MID-CAROLINA
Workforce Development Board

Policy Letter #16

TO: **All Mid-Carolina Workforce Development Service Providers**

FROM: **Mid-Carolina Workforce Development Staff**

SUBJECT: **Electronic File Storage and Protecting Personally Identifiable Policy**

PURPOSE

This policy provides guidance on the use of electronic file storage, protecting Personally Identifiable Information (PII), and retrieval of the workforce and other federal funds, participant, program, and financial documents.

BACKGROUND

Local Workforce Development Areas and the North Carolina Division of Workforce Solutions (DWS) must maintain many forms of documentation and data for federal funds purposes. These documents and data may be stored electronically and must have the ability to be retrieved as per the guidance in this policy statement.

US Department of Labor (USDOL) Training and Guidance Letter (TEGL) No. 39-11 provides additional "Guidance on the Handling and Protection of Personally Identifiable Information."

POLICY

Mid-Carolina Workforce Development area and DWS office must meet the minimum requirements as outlined in Attachment I of OG 17-2021 to maintain and protect information. Local Workforce Development areas must also protect consumer Personally Identifiable Information (PII) as outlined in Attachment II. All participant and program-related documents must be scanned in and stored in NCWorks Online.

PROCEDURE

It is expected that Mid-Carolina Workforce Development staff, NCWorks staff, and Service Providers will take necessary steps to protect Personally Identifiable Information data collected from individuals and employers. This includes redacting any unnecessary personal identifiable data when using for verification.

Attachment III of OG 17-2021 outlines the processes and procedures that must be followed when scanning documents into the system.

In addition to the NCWorks Online data, all customer information must be protected as outlined in OG 17-2021 and TEGL No. 39-11.

Redaction should be completed on all documents to remain compliant with federal, state and local policies where applicable. At a minimum, all instances of an individual's driver's license, credit card numbers, bank account numbers, and the first five digits of the SSN ***must*** be redacted. No PII data that is loaded into the state's NCWorks.gov system should be stored or transferred on any portable device.

NC General Statute (NCGS) 20-30 makes it unlawful "To make a color photocopy or otherwise make a color reproduction of a driver's license, learner's permit, or special identification card…" All documents that are scanned into NCWorks.gov ***must be*** scanned in grayscale.

The Mid-Carolina Workforce Development Board requires that eligibility data validation and supporting documentation be uploaded within 14 calendar days from the date of the action. Any exceptions are to be documented in case notes.

REFERENCES

TEGL 39-11: Guidance on the Handling and Protection of Personally Identifiable Information
OG 17-2021: Electronic File Storage and Protecting Personally Identifiable Information

ATTACHMENT

Attachment A: DWS Operational Guidance: OG 17 – 2021

1: North Carolina Guidance for WIOA and Other Federal Funds Electronic Image Storage
2: North Carolina Guidance for WIOA and Other Federal Funds, Protection of Personally Identifiable Information (PII)
3: North Carolina Guidance for WIOA and Other Federal Funds, Scanning Procedures for Consumer Documents in NCWorks

Attachment B: Redaction & Document Saving Procedure

CREATION DATE

July 2022

REVISION DATE

January 2024
December 2024
June 2025

EMPLOYMENT AND TRAINING ADMINISTRATION **ADVISORY SYSTEM** **U.S. DEPARTMENT OF LABOR** **Washington, D.C. 20210**	**CLASSIFICATION** Personally Identifiable Information **CORRESPONDENCE SYMBOL** OFAM **DATE** June 28, 2012

ADVISORY: TRAINING AND EMPLOYMENT GUIDANCE LETTER NO. 39-11

TO: ALL DIRECT ETA GRANT RECIPIENTS
ALL STATE WORKFORCE AGENCIES
ALL STATE WORKFORCE LIAISONS
STATE WORKFORCE ADMINISTRATORS
STATE AND LOCAL WORKFORCE INVESTMENT BOARDS
ONE-STOP CAREER CENTER SYSTEM LEADS

FROM: JANE OATES
Assistant Secretary Jane Oates

SUBJECT: Guidance on the Handling and Protection of Personally Identifiable Information (PII)

1. **Purpose**. To provide guidance to grantees on compliance with the requirements of handling and protecting PII in their grants.

2. **Background**. As part of their grant activities, Employment and Training Administration (ETA) grantees may have in their possession large quantities of PII relating to their organization and staff; subgrantee and partner organizations and staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files and other sources.

