Missouri Office of Workforce Development

Workforce Development System
Confidentiality and Information Security Plan

Section:

1. PURPOSE

The Workforce Innovation and Opportunity Act (WIOA)[1] (as well as other laws affecting Trade Act Assistance, education, and social services) directs the Missouri Workforce Development System. That system includes the Missouri State Workforce Development Board, the Office of Workforce Development (OWD), Local Workforce Development Boards (Local WDBs) and their subrecipients, and partner agencies. Among those partners, OWD collaborates most closely with the Missouri State Education System and the Division of Employment Security, which require additional safeguards peculiar to their databases. All these entities use confidential information daily.

This Plan is for Workforce Development System users of confidential information and their supervisors. It discusses defense against external attacks on information security and reducing breaches due to internal errors and misuse. This Plan also establishes a "proportional" response to accidental breaches. The best defense is having conscientious users committed to protecting the security of customers' information.

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[2] or fraud[3]; and
- shielding customers from discriminatory programmatic or hiring practices by keeping certain details about their barriers to employment in strict confidence.

This Plan defines "confidential information." It establishes procedures for preventing access by "unauthorized users." Numerous federal, State, and local laws, regulations, and policies have confidentiality requirements. This Plan will lay out OWD's expectations for compliance.

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

> *"Recipients and subrecipients 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 subrecipient considers to be sensitive, consistent with applicable Federal, State and local privacy and confidentiality laws."* [4]

A Local WDB's Confidentiality and Information Security Plan must concur with *this* Plan. Local WDBs must ensure that subrecipients' confidentiality policies concur with *both* plans.[5]

---

[1] Pub. Law 113-128 [29 U.S.C. 3101 et seq.].

[2] "Identity theft" involves the misuse of any identifying information, which could include name, SSN, account number, password, or other information linked to an individual, to commit a violation of federal or state law. (Pub. Law 105-318, "Identity Theft Assumption and Deterrence Act" [18 U.S.C. 1028]).

[3] As used in this Plan, "fraud" covers a wide range of financial crimes, including credit-card fraud, phone or utilities fraud, bank fraud, mortgage fraud, employment-related fraud, government-documents or benefits fraud, loan fraud, and health-care fraud.

[4] 20 CFR 683.220(a).

[5] Uniform Guidance at 2 CFR 200.303(e), "Internal controls."

2. DEFINITIONS

2.1 Authorized users:

Workforce Development staff, Employment Security staff, and applicable Education system staff are among authorized users, as are other entities or persons having routine access to workforce, wage record, or education system confidential information or data. Supervisors identify authorized users on the Confidential Information Authorized User List. No organization, entity, or person currently under suspension or debarment by any State or federal agency may have access to secure data systems.[6]

2.2 Breach:

A *breach* is an unauthorized or unintentional exposure, disclosure, or loss of sensitive information. A *breach of security* is "unauthorized access to, and unauthorized acquisition of, personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information."[7] Four causes of breaches are:

- Malware and hacking — Breaches caused by intentional intrusions into computer systems by unauthorized outsiders with malicious or criminal intent.
- Physical breaches — The theft or loss of unencrypted data (or access codes or passwords) stored on laptops, desktop computers, hard drives, USB drives, data tapes, or paper documents.
- Errors — Breaches that result from anything authorized users unintentionally do, or leave undone, that exposes personal information to unauthorized individuals.
- Misuse — Breaches resulting from "trusted," authorized users intentionally using privileges with willful disregard or in unauthorized ways for personal purposes.

Unauthorized discussion of a breach with co-workers or others is *also* a breach. Gossip can seriously obstruct internal reviews or external criminal investigations.

2.3 Confidential information *(see also "Personally Identifiable Information")*:

Any PII that alone, or in combination, is linked or linkable to a specific person or employer that would allow identification of that individual or employer. Unless otherwise required by law to be disclosed, it may include, but is *not limited* to:

- Name
- Social Security Number (SSN)
- Passport number, driver's license number, or any unique government-issued ID number
- Ethnicity
- Age
- Date of birth
- Gender
- Addresses
- Email addresses
- Telephone numbers
- Physical description
- Family and household composition
- Domestic violence
- Education
- Medical or disability history
- Employment history

[6] Executive Order (EO) 12549, Feb. 18, 1986; 29 CFR 94.630; and 2 CFR Part 180.
[7] RSMo 407.1500.1(1).

- Wages or wage histories[8]
- Benefits and reimbursed expenses
- Dates and locations of services and training received
- Federal Employer Identification Number (FEIN)
- North American Industrial Classification System (NAICS) and other industry codes
- Unemployment Insurance (UI) claims, payments, or benefits information
- UI account information or status
- Financial matters or bank account information
- Credit or debit card numbers or account information
- Information about employees
- Employer history
- Salaries

"Confidential" includes statements made by, or attributed to, the individual or any employer.

2.4 Disability-related information:
Any information, whether oral or written, in any form or medium, relating to a physical or mental impairment that substantially limits one or more major life activities.

2.5 Disclosure:
To disclose, release, transfer, disseminate, or otherwise communicate all or any part of confidential information, records, or data verbally, in writing, electronically, or by any other means to any person or entity.

2.6 Incident: [9]
An occurrence that:

- actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

2.7 Information security: [10]
Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Information security provides:

- integrity—guarding against improper information modifications or destruction, and ensuring information is authentic and irrefutable;
- confidentiality—preserving authorized restrictions on access and disclosure to protect personal privacy and proprietary information; and
- availability—ensuring timely and reliable access to, and use of, information.

[8] Missouri State law imposes criminal penalties for unauthorized public disclosures of Division of Employment Security wage records that reveal an individual or employer's identity (RSMo 288.250). The first offense of this statute is a Class A misdemeanor subject to up $10,000 in fines and/or one year in jail. A subsequent continuing offense is a Class E felony, subject to up to $10,000 in fines and/or four years' imprisonment.

[9] Federal definition at 44 U.S.C. 3552(b)(2), Federal Information Security Modernization Act (FISMA) of 2014, as amended.

[10] Federal definition at 44 U.S.C. 3552(b)(3), Federal Information Security Modernization Act (FISMA) of 2014, as amended; *see also* National Institute of Standards and Technology, FIPS Pub 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

.

2.8 Medical and disability information:

Any information, oral or written, in any form or medium, relating to the past, present, or future mental or physical condition of an individual or to the provision of medical services. Although the *existence* of a disability or medical condition is collected as a customer record data element, specific details must be maintained in a separate secure location.[11] Rules changes from the U.S. Department of Labor (DOL) Civil Rights Center emphasize the confidentiality distinction between knowledge *of* a condition or disability and access to *details* of that condition or disability, on a "need-to-know" basis:

> *"…the range of persons who may be permitted to have* ***access to files*** *containing medical and disability-related information about a particular individual is* ***narrower*** *than the range of persons who may be* ***permitted to know generally*** *that an individual has a disability. These changes make the regulations consistent with DOL's regulations implementing § 504 of the Rehabilitation Act, and with the EEOC's regulations implementing Title I of the ADA. The change is also intended to provide recipients with information necessary to enable them to develop protocols that are consistent with these requirements."* [12]

2.9 Partners or partner agencies:

Any *State agency* that is part of the Missouri Job Center system [besides the Department of Higher Education and Workforce Development (DHEWD)/Office of Workforce Development (OWD)], including:

- Office of Administration (OA)
  - OA Information Technology Support Division (ITSD)
- Department of Labor and Industrial Relations (DOLIR)
  - DOLIR Division of Employment Security (DES)
- Department of Social Services (DSS)
  - DSS Family Support Division (FSD)
    - Rehabilitation Services for the Blind (RSB)
- Department of Corrections (DOC)
- Department of Elementary and Secondary Education (DESE)
  - DESE Division of Learning Services, Office of Adult Learning and Rehabilitation Services, Vocational Rehabilitation (VR)
  - DESE Division of Learning Services, Office of Adult Learning and Rehabilitation Services, Missouri Adult Education and Literacy (AEL) Program
- Coordinating Board for Higher Education (CBHE)
- Department of Health and Senior Services (DHSS)
- Department of Economic Development (DED)

This includes State agencies acting under the delegated authority of the above-listed agencies. Local WDBs and their subrecipients are also partner agencies.

