Electronic Case Files - WIOA

Effective Date: 3.14.18
Revised: 9.12.18, 3.13.24
Duration: Indefinite

I. Purpose

This document provides guidance for uniform, paperless documentation of participant files and includes instructions to protect customer information. Standardizing the collection of participant information expedites participant eligibility determinations and allows One-Stop Centers more time to focus on providing services. This guidance provides instruction for the collection, dissemination, storage, and protection of information contained within digital files.

II. Background

This guidance originates from multiple regulations related to government agencies' transition from paper to digital files. Among these are: the E-Government Act of 2002, Government Paperwork Elimination Act of 1998, Paperwork Reduction Act of 1995, State of Tennessee's Paperwork Reduction and Simplification Act of 1976, and Tennessee Electronic Records Policy. Section 185 of the Workforce Innovation and Opportunity Act (WIOA) requires recipients of Title I funds to keep records that are sufficient to prepare reports and permit the tracing of expenditures to adequately ensure that funds have not been spent unlawfully. This guidance applies to electronic file storage and documentation imaging standards in the administration of the following Federal programs: WIOA, Wagner Peyser (WP), Trade Adjustment Assistance (TM), and related assistance programs.

III. Instructions

The Tennessee Department of Labor and Workforce Development (TDLWD) - along with numerous other state agencies - has transitioned to paperless record keeping by using an electronic document imaging and storage system. To capitalize on the increased efficiency of data storage and retrieval, TDLWD revised the documentation process for determining eligibility and the maintenance of pertinent records. TDLWD elects to first utilize electronic documents and requires electronic verification of eligibility requirements. Jobs4TN allows internal and external access to provide all servicing partners the means to efficiently administer services to their participants.

Access Management

To gain access to Jobs4TN system, every user must have their own staff account with the minimum privileges necessary to perform their role, as outlined by TDLWD. To request a new account for a staff member, the supervisor must submit a completed Acceptable Use Policy to LWDB staff. LWDB staff will submit a request to TDLWD, which will issue a VOS ID/password that is intended to authenticate and authorize a single user. Sharing access credentials is prohibited and staff are accountable for safeguarding their authentication information. LWDB Staff will review and validate user access on a regular basis. Supervisors are required to notify via email the One-Stop Operator and LWDB staff immediately upon any change in the employment status of a staff member (resignation, termination, suspension, extended leave, job abandonment, etc), including the staff member's VOS ID. LWDB staff will enter the date for termination of access to VOS at the earliest possible date.

Electronic Records

The Jobs4TN system eliminates the need for paper applications for registration and ensures that all Local Workforce Development Boards (LWDBs) are using identical criteria to determine participant eligibility. Customers will receive the same high-quality, efficient service regardless of the local area in which they

reside. In order to case manage participants, LWDBs and the American Job Center (AJC) System must use Jobs4TN to:

- Create participant applications
- Record provided services
- Upload supporting documentation to verify eligibility
- Provide case notes regarding interactions with participants

One-Stop Operator(s) in LWDA5 shall ensure that the use of paperwork is reduced to a minimum (WIOA Section 308[c][2J[FJ[ii]). All forms currently used during an individual's registration within an AJC, specifically following the initial assessment to determine which services are applicable to the long-term success of a program participant, will be replaced by the use of Jobs4TN and its use must be adopted by all AJCs.

All AJCs should utilize the electronic registration whenever possible. The use of electronic records:

- Eliminates the need for storage areas and storage costs associated with paper files
- Saves supply costs and decreases paper waste
- Provides for an easily accessible, single-point of access for file review
- Reduces staff time accessing hard copy documentation
- Ensures more secure storage of sensitive information
- Eliminates lost or misfiled paper documents
- Increases the consistency of file documentation
- Ensures complete verification for program eligibility

The electronic information will be made available to any US Department of Labor or State auditor or monitor who needs access to carry out their official duties. Information will be made available by granting full access to the VOS system or in paper format if requested.

Medical Records

Records containing identifiable health information - also known as protected health information (PHI) under the HIPM Act of 1996 - such as health status, provision of health care, or payment for health care should be maintained in a secure area and in paper format.

Data Validation

The State is required to establish procedures, consistent with the guidelines issued by the Secretaries of Labor and Education, to ensure the information contained in the WIOA federal reports is valid and reliable. Data validation is the process intended to review participant files for accuracy and compliance. Eligibility and verification documentation are reviewed in this process. Additionally, the State requires that the Local Workforce Development Areas (LWDAs) use VOS to upload required participant documentation for data validation. Data validation is an annual review of a sample of participants from the federal report. TDLWD staff will validate that the information recorded in the system on each participant is correct by verifying supporting documentation. This procedure eliminates the need for paper files to be provided by staff in the field, allowing TDLWD to virtually validate supporting documentation. As of the effective date of this guidance, all documents should be uploaded into participant files as they are received by the case manager. The LWDB staff will work with provider staff to establish a process and guidance to ensure each provider has the tools necessary for compliance with the TEGL 39-11, Guidance on Handling and Protection of Personally Identifiable Information (PII) which specifically address the method for uploading and sharing of PII in information management systems.

