Policy Number: WIOA I-B – 4.1 Updated Effective Date: August 27, 2018

Confidentiality

PURPOSE: The purpose of this policy is to describe and to detail the requirements for a local confidentiality policy, in accordance with the rules and regulations of Workforce Innovation and Opportunity Act of 2014 (WIOA), the WIOA Final Rule, Training and Employment Guidance Letters (TEGLs) published by the Employment and Training Administration of the U.S. Department of Labor (ETA), and the policies of the Arkansas Workforce Development Board (AWDB).

REFERENCE:

WIOA § 116(i)(3)
TEGL 7-16
20 CFR 677(c)(3)
20 U.S.C. 1232g (Family Education Rights and Privacy Act)
29 CFR 38
ADWS Information Security Policy Manual

POLICY:

Information is critical to the WIOA Title I-B programs. Case managers and other WIOA Title I-B employees have access to personal information that must remain confidential or that may be dispersed only to certain other entities. Every individual with access to such personal information must comply with the Family Education Rights and Privacy Act (20 U.S.C. 1232g) *[WIOA §116(i)(3)]*. Additional security measures are required for information concerning disabilities, for other information provided by vocational rehabilitation agencies *[TEGL 7-16]*, and for state unemployment compensation information *[20 CFR part 603]*.

Any person with access to personal information must read and understand the Family Education Rights and Privacy Act (FERPA) and must receive training on the local confidentiality policy. A signed confidentiality agreement with knowledge and acceptance of the requirements of the FERPA and local policies and the penalties for violation of the requirements, must be maintained in the local files. Confidentiality agreements also must be signed by non-ADWS user of ADWS confidential information *[ADWS Information Security Policy Manual]*.

Written agreements are executed between ADWS and other entities that are allowed access to ADWS confidential information. When a local area uses an ADWS Local Area Network (LAN), written instructions for telecommunications security must be included as part of the agreement. All servers that are connected to the statewide ADWS network must be configured to automatically download and install critical and security updates for the operating system and updates to the anti-virus software on a daily basis, unless otherwise approved by the ADWS Information Security Officer *[ADWS Information Security Policy Manual]*.

Local areas must develop confidentiality policies and procedures to promote the security and confidentiality of personal information. These policies and procedures may be modeled after the appropriate section of ADWS Information Security Policy Manual. The policies and procedures may include, but are not limited to:

- What information must be kept confidential and what information can be disclosed
- To whom confidential information may be given
- Information may be disclosed only on a "need to know" basis
- The manner for storing confidential information that must be maintained for reporting reasons *[29 CFR 38.41(b)(2)]*
- All medical or disability-related information obtained about a particular individual must be collected on forms separate from other information collected from the individual, and treated as confidential. Whether these files are electronic or hard copy, they must be locked or otherwise secured (for example, through password protection) *[29 CFR 38.41(b)(2)]*.
- Forms signed by individuals allowing WIOA to release appropriate information to other entities that might be helpful to the participant
- A process for individuals who request that normally-public information not be disclosed (for example, address of a person who is escaping an abusive ex-spouse)
- Regulations concerning the security of laptop computers when not in use, when taken home, and when traveling
- All computers must be password protected
- All computers must have screen savers with password protection or keyboard locking program activated on them
- Penalties for misuse, mishandling, or unauthorized disclosure or confidential information
- Sensitive personally identifiable information (information that could result in harm to the individual whose name or identity is linked to the information) may not be electronically transmitted unless it is specifically protected by secure methodologies. Sensitive information includes, but is not limited to, place of birth, date of birth, mother's maiden name, driver's license number, biometric information, medical information (except brief references to absences from work), personal financial information, Social Security numbers (including documentation containing only the last four digits), credit care or debit card account numbers, passport numbers, potentially sensitive employment information (e.g., personnel ratings, disciplinary actions, and results of background investigations), criminal history, and any information that may stigmatize or adversely affect an individual *[ADWS Information Security Policy Manual]*.
- Non-sensitive personal identifiable information that may be transmitted electronically without protection include work phone numbers, work addresses, work and personal e-mail addresses, or resumes that do not include a Social Security number or where the Social Security number has been redacted *[ADWS Information Security Policy Manual]*.
- Procedure for disaster recovery of paper and electronic information
- Prohibition on downloading or installing any software or program without consent
- Background checks may be required for individuals with access to confidential information
- The use of the internet is confined to official business only
- The use of network activity may be monitored without an employee's knowledge or consent
- A confidentiality notice that must be appended to all e-mail messages

- Confidential information cannot be discussed or disclosed in telephone conversations unless it is certain that the other party has authorized access to the information
- Prohibition on recording telephone conversations without the consent of the individuals being recorded
- Paper documents must be secured in a manner so that unauthorized access (such as by individuals walking into the room) is unlikely
- Computer monitors must be positioned such that unauthorized viewing is unlikely
- Documents and papers containing confidential information must be shredded personally or taken to a secure storage place to be shredded.
- Computers may be used for business use only
- All servers must contain anti-virus software that is updated automatically