The term "one-stop partners" specifically refers to WIOA-designated entities[13] that provide access to their programs and services through the comprehensive one-stop center, contribute to its operation and maintenance, and are parties to a Memorandum of Understanding with the other WIOA-designated partners.

---

[11] OWD Issuance 09-2015-Change 1, "Statewide Service Notes Policy," December 23, 2015. [This State records-isolation policy is now also federal policy, per the new rule at 29 CFR 38.41(b)(3)].

[12] Preamble commentary for 29 CFR 38.41(b)(3), *Notice of Proposed Rulemaking,* 29 CFR Part 38, "Implementation of the Nondiscrimination and Equal Opportunity Provisions of the Workforce Innovation and Opportunity Act, 81 FR 4493-4571, January 26, 2016. Final Rules for Part 38 were published on December 2, 2016, and became effective on January 3, 2017.

[13] WIOA sec. 121(b); [29 U.S.C. 3151(b)].

2.10 Personally Identifiable Information (PII) *(see also Confidential Information)*:
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 not only *direct* identifiers, like name and SSN, but also *indirect* identifiers such as date-and-place of birth. PII includes any information that, alone or in combination, is linked or linkable to a specific person that would allow identification of that person. The federal Office of Management and Budget (OMB) Uniform Guidance[14] notes that:

> *"Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be 'Public PII' and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual."*

For example, a name selected randomly from a phone book is not confidential. That name, when also identified as a Job Center customer, *becomes* a confidential piece of information. The OMB Uniform Guidance establishes the general premise that **linkage** of certain pieces of PII is what determines the need for confidentiality:

> "**Protected** *PII means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date-and-place of birth, mother's maiden name, criminal, medical, and financial records, [and] educational transcripts. This does not include PII that is required by law to be disclosed."* [15]

2.11 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 of 1974.[16, 17]

2.12 ACRONYMS USED IN THIS GUIDE

AEL	Missouri Adult Education and Literacy Program (DESE)
APPID	Applicant ID
CBHE	Missouri Coordinating Board for Higher Education
CEO	Chief Elected Official of an LWDA
CFR	*Code of Federal Regulations*
CSU	Technical Support Unit (OWD)
DATA Act	Digital Accountability and Transparency Act of 2014
DED	Missouri Department of Economic Development
DES	Missouri Division of Employment Security (DOLIR)
DESE	Missouri Department of Elementary and Secondary Education

[14] 2 CFR 200.79.
[15] 2 CFR 200.82
[16] The OMB Uniform Guidance, including some of the above definitions, is recapped in 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, which is included as *Attachment 4* to the accompanying Issuance.
[17] The Privacy Act of 1974, as amended, principally deals with the contents and disclosure procedures for records kept by *federal* agencies, as well as individuals' access to those records. However, some federal awards and grants require recipient's assurances to abide by certain requirements or procedures in the Act.

DHEWD	Missouri Department of Higher Education and Workforce Development
DOB	Date of Birth
DOC	Missouri Department of Corrections
DOL	U.S. Department of Labor
DOLIR	Missouri Department of Labor and Industrial Relations
DSS	Missouri Department of Social Services
ED	U.S. Department of Education
ETA	Employment and Training Administration (*also* DOLETA; DOL)
FEIN	Federal Employer Identification Number
FERPA	Family Educational Rights and Privacy Act
FFATA	Federal Funding Accountability and Transparency Act of 2006
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FR	*Federal Register*
FSD	Missouri Family Support Division (DSS)
HSS	Missouri Department of Health and Senior Services
IP	Intellectual Property
ITSD	Missouri Information Technology Support Division (OA)
LFA	Local Fiscal Agent
Local WDB	Local Workforce Development Board
LWDA	Local Workforce Development Area
NAICS	North American Industrial Classification System
NIST	National Institute of Standards and Technology
NRS	National Reporting System
OA	Missouri Office of Administration
OMB	Federal Office of Management and Budget
OWD	Missouri Office of Workforce Development (DHEWD)
PII	Personally Identifiable Information
RSB	Missouri Rehabilitation Services for the Blind (DSS/FSD)
RSMo	*Revised Statutes of the State of Missouri*
SAOP	Senior Agency Official for Privacy
SSA	Social Security Act (*also,* Social Security Administration)
SSN	Social Security Number
TEGL	Training and Employment Guidance Letter (DOL/ETA)
U.S.C.	*United States Code*
UAF	User Attestation Form
UC	Unemployment Compensation
UI	Unemployment Insurance
VR	Missouri Vocational Rehabilitation (DESE)
WIOA	Workforce Innovation and Opportunity Act
WOTC	Work Opportunity Tax Credit
WIPS	Workforce Integrated Performance System
WRIS	Wage Record Interchange System

3. SOURCES OF CONFIDENTIAL INFORMATION

3.1 Sources of confidential information in the workforce system include:

3.1.1 Customer individual record files (paper copy, statewide electronic case-management system case files, etc.) and eligibility documentation.[18]

3.1.2 OWD statewide electronic case-management system Reports (Employment and Training Reports, assessment records, performance outcomes, etc.).

3.1.3 Individual performance roster data.

3.1.4 Unemployment Insurance (UI) wage records.

3.1.5 Wage Record Interchange System (WRIS) data.

3.1.6 The Work Opportunity Tax Credit (WOTC) database.

3.1.7 U.S. Department of Labor Workforce Integrated Performance System (WIPS).[19]

3.1.8 National Reporting System (NRS).

3.1.9 State Education System records *(see also Section 4.5)*.

3.2 OWD oversees or operates various federal and State programs that collect confidential information on customers. The Local WDBs also contract with service providers that use confidential information in their operations. A customer's **confidential information may be shared** among various *authorized* users at partner agencies that coordinate services through the Workforce Development System, *provided* it is for the *sole intention* of fulfilling an employee's job duties to deliver authorized services to the customer or program participant.

3.3 The complainant's name and other particulars, records, or interviews associated with any **Equal Opportunity complaint** under WIOA Section 188 must be kept confidential.[20] This includes *any* information that could identify a particular individual as having filed a complaint.

3.4 The complainant's name and other particulars, records, or interviews associated with any **Wagner-Peyser Employment Service complaint** are confidential,[21] including *any* information that could lead to identification of a particular individual as having filed a complaint.

3.5 Consistent with the above confidentialities, it is State policy that the complainant's name and other particulars, records, or interviews associated with any **WIOA programmatic complaint** under WIOA sec. 181(c) Grievance Procedures[22] are also confidential, including *any* information that could lead to identification of a particular individual as having filed a complaint.

---

[18] This includes all eligibility documentation as required by OWD Issuance 01-2015: "WIOA Adult and Dislocated Worker Programs Eligibility and Documentation Technical Assistance Guidance Policy," July 1, 2015, and by OWD Issuance 02-2015: "Workforce Innovation and Opportunity Act (WIOA) Youth Program Eligibility and Documentation Technical Assistance Guidance Policy," July 1, 2015.

[19] Unauthorized use or misuse of WIPS may be subject to federal fines or imprisonment (18 U.S.C. 1030).

[20] 29 CFR 38.41(c).

[21] 20 CFR 658.411(a)(3).

[22] Implemented at 20 CFR 683.600.

4. LEGAL REQUIREMENTS

4.1 Numerous State and federal legal provisions cover various programs and services offered through the State workforce development system. (Section 7 lists some prominent legal provisions. This list is *not exhaustive*. Various other civil and criminal provisos surround confidential information and/or identity theft and may apply to this Plan.)

