Missouri Office of Workforce Development

Workforce Development System
Confidentiality and Information Security Plan

Section:

1. PURPOSE

This Workforce Development System Confidentiality and Information Security Plan (the Plan) provides guidance for authorized users of the Workforce Development System, including their supervisors, and the use confidential information. The purpose of this Plan is to communicate the requirements to protect personal and confidential information for customers receiving services through WIOA or other funding sources.

2. BACKGROUND

The Workforce Innovation and Opportunity Act (WIOA) (as well as other laws affecting Trade Act Assistance, education, and social services) directs the Missouri Workforce Development System. The Missouri Workforce Development System includes the Missouri State Workforce Development Board, the Office of Workforce Development (OWD), Local Workforce Development Boards (Local WDBs), their sub-recipients, other sub-recipients, and partner agencies.

The Workforce Development System must ensure the privacy of customers and safeguard their confidential information. Those actions serve customers by:

- protecting customers' eligibility for workforce programs, services, and benefits;
- maintaining consumer confidence in the workforce development system by preserving privacy and minimizing the risk of identity theft or fraud; and
- shielding customers from discriminatory programmatic or hiring practices by keeping certain details about their barriers to employment in strict confidence.

The WIOA regulations require confidentiality policies, such as this Plan, to protect Personally Identifiable Information (PII):

> *"Recipients and sub-recipients of WIOA title I and Wagner-Peyser Act funds must have an internal control structure and written policies in place that provide safeguards to protect personally identifiable information, records, contracts, grant funds, equipment, sensitive information, tangible items, and other information that is readily or easily exchanged in the open market, or that the Department or the recipient or sub-recipient considers to be sensitive, consistent with applicable Federal, State and local privacy and confidentiality laws."*

A Local WDB's Confidentiality and Information Security Plan must concur with *this* Plan. Additionally, Local WDBs must ensure that sub-recipients' confidentiality policies concur with *both* plans.

3. DEFINITIONS

3.1 Personally Identifiable Information (PII):

Information in records, such as a name or identification number, used to distinguish or trace an individual's identity, directly or indirectly, through linkages with other information. PII includes *direct* identifiers (e.g. name and SSN), and *indirect* identifiers (e.g. birth certificate information). PII also includes any

information that, alone or in combination, is linked or linkable to a specific person that would allow identification of that person.

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

3.3 Protected PII:
Information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.) medical history, financial information, and computer passwords.

3.4 Non-sensitive PII:
Information that, if disclosed by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include, but are not limited to, first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number, a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the customer's information is so important.

4. LEGAL REQUIREMENTS

4.1 Federal law, Office of Management and Budget (OMB) guidance, Department of Labor Employment and Training Department (DOL ETA), State law, and DHEWD policies require that PII and other confidential or sensitive information be protected.

4.2 DHEWD policy obligates OWD employees to confidentiality and information security. See DHEWD "Personal Accountability and Conduct" policy, issued August 28, 2019.

4.3 Failure to comply with the requirements of this Plan, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of grant funds, or the imposition of special conditions or restrictions, or such other actions deemed necessary to protect customer's privacy or the integrity of data.

4.4 The misuse or unauthorized release of personal and confidential information or

records by OWD, sub recipients, or other personnel, may be subject to a Class A Misdemeanor, or up to one year in jail and/or a civil penalty of $2,000, and other applicable sanctions under State and federal law.

5. PROCEDURES

5.1 Training of Authorized Users:

5.1.1 Any authorized user must read this Plan in its entirety upon hire and sign an attestation acknowledging they understand and will adhere to the policy. A review of this policy and signed attestation is required annually in December. Failure to do so will result in staff not having access to MoJobs and UInteract or current accounts to be locked out.

5.1.2 OWD CSU will upload signed attestations into the users case management admin account.

5.1.3 Authorized users must immediately report any breach or suspected breach of PII to their supervisor.

5.1.4 See "Missouri Cyber Security State Employee Computer Security Tips" for additional cyber security tips: https://cybersecurity.mo.gov/employee_tips.

5.2 Access Eligibility and Registry Process:

5.2.1 Supervisors of any authorized user will be responsible for ensuring that staff have read this Plan, and that they have signed the user attestation form attached this Plan. For partner agency staff, the Missouri Job Center Manager will submit complete user attestation forms to the respective agency's personnel office.

5.2.2 OWD will maintain copies of signed attestations within the electronic case management admin accounts of each user.

5.2.3 Local WDB Directors and Manager will oversee this process for LWDAs and Missouri Job Centers (and sub-recipients), ensuring that all partners properly maintain their user lists. (OWD CSU will oversee the local OWD staff.) This custodial role must be included in the local Memorandum of Understanding and the Local Plan. OWD may monitor for compliance.