Federal agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. The Appendix lists a brief overview of efforts at the Federal level to protect PII. As the grantor agency, ETA is providing this Training and Employment Guidance Letter (TEGL) to grantees to notify them of the specific requirements grantees must follow pertaining to the acquisition, handling, and transmission of PII.

3. **Definitions.**

- PII - OMB defines PII 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.[1]

[1] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), available at http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf

RESCISSIONS None	**EXPIRATION DATE** Continuing

NORTH CAROLINA DEPARTMENT OF COMMERCE
DIVISION OF WORKFORCE SOLUTIONS

DWS Operational Guidance: OG 17-2021

Date: May 28, 2021

Subject: Electronic File Storage and Protecting Personally Identifiable Information (PII)

From:

Chet Mottershead
Assistant Secretary for Workforce

Purpose: To provide guidance on the use of electronic file storage, protecting PII and retrieval of workforce and other federal funds' participant, program and financial documents and to rescind PS 08-2017.

Background: Local Workforce Development Areas (Local Areas) and the North Carolina Division of Workforce Solutions (DWS) must maintain many forms of documentation and data for federal funds purposes. These documents and data may be stored electronically and must have the ability to be retrieved as per this Operational Guidance.

U.S. Department of Labor (USDOL) Training and Employment Guidance Letter (TEGL) No. 39-11 provides additional "Guidance on the Handling and Protection of Personally Identifiable Information."

Action: Local Areas and DWS offices using electronic file storage and retrieval systems must meet the minimum requirements as outlined in Attachment 1 of this Operational Guidance to maintain and protect information. Local Areas must also protect consumer PII as outlined in Attachment 2. Effective July 1, 2015, all WIOA Title I and Title III Wagner-Peyser participant and program-related documents must be scanned in and stored in NCWorks.gov, unless stated differently, for a DWS initiative or activity. Attachment 3 outlines the processes and procedures that must be followed when scanning documents into the system. In addition to NCWorks.gov data, all customer information must be protected as outlined in this Operational Guidance and referenced TEGL.

DWS must use all preventive measures to ensure that the confidentiality and integrity of all PII remains intact. It is expected that all Local Area Workforce Development Boards (WDB), their representatives, and DWS staff will take necessary steps to protect PII data collected from individuals and employers. This includes redacting any unnecessary PII data when using for verification. Further, all PII data collected for use in Workforce Innovation and Opportunity Act (WIOA) programs must comply with the Statewide Security Information Manual.

https://files.nc.gov/ncdit/documents/Statewide_Policies/Statewide-Information_Security_Manual.pdf

Effective Date: Immediately

Expiration: Indefinite

Contact: DWS Program Monitor

Attachment 1: North Carolina Guidance for WIOA and Other Federal Funds Electronic Image Storage
Attachment 2: North Carolina Guidance for WIOA and Other Federal Funds Protection of Personally Identifiable Information (PII)
Attachment 3: North Carolina Guidance for WIOA and Other Federal Funds Scanning Procedures for Consumer Documents in NCWorks.gov

NORTH CAROLINA GUIDANCE FOR WIOA AND OTHER FEDERAL FUNDS

ELECTRONIC IMAGE STORAGE

At a minimum, Electronic Storage and Retrieval Systems must:

- ensure the integrity, accuracy, authenticity, and reliability of the records kept in an electronic format;
- be capable of retaining, preserving, retrieving, and reproducing the electronic records;
- be able to update/convert the records as new technology develops;
- be able to organize documents in a manner consistent with applicable DWS policies;
- ensure that financial and program records maintain a completeness of documentation, are organized by Program Year, and are sufficient for a complete audit trail;
- have adequate disaster recovery plans, including proper anti-virus protection, tamper proof secondary/supplementary data storage facilities such as regular backup in an external hard drive, and stored in a safe location;
- have the ability to convert paper originals stored in electronic format back into legible and readable paper copies; and
- have adequate records management practices in place.

Before implementing the use of an Electronic Storage and Retrieval System, the following requirements must be met by the Local Area:

1. Electronic Data Storage and Retrieval Policies, Procedures and/or Guidelines in place that adhere to all federal, state, and local laws and policies governing the use and storage of electronic data.
2. Adequate computer hardware necessary for implementation, including scanners.
3. Appropriate electronic document storage and retrieval software to include capacity to scan and retrieve documents in universally accepted file formats such as PDF.
4. Adequate organization server storage capacity which complies with record retention and access regulations as outlined by the Workforce Innovation and Opportunity Act, Public Law 113-128, Section 185.
5. Adequate security measures, for example, password protected assigned access.
6. Documented compliance with vendor recommendations regarding security and login identification and conformity with all software vendor licensing guidelines.
7. Appropriate licensure for software including adequate user licenses as recommended by vendor.
8. Appropriate archiving procedures for storing outdated and/or no longer useful documents.
9. Access capability for DWS and federal officials for data validation, monitoring, and auditing as needed.
10. A notification system to contact impacted individuals if data is compromised.