4.2 The Annual Agreement contract between OWD and each Local Workforce Development Area (LWDA), through the Chief Elected Official (CEO) or the CEO's Local Fiscal Agent (LFA), specifies confidentiality requirements in its Assurances. Local Areas *and* their subrecipients must comply with the confidentiality requirements of WIOA Sec. 116(i)(3)[23] and with the internal controls protection requirements for non-Federal recipients in the Uniform Guidance at 2 CFR 200.303. Conformity with this section is requisite to continuity of funding.

4.3 Missouri State Law[24] **requires notification** of an individual in the event of an uncontained breach of certain data elements of that individual's personal information. The law requires additional procedures if a breach involves a large number of individual records. Besides commercial databases, this statute specifically applies to government, governmental subdivisions, governmental agencies, and governmental instrumentalities. (*See Section 5.9.5.1 for more discussion.)* Therefore, reporting all data breaches and possible data breaches is mandatory.

4.4 DHEWD policy[25] obligates OWD employees to confidentiality and information security:

- An employee is prohibited from using information learned in the performance of job duties for personal benefit, including favoritism, professional advancement, and/or monetary gain.
- An employee is responsible for safeguarding confidential and sensitive information.
- An employee shall not disclose confidential information gained by reason of their position to individual(s) within the Department who do not have a need-to know and who do not have authority to receive such information.
- An employee shall not seek information for which the employee does not have a need-to-know or authority to receive.
- An employee shall not disclose confidential information to individual(s) outside of Departmental personnel unless required by law to do otherwise in the discharge of the duties of their position.
- An employee is to inform their supervisor or manager if he/she receives information to process on a relative or friend. The supervisor or manager will reassign the request to another staff member.

OWD expects all authorized users to adhere to these same rules.

4.5 The federal Family Educational Rights and Privacy Act (FERPA)[26] mandates certain confidentiality protocols involving student records. Compliance with FERPA is incorporated by reference into several Missouri education and privacy statutes.[27]

---

[23] This section references compliance with Section 444 of the General Education Act (20 U.S.C. 1232g), also known as The Family Educational Rights and Privacy Act (FERPA). It provides for confidentiality of student records and open access to the records of minor children by their parents or guardians.

[24] RSMo 407.1500, "Definitions—notice to consumer for breach of security, procedure—attorney general may bring action for damages."

[25] DHEWD "Personal Accountability and Conduct" policy, August 28, 2019

[26] Section 444 of the General Education Provisions Act, Pub. Law 93-380, as amended [20 U.S.C. 1232g].

[27] RSMo 161.096, 161.825, and 210.145.

5. PROCEDURES

5.1 Authorized users:

5.1.1 OWD Central Office staff that have access to confidential information include the Director, Assistant Directors, Program Administrators, Central Office Managers, and their designated staffs. Others with access may include staff from ITSD, Performance and Planning, Regulatory Compliance, JobStat, Training, Technical/Customer Support, Financial, and other staff designated by their supervisors, and federal program staff.

5.1.2 Local staff with access to confidential information includes Local WDB members and staff and subrecipients, Functional Leaders, partner agency staff, and local OWD staff. It is the responsibility of the various organizations' supervisors to determine which individuals should be designated as authorized users.

5.2 Training of authorized users:

5.2.1 Staff must read this policy in its entirety and sign an attestation acknowledging they understand and will adhere to the policy.

CSU may require training and/or a new user attestation form if repeated in cases of:

- expired passwords;
- lengthy periods between access or use;
- a change in the user's employer of record;
- retraining to correct user errors;
- new legal, regulatory, or policy requirements; or
- system updates or technical alterations.

5.2.2 System Access Request Forms (OWD-4) for partner users must be counter-signed and dated by the immediate supervisor and the OWD CSU individual assigned to maintain the Confidential Information Authorized User List.

5.2.3 Training must advise a prospective authorized user of the following State information-security concepts:[28]

- Never share passwords with anyone, including help-desk staff.
  - The password confirms identity. Persons are responsible for anything performed under the assigned username and password combination. Access may be granted to supervisors and co-workers to the email application information without sharing the password.
- Create strong passwords by including special characters and using both upper- and lower-case letters.
- Do not write user ID or passwords down and leave them unattended.
  - Leaving post-it notes or other loose paper containing passwords near computers jeopardizes access to sensitive information.
- Always encrypt and password-protect sensitive information.
  - State and Federal laws protects Social Security numbers, credit-card numbers, and healthcare information. By default, email offers no information security. Encryption is required for any sensitive information,

[28] Missouri Cyber Security State Employee Computer Security Tips(https://cybersecurity.mo.gov/employee_tips/)

whether residing on a network, a share drive, or other storage device.

- Always lock computers when leaving the workspace.
  - Locking computers protects logged-in accounts, such as email and network shares, from unauthorized use.
- Always store CDs, USB drives or other removable devices containing sensitive information in locked drawers.
  - Physically securing workspace devices deters unauthorized access.
- Professional IT staff must properly erase any electronic device used to store State information *before* discarding or disposing of via property transfer or surplus.
  - Sensitive information is still accessible—even after deleting files or reformatting a storage device.
- Use the network drives provided to save all important files and documents.
  - These drives are routinely backed up to prevent data loss.
- Connect State-issued laptops to the State's network every 30 days or less for security updates and patches.
  - Ensuring that assigned laptops are up-to-date with the latest security updates and patches prevents future problems.
- Do not install third-party software applications without IT approval.
  - Always check with professional IT staff prior to installing any third-party software. Shareware often carries strict licensing requirements. Software also may have compatibility or vulnerability issues.
- Never open email attachments if unsure about its file type or purpose.
  - Even if an attachment appears to be from a friend or coworker, think twice before opening.
- Email messages sent become the property of the recipient.
  - Emails to and from State government websites or addressees also may be publicly accessible under the provisions of the Missouri Sunshine Law (RSMo Chapter 610).
- Think before clicking on a link.
  - Don't immediately trust links provided within email messages, PDFs, search engine results, or even trusted websites. If suspicious, do not click on the link.

5.3 Access eligibility and registry process:

5.3.1 OWD CSU will maintain the Confidential Information Authorized User List composed of the statewide electronic case-management system and other online data systems users.

5.3.2 Local WDB Directors and Functional Leaders will oversee this process for LWDAs and Missouri Job Centers (and subrecipients), 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.

5.3.3 Supervisors of authorized OWD staff users will be responsible for ensuring that staff have read this policy, and that they have signed the user attestation form. For partner agency staff, the Missouri Job Center Functional Leader will submit complete user attestation forms to the respective agency's personnel office.

5.3.4 When posting names to the Confidential Information Authorized User List, the

supervisor also will designate the types of information the user will be accessing (i.e., UI data, statewide electronic case-management system, and Performance rosters).

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

5.4 Acknowledgement of confidential information:

5.4.1 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."*

Customers registering in-person with Job Center staff also must be reminded of this statement.

5.4.2 Paper copies of confidential information should be marked, "Confidential."

5.4.3 Email and faxes are not secure transmissions for confidential information and have the potential of being viewed by unintended recipients. Before sending documents, verify the accuracy of email addresses and fax numbers. When faxing, call the recipient to ensure an authorized user will be receiving the fax. If an email or fax with confidential information is sent or received in error, notify the sender/receiver immediately with instructions for safeguarding the information.

5.4.4 Emails, IQ Ticketing System, and faxes must not contain a customer's full Social Security Number (SSN). Rather, the customer's full name, with middle initial, followed by the last four digits of their SSN, the customer's programmatic identification code, or the statewide electronic case-management system Applicant ID (APPID) number, if applicable, will be used to protect their identity when providing communication documents.

