Share login credentials
- Store sensitive information on unsecured devices
- Use public or unsecured Wi-Fi to access sensitive data without approved protection
- Transmit PII through unsecured email systems
- Store Sensitive PII on personal devices or personal email accounts

Portable storage devices containing PII are strongly discouraged and must be encrypted if used.

9.5 Physical File Security

If physical participant files are maintained:

- Files must be stored in locked cabinets
- Access must be restricted to authorized staff
- Files must not be left unattended in public areas
- Files must not be removed from secure offices without authorization

Workspaces must be secured at the end of each workday.

9.6 Data Transmission

When transmitting participant information:

- Secure file transfer systems should be used whenever possible
- Sensitive information must be encrypted when required
- Fax transmission of PII should be avoided unless secure
- Email containing PII must follow organizational encryption standards

Staff must verify recipient identity prior to transmission.

Sensitive PII must not be transmitted through unsecured email or unencrypted portable storage devices.

9.6.1 Prohibited Transmission Methods

To reduce risk of unauthorized disclosure, the following transmission methods are prohibited for Sensitive PII unless specifically authorized in writing by the Executive Director and protected by approved encryption controls:

• Sending Sensitive PII through unencrypted email or including Sensitive PII in email subject lines
• Sending Sensitive PII by text message, chat tools, or social media messaging
• Storing or transferring Sensitive PII on unencrypted removable media including USB drives, CDs, DVDs, or external hard drives
• Uploading Sensitive PII to personal cloud storage accounts or non-approved file-sharing platforms

If Sensitive PII must be transmitted electronically, staff must use Board-approved secure methods such as encrypted email, secure portals, or secure file transfer systems.

9.7 Data Sharing and Partner Access

Participant information may be shared with:

• Authorized One-Stop partners
• Subrecipients
• Contractors
• State or federal oversight agencies

Sharing must:

• Be limited to what is necessary
• Be authorized by law or agreement
• Comply with nondisclosure requirements
• Be documented when appropriate

Data-sharing agreements must include confidentiality provisions.

9.8 Breach Response

If a potential breach of confidential information occurs:

• The incident must be reported immediately to the Executive Director
• Steps must be taken to secure the affected information
• An internal review must be initiated
• Virginia Works or the appropriate funding agency must be notified when required
• Corrective action must be implemented

Failure to report suspected breaches may result in disciplinary action.

Breaches must be reported and addressed in accordance with TEGL 39-11 and VWL 19-05 Change 1.

9.8.1 Breach Response Procedure

A suspected or confirmed breach includes, but is not limited to:

- Lost or stolen devices
- Misdirected emails containing PII
- Unauthorized system access
- Physical records that are lost, stolen, or accessed by unauthorized individuals

Upon discovery, staff must:

1. Report immediately to the Executive Director or designee.
2. Contain and secure the incident by preventing further disclosure.
3. Preserve evidence including emails, logs, and related records.
4. Document the incident including data involved and actions taken.
5. Notify Virginia Works or funders when required.
6. Implement corrective action to prevent recurrence.

9.9 Confidential Information and Nondiscrimination

Information related to disability, medical condition, accommodation, or protected status must:

- Be stored separately when required
- Be accessed only by authorized personnel
- Not be used in discriminatory decision-making

All staff must comply with nondiscrimination regulations under 29 CFR Part 38.

9.10 Record Retention

Participant records shall be retained in accordance with:

- 2 CFR §200.333–200.337
- Virginia Works guidance
- Grant-specific retention requirements

All records — financial records, supporting documentation, statistical records, and other records pertinent to a federal award — must be retained for a minimum of three (3) years from the date of submission of the final expenditure report unless a longer period is required.

Records must remain accessible for monitoring, audit, investigation, or litigation throughout the retention period.

9.11 Secure Destruction

Upon expiration of the retention period:

- Paper records must be shredded
- Electronic records must be permanently deleted
- Destruction must prevent reconstruction of sensitive information

Destruction procedures must comply with organizational standards.

9.12 Staff Training

Staff with access to participant information shall:

- Receive training on confidentiality standards
- Receive training on data security
- Understand breach reporting requirements
- Acknowledge responsibility for safeguarding information

Failure to comply with confidentiality standards may result in disciplinary action.

9.13 Monitoring and Enforcement

Supervisory staff shall periodically review:

- File security practices
- Electronic access controls
- Data transmission practices
- Compliance with confidentiality standards

Violations may result in:

- Corrective action
- Disciplinary action
- Reporting under fraud or misconduct procedures

9.14 Service Provider Records Retention and Access

(Subrecipients, Contractors, and Partners)

All subrecipients, contractors, service providers, and partners that create, receive, maintain, or have access to records related to programs administered or overseen by the New River/Mount Rogers Workforce Development Board must comply with federal and state record retention and access requirements.

A. Records Covered

Service providers must retain and make available, at a minimum:

- Financial records and accounting records
- Supporting documents and source documentation
- Statistical records and performance documentation
- Participant eligibility, enrollment, service, outcome, and follow-up documentation
- Procurement, contract, and invoicing records
- Any other records necessary to document compliance

B. Minimum Retention Period

Service providers must retain covered records for three (3) years from the date the final expenditure report is submitted unless a longer period is required.

C. Exceptions and Extended Retention

If any audit, monitoring review, investigation, litigation, or other action is initiated before the end of the three-year period, records must be retained until all issues are fully resolved.

D. Collection, Storage, and Transfer Standards

Service providers must maintain records that are:

- Complete, legible, and auditable
- Secure from unauthorized access
- Organized for retrieval
- Backed up when stored electronically
- Transferred securely to the Board when requested

E. Access to Records

Service providers must provide the Workforce Development Board, Virginia Works, and federal oversight entities **timely access to records** for monitoring, audit, inspection, and investigation.

F. Contract Clause Requirement

All service provider agreements must include record retention and access clauses consistent with this Section and the Financial Management and Procedures Manual.

Failure to comply may result in corrective action, repayment, sanctions, or termination of the agreement.