NORTH CAROLINA GUIDANCE FOR WIOA AND OTHER FEDERAL FUNDS

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Each Local Area must take all necessary precautions to protect the PII of consumers. USDOL TEGL No. 39-11 gives the following definitions and information related to PII:

- PII – Federal Office of Management and Budget defines PII 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. [1]

- Sensitive Information – any unclassified 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 USDOL 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.

  1. 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 numbers (SSN), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse name, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information, and computer passwords.

  2. Non-sensitive PII is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked 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 or sensitive PII.

  To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a SSN, a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

TEGL 39-11 lists a number of requirements that must be followed by all grantees to ensure the protection of PII including taking the steps necessary to protect the data from unauthorized disclosure. In addition, the appendix of TEGL 39-11 lists a number of federal laws related to data privacy, security, and protecting PII. These laws should be reviewed and followed by each Local Area in order to fully protect consumer PII from being inappropriately disclosed. Local Areas should stay abreast of current federal, state, and local legislation pertaining to privacy and security of consumer data.

When uploading verifying documentation in NCWorks.gov, protected PII that, if disclosed, could result in harm to the individual whose name or identity is linked to that information should be redacted. **At a minimum all instances of an individual's driver's license, credit card numbers, bank account numbers, and the first five digits of the SSN must be redacted**. Please consult the scanning procedures in Attachment 3 of this document for specific information on how to redact information in NCWorks.gov. NC General Statute 20-30 makes it unlawful "To make a color photocopy or otherwise make a color reproduction of a driver's license, learner's permit or special identification card…" When scanning driver's licenses and social security cards into NCWorks.gov, please be sure that all images are in grayscale.

No PII data that is loaded into the state's NCWorks.gov system should be stored or transferred on any portable devices. This includes laptops, tablets, mobile phones, thumb drives, CDs or other similar devices that are not protected by "Encryption Technology" (North Carolina Statewide Information Security Manual section 0401002).

[1] OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)

NORTH CAROLINA GUIDANCE FOR WIOA AND OTHER FEDERAL FUNDS

SCANNING PROCEDURES FOR CONSUMER DOCUMENTS IN NCWORKS.GOV

In order to ensure consistent consumer information is entered in NCWorks.gov and case files are as complete as possible while still ensuring the protection of consumer PII, the following processes and procedures must be followed when scanning documents into the system.

- NC General Statute (NCGS) 20-30 makes it unlawful "To make a color photocopy or otherwise make a color reproduction of a driver's license, learner's permit, or special identification card…" All documents that are scanned into NCWorks.gov will be scanned in grayscale.

- In addition to the items outlined in NCGS 20-30, any document that would pose an identity theft risk to the individual if stolen should not be scanned in color. This includes but is not limited to the following: social security cards, passports, and birth certificates.

- Each document must be reviewed carefully prior to scanning to identify all items needing redaction. **At a minimum, all instances of an individual's driver's license, credit card numbers, bank account numbers, and the first five digits of the SSN must be redacted**.

- Verify that the documents are complete before scanning. Signature pages should not be scanned separately from the core document. Examples: Applications/intakes, Individual Employment Plans (IEPs), and Individual Service Strategy (ISS) documents.

- Documents must be scanned as separate files into the system rather than as one electronic file containing all the consumer's records. This includes scanning identification documents such as the driver's license and social security card separately.

- Document tags and, where possible, filenames must be clear so that it is obvious what each document in the file list is prior to opening it. Use of a standardized naming system within the board is encouraged.

- After scanning/uploading documents into NCWorks.gov, use the 'redaction tool' found in the "Create Annotations" toolbar to draw a shape over information that needs redacting. Before saving the altered image, make certain that staff has selected under the "Annotation Options" to make the redaction a "Separate layer that can be changed later." Do NOT try to redact information PRIOR to loading it into NCWorks.gov.

- The contents of the electronic file in NCWorks.gov should be identical to the hard copies (or originals) used by staff to capture the information electronically. If a document is updated, such as the Individual Employment Plan (IEP) or work experience agreement, the entire updated document must be scanned into the system as a separate file. Once documents are preserved in NCWorks.gov, when appropriate, their originals should be securely destroyed or secured to further protect customers' information.