5.4.5 Faxes and emails containing confidential information must include the statement below in the email or on the fax cover sheet. The fax form [OWD-ADM-2 (2015-03)] https://jobs.mo.gov/sites/jobs/files/fax_transmittal_rev03-2015_dwd-adm-2.pdf includes this language:

> *"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."*

An email confidentiality tag line (message footer) containing the above advisory has been a required component of all OWD staff email correspondence signature blocks and those of all partner staff statewide electronic case-management system users

since 2008.[29] **This requirement remains in force.** This appropriately covers any intentional or unintentional inclusion of confidential client data. All SECSM users must use a confidentiality tag line similar to the one above. Users can copy and paste the text into their personal signature block in their email application. (For Microsoft Outlook users, this is usually accessed through **Tools>Options>Mail Format>Signatures**.)

5.4.6 *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. The Missouri State Government Privacy Policy[30] provides legal notice for the entire ".mo.gov" domain that any emails to the State are not necessarily secure or confidential. When receiving unsolicited PII electronically from a customer, it is advisable to send a follow-up reply (after *removing* the PII text in the original message) cautioning that customer to supply only information needed to answer a question or process a request. Once unsolicited confidential information or PII is received, however, its custody must be managed in a manner consistent with this Plan.

5.5 Medical- and disability-related information:

5.5.1 As per Section 5.6.2, keep medical- and disability-related information in a separate, secure location, physically removed from the main files for participants or employees. The Local WDB, partner agency staff, and OWD will take measures, with the support of ITSD, to ensure all access to medical- and disability-related information is treated every bit as "confidential" as other information identified in Sections 2.3 and 3. It is mandatory to keep electronic files password-protected and to keep physical files in a secure, locked location.

5.5.2 The use or disclosure of medical- and disability-related information is limited to specific, lawful purposes.

5.5.3 Direct all inquiries or comments about secure medical and disability records to Danielle Smith, State Equal Opportunity Officer, at (573) 751-2428 or email danielle.smith@dhewd.mo.gov

5.6 Storage of confidential information:

5.6.1 Store confidential information that is in paper or portable media format in a secure location to prevent unauthorized access. "Secure location" means a locked drawer, file safe, cabinet, or room physically accessible only by a known list of authorized users.

5.6.2 Customer medical- and disability-related information must be stored in a separate, secure location. The location of the medical- and disability-related information must be noted in the customer's main file.[31] *(See also Section 5.5.)*

5.6.3 Confidential information stored electronically must be protected by security programs to prevent unauthorized users from accessing this information.

---

[29] OWD Issuance: 01-2008, "Office of Workforce Development Confidentiality and Information Security Plan," September 1, 2008, and subsequent Change 1 (February 1, 2011) and Change 2 (September 15, 2011).
[30] http://www.mo.gov/privacy-policy/.
[31] For detailed policy on proper service or case note procedures, see OWD Issuance 09-2015, Change 1, "Statewide Service Notes Policy," December 25, 2015.

5.6.4 Authorized users must not leave confidential information exposed. Computers and screens should be "locked" (i.e., CTRL + ALT + DELETE) 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.

5.6.5 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.

5.6.6 When a staffing change occurs, it is the responsibility of the supervisor to ensure that all confidential information is returned and to terminate the departing user's access, as appropriate. This includes, but is not limited to, submitting an Access Request (Form OWD-4) to OWD CSU within two weeks prior to the employment action taking effect, or as soon as possible, if not given notice.

5.6.7 *Social Security Numbers (SSNs)* — 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, such as using a truncated (last-four-digits) SSN.

5.7 Sharing of confidential information:

5.7.1 Sharing confidential information is a necessity to operate the programs mentioned in Section 2 of this Plan. Any user of confidential information must be authorized. Authorized disclosures are of two types, permissive and required. Permissive disclosures involve 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. Required disclosures are releases of information mandated by law or regulation that do not require the informed consent of the subject of the information.

5.7.2 When transmitting paper copies of confidential information, they should be placed in folders or envelopes marked "Confidential." These should be placed in a secure location when not in use.

5.7.3 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.** Procedure must be followed according to 20 CFR Part 603.7. This Plan and Policy incorporates, by reference, 20 CFR Part 603 *(and any subsequent changes to that part; see Attachment 3 to the accompanying Issuance).*[32] *(See also Section 6, "Informed Consent and Permissive Disclosures.")*. Besides the requirements of federal regulation, an interagency agreement between DES and OWD mandates these procedures. All authorized users must adhere to these requirements.

5.7.4 The 20 CFR Part 603 regulations permit 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

[32] "Part 603—Federal-State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information." The WIOA Final Rules amended sections 603.2, 603.5, and 603.6.

the State UC agency to obtain the data.[33] 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.

In this context, an "agent" is a person or an entity acting instead of, and on the behalf of, a principal. A contractor is a person or entity with whom a public official enters into an agreement to provide services, usually, in this context, for data analysis. ["Public official" in this context is not the same as used in the subpoena provisions of 20 CFR 603.7, discussed previously in Section 5.6.3, or as used regarding an elected official acting as an agent, as discussed later in section 6.1.2.2.]

5.7.5 A record must be kept of all disclosures of PII to the customer, or to the customer's agent, or to authorized third parties not involved with the day-to-day use of a customer's PII. (That is, authorized everyday PII use by employees of the agency owning the database or its partner agencies does not need to be recorded.) Likewise, a record must be kept of all requests received for a customer's PII, whether the request was fulfilled or not. These request and disclosure records must be retained for a period of at least five years, or the life of the PII record, whichever is longer.[34]

5.7.6 *Encryption* — All grantees must comply with all of the following DOL Employment and Training Administration (ETA) policies:[35]

- To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via email or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module.
- Grantees must not email unencrypted sensitive PII to any entity, including ETA or contractors.
- Accessing, processing, and storing of ETA-grant PII data on personally owned equipment at off-site locations (e.g., employee's home, and non-grantee-managed IT services, such as private email servers) is strictly prohibited unless approved by ETA.
- Data may be downloaded to, or maintained on, mobile or portable devices only if encrypted using NIST-validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.

[33] 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.

[34] This procedure complies with the Privacy Act of 1974 at 5 U.S.C. 552a(c).

[35] 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, which is included as *Attachment 4* to the accompanying Issuance

5.8 Destroying confidential information:

5.8.1 When paper or disposable media copies of confidential information are no longer needed, they should be disposed of according to applicable State and federal record-retention guidelines, and using appropriate methods (i.e., shredding on site, placing in a locked receptacle for shredding later, and otherwise ensuring they are not accessible to others) to maintain confidentiality.

5.8.2 Per Missouri statute[36] and policy,[37] 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. Because the server has captured a master image already, the statutory requirement is fulfilled. The State transparency statute also specifically bows to RSMo 610.21 in the Missouri Sunshine Law, which excludes 23 classes of records (including PII, as used in the workforce system) from public disclosure.

5.9 Data breaches in general:

5.9.1 The term "data breach" generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive information. A data breach can leave individuals vulnerable to fraudulent activity, (such as identity theft), discrimination (through breach of medical or disability information), or outright theft (breach of accountholder information).

Any disclosure of confidential information, whether unintentional (negligent or accidental) or intentional, to *unauthorized individuals* is considered a "**breach**." Unauthorized **modifications** or **deletions** of information, or other violations of procedures listed in this Plan, are also "breaches."

Information *regarding* a confidential security breach is *also* confidential information, and it must not be shared freely. Do not discuss the reporting of, assessment of, or response to a breach with anyone other than your immediate supervisor. Such actions may result in corrective, disciplinary, or legal actions.

As stated in Section 1, the goals of this plan are to safeguard customers and to secure their information. The purpose of this plan is not to perfect a punitive system for breaches. It is to manage information and case-management systems better by minimizing accidents and negligence.

