Policy Number: Section 1 Policy 6 Effective Date: 12-9-2024

Confidentiality Policy

Purpose:

The purpose of this policy is to describe and to detail the Confidentiality policy for the Central Area under the WIOA Program.

References:

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 Policy No. – 4.1 (Confidentiality)

Policy:

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.

A signed confidentiality agreement with knowledge and acceptance of the requirements of FERPA and this policy and the penalties for violation of the requirements, must be maintained with the CAWDB's administrative entity.

CAWDB workforce staff shall develop and implement procedures to ensure confidentiality and security of information. They procedures need to address:

- 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
- 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)
- 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].
- Prohibition on downloading or installing any software or program without consent
- 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
- Confidential information cannot be discussed or disclosed in telephone conversations unless it is certain that the other party has authorized access to the information
- 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
- Disposition of documents
- Computers may be used for business use only
- Procedure for disaster recovery of paper and electric information
- Background check may be required for individuals with access to confidential information
- A confidentiality notice that must be appended to all e-mail messages
- Prohibition on recording telephone conversations without the consent of the individuals being recorded
- Documents and papers containing confidential information must be shredded personally or taken to a secure storage place to be shredded
- All servers must contain anti-virus software that is updated automatically

Approved by: Michael Flores Date: 12/9/2024

Title: CAWDB Chairperson