- Once in NCWorks.gov, redacted information must be completely unreadable unless the user has the proper permissions to remove the redaction. As stated in Attachment 1, DWS staff and federal officials should have the ability to access redacted information for data validation, monitoring, and auditing purposes. Therefore, redaction should be done in NCWorks.gov ONLY so that the ability to convert paper originals stored in electronic format back into legible and readable paper copies remains.

NORTH CAROLINA GUIDANCE FOR WIOA AND OTHER FEDERAL FUNDS ELECTRONIC IMAGE STORAGE

At a minimum, Electronic Storage and Retrieval Systems must:

- Ensure the integrity, accuracy, authenticity, and reliability of the records kept in an electronic format;
- Be capable of retaining, preserving, retrieving, and reproducing the electronic records;
- Be able to update/convert the records as new technology develops;
- Be able to organize documents in a manner consistent with applicable DWS policies;
- Ensure that financial and program records maintain a completeness of documentation, are organized by Program Year, and are sufficient for a complete audit trail;
- Have adequate disaster recovery plans, including proper anti-virus protection, tamper proof secondary/supplementary data storage facilities such as regular backup in an external hard drive, and stored in a safe location;
- Have the ability to convert paper originals stored in electronic format back into legible and readable paper copies; and
- Have adequate records management practices in place.

Before implementing the use of an Electronic Storage and Retrieval System, the following requirements must be met by the Local Area:

1. Electronic Data Storage and Retrieval Policies, Procedures and/or Guidelines in place that adhere to all federal, state, and local laws and policies governing the use and storage of electronic data.
2. Adequate computer hardware necessary for implementation, including scanners.
3. Appropriate electronic document storage and retrieval software to include capacity to scan and retrieve documents in universally accepted file formats such as PDF.
4. Adequate organization server storage capacity which complies with record retention and access regulations as outlined by the Workforce Innovation and Opportunity Act, Public Law 113-128, Section 185.
5. Adequate security measures, for example, password protected assigned access.
6. Documented compliance with vendor recommendations regarding security and login identification and conformity with all software vendor licensing guidelines.
7. Appropriate licensure for software including adequate user licenses as recommended by vendor.
8. Appropriate archiving procedures for storing outdated and/or no longer useful documents.
9. Access capability for DWS and federal officials for data validation, monitoring, and auditing as needed.
10. A notification system to contact impacted individuals if data is compromised.

NORTH CAROLINA GUIDANCE FOR WIOA AND OTHER FEDERAL FUNDS PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Each Local Area must take all necessary precautions to protect the PII of consumers. USDOL TEGL No. 39-11 gives the following definitions and information related to PII:

- PII – Federal Office of Management and Budget defines PII 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. [1]

- Sensitive Information – any unclassified 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 USDOL 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.

  1. 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 numbers (SSN), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse name, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information, and computer passwords.

  2. Non-sensitive PII is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked 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 or sensitive PII.

To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a SSN, a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

TEGL 39-11 lists a number of requirements that must be followed by all grantees to ensure the protection of PII including taking the steps necessary to protect the data from unauthorized disclosure. In addition, the appendix of TEGL 39-11 lists a number of federal laws related to data privacy, security, and protecting PII. These laws should be reviewed and followed by each Local Area in order to fully protect consumer PII from being inappropriately disclosed. Local Areas should stay abreast of current federal, state, and local legislation pertaining to privacy and security of consumer data.

When uploading verifying documentation in NCWorks.gov, protected PII that, if disclosed, could result in harm to the individual whose name or identity is linked to that information should be redacted. **At a minimum all instances of an individual's driver's license, credit card numbers, bank account numbers, and the first five digits of the SSN must be redacted**. Please consult the scanning procedures in Attachment 3 of this document for specific information on how to redact information in NCWorks.gov. NC General Statute 20-30 makes it unlawful "To make a color photocopy or otherwise make a color reproduction of a driver's license, learner's permit or special identification card…" When scanning driver's licenses and social security cards into NCWorks.gov, please be sure that all images are in grayscale.

No PII data that is loaded into the state's NCWorks.gov system should be stored or transferred on any portable devices. This includes laptops, tablets, mobile phones, thumb drives, CDs or other similar devices that are not protected by "Encryption Technology" (North Carolina Statewide Information Security Manual section 0401002).