5.9.2 **Incident response** — The phases of dealing with an incident are, generally: ***reporting*** the breach, initial ***assessment*** (risk analysis), ***notification*** (if necessary), ***remediation***, and incident ***review.***

All breaches, whether internal or external, must be ***reported*** to a supervisor, either by the "breacher" or by the first employee to discover the breach. Failure to report, or attempting a correction without first discussing with a supervisor, is as serious as a breach itself. *(If the breach involves up-line management, you may report directly to the OWD*

[36] RSMo 37.070, "Transparency policy—public availability of data—broad interpretation of sunshine law requests—breach of the public trust, when.

[37] Missouri Department of Higher Education and Workforce Development, "Acceptable Computer Use Policy," August 28, 2019.

Assistant Director for Administration. See Section 5.10.8.) Do not let personal embarrassment or fear of disciplinary action jeopardize our accountability to workforce customers. Do not self-correct a breach before a supervisor has assessed the situation and approved the action. It is equally incumbent on supervisors not to make breach reporting an uncomfortable or threatening experience. Supervisors (and Functional Leaders, where they serve as supervisors for non-State staff) must report all breaches of confidentiality to their superiors and to OWD CSU. **Reporting an incident is *not* "discretionary."**

Do not assume that every incident actually *is* a breach of PII; it may not be. Validating that fact is part of assessment.[38] Nevertheless, a *suspected* breach should be reported.

Any sub-state local monitor, state-level OWD Regulatory Compliance monitor, or the OWD Customer Support Unit also may initiate a breach-incident report.

5.9.3 If the breach involves information from OWD or a partner agency *(see Section 2.9)*, the user who discovered or detected the breach must notify the supervisor immediately. If the supervisor is, or is expected to be, absent, the supervisor's superior should be notified of the breach. Otherwise, it is the supervisor's responsibility to notify the agency's appropriate up-line management.

5.9.4 If a breach occurs within OWD, the OWD Senior Manager over CSU (or assigned designee) will be responsible for notifying the partner agency owning the source information compromised.

If the breach occurs within a partner agency, the Director from that partner agency is responsible for notifying the partner agency that is the owner of the information compromised. (i.e., OWD or another agency listed in Section 2.9).

5.9.5 If a breach occurs, the agency owning or otherwise responsible for the database will be responsible for assessing whether the breach is significant enough to require advising the customer. If so, that agency will notify the individual or company about the breach (and arrange for mitigation services, if necessary).

If the notifying agency is a subrecipient acting under the authority of OWD, the OWD Senior Manager over CSU (or assigned designee) will be involved in the customer-notification process.

5.9.5.1. *Customer's right to know* — As of the date of this Issuance, there is no general, overarching, *federal* data-breach law or regulation. There is no discussion of breach notification in either the DOL rules on UI-recipient data confidentiality[39] or in the U.S. Department of Education (ED) rules about student record-data confidentiality.[40]

Nevertheless, **Missouri State law[41]** *does* require OWD (and its subrecipients, as well as partner agencies), to notify the affected consumer (Missouri resident) of a breach of personal-information security *if* that breach includes,

[38] U.S. Department of Education "Data Breach Response Checklist," PTAC-CL, September 2012.
[39] 20 CFR Part 603.
[40] 34 CFR Part 99.
[41] RSMo 407.1500.

in an unredacted or unencrypted form, that individual's **first name (or first initial) and last name combined with *one or more* of the following data elements:**

- Social Security Number;
- Driver's license number or other unique identification number created or collected by a government body;
- Financial account number, credit card number, or debit card number in combination and access code or password;
- Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit account access;
- Medical information; or
- Health-insurance information.

If the agency's investigation of the breach determines, according to statutory guidelines, that the breach does *not* pose a risk of identity theft or fraud to the customer, notification may be determined to be unnecessary. However, that conclusion must be *documented in writing* and kept on file for a period of five years.

When customer notification *is* required, the process and the required contents and format of that notice are prescribed by statute. **Therefore, unauthorized persons *must not* contact the customer directly.** If a breach involves a large number (>1,000) of individual notifications, State law requires additional notifications to the Missouri Attorney General and certain consumer-reporting agencies.

5.10 Breach of statewide electronic case-management data confidentiality:

The following procedures address **internal breaches** of confidentiality due to system misuse or human error. In the event of an apparent or suspected **external** attack (a criminal intrusion) into the electronic case-management system, OWD CSU must be notified **within the hour** of first discovery. That notification should include preliminary details of how data **confidentiality, integrity,** or **availability** have been compromised *(see Section 2.7)* and whether the potential impacts in each of those three areas are **low, moderate,** or **high.**[42]

5.10.1 The Department of Higher Education and Workforce Development "Acceptable Computer Use Policy" governs the use of State systems and applies to all DHEWD employees and/or state system users, regardless of whether system use occurs on state property. This policy cannot be modified by a supervisor's statement or conduct.

5.10.2 Each DHEWD system user is responsible for all computer/Internet use associated with their assigned user ID. It is prohibited for a DHEWD system user to use another person's user ID and confidential password without authorization. DHEWD system users **shall not** give their user ID and/or password to any other individual and must take reasonable measures to guard against unauthorized access to their assigned equipment or accounts.

[42] That is, whether the damage is easily reparable, or requires immediate or emergency attention, or is irreparable and puts the agency at risk. *(See 5.10.3.4.)*

5.10.3 Although this policy refers to case-management system data, it also applies to any physical copies or representations of that data.

When notified by the user who caused a breach (or the first employee to detect the breach), the supervisor will perform a preliminary **assessment** of the breach **before** any mitigating, remedial, corrective, or disciplinary actions are taken. Time must be taken to determine the scope of a breach and to secure the system. *Treat the assessment itself as confidential information.*

The assessment, or risk analysis, should determine the **type** of breach, the **cause** of the breach, the **magnitude** of the breach, and recommend the first **proportional response** to the breach. **The supervisor's assessment and recommendation for corrective actions are subject to review and approval by OWD.**

5.10.3.1 This preliminary assessment should characterize the **nature** of the breach as:

- An *electronic* security breach (unauthorized storage, transmission, deletion, or alteration of files or records.); *or*
- A *physical* security breach (involving hard copies of data files or records, physical correspondence, or physical access to a secure storage, the workspace, or the premises in general).

Basic information concerning the breach should be recorded, including:

- The **person** causing (or the person detecting) the breach.
- The assigned **user ID and employer of record** for that person
- The **date** and estimated **time** of the breach, or its detection.
- The center, office, or other **location** where the breach occurred.
- In a case of compromised electronic communications or records, the **platform** involved (e.g., email, case-management system, website, etc.). Give the **physical location** in cases of breaches of physical security.
- Is the system or location currently **secure**, or is it still **vulnerable**? (Has system access been compromised, or has a lock been broken, etc.?)
- What general **type of information** is compromised (e.g., "name, DOB, and SSN," "APPID and SSN," "medical/disability," etc.), and **how many records** are involved?
- Specify whether the unauthorized breach was a **deletion**, a **modification**, or an **exposure** of information.

5.10.3.2 Assess the **magnitude**[43] of the breach as:

1. **Other than Serious —** An inadvertent breach with minimal or no impact; situations where intra-agency, or interagency, mitigation of the breach can prevent widespread, or uncontrolled distribution of the compromised information). In short, any situation where the error can be contained and full confidentiality can be restored. "Other than serious" also may apply to cases where it is not possible to link the breached data with a specific individual or employer.

2. **Serious —** Examples include a risk to a customer's identity, privacy, rights, benefits, or financial security; information that could lead to discrimination against the customer; information affecting multiple customers [e.g., lost lists]; agency, recipient, or subrecipient liability for fines or penalties; retaliation against a customer; or a breach of the material terms of an interagency agreement.