5.2.4 OWD's CSU will provide access (including requests from Local WDBs) to authorized users.

5.3 Acknowledgement of Confidential Information:

5.3.1 Jobseeker customers creating new accounts on *jobs.mo.gov* are informed about information they submit:

> *"You are accessing a trusted, secure government website. The State of Missouri does not share your personal information with other entities. For more information about*

the State of Missouri Privacy Policy, go to www.mo.gov/privacy-policy."

5.4 Handling Confidential Information:

5.4.1 Paper copies of confidential information should be marked as "Confidential."

5.4.2 PII and sensitive information must not be communicated via email or stored on a CD, DVD, thumb drives, etc., unless the device is encrypted.

5.4.3 Customer information must only be communicated through agency approved email addresses and not through third-party or personal email addresses.

5.4.4 Social security numbers must not be delivered through email. In the event an authorized user or staff member receives social security numbers via email, the authorized user must immediately delete the email and caution that customer to supply only information needed to answer a question or process a request.

5.4.5 Authorized users must be discreet when verbally communicating personal and confidential information and ensure the receiver(s) are authorized to receive the information.

5.4.6 Faxes and emails containing confidential information must include the statement below in the email or on the fax cover sheet:

> *"CONFIDENTIALITY STATEMENT: This message and any attachments are intended only for those to whom it is addressed and may contain information which is privileged, confidential, and prohibited from disclosure or unauthorized use under applicable law. If you are not the intended recipient of this message, you are hereby notified that any use, dissemination, or copying of this email or the information contained in this message is strictly prohibited by the sender. If you have received this transmission in error, please return the material received to the sender and delete all copies from your system."*

5.4.7 *Receipt* of *unsolicited* confidential information or PII submitted via fax or email from customers to the State email-system users is *not* a breach of confidentiality or this Plan.

5.5 Storage of Confidential Information:

5.5.1 Store confidential information that is in paper or portable media format in a secure location to prevent unauthorized access.

5.5.2 Confidential information stored electronically must be protected by security

programs to prevent unauthorized users from accessing this information.

5.5.3 Authorized users must not leave confidential information exposed. Computers and screens should be "locked" before leaving the work area. Authorized users also must avoid situations where unauthorized persons, such as other customers, can read records information displayed on the user's screen.

5.5.4 Any portable-media electronic record containing confidential information (i.e., diskettes, disk drives, flash drives, CD-ROMs, tapes, etc.) must be properly secured (i.e., locked in a drawer or cabinet) to prevent unauthorized access.

5.5.5 Records shall be stored, maintained, and destroyed in accordance with Missouri Record Retention and Disposition schedules: Records Retention and Disposition Schedules (mo.gov).

5.5.6 Whenever possible, use unique identifiers (such as Applicant IDs [APPIDs]) for participant tracking instead of SSNs after the SSN is entered for required federal performance tracking. If SSNs must be used for participant tracking, they must be stored or displayed in a way that is not linked to a particular individual.

5.6 Medical and Disability Information:

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

- Personal and confidential information that contains health information related to a physical or mental disability, mental diagnosis, or perception of a disability related to the individual must be kept in a separate locked file (if in paper form) and apart from working files.
- Any medical information contained in case notes must be redacted from the customer file; the original notes must be placed in the participant's medical file.
- To minimize the need for staff to access a medical file, only the portion of the customer's information that reveals the presence of a disability should be included in the medical file.

5.7 Access to Medical Files:

5.7.1 Must be limited and should only be accessed with the approval of a supervisor and when such access is necessary to facilitate customer's access to services or to support an ongoing service plan; or

5.7.2 First aid and safety personnel may be provided a customer's medical information in the event of an emergency; or

5.7.3 Local, state, or federal monitors in compliance with 29 CFR Part 34.22(c)

and 29 CFR Part 38.60 may have access to medical files for monitoring purposes.

5.7.4 When all services, including follow-up services, are complete and the participant file is ready to be archived, customer medical and disability related information that had been previously filed away from the active file must be placed in a sealed envelope and marked "Medical and Disability Information" and secured in the participant file.

5.8 Sharing of Confidential Information:

5.8.1 Permissive disclosures shall include a signed request from the subject of the information or a signed release directing that specific information be conveyed to a specific third party for a specific use.

5.8.2 Required disclosures shall be considered as the release of information mandated by law or regulation that do not require the informed consent of the subject of the information.

5.8.3 Any authorized users must permit authorized federal, state, and local personnel to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to ensure compliance with the confidentiality requirements described in this Plan, federal, and State law.