[1] OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)

NORTH CAROLINA GUIDANCE FOR WIOA AND OTHER FEDERAL FUNDS SCANNING PROCEDURES FOR CONSUMER DOCUMENTS IN NCWORKS.GOV

In order to ensure consistent consumer information is entered in NCWorks.gov and case files are as complete as possible while still ensuring the protection of consumer PII, the following processes and procedures must be followed when scanning documents into the system.

- NC General Statute (NCGS) 20-30 makes it unlawful "To make a color photocopy or otherwise make a color reproduction of a driver's license, learner's permit, or special identification card…" All documents that are scanned into NCWorks.gov will be scanned in grayscale.

- In addition to the items outlined in NCGS 20-30, any document that would pose an identity theft risk to the individual if stolen should not be scanned in color. This includes but is not limited to the following: social security cards, passports, and birth certificates.

- Each document must be reviewed carefully prior to scanning to identify all items needing redaction. **At a minimum, all instances of an individual's driver's license, credit card numbers, bank account numbers, and the first five digits of the SSN must be redacted**.

- Verify that the documents are complete before scanning. Signature pages should not be scanned separately from the core document. Examples: Applications/intakes, Individual Employment Plans (IEPs), and Individual Service Strategy (ISS) documents.

- Documents must be scanned as separate files into the system rather than as one electronic file containing all the consumer's records. This includes scanning identification documents such as the driver's license and social security card separately.

- Document tags and, where possible, filenames must be clear so that it is obvious what each document in the file list is prior to opening it. Use of a standardized naming system within the board is encouraged.

- After scanning/uploading documents into NCWorks.gov, use the 'redaction tool' found in the "Create Annotations" toolbar to draw a shape over information that needs redacting. Before saving the altered image, make certain that staff has selected under the "Annotation Options" to make the redaction a "Separate layer that can be changed later." Do NOT try to redact information PRIOR to loading it into NCWorks.gov.

- The contents of the electronic file in NCWorks.gov should be identical to the hard copies (or originals) used by staff to capture the information electronically. If a document is updated, such as the Individual Employment Plan (IEP) or work experience agreement, the entire updated document must be scanned into the system as a separate file. Once documents are preserved in NCWorks.gov, when appropriate, their originals should be securely destroyed or secured to further protect customers' information.

- Once in NCWorks.gov, redacted information must be completely unreadable unless the user has the proper permissions to remove the redaction. As stated in Attachment 1, DWS staff and federal officials should have the ability to access redacted information for data validation, monitoring, and auditing purposes. Therefore, redaction should be done in NCWorks.gov ONLY so that the ability to convert paper originals stored in electronic format back into legible and readable paper copies remains.

MID-CAROLINA
Workforce Development

Redaction & Document Saving Procedure

This procedure guides the use of electronic file storage, protecting Personally Identifiable Information (PII - Board Policy #16), and retrieval of the workforce and other federal funds, participant, program, and financial documents enrolled in the WIOA program.

It is expected that Mid-Carolina Workforce Staff, (including Sub-Recipients) will take the necessary steps to protect Personally Identifiable Information (PII) data collected from individuals and employers. This includes redacting any unnecessary personal identifiable data when uploading as verification.

Redaction should be completed on all documents as applicable for compliance with federal, state, and local policies and guidance (OG 17-2021).

Documents for Redaction and File Naming

Eligibility Documents

Social Security Card

All documents containing the participant's social security number(s) should be redacted; *only* the last four digits should be visible with an authorized signature.

- *if the participant does not wish to sign the social security card, please case note*
- *For certain documents, the social security number may already be protected example: xxx-xx-1234, nothing to redact.*

Document/File Name: (SSN) Social Security Card

DD-214

The participant's name and last four SSN, with the word "*honorable discharge*" and authorized signature should be visible.

Document/File Name: (SSN) Social Security Card

School Records

The participant's name, last four SSN, and the enrollment, graduation, and/or expiration date.

Document/File Name: (SSN) Social Security Card

Selective Service

Redact social security number, address, and date of birth. All male U.S. citizens born after December 31, 1959, who are 18 but not yet 26 years old are required to register 30 days before their 18th birthday.

- Selective Service (males 18-25) register at www.sss.gov;
- If using a selective service card, ensure it is signed; and
- If using a selective service notification letter (redact and label accordingly).

Document/File Name: Selective Service (Card &/or Notification Letter)

Family Income / Low Income

- Self-Attestation if applicable
- A family whose total income that does not exceed the higher of – the poverty line; or 70 percent of the lower living standard income level;

Document/File Name: Family Income

Public Assistance
Only the participant's name, date of eligibility, and approval/denial status (eligibility line) should be visible.