3. **Repeated Serious —** A violation (breach) of a **serious** nature that is materially similar to a prior serious breach in the past 12 months that required advanced corrective or disciplinary action, including access restrictions or suspensions.

4. **Willfully Repeated —** The user *knew* that a policy, regulation, or law prohibited his or her conduct but nevertheless disregarded, or acted with plain indifference to, that prohibition. **Moreover,** the breach is of such a nature that the recipient is bound to report it to the State, DOL, or another federal agency; it may involve civil monetary penalties, such as damages, fines, funding adjustments, restitution or protection for the customer; or if agency integrity is jeopardized.

5. **Pervasive Violation —** A case where an individual (and/or the *organization* that employs the individual), reflects a basic disregard for policies, regulations, and laws. That disregard is demonstrated by a pattern of serious and/or willful violations, continuing violations, or numerous violations. Pervasive violations must be multiple. Any organization that regards sanctions for violations as merely the "cost of doing business" must be considered to be a pervasive violator.[44] The State may initiate suspension of privileges, access, or funding for that partner, recipient, subrecipient, or contractor. The State also may commence debarment procedures to prohibit that organization from competing for or contracting for certain governmental services.

6. **Criminal activity or intent —** Cases where the mining, passing, or use of confidential information for personal gain, retribution, or advantage—including, but not limited to, monetary gain and bribery—is involved. This includes any *solicitation* by the authorized user(s) to pass along such information for personal gain, retribution, or advantage. The felony

[43] This scale derives from DOL guidance for characterizing violations of federal labor laws. It was published as Final Guidance for 48 CFR Parts 22 and 52 in the *Federal Register* on August 25, 2016 (81FR58653–58758).
[44] DOL Final Guidance at Section III(A)(4) "Pervasive violations," 81FR58732.

offense of "acceding to corruption"[45] applies if a public servant knowingly solicits, accepts, or agrees to accept any benefit (direct or indirect) in return for his or her action (or withheld action) as a public servant. It includes violation of a known legal duty as a public servant. The "misuse of official information" is a misdemeanor under Missouri law.[46] "Misuse" refers to using insider confidential information about a customer for private gain. OWD will direct criminal activity cases to the attention of the appropriate authorities. Immediately report any evidence, or significant suspicion, of criminal activity by an authorized user to the OWD Senior Manager over CSU. This policy (Section 5.10.8) and federal law (41 U.S.C. 4712) mandate protection of whistleblowers from reprisals.

Regardless of the magnitude of the breach, the assessment must continue, to establish the *extent* of the breach and to determine mitigation requirements.

5.10.3.3 Preliminary assessment should then characterize the **cause** of the breach. Assess breaches on a case-by-case basis in light of the totality of the circumstances, including the severity of the breach, the user's level and extent of access, and any mitigating factors. "No fault" breaches are rare, and responsibility should be assigned. In some cases, the organization employing the individual might be as culpable. Causes can be:

- **Negligence/Accident** (the breach of information or procedure was unintentional or unavoidable). Examples might include:
    - Failure to redact sensitive information, especially social security numbers, before sending or forwarding an email or submitting an IQ ticket.
    - Accidentally emailing to the wrong person because of the mnemonic autocomplete feature in the "To…" window.
    - Attaching or inserting information in a reply and inadvertently clicking "Reply to All."
    - Sending or replying to address groups or distribution lists that include unauthorized persons.
    - Hitting a preloaded addressee and emailing a copier/scanner document to an unintended recipient; leaving confidential information in public area printer/copier output trays.
    - Failure to place confidential files or portable storage devices in secure lockdown; failure to lock the secure location.
    - Online posting of sample text, PowerPoints examples, or deskaids that include actual customer data instead of mock data.
    - Online posting of sensitive information in unsecured website directories, even if that directory is invisible to a web browser.
    - Failure to check the content of attachments before forwarding.

[45] RSMo 576.020 "Public servant acceding to corruption—penalty." This Class E felony carries penalties of up to $10,000 in fines and/or up to four years' imprisonment. Note that all state merit staff, city or county staff, Chief Elected Official appointees/designees, *and* Local WDB staff are public servants. *See also* OWD Issuance 23-2015, "Policy on Reports and Complaints about Criminal Fraud, Waste, Abuse, or Other Criminal Activity Related to Federal Awards," June 14, 2016, *and* 2 CFR 200.113 "Mandatory disclosures."

[46] RSMo 576.050, "Misuse of public information—penalty." This Class A misdemeanor carries penalties of up to $10,000 in fines and/or up to one year in jail.

- Failure to remove information about medical, disability, substance abuse, etc., from service notes to a separate secure location, per State policy and federal laws and regulations.[47]
- Access or performance was compromised when a user was hoaxed, allowing malware, phishing, spam, spyware, etc., into the system.
- Compromised voicemail access or messages content.
- Improper destruction of confidential documents (not shredding or placing in secure holding for shredding; i.e., placed in unsecured trash).

- **Willful disregard** for policies or procedures for reasons of apathy, sloth, or expediency. "Willful," in a legal sense, means, "intentional," as distinguished from "accidental" or "involuntary." (An error based upon a mistaken understanding of proper procedure, done in good faith, would be *negligent,* not *willful.*) For this plan, "willful" means being fully aware of proper policies or regulations—and acting otherwise. Examples include:
  - Repeated specific errors, as per the above examples, in spite of specific correction or retraining.
  - Leaving a customer, or any other unauthorized person, unattended in a workspace or secure area; allowing them to sit in view of onscreen classified information or IDs/pass codes; failing to monitor access to the workspace or materials.
  - Posting/discussion of sensitive information on social-media sites.
  - Being aware of, but *ignoring*, protocols for securing or transmitting data, securing confidential files, or securing the desktop, workspace, or peripheral equipment (retrieving confidential output from copiers, printers, scanners, etc.)
  - An habitual unconcern with security procedures.
  - An unwillingness to change personal habits to accommodate security.
  - Bypassing security because of a deadline, a time-dependent request, or a similar excuse for "shortcutting" procedures, without supervisor approval.

- **Suspicious activity** (unauthorized and potentially unlawful actions). Examples might include:
  - By adding "cc" or "bcc" recipients, distributing messages containing confidential information or PII to unknown or unauthorized addressees, or to personal email accounts.
  - Uploading data to unauthorized URLs or file-transfer portals.
  - Copying information to personal diskettes or flash drives; use of camera-phone to capture screen images or files.
  - Removing electronic or physical files, records, or printouts from the workplace.

Suspicious activity won't be "self-reported." Because it may lead to serious disciplinary or legal action, supervisors should be extremely prudent when

[47] OWD Issuance 09-2015, Change 1, "Statewide Service Notes Policy," December 25, 2015; also 29 CFR 38.41(b)(3), "Collection and maintenance of equal opportunity data and other information."

receiving reports of suspicious activity from one staff member regarding another. Impose a gag rule to avoid jeopardizing any investigation.

5.10.3.4 The supervisor's assessment should next quantify the **extent** (effect) of the breach. (This may be a preliminary guess. Subtle database alterations might only be apparent to an IT expert.) In general, though, estimate if the breach is:

1. easily **reparable** (low impact); or
2. requires **emergency attention** (moderate impact); or
3. is **irreparable** (high impact) and/or poses serious **liability** for the agency.

5.10.4 Answer the following questions to inform that assessment:

5.10.4.1 Is the confidential information or PII now available *outside* the universe of authorized workforce-development system users?

- For example, if this was a breach of procedure, does the confidential information remain in the hands of authorized users? That is, will redaction of messages or other materials seal this breach?

5.10.4.2 Does the compromised information pose a risk or threat of loss of rights, privileges, or benefits to the customer(s)?

5. 10.4.3 Does the compromised information pose a risk or threat of identity theft, fraud, or cyberattack to the customer(s)?

5. 10.4.4 Does the compromised information pose a risk or threat of information theft, fraud, or cyberattack to workforce records, systems, or websites?

