POLICY: CONFIDENTIALITY & PROTECTING PERSONAL INFORMATION

EFFECTIVE DATE: DECEMBER 8, 2016 **POLICY NUMBER: 2016-05**

PURPOSE

The Montgomery County Workforce Development Board (WDB) and WorkSource Montgomery (WSM) 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.

BACKGROUND

Under the Workforce Investment 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 of WSM with access to participant information maintain confidentiality of information to which they are privy.

CANCELLATIONS

- Policy 2012-03 – Client Confidentiality Policy and Confidentiality Statement

ACTION REQUIRED

It is the service provider's (e.g., subcontractors, partners) responsibility to inform all staff of the policy and ensure adherence and accountability of its contents.

QUESTIONS

Questions relating to this policy should be directed to the VP of Business and Employment Services at policy@worksourcemontgomery.com or 240-403-4102.

ATTACHMENTS

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

CONFIDENTIALITY

Respecting the privacy of our clients and protecting their confidential information is a basic value of WSM. Employees, contractors, consultants, volunteers and board members of WSM (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 WSM that such information must be kept confidential both during and after employment or volunteer service.

"Confidential" means that an individual is free to talk about WSM, Inc. and about the programs, but an individual is 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. WSM 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

Individuals must be informed in writing via the Confidentiality Agreement in 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 WIOA or other WSM services 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.

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, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

MEDICAL AND DISABILITY RECORDS

Medical and disability records are additionally protected as confidential information. To ensure the information is protected, any medical or disability 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 of a disability or other data element should be included in the participant's file to minimize staff and representative access to medical files.

Once collected, access to the medical 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 or other WSM 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."

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 WorkSource Montgomery emails and not through third party or personal email addresses.

PII and other sensitive data transmitted via email or stored on mobile data storage (such as thumb drives) must be encrypted. Staff and representatives must not e-mail unencrypted sensitive PII to any entity, including the Department of Labor, WDB staff, or contractors.

Staff and representatives should discourage participants from emailing personal and confidential information to their case managers. 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 WSM and the Workforce Development Board if the breach is believed to cause harm. WSM will inform the Maryland Department of Labor, Licensing and Regulation (DLLR) of 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 within 3 business days and should be concise.

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

WSM acknowledges that the U.S. Department of Labor and the State of Maryland 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, WSM 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.

DISCLAIMER

This policy is based on WSM's interpretation of the Workforce Investment and Opportunity Act, Final Rule released by the U.S. Department of Labor, and federal and state policies relating to WIOA implementation. This policy will be reviewed and updated based on any additional federal or state guidance.

REFERENCES

Law

- Workforce Innovation and Opportunity Act of 2014 (WIOA)
- Privacy Act, Section 7 – 5 U.S.C. Section 552a Note (Disclosure of Social Security Number)

Federal Guidance

- Training and Employment Guidance Letter (TEGL) 05-08 – Policy for collection and Use of Workforce System Participants' Social Security Numbers
- TEGL 39-11 – Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- OMB Memorandum M-07-16 – Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Approved
CEO of WorkSource Montgomery, Inc.
Montgomery County Workforce Development Board

Attachment A: Staff Confidentiality Agreement

WorkSource Montgomery Confidentiality Agreement

I, _____ [print name], understand that, by virtue of my position within the Montgomery County Workforce Development System (through the Workforce Development Board, WorkSource Montgomery, or as vendors to WorkSource Montgomery), I may have access to customer and employer confidential records.

I have read and understand the Workforce Development Board's Policy on Confidentiality and Protecting Personal Information. I understand that it is my responsibility as part of the workforce development system in Montgomery County to protect the confidentiality of all Workforce Investment and Opportunity Act (WIOA) applicants and participants, as well as customers utilizing the Montgomery County American Job Centers and any affiliated sites and programs. I understand that in the workforce system's collection, usage, storage and transmission of customer information, the tenets of confidentiality are to be strictly enforced.

I understand that violation of this policy could result in disciplinary action, which could include verbal counseling, written warning or termination of my employment or position. I also understand that violations of confidentiality may be subject to civil and criminal liability under state and/or federal law.

By signing below, I acknowledge that I have read and understand this policy and agree to be bound by those terms and conditions throughout my participation in the workforce system. WorkSource Montgomery staff or their designee have answered any questions I may have had regarding this policy.

_____

Print Name

_____ _____

Employee/Volunteer Signature Date

Attachment B: Participant Confidentiality Agreement

PARTICIPANT CONFIDENTIALITY AGREEMENT

It is the policy of the Montgomery County Workforce Development Board to protect the confidentiality of all customer information.

Access to Data

Program operators must collect data in order to document eligibility and provide services per federal regulation under the Workforce Innovation and Opportunity Act. The Workforce Development Board, WorkSource Montgomery and subcontractors will make every effort to collect and store data in a secure manner. Access to any personal customer information is restricted to only those staff and representatives who need it in their official capacity to perform duties pertaining to service delivery.

For auditing and monitoring purposes, individual's personal and confidential information may be shared among federal and state agencies, partner staff and contractors under the WorkSource Montgomery umbrella. Access is for the purpose of determining compliance with, and ensuring enforcement of the provisions of the Workforce Innovation and Opportunity Act.

Use and Release Data

Data will only be used for the purposes of verifying eligibility, delivering services, and verifying performance measures. Any other use of individual data will require written consent from the customer or customer's parent/legal guardian. Upon request, data can be released to the subject of the information.

All sensitive individual data is stored in an area that is physically safe from access by unauthorized persons at all times and data transmitted electronically is encrypted.

Medical and disability records are additionally protected as confidential information. Any medical or disability records are kept separately in a secured physical and/or electronic location. Social security numbers are also protected as high-risk information. Whenever possible, staff and representatives will use unique identifiers to track individual data.

By signing below, I acknowledge that I have explained this agreement to the WorkSource Montgomery-affiliated customer.

Staff Signature: _____ Date _____

By signing below, I acknowledge that I have read and understand this agreement. WorkSource Montgomery staff have explained this agreement and answered any questions I may have had.

Individual Signature: _____ Date _____

Definitions of Key Terms

Personally Identifiable Information (PII) as defined by OMB Memorandum M-07-16 is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal information that is linked or linkable to a specific individual.

There are two types of PII based on the "risk of harm" that could result from the release of the PII.

- Protected PII – as defined by the U.S. Department of Labor is any information that if disclosed could result in harm to the individual whose name or identify is linked to that information. Examples include, but are not limited to, social security numbers, credit card numbers, bank account numbers, personal telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometrics identifiers, medical history, financial information, and computer passwords.
- Non-Sensitive PII – As defined by the Department of Labor, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm as it is not linked or closely associated with any protected or unprotected PII. Examples include first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race.

A combination of non-sensitive PII could potentially be categorized as protected PII. As example, a name and business e-mail address will not result in a high degree of harm to an individual. A name linked to a social security number and date of birth could result in identity theft.

Security Breach is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Sensitive Information is any unclassified information whose loss, misuse or unauthorized access to or modification of could adversely affect the interest of the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.