

---

## Western Arkansas Workforce Development Area Policies and Procedures

---

<b>TITLE</b>	Confidentiality
<b>NUMBER</b>	P#0008-18
<b>TYPE</b>	Policy – Operations
<b>APPROVING AUTHORITY</b>	Western Arkansas Workforce Development Board
<b>EFFECTIVE DATE</b>	6-26-18
<b>MODIFIED DATE(S)</b>	None
<b>NEW/REPLACED</b>	Replace

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. Additional security measures are required for information concerning disabilities and other information provided by vocational rehabilitation agencies [TEGL 7-16] and for state unemployment compensation information [20 CFR part 603]. Confidentiality records are kept in a separate file. The policies and procedures may include, but are not limited to:

- I. What information must be kept confidential and what information can be disclosed;
- II. To whom confidential information may be given;
- III. Information may be disclosed only on a “need to know” basis;
- IV. The manner for storing confidential information that must be maintained for reporting reasons [29 CFR 38.41(b) (2)];
- V. All medical or disability-related information obtained about an 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)];
- VI. Forms signed by individuals allowing WIOA to release appropriate information to other entities that might be helpful to the participant;
- VII. 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);
- VIII. Regulations concerning the security of laptop computers when not in use, when taken home, and when traveling;
- IX. All computers must be password protected;
- X. All computers must have screen savers with password protection or keyboard locking program activated on them;
- XI. Penalties for misuse, mishandling, or unauthorized disclosure of confidential information;
- XII. 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 only the last four digits), credit card 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];
- XIII. Non-sensitive personal identifiable information that may be transmitted electronically without protection include work phone numbers, work addresses, work and personal e-mail addresses, resumes that do not include a Social Security number or where the Social Security number has been redacted [ADWS Information Security Policy Manual];
- XIV. Procedure for disaster recovery of paper and electronic information;
- XV. Prohibition on downloading or installing any software or program without consent;

---

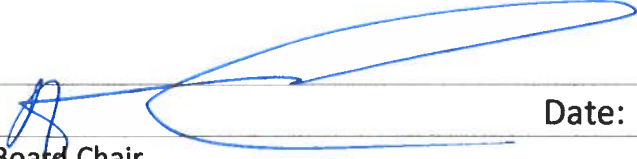
**Western Arkansas Workforce Development Area  
Policies and Procedures**

---

- XVI. Background checks may be required for individuals with access to confidential information;
- XVII. Confidential information cannot be discussed or disclosed in telephone conversations unless it is certain that the other party has authorized access to the information;
- XVIII. Prohibition on recording telephone conversations without the consent of the individuals being recorded;
- XIX. Paper documents must be secured in a manner so that unauthorized access (such as by individuals walking into the room) is unlikely;
- XX. Documents and papers containing confidential information must be shredded personally or taken to a secure storage place to be shredded;
- XXI. All servers must contain anti-virus software that is updated automatically.

---

Approval Signature:



Date: 6/26/18

Miles Crawford, Board Chair