5. 10.4.5 Does this affect the performance or reliability of computer hardware or infrastructure seriously enough to involve OA-ITSD support services?

5. 10.4.6 Does the compromised information pose a risk or threat to the records or systems of any partner agency or other subrecipient?

5. 10.4.7 Does the compromised information or access pose a risk to the Intellectual Property (IP) rights of any of the State's software vendors?

5. 10.4.8 Does the breach involve more than one individual's record? Provide an accurate-as-possible estimate of the number of records involved.

5.10.5 Apply a **proportional response** when assessing damage repair and corrective action for users involved in a breach. Several factors may weigh either in favor of **leniency** or in favor of **sterner measures**:

- Mitigating factors that weigh in favor of **leniency** may include:
  - Self-reporting of the breach.
  - Good-faith effort to comply with security procedures.
  - Remediation of the condition, behavior, or procedure that caused the breach, in an effort to prevent recurrences.
  - Only violation and/or a low number of previous significant violations. (However, "It's a first-time offense" does not negate the actual **effect** of a breach.)
  - A long, uninterrupted record of compliance.

- Recent legal or regulatory changes have not been delivered to the user as training or guidance.
- The user was acting on good faith and reasonable grounds; trusting a usually reliable co-worker or source that the action was within the bounds of proper procedure.

- Factors that weigh in favor of **more rigorous corrective measures** may include:
  - Intentionally disowning the breach or trying to cover it up.
  - Pervasive violations; another example in a pattern of basic disregard for proper security procedures.
  - Violations that are "willfully repeated" in magnitude *and* "willful" in causality, thereby indicating a disinterest in customer confidentiality. This is unacceptable for an authorized user, regardless of how minimal the damage may have been.
  - The gravity of the breach has serious financial consequences for the customer or serious operational, contractual, or legal consequences for the workforce system.
  - Any violation of a type for which a previous monitoring or independent audit issued an unresolved concern or a finding.
  - Repeat violations by an organization, or actions for which a federal or State agency already imposed suspensions or penalties.

5.10.6 *Evaluation* — Although there might be a situation where a "no-fault" ruling is justified, that decision is reserved to the OWD Senior Manager over CSU, not the supervisor.[48]

The preceding risk-assessment process should have provided preliminary answers to the following questions:[49]

- What is the nature of the data elements breached?
- What is the number of individuals (or companies) affected?
- What is the likelihood the information is accessible and usable?
- What is the likelihood the breach may lead to harm?
- What is the ability of the agency to mitigate the risk of harm?

The answers to these questions should influence scoring using the following incident-assessment tables.

[48] The OWD Senior Manager over CSU will function as the Senior Agency Official for Privacy (SAOP), using the federal vernacular of OMB Circular A-130, "Managing Information as a Strategic Resource," July 2016.

[49] U.S. Department of Education, Departmental Directive OM:6-107, April 15, 2008, "External Breach Notification Policy and Plan." *See also* National Institute of Standards and Technology, FIPS Pub 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

5.10.6.1 Incident-assessment tables.

The following scoring-system tables should *guide* corrective or disciplinary actions that follow an assessment of an *internal* breach. This will provide a timesaving approach for supervisors to arrive at the proper proportional response to a breach. It allows them to hold, in that balance of judgment, the magnitude, cause, and effect of the breach. The supervisor should have latitude to weigh in additional mitigating or negative factors, as in Section 5.10.4 above, plus or minus five points in total. Any user who wishes to appeal the assessment and corrective action may do so within 30 calendar days of the decision. Appeals can be made to the OWD Senior Manager over CSU.

MAGNITUDE		CAUSE		EFFECT		
Other than Serious*	10	Negligence or Accident	5	Reparable†	10	25
Other than Serious	10	Willful	10	Reparable	10	30
Other than Serious	10	Suspicious	20	Reparable	10	40

* To be "Other than Serious," the breach must not be as described in Section 5.9.5.1, *or* OWD must approve a written determination of "no risk" of identity theft or fraud.
† Given the definition of "Other than Serious," only "Reparable" effects are possible.)

MAGNITUDE		CAUSE		EFFECT		
Serious	20	Negligence or Accident	5	Reparable	10	35
Serious	20	Negligence or Accident	5	Emergency	20	45
Serious	20	Negligence or Accident	5	Irreparable or Liable	30	55
Serious	20	Willful	10	Reparable	10	40
Serious	20	Willful	10	Emergency	20	50
Serious	20	Willful	10	Irreparable or Liable	30	60
Serious	20	Suspicious	20	Reparable	10	50
Serious	20	Suspicious	20	Emergency	20	60
Serious	20	Suspicious	20	Irreparable or Liable	30	70

MAGNITUDE		CAUSE		EFFECT		
Repeated Serious	30	Negligence or Accident	5	Reparable	10	45
Repeated Serious	30	Negligence or Accident	5	Emergency	20	55
Repeated Serious	30	Negligence or Accident	5	Irreparable or Liable	30	65
Repeated Serious	30	Willful	10	Reparable	10	50
Repeated Serious	30	Willful	10	Emergency	20	60
Repeated Serious	30	Willful	10	Irreparable or Liable	30	70
Repeated Serious	30	Suspicious	20	Reparable	10	60
Repeated Serious	30	Suspicious	20	Emergency	20	70
Repeated Serious	30	Suspicious	20	Irreparable or Liable	30	80

MAGNITUDE		CAUSE		EFFECT		
Willful Repeated	40	Negligence or Accident	5	Reparable	10	55
Willful Repeated	40	Negligence or Accident	5	Emergency	20	65
Willful Repeated	40	Negligence or Accident	5	Irreparable or Liable	30	75
Willful Repeated	40	Willful	10	Reparable	10	60
Willful Repeated	40	Willful	10	Emergency	20	70
Willful Repeated	40	Willful	10	Irreparable or Liable	30	80
Willful Repeated	40	Suspicious	20	Reparable	10	70
Willful Repeated	40	Suspicious	20	Emergency	20	80
Willful Repeated	40	Suspicious	20	Irreparable or Liable	30	90

MAGNITUDE		CAUSE		EFFECT		
Pervasive	50	Negligence or Accident	5	Reparable	10	65
Pervasive	50	Negligence or Accident	5	Emergency	20	75
Pervasive	50	Negligence or Accident	5	Irreparable or Liable	30	85
Pervasive	50	Willful	10	Reparable	10	70
Pervasive	50	Willful	10	Emergency	20	80
Pervasive	50	Willful	10	Irreparable or Liable	30	90
Pervasive	50	Suspicious	20	Reparable	10	80
Pervasive	50	Suspicious	20	Emergency	20	90
Pervasive	50	Suspicious	20	Irreparable or Liable	30	100

5.10.6.2 Administrative action.

Based on the above scoring, it is OWD's policy that the following corrective actions or disciplinary measures are **equitable and proportional responses** for dealing with a breach caused by an authorized user of a OWD-administered system:

ADMINISTRATIVE CONSEQUENCES TABLE	
MAGNITUDE, CAUSE, AND EFFECT ASSESSMENT RATING	**CORRECTIVE OR DISCIPLINARY ACTION**
20	If a supervisor's intercession, based on mitigating factors, reduces a "25" rating to a "20," the user may be let off with a verbal warning. The supervisor must justify the rating in writing and still must notify OWD CSU. This option is applicable only if the breached data remains in the possession or control of authorized users (for example, in an unencrypted email sent in-network to another user).
25–30	For State staff, a written reprimand will be issued to the user and copied to the OWD Senior Manager over CSU. For board staff or other subrecipients, an incident report will be forwarded to the Local WDB Executive Director.
35–40	For State staff, a written reprimand will be copied to DHEWD HR and to the OWD Senior Manager over CSU. For board staff or other subrecipients, an incident report will be forwarded to the Local WDB Executive Director. **ALL USERS** receiving this assessment must undergo mandatory retraining on confidentiality procedures, be recertified, and re-sign the attestation form. The Supervisor should forward any recommendations for remedial measures or compliance assistance to CSU. Temporary reduction of level of authorized access (reduced to probationary access only).
45–60	For State staff, a written reprimand will be copied to DHEWD HR and the OWD Senior Manager over CSU. For board staff or other subrecipients, an incident report will be forwarded to the Local WDB Executive Director. **ALL USERS** receiving this assessment must undergo mandatory retraining on confidentiality procedures, be recertified, and re-sign the attestation form. Temporary suspension of authorized access for a specific length of time (not to exceed two weeks), to be determined by the OWD CSU Manager.
65–80	For State staff, a written reprimand and notice of a concern will be copied to DHEWD HR and the OWD Senior Manager over CSU. For board staff or other subrecipients, an incident report and notice of a concern will be forwarded to both the **Local WDB Chair** and the Local WDB Executive Director. The user will be permanently debarred from authorized access to OWD-administered systems. For State staff, potential reassignment of duties or reduction in grade if this loss of access affects the ability to perform one's current job.
85–100	Immediate debarment from authorized access to <u>all</u> DHEWD systems. For State staff, a letter recommending dismissal for cause, per the DHEWD Personal Accountability and Conduct Policy (2019-08-28), will be sent by the OWD Senior Manager over CSU to DHEWD HR. For board staff or other subrecipients, an official notice of debarment will be sent to the Local WDB Chair and the Local WDB executive director. The OWD Senior Manager over CSU may instruct OWD Fiscal to conduct a compliance review to determine contract, funding, or award repercussions of the incident.

5.10.8 *Whistleblower clause* —All DHEWD employees and DHEWD system users should report any potential breach of confidentiality through their respective lines of supervision. If you feel that reporting any issue in that manner might adversely affect your job, you can report directly to the OWD Senior Manager over CSU at OWD Central Office. Any reported incident will be investigated by OWD Central Office staff or designee, and will be held in strictest confidence until the results are conclusive. Federal procurement law (41 U.S.C. 4712) prohibits reprisals for reporting violations of a law, rule, or regulation related to a federal award.

5.10.9 The statewide electronic case-management system is the official system of record, and the data therein is the official "data of record." The Annual Agreement between OWD and its subrecipients specifies that if any subrecipient "uses any additional external data tracking system, it must have security protocols that are consistent with State standards, in order to safeguard any Personally Identifiable Information." Confidential information or PII on a non-governmental or non-State (private or non-profit) computer system must be secure. The State holds subrecipients financially liable for breaches of information placed on unprotected systems. OWD may enter agreements with other State agencies that allows their staff to access OWD's electronic statewide case management system. **Anyone accessing information from OWD's electronic statewide case management system must adhere to the information in this Plan**. OWD will conduct monitoring and privacy-protection services to ensure that confidential information is not disclosed or comprised. OWD holds subrecipients and other state agency staff accountable for that cost if they allow transfer of secure information to an unprotected computer system lacking adequate firewalls, anti-viral, or intrusion protection. (Creation and maintenance of systems without appropriate content filters are also disallowed expenditures. *See Section 7, "Federal Laws."*) OWD will review access rights for such subrecipients.

5.11 Mitigation of a breach:

5.11.1 Remediation and mitigation procedures that are allowable, prior to approval by the OWD Senior Manager over CSU, include:

- Redaction or deletion of sent and received email. Permanent images of such files will remain in the master email server database. However, redaction or deletion will prevent the information from being sent again inadvertently, or forwarded.
- Tightening local physical security, such as at workstation cubicles, secure file safes or cabinets, and other parts of the premises. Floor-plan adjustments may need to be made to keep display screens out of public line-of-sight. Physical access to printers, copiers, scanners, etc., may need to be restricted. State and local monitors may look for these precautions in their regular monitoring visits.

5.11.2 Other than the redaction or deletion of emails exchanged wholly within the sphere of authorized users, and modification of habits, procedures, or methods that led to the breach, **no data affected by a breach is to be deleted or modified except under the direction of OWD Senior Manager over CSU.**

5.11.3 Notification Trigger and Timing — The requirement to notify a customer is generally triggered by the acquisition, or reasonable belief of acquisition, of personal information by an unauthorized person. OWD will provide notifications to customers, if warranted, regarding the occurrence of an information breach, per Section 5.9.5.1. **Unauthorized or premature discussion of a breach with a customer is itself a breach of confidentiality.** (State law also provides an option for *delaying notification* of

affected customers if that notification might alert a suspect and jeopardize an investigation of the incident by law enforcement.)

6. INFORMED CONSENT AND PERMISSIVE DISCLOSURES

6.**1** The procedures for handling confidential UC information in UC Wage Records are dictated by 20 CFR Part 603 *(see Attachment 3 to the accompanying Issuance)*. Adherence to these procedures is formalized by an agreement between DES and OWD, and by contract between OWD and each LWDA. Part 603's provisions include:

6.1.2 Disclosure of confidential UC information through **informed consent** is permissible to an **agent** whom an individual or an employer has empowered. However, the agent must present a **written, signed release** from the individual or employer the agent represents. (The State may accept an electronically submitted release *if* the State is satisfied that the release is authentic.)

6.1.2.1 When a written release is impossible or impracticable to obtain, the agent may present another form of consent as permitted by the State UC agency in accordance with State law (e.g., a Power of Attorney or Durable Power of Attorney for an attorney-*in-fact*).

6.1.2.2 An elected official performing **constituent services** [e.g., a State legislator acting on behalf of a person or business resident in that legislator's district], may act as an agent. The official must present *reasonable evidence*[50] (such as a **letter** from the individual or employer requesting assistance, or a **written record** of a telephone request from the individual or employer) that the individual or employer has authorized such disclosure.

6.1.2.3 A licensed attorney (attorney-*at-law*) retained for purposes related to the State's UC law is also an agent when representing the individual or employer.

6.1.3 Disclosures to any other third party (other than an agent) or any ongoing disclosures (e.g., regular reports to another agency) of confidential information require a *written release* and are limited in scope.

6.1.3.1 The release must be **signed** by the individual or employer to whom the information pertains. It must specifically identify the information to be disclosed. It must acknowledge that State government files will be accessed to obtain that information. It must declare the specific purpose(s) for which the information is sought. It must stipulate that information obtained under the release will be used only for the declared purpose(s) and disclose all the parties who might receive the information. The declared purpose in the release must be limited to:

- providing a service or benefit to the individual signing the release; or
- administration/evaluation of a program to which the release pertains.

6.1.3.2 Electronic signatures on consent forms may be accepted.[51] However, if any question exists about the authenticity of the electronic signature, OWD CSU may be consulted before accepting it.

6.1.4 OWD CSU will provide written procedures for release of information and an accompanying release form. These must be used for all transactions.

[50] 20 CFR 603.5(d)(1)(ii).
[51] 20 CFR 630.5(d); RSMo 432.230.

6.2 A jobseeker customer (if a youth, the parents or legal guardian) has a right to request and receive a copy of the contents of the **service notes** in the customer's case file.[52, 53]

6.2.1 Never capture and deliver personally requested information to an individual, agent, or third party by means of a statewide electronic case-management system PRINT-SCREEN command, PDF conversion, clipping tool, or similar means. The formatting, coding, or proprietary information on the case-management screen or file is not to be conveyed. Copy and paste, or transcribe, the customer's desired personal information into a neutral medium before presenting to the customer or agent.

6.2.2 The customer *does not necessarily have a right* to <u>all</u> information located in case-management or file records. Information that the customer did not **personally disclose** for inclusion in that file or record is **confidential** from the customer. For example, information regarding that customer that originated with, or was created by, another agency, