Approved/Amended Date: _____

SOUTHEAST ARKANSAS WORKFORCE DEVELOPMENT BOARD
P. O. BOX 6806
PINE BLUFF, AR 71611

Phone (870) 536-1971 **Fax (870) 536-7718**

southeastarkansas.org/services/workforce/

Confidentiality Policy & Procedures

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) and the Southeast Arkansas Workforce Development Board (SEAWDB).

Reference: (WIOA Law)
https://www.congress.gov/113/bills/hr803/BILLS-113hr803enr.pdf

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 SEAWDB 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].

SEAWDB has developed confidentiality policies and procedures to promote the security and confidentiality of personal information. These policies and procedures are modeled after the appropriate sections of ADWS Information Security Policy Manual.

The policies and procedures 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; passwords should be shared with management/WIOA administration.
- 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

Definitions: Personal and Confidential Information - includes but is not limited to an individual's name; address; telephone number; email address; social security number; date of birth; age; educational records as described in the Family Educational Rights and Privacy Act of 1974, 20 USC 1232g(a)(4); gender; race/ethnicity; employment history (e.g.: employer name, wages, work hours, etc.); financial information (such as household income and student financial aid information, including award status and amounts); and eligibility for special programs (e.g., disability, veteran, dislocated worker, economically disadvantaged, youth, public assistance, SNAP, unemployment insurance programs, offender, ex-offender, foster care, homeless) and any other information that identifies an individual as a special/targeted population participant.

It is the policy of the SEAWDB to protect and safeguard personal and confidential information provided by individuals seeking WIOA or other funded services. Individuals seeking services must be informed in writing via the Authorization of Release and Obtain Information forms that their personal and confidential information:

• May be shared among the SEAWDB partners, staff and subcontractors;
• Is used only for the purpose of delivering services and that further disclosure of their confidential information is prohibited; and

Whether written or oral and regardless of format, staff must maintain confidentiality of the following:

• Information that was created or received by a healthcare provider, health plan, employer or healthcare clearinghouse.
• Information that is related to an individual's physical or mental health or medical condition in the past, present or future; healthcare provided or to be provided to an individual; or payment for healthcare provided to an individual in the past, present, or future.
• Information that identifies an individual, employee or participant as an offender or ex-offender.

The misuse or unauthorized release of personal and confidential information or records may be subject to a civil penalty to the employee or partner of SEAWDB.

Procedures

1. Every individual receiving WIOA or other services must read, sign, and date the Authorization of Release and Obtain Information form and the form shall be kept in the participant's file.
2. Staff should avoid communicating highly sensitive personal and confidential information about an applicant/participant to partner agencies via email. If it is absolutely necessary, staff must ensure that the recipient is the only person who has access to the information and that the recipient understands they also must protect the information. Further, participant information must only be communicated through agency approved email addresses and not through third party or personal email addresses such as Hotmail, Yahoo, Gmail, etc.
3. Social security numbers may not be delivered through email. Staff should discourage participants from emailing personal and confidential information, such as social security numbers to their case managers. However, in the event a staff person receives participant confidential information via email, the case manager should immediately delete the email and subsequently delete the email from the "Deleted Items" folder in Outlook.
4. Should a customer request that personal and confidential information not be shared, this should be noted in ARJobLink and a written statement should be placed at the front of the participant's file.
5. Staff should be discreet when verbally communicating personal and confidential information and ensure the receiver(s) are authorized to receive the information.
6. Staff must not leave personal and confidential information lying out in the open and unattended (e.g., copies or print jobs left unattended on the copy machine or printers).
7. Personal and confidential information must be stored in a secure location when not in use or shredded if no longer necessary. Personal and confidential information should not be tossed in the regular trash or recycle bins.
8. Case notes submitted in ARJobLink (AJL) shall not disclose any highly sensitive personal and confidential information. (e.g. specific health diagnosis, criminal offenses). Case managers should state the barrier to employment or situation generally as categorized in eligibility checklists, but not specifically state any details. The phrase "see confidential file' should be entered in case notes to redirect monitors.
9. Each SEAWDB Workforce Center office will have a designated file cabinet that remains locked for confidential information. The files will contain medical records, criminal history records and other highly sensitive information as described in this policy. This cabinet shall be kept separate from active participant paper files.

10. Active participant files shall be kept in locked designated cabinets at each office.
11. When all services, including follow-up services, are complete and the participate file is ready to be archived, all information from the confidential file that had been previously filed away separately from the active file must be placed in a sealed envelope and marked "Confidential Information" and secured in the participant file. Archive boxes must be clearly marked as containing personal and confidential information.
12. SEAWDB and Workforce Center staff must not use computers for personal use or download any software without prior consent from administration.
13. Equipment that is used for WIOA services must be housed in secure and protected locations at all times. SEAWDB discourages the use of WIOA equipment outside of the office or designated places that are used to conduct WIOA business. When not in use, WIOA equipment should be password-locked and/or stored in a secure place. When traveling for business, the use of WIOA equipment should be authorized by management prior to travel.
14. Participant files containing confidential and personal information shall not be taken away from the Workforce Center or the corporate office of the SEAWDB/SEAEDD.
15. Compliance: All records may be reviewed for monitoring purposes by local state and federal monitors.

Approved:

SEAWDB Chairperson Date

Amended:

SEAWDB Chairperson Date