West Central Arkansas Workforce Development Board
Larry Carr, Chairman
P O Box 6409, Hot Springs, AR 71902

Confidentiality and Personally Identifiable Information
Policy and Procedures

Purpose:
The West Central Arkansas Workforce Development Board (WDB) and West Central Arkansas Planning and Development District (WCAPDD) are committed to ensuring client confidentiality and appropriate handling of sensitive information. The purpose of this policy is to specify the requirements for the use, storage, and security of sensitive and confidential information.

References:
5 U.S.C. Section 552a Note TEGL 39-11

Policy:
Under the Workforce Innovation and Opportunity Act (WIOA), staff obtain personal and confidential information from individuals as part of eligibility determination and continuation of services. WIOA stipulates implementation of confidentiality policies and procedures. This policy is required to ensure that representatives with access to participant information maintain confidentiality of information to which they are privy.

It is the service provider's responsibility to inform all staff of the policy and ensure adherence and accountability of it s contents.

Confidentiality - Respecting the privacy of our clients and protecting their confidential information is a basic value of WDB. Employees, contractors, consultants, volunteers and board members of service provider (herein "staff and representatives") may be exposed to information which is confidential and/or privileged and proprietary in nature. As part of grant activities, staff and representatives may have access to large quantities of Personally Identifiable Information (PII) relating to staff and individual program participants. This information could be found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files, and other sources.

All staff and representatives are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. It is the policy of the WDB that such information must be kept confidential both during and after employment or volunteer service.

"Confidential" means that an individual not permitted to disclose clients' names or talk about them in ways that will make their identity known. No information may be released without appropriate authorization. WDB expects all its agents to respect the privacy of clients and to maintain their personal and financial information as confidential.

Access to any PII must be restricted to only those staff and representatives who need it in their official capacity to perform duties pertaining to the scope of work in the grant or contract agreement.

Procedures

All Title I-B staff must complete and sign the Staff Confidentiality Agreement (Attachment A) to document understand this policy and agree to be bound by those terms and conditions throughout their participation in the workforce system.

All Applicant must be informed in writing via the Confidentiality Agreement (Attachment B) that their information will be protected and that their personal and confidential information:

- May be shared among federal and state agencies, partner staff and contractors;
- Is used only for delivering services and that further disclosure of their confidential information is prohibited; and that
- PII will be used for grant and eligibility purposes only.

Every individual receiving an application must read, sign and date a Release of Information Form to share their information with partner agencies. Individuals must be informed that they can request their information not be shared among partner agencies and that this does not affect their eligibility for services by addressing that on that section of the application.

Staff and representatives should engage in practical ways to reduce potential security breaches and protect sensitive information and PII by:

- Reducing the volume of collected and retained information to the minimum necessary;
- Limiting access to only those individuals who must have such access; and
- Using encryption (when possible), strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

Note: See Attachment C for definitions of key terms.

Medical, Disability and Offender Records

Medical, disability and Offender records are additionally protected as confidential information. To ensure the information is protected, any medical, disability or offender records must be kept separately from working participant files and kept in a secured physical and/or electronic location. Only the portion of the participant's information that reveals the presence data element should be included in the participant's file to minimize staff and representative access to files.

Once collected, access to the file should be limited and only accessed:

- With the approval of program management and only when necessary for WIOA service delivery,
- By first aid and safety personnel in the event of an emergency, or
- By local, state, or federal monitors.

When all WIOA services are complete and the participant file is ready to be archived, participant medical and disability-related information must be placed in a sealed envelope and marked "Medical and Disability Information" or "Offender Information" and placed in participant's file.

Social Security Numbers
Social security numbers are additionally protected as high-risk information. When requesting a participant's social security number, staff and representatives should explain how the social security number will be used and how the participant's privacy will be ensured.

An individual is not required to provide their social security number to receive WIOA services, and services cannot be denied to an individual due to their refusal to disclose their social security number (5 U.S.C. Section 552a Note).

Whenever possible, staff and representatives should use unique identifiers such as state ID numbers for participant tracking instead of social security numbers. While social security numbers may be needed for initial eligibility or performance purposes, a unique identifier should be linked to each individual record and used thereafter. This includes such records as training or contract documents. If social security numbers are to be used for specific tracking purposes, they must be stored or used in such a way that it is not attributable to the individual. For example, a training document should not include the participant name and social security number, rather the participant name and a truncated social security number.

Physical Data Security Requirements
All sensitive or PII data obtained should be stored in an area that is physically safe from access by unauthorized persons at all times. Staff and representatives must not leave personal and confidential information lying out in the open and unattended.

When a staff or representative's desk is unattended, it is the staff or representative's responsibility to ensure that personal and confidential information, including PII, is properly filed and stored. This means that all documents containing personal and confidential information must not be left on desks, fax machines, printers, or photocopiers unattended. In addition, any electronic files that are open on the desktop with PII should be closed and computers logged off when unattended to reduce inadvertent security risks.

The WDB expects all staff to secure mobile equipment, such as laptop computers and other devices that may have PII stored on them. Devices should be password protected and safeguarded when not in use.

When not directly working with these documents, documents must be properly filed or stored to prevent inadvertent disclosure of information. Information must be stored in a secure location when not in use or shredded if no longer necessary. Accessing and storing data containing PII on personally owned equipment is discouraged.

Any participant files stored for performance or archiving purposes must be clearly marked as containing personal and confidential information. Staff and representatives should retain

participant PII only for the period required for assessment or performance purposes. Thereafter, all data must be destroyed by a qualified company to minimize risk of breach.

Transmission of Confidential Information

Staff and representatives should avoid communicating sensitive information or PII about an applicant or participant to partner agencies or other staff via email. If it is necessary, staff and representatives must ensure that the intended recipient is the only individual that has access to the information and that the recipient understands they must also protect the information. Staff and representatives must only communicate sensitive information or PII through WIOA emails and not through third party or personal email addresses.

Staff and representatives should discourage participants from emailing personal and confidential information to their career advisors. If a participant sends a staff or representative PII via email, the staff or representative should immediately delete the email and subsequently delete the email from the "Deleted Items" folder in their email.

Any information posted to social media sites is considered public record and is subject to public disclosure. No sensitive information or PII should be posted to social media sites.

Care shall also be taken to ensure that unauthorized individuals do not overhear any discussion of confidential information.

Security Breaches

Any staff or representative who becomes aware of any security breach resulting from the inadvertent or intentional leak of release of confidential information, including PII, shall immediately inform their direct supervisor. Supervisors should assess the likely risk of harm caused by the breach and then assess the level of breach. Supervisors should bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion.

Four factors should be considered to assess the likely risk of harm:

- Nature of the Data Elements Breached
- Number of Individuals Affected
- Likelihood the Information is Accessible and Usable
- Likelihood the Breach May Lead to Harm

Notification of the security breach should be provided to WDB staff if the breach is believed to cause harm and WDB staff should notify Arkansas Division of Workforce Services (ADWS) of all breaches believed to cause harm. Breaches subject to notification requirements include both electronic systems as well as paper documents. The notification should be provided in writing as soon as the breach is found.

The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.);
- What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches.

Staff Compliance

All staff and representatives shall sign an Acknowledgement that they have read the policy, understand the confidential nature of participant and staff data and the potential sanctions for improper disclosure, and agree to abide by all other requirements and terms contained therein.

Unauthorized disclosure of confidential or privileged information is a serious violation of this policy. Any failure to comply with confidentiality requirements identified in this policy may result in termination of suspension of contract or employment, or the imposition of special conditions or restrictions to protect the privacy of participants or the integrity of PII data. Misuse or noncompliance with PII data safeguards could lead to civil and criminal sanctions per federal and state laws.

Staff and representatives are expected to return materials containing privileged or confidential information at the time of separation from employment or expiration of service.

Monitoring

WDB acknowledges that the U.S. Department of Labor, Arkansas Division of Workforce Services, Administrative Entity and their representatives have the authority to monitor and assess compliance with federal, state, and local confidentiality requirements. To ensure that policies are being followed and expectations are being met, WDB staff or a designee will conduct onsite inspections periodically to ensure confidentiality compliance. It will be the responsibility of the program operator to make any corrections and to conduct an internal review if areas of concern are found.

Attachments:

- Attachment A: Staff Confidentiality Agreement
- Attachment B: Participant Confidentiality Agreement
- Attachment C: Definition of Key Terms

Larry Carr
Larry Carr, Chair

12-12-19
Date

Approved on: 12-12-19