Deleting Images
Only under limited circumstances will staff be allowed to delete an image that has already been saved to an applicant's electronic file. The process of deleting an already saved image should be performed by the LWDB Staff Performance Coordinator. The LWDB Performance Staff reviews requests for deletion of documents and if determined appropriate, will submit the request for deletion to the Performance and Compliance Unit (ryan.allen@tn.gov), and workforce.board@tn.gov should be cc'd.

Record Maintenance
Subrecipients of funds shall keep records that are sufficient to permit the preparation of reports and to permit the tracing of funds to a level of expenditure adequate to ensure that the funds have not been spent on nonallowable activities. This applies to both paper and digital records. Although digital files are intended to replace paper documents, records must be maintained in a manner that enables staff to produce a tangible, paper copy immediately upon request. Under the direction of the LWDB, LWDA5 will maintain records Pursuant to Records Disposition Authorizations (RDAs) 1586 and 2207 from the State of Tennessee Comptroller of the Treasury, TDLWD which requires the maintenance of records for a period of five (5) years.

Confidentiality of Data or Information and Required Release Forms
Data or information acquired by an agency under a confidentiality agreement, to be used exclusively for statistical purposes, shall not be disclosed by an agency in identifiable form for any use other than an exclusively statistical purpose. Use of this information is prohibited except with the informed consent of the respondent (Public Law 107-347 Title V Section 512[b][1]).

All providers will have a release of information form signed and dated by the participant and the case manager. This form should state that the participant's information may be used for reporting purposes as a result of federal regulations associated with the benefit of federal funds, and that the participant's personal information will remain confidential. The release form will be uploaded into the participant file in VOS to validate that the participant agrees to the release of information for reporting purposes. This standardized form will be made available by the LWDB staff and may be used as a stand-alone form or may be incorporated into other release forms used by the LWDAs.

Family Educational Rights and Privacy
Educational records are covered under the Family Educational Rights and Privacy Act, enacted in 1974. This federal law protects the privacy of student education records. Under this law, students have the right to control disclosure of their education records. Student's education records may be disclosed only with the parent or student's prior written consent, unless (34 CFR 99.31):

- The disclosure is to other school officials, including teachers, within the agency or institution whom the agency or institution has determined to have legitimate educational interests;
- A contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions may be considered a school official under this paragraph provided that the outside party;
- Performs an institutional service or function for which the agency or institution would otherwise use employees;
- Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and
- Is subject to the requirements of§ 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

- An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective and that it remains in compliance with the legitimate educational interest requirement of this section.
- The disclosure is, subject to the requirements of § 99.34, to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer.

Participants who attend training through **WIOA-funded** programs should sign and date a form authorizing the release of educational records to obtain information or copies of certifications or diplomas from educational institutions for data validation and reporting purposes.

Legal Status of Electronic Documents
Electronic records submitted or maintained in accordance with procedures developed under this title, or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form (Public Law 105-277 Title XVII Section 1707).

Attachment A: Acceptable Use Policy: Network Access Rights and Obligations

AUTHORIZED BY:

Michele Holt (Mar 13, 2024 16:29 EDT)
Michele Holt, Director, Workforce Development — Mar 13, 2024 — Date

Marshall Graves (Mar 13, 2024 17:49 EDT)
Marshall Graves, Chair, Workforce Development Board — Mar 13, 2024 — Date

Electronic Case Files Policy effective 3/14/2018; revised 9/12/2028, 3/13/2024

STATE OF TENNESSEE

Acceptable Use Policy
Network Access Rights and Obligations

Purpose:
To establish guidelines for State-owned hardware and software, computer network access and usage, Internet and email usage, telephony, and security and privacy for users of the State of Tennessee Wide Area Network.

Reference:
Tennessee Code Annotated, Section 4-3-5501, et seq., effective May 10, 1994.
Tennessee Code Annotated, Section 10-7-512, effective July 1, 2000.
Tennessee Code Annotated, Section 10-7-504, effective July 1, 2001.
State of Tennessee Security Policies.

Objectives:
- Ensure the protection of proprietary, personal, privileged, or otherwise sensitive data and resources that may be processed in any manner by the State, or any agent for the State.
- Provide uninterrupted network resources to users.
- Ensure proper usage of networked information, programs and facilities offered by the State of Tennessee networks.
- Maintain security of and access to networked data and resources on an authorized basis.
- Secure email from unauthorized access.
- Protect the confidentiality and integrity of files and programs from unauthorized users.
- Inform users there is no expectation of privacy in their use of State-owned hardware, software, or computer network access and usage.
- Provide Internet and email access to the users of the State of Tennessee networks.

Scope:
This Acceptable Use Policy applies to all individuals who have been provided access rights to the State of Tennessee networks, State provided email, and/or Internet via agency issued network or system User ID's. The scope does not include State phone systems, fax machines, copiers, State issued cell phones or pagers unless those services are delivered over the State's IP network.

Use and Prohibitions:

A. Network Resources
State employees, vendors/business partners/subrecipients, local governments, and other governmental agencies may be authorized to access state network resources to perform business functions with or on behalf of the State. Users must be acting within the scope of their employment or contractual relationship with the State and must agree to abide by the terms of this agreement as evidenced by his/her signature. It is recognized that there may be incidental personal use of State Network Resources. This practice is not encouraged and

employees should be aware that all usage may be monitored and that there is no right to privacy. Various transactions resulting from network usage are the property of the state and are thus subject to open records laws.

Prohibitions

- Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation.
- Installing software that has not been authorized by the Office for Information Resources of the Department of Finance and Administration.
- Attaching processing devices that have not been authorized by the Office for Information Resources of the Department of Finance and Administration.
- Using network resources to play or download games, music or videos that are not in support of business functions.
- Leaving workstation unattended without engaging password protection for the keyboard or workstation.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using network resources in support of unlawful activities as defined by federal, state, and local law.
- Utilizing network resources for activities that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.

B. Email

Email and calendar functions are provided to expedite and improve communications among network users.

Prohibitions

- Sending unsolicited junk email or chain letters (e.g. "spam") to any users of the network.
- Sending any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
- Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher.
- Sending or receiving communications that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.
- Sending confidential material to an unauthorized recipient, or sending confidential e-mail without the proper security standards (including encryption if necessary) being met.

Email created, sent or received in conjunction with the transaction of official business are public records in accordance with T.C.A 10-7-301 through 10-7-308, and the rules of the Public Records Commission. A public record is defined as follows:

"Public record(s)" or "state record(s)" means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (T.C.A. 10-7-301 (6)).

State records are open to public inspection unless they are protected by State or Federal law, rule, or regulation. Because a court could interpret state records to include draft letters, working drafts of reports, and what are intended to be casual comments, be aware that anything sent as electronic mail could be made available to the public.

C. Internet Access

Internet access is provided to network users to assist them in performing the duties and responsibilities associated with their positions.

Prohibitions

- Using the Internet to access non-State provided web email services.
- Using Instant Messaging or Internet Relay Chat (IRC).
- Using the Internet for broadcast audio for non-business use.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using the Internet when it violates any federal, state or local law.

Statement of Consequences

Noncompliance with this policy may constitute a legal risk to the State of Tennessee, an organizational risk to the State of Tennessee in terms of potential harm to employees or citizen security, or a security risk to the State of Tennessee's Network Operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the State network could lead to liability on the part of the State as well as the individuals responsible for obtaining it.

Statement of Enforcement

Noncompliance with this policy may result in the following immediate actions.

1. Written notification will be sent to the Agency Head and to designated points of contact in the User Agency's Human Resources and Information Technology Resource Offices to identify the user and the nature of the noncompliance as "cause". In the case of a vendor, subrecipient, or contractor, the contract administrator will be notified.
2. User access may be terminated immediately by the Systems Administrator, and the user may be subject to subsequent review and action as determined by the agency, department, board, or commission leadership, or contract administrator.

STATE OF TENNESSEE

Acceptable Use Policy
Network Access Rights and Obligations
User Agreement Acknowledgement

As a user of State of Tennessee data and resources, I agree to abide by the Acceptable Use Network Access Rights and Obligations Policy and the following promises and guidelines as they relate to the policy established:

1. I will protect State confidential data, facilities and systems against unauthorized disclosure and/or use.
2. I will maintain all computer access codes in the strictest of confidence; immediately change them if I suspect their secrecy has been compromised, and will report activity that is contrary to the provisions of this agreement to my supervisor or a State-authorized Security Administrator.
3. I will be accountable for all transactions performed using my computer access codes.
4. I will not disclose any confidential information other than to persons authorized to access such information as identified by my section supervisor.
5. I agree to report to the Office for Information Resources (OIR) any suspicious network activity or security breach.

Privacy Expectations

The State of Tennessee actively monitors network services and resources, including, but not limited to, real time monitoring. Users should have no expectation of privacy. These communications are considered to be State property and may be examined by management for any reason including, but not limited to, security and/or employee conduct.

I acknowledge that I must adhere to this policy as a condition for receiving access to State of Tennessee data and resources.

I understand the willful violation or disregard of any of these guidelines, statute or policies may result in my loss of access and disciplinary action, up to and including termination of my employment, termination of my business relationship with the State of Tennessee, and any other appropriate legal action, including possible prosecution under the provisions of the Computer Crimes Act as cited at TCA 39-14-601 et seq., and other applicable laws.

I have read and agree to comply with the policy set forth herein.

Type or Print Name	Last 4 digits of Social Security Number
Signature	Date