5.8.4 When confidential information is subpoenaed as part of a civil or criminal case or investigation, OWD Administration will handle all such requests, and **no information is to be released at the local level without prior authorization from OWD.**

5.8.7 Section 20 CFR Part 603 permits disclosure of confidential Unemployment Compensation (UC) information to agents and contractors of public officials. State UC agencies may disclose confidential UC information to the agent or contractor of a public official so long as the public official has a written, enforceable agreement with the State UC agency to obtain the data.[1] The public official must:

- agree to be responsible for any failure by the agent or contractor to comply with the safeguards and security requirements of 20 CFR 603.9 and 603.10(a);
- affirm that the confidential UC information will be used for a permissible purpose; and
- affirm that the requirements for all agreements in 20 CFR 603.10(b) are met.

5.8.8 A record of all PII disclosed to the customer, the customer's agent, or to an authorized third party (not involved with the day-to-day use of a customer's

[1] U.S. Department of Labor, Training and Employment Administration, Training and Employment Guidance Letter 7-16, "Data Matching to Facilitate WIOA Performance Reporting," Attachment 1, "Joint Guidance with the Department of Education for Matching PII From Educational Records and Personal Information from Vocational Rehabilitation Records with Unemployment Compensation Wage Records," August 23, 2016.

PII), must be retained. Furthermore, a record of all requests received for a customer's PII must be retained, whether or not the request was fulfilled.

5.8.9 Archive boxes must be clearly marked as containing personal and confidential information.

5.9 Destroying Confidential Information:

5.9.1 Personal and confidential information must not be tossed in the regular trash and recycle bins. Use appropriate methods for destroying sensitive PII in paper files, (i.e., shredding) and securely deleting sensitive electronic PII.

5.9.2 Per Missouri statute and policy, electronic documents and emails on State email servers are archived and cannot be destroyed. Nevertheless, deletions can be made from a user's sent or received folders to prevent (further) dissemination of breached information.

6. INFORMED CONSENT AND PERMISSIVE DISCLOSURES

In accordance with federal and state law, customers must be provided an opportunity to submit written authorization allowing authorized users to share their personal and confidential information and records. Each customer must also be informed that they can request their personal and confidential information not be shared among partner agencies and such request does not affect their eligibility services.

Customers shall be informed and agree to the Privacy Policy electronically to register in the MoJobs. By agreeing to such Privacy Policy, they acknowledge and agree that their personal and confidential information:

- May be shared among the agency partner staff and sub recipients,
- Is used only for the purpose of delivering services and that further disclosure of their confidential information,
- Will not be shared among partner agencies if the individual declines to share their confidential information and the decline to share will not impact their eligibility for services.

7. LEGAL, REGULATORY, AND POLICY REFERENCES

The following federal and state legal provisions may affect the programs and services offered through the local workforce investment system. This list is <u>not</u> exhaustive. Varieties of civil and criminal provisions surround confidential information or identity theft and may apply to this Plan.

- Federal laws and regulations
  - Workforce Innovation and Opportunity Act, Pub. Law 113-128, [29 U.S.C. 3101 et seq.].
  - Workforce Innovation and Opportunity Act (WIOA), Section 188, "Nondiscrimination," Pub. Law 113-128 [29 U.S.C. 3248] and implementing regulations at 29 CFR Part 38.

- 2 CFR 200.303, “Internal controls”.
- 2 CFR 200.337, “Restrictions on public access to records”.
- 2 CFR 200.113, “Mandatory disclosures”.
- 34 CFR 361.38, “Protection, Use, and Release of Personal Information”.
- 20 CFR 683.220(a) “What are the internal controls requirements for recipients and subrecipients of Workforce Innovation and Opportunity Act title I and Wagner-Peyser Act funds?”
- 20 CFR 658.411 “Action on complaints”.
- 20 CFR 683.600 “What local area, State, and direct recipient grievance procedures must be established?”
- The Privacy Act of 1974, Pub. Law 93–579, [5 U.S.C. § 552a et seq.].

- Federal guidance and standards
  - U.S. Department of Labor, Employment and Training Administration, Training and Employment Guidance Letter (TEGL) No. 39-11, “Guidance on the Handling and Protection of Personally Identifiable Information (PII),” June 28, 2012.

- Missouri State laws
  - RSMo 37.070, “Transparency policy—public availability of data—broad interpretation of sunshine law requests—breach of the public trust, when.”
  - RSMo 576.020 “Public servant acceding to corruption—penalty.”
  - RSMo 576.050, “Misuse of public information—penalty.”
  - Missouri Retention and Disposition Schedules.

- DHEWD/OWD Policies
  - DHEWD “Acceptable Computer Use Policy,” August 28, 2019.
  - DHEWD “Personal Accountability and Conduct” policy, August 28, 2019.
  - OWD Issuance: 01-2008, “Office of Workforce Development Confidentiality and Information Security Plan,” September 1, 2008, and subsequent changes.
  - Applicable OWD Policy Issuances are available at https://jobs.mo.gov/dwdissuances.
  - http://www.mo.gov/privacy-policy/.

8. FORMS

Confidential Information User Attestation Form attachment II.