- Supplemental Nutrition Assistance Program (SNAP), formerly known as food stamps, is a federal nutrition program that helps with food budget and buying healthy foods.
- Temporary Assistance for Needy Families (TANF) is a time-limited assistance program to assist with a family's basic needs.
- Free Lunch Program: is a federally assisted meal program that provides low-cost balanced meals.

  Note: If the participant is deemed to be Low Income at the time of enrollment the NCWorks system gives the option to skip the Family Size and Income portion of the application.

Document/File Name: Public Assistance (i.e., SNAP or TANF)

Family Size

- *Self-Attestation, if applicable*
- Family: two or more persons related by blood, marriage, or decree of the court, who are living in a single residence and are included in one or more of the following categories:
- A married couple and dependent children,
- A parent or guardian and dependent children, or
- A married couple
- The composition of a family is determined at the *date of the application*. Members in the household who do not meet one of the categories identified in the definition of family are not included in family size.
- Dependent child of family includes children living in a single residence with parent(s) or guardian(s) and who DO NOT meet the definition of the independent child based on the Free Application for Federal Student Aid (FAFSA) guidelines.

Document/File Name: Family Size

Independent Child
Shall include those children living in a single resident with parent(s) or guardian(s) and who fall into one (or more) of the following categories:

- Is 24 years of age or older by December 31 of the current year.
- Is an orphan or ward of the court or was a ward of the court until the individual reached the age of 18.
- Is a graduate or professional student (in college, beyond a bachelor's degree);
- Is a veteran of the Armed Forces of the United States.

- Is a married individual.
- Has legal dependents other than a spouse.
- Is currently living with parents(s) or guardian(s) but provides more than 50% of his/her support

Document/File Name: Family Size

Verification Documents for Date of Birth
For verifying the *date of birth*, follow the below validation information:

- Driver’s License: the participant’s name, date of birth, expiration date, and authorized signature should be visible.
- Passport and/or Birth Certificate: the participant’s name, date of birth, expiration date, and authorized signature should be visible.
- Alien Registration Card: the participant’s name, expiration date, and residence effective (*since*) date should be visible.
- School Records: the participant’s name, current term/year, and date of birth should be visible.
- DD-214 (Department of Defense): the participant's name, date of birth, the words “honorable discharge” and authorized signature should be visible.

Document/File Name: DOB Verification

Verification Documents for Address
For verifying addresses follow the below validation information.

- Driver’s license: the physical address, expiration date, and authorized signature should be visible.
- Utility bills: the address section, billing period, and participant’s name should be visible.
- Lease Agreement the participant’s name, address, termination/expiration date, and authorized signature should be visible.
- VA Income Verification Letter: only the participant’s name and address should be visible.
- *DD-214* (Department of Defense): Certificate of Release or Discharge from Active
- Duty, is a document of the United States Department of Defense, issued upon a military service member's retirement, separation, or discharge from active duty in the Armed Forces of the United States, *only the name, address the words “honorable discharge” and authorized signature should be visible.*
- Enlisted Record Brief (ERB): Also known as Soldier Record Brief (SRB), is a multi-component snapshot that provides the soldier's military career record/information. The below is relating to the document redaction process; *only the name and address information should be visible, and all other information should be redacted.*

Document/File Name: Address Verification (All WIOA funding streams)

Youth- Low Income/High Poverty Area
“Youth living in a high poverty area are automatically considered to be low-income. A high poverty area is a census tract, a set of contiguous census tracts, Indian reservation tribal land, or native

Alaskan village or county that has a poverty rate of at least 30 percent."

- Eligibility required documentation:
- Staff verified based upon address. The Census map tool must be used to determine which areas in the regions may be considered as high poverty. The map must be uploaded in color to the participant's file.

Document/File Name: Youth High Poverty Area

VA Income Verification Letter

This is a letter issued by the Department of Veterans Affairs that verifies financial information used to determine eligibility for VA health care services. Only the participant's name should be visible.

Document/File Name: VA Income Verification Letter

School Verification

- Self-Attestation, if applicable

Document/File Name: Education Verification

School Records

- Diplomas (GED / HSD), Degrees, Certifications (Trade/Vocational), and/or Drop out Letter.

Document/File Name: Education Verification

School Records / Transcripts

Documented evidence of a student's permanent academic record, which usually means all courses taken, all grades received, all honors received, and degrees conferred to a student from the first day of school to the current school year.

- The participant's name, school term/year, school name, and address should be visible; all other information should be redacted.

Document/File Name: Education Verification

Enlisted Record Brief (ERB)

Also known as Soldier Record Brief (SRB), is a multi-component snapshot that provides the soldier's military career record/information. The below is relating to the document redaction process:

- The participant's name, civilian education, technical certification, military education, awards & decorations, and foreign language, including "honorable discharge" should be visible, and all other information should be redacted.

Document/File Name: Education Verification

Education Verification: Highest Level Completed

- If a participant completes high school and earns a bachelor's degree, the highest level completed is the bachelor's degree, or
- if the participant completes high school and one semester of college, the highest level completed is high school.

Document/File Name: Education Verification Highest Level Completed

WIOA Enrollment Documents

WIOA Application – WIOA Initial Assessment 200 service code/417 service code

Document/File Name: WIOA Application

Objective Assessment 203 service code/412 service code

Document/File Name: OA or Objective Assessment

Individual Employment Plan (IEP) 205 service code

Document/File Name: IEP or Individual Employment Plan

Updated IEP 20A service code

Document/File Name: Updated IEP or Individual Employment Plan

Individual Service Strategy (ISS) 413 service code

Document/File Name: ISS or Individual Service Strategy

Updated ISS 41A service code Individual Service Strategy

Document/File Name: Updated ISS or Individual Service Strategy

Assessments – TABE and/or Work Skills 204 service code/417 service code

Document/File Name: TABE Assessments (youth only)

Document/File Name: Work Skills Assessment (type of assessment)

Short Term Pre-Vocational Services 215 service Code / 401 service code

Document/File Name: HRD Course (example)

Enrollment and/or Orientation Documents

The below documents must be completed for all participants enrolling in WIOA Title I Programs which consist of Adults, Dislocated Workers, and/or Youth & Young Adults: 202 service code / 417 service code.

Note: The following orientation documents are to be scanned together as one file; if a document requires updating/correcting only that one document should be corrected, labeled accordingly, and scanned separately.

- Orientation Checklist
- Consent to Release Confidential Information
- Rules & Regulations Governing WIOA Participant
- Nondiscrimination Agreement
- Photo Media Release Form
- HATCH Act (Transparency & Integrity)
- Follow-Up Agreement
- Notice of Selective Service (male only)

Document/File Name: Enrollment and/or Orientation Package

Individual Training Accounts (ITA)

An Individual Training Account (ITA) is a payment agreement established on behalf of a participant with an eligible training provider. The ITA is for tuition and training-related costs noted as mandatory on a course description and/or class syllabus. (BP# 8)

- When the ITA voucher is issued it must be used within 30 days or the semester specified on the voucher.
- If the participant does not enroll in training within the time frame on the voucher a new voucher for services will need to be issued, and the reason for the additional voucher should be case noted.
- The ITA must be completed in its entirety to include the authorized Case Manager and Program Manager's signatures, and the date must be current.

Document/File Name: ITA (course of study semester/term)

Example: CTE Course: ITA – Phlebotomy

Example: Curriculum Course: ITA - CNA Fall Semester

Attendance Records

The Rules & Regulations Governing WIOA Participants (BP# 2), states participants enrolled in WIOA-sponsored training must complete and submit bi-weekly attendance forms. Failure to submit bi-weekly attendance forms within 30 days, may result in termination of WIOA sponsorship.

To comply with BP# 2 of the Rules & Regulations Governing WIOA Participants:

- Can collect the attendance forms (in-person/email), from the case managers.
- Must complete the attendance form in its entirety, with their signature.
- Will then forward the completed form to their instructors via email/in-person, for the instructor's authorization.
- Instructors can then email the authorized attendance form with an email confirmation to the student/case manager.
- Will then remit (in-person/email) the authorized attendance form to the Career Center Case Manager, as attendance verification.
- Note: A snapshot of the Blackboard activities can be used to show attendance and good standing.

Document/File Name: Attendance records (date of attendance)

Example: Attendance records 7.20.2022 – 7.25.2022

Mileage Reimbursement

ONLY if the attendance form is also used to redeem mileage reimbursement, (the mileage redemption portion is located on the same form). The mileage section must be completed and authorized, and attendance records are required as verification for mileage reimbursement.

Document/File Name: Attendance records (date of attendance)

Example: Attendance records 7.20.2022 – 7.25.2022

Supportive Services
Supportive services (BP# 13) may be provided when necessary to enable individuals to participate in career services or training activities. All WIOA Title I participants, that require supportive services, should be stated on the IEP/ISS, and an ITA should be issued and authorized for approval.

Document/File Name: CSS (name of provider)

Example: CSS – Castle Uniforms 7.25.22

Work Experience (WEX)
All sections of the WEX Agreement must be completed and signed by the authorized individuals, the Sub-Recipient of Mid-Carolina, and the Worksite Representative (employer). (BP# 10)

- If the participant is under the age of 18, the Parent &/or Legal Guardian must also sign.
- The WEX Agreement must be signed before the participant begins work at the Worksite
- The WEX Agreement consists of two (2) separate sections the Participant Agreement and Worksite Agreement, both agreements can be scanned as one (1) complete document.

Document/File Name: WEX Agreement

On-the-Job Training (OJT)
All sections of the OJT Contract must be completed and signed by the authorized individuals, the Sub-Recipient of Mid-Carolina, and the Worksite Representative (employer). (BP# 12)
Note: include Workers Compensation Verification (hard copy).

The complete OJT contract consist of the following:

- *Pre-Award Analysis*: contains four (4) sections that must be completed and signed.
- Section 1 Employer Information
- Section 2 Criteria for OJT Employers
- Section 3 Authorized Signatures
- Section 4 Outcome of Pre-Award Interview

Employer Agreement: contains four (4) sections that must be completed and signed.

- Section 1 Contact Information
- Section 2 Contract Agreement
- Section 3 Authorized Signatures
- Section 4 Contract Agreement Modification, if applicable

Training Plan / Training Outline: contains three (3) sections that must be completed and signed.

- Section 1 General Information
- Section 2 Training Outline
- Section 3 Authorized Signatures

Document/File Name: OJT contract

Trainee Evaluation
Can be included in the original OJT contract when uploading (optional),

however, it must be completed following the evaluation criteria Midpoint and/or Final Evaluation.

- Section 1 Evaluation
- Section 2 Authorized Signatures

Document/File Name: OJT Trainee Evaluation (Midpoint and/or Final Evaluation)

Proof of Payment

Any expenditures for WIOA Title 1 (WEX, OJT reimbursement, training providers, supportive services, etc.) require proof of payment to be scanned and labeled accordingly in NCWorks. The payment should specify the purpose, applicable dates, etc., with case note details.

Document/File Name: Proof of Payment

Example: Proof of Payment (WEX PPE 8/5/22)

Example: Proof of Payment (OJT 7/1-31/22)

Example: Proof of Payment (Castle Uniforms 7/25/22)

Payroll Information

Bank Account information: *the participant's name should be visible.* All bank information should be redacted such as.

- Routing number.
- Account number; and
- Bank name and physical address

Document/File name: Bank Account (payroll)

Payroll Documents (Pay Stubs)

- Participants' paystubs can be used for several verifications, as such the participant's name, pay period, and dollar amount should be visible; all other information should be redacted.
- If used for address verification, the participant's address should also be visible.
- Note: If participants are using paystubs to determine the WIOA funding stream, please ensure to case notes; and
- Per OG 16- 2021 *** Note: Staff is not allowed to print and upload UI information from the UI reporting system. Staff may review the UI information and record the appropriate data in the participant's case notes in NCWorks Online. *** which is the Mid-Carolina Local Area recommendation.

Document/File name: Paystubs 7.20.2021 – 7.25.2022 (can include pay period)

Timesheets

If a participant is enrolled in WEX and/or OJT the file should include the participant's completed signed timesheets and a copy of the paycheck/bank deposit (payment verification) for each pay period per month. Timesheets are to be:

- Completed, and scanned with the correct File name
- Correct date worked and number of hours worked,
- Must have the correct Authorized Employer (supervisor) Signatures,
- If the authorized signatures differ, please case note

- Case notes must also contain hours worked and remaining hours, along with any changes that may differ.

Document/File Name (Examples):

Timesheets for PP 07/01/2022 – 07/08/2022
Timesheets for PP 07/10/2022 – 07/15/2022
Payment verification for PP 07/01/2022 – 07/15/2022 (bi-weekly)

Tax Forms

The participant's name should be visible; Tax forms should be redacted as follows:

- For the social security number, only the last four digits should be visible.
- Participant's Address; and

- Tax Identification Number and/or Employee Number

  Document/File name: (type of tax form) i.e., W2 Form

File Name for Document Corrections

- All documents that are being rescanned due to correction should have the word "Update" and case note, where applicable.

  Document/File Name: Updated (document name)

To Avoid Duplication of Documents please DO NOT LINK.

The above-mentioned documents include some but not all the required eligibility documents, please refer to the **WIOA and Wagner Peyser Employment Act Participant Eligibility Reference Guide OG 06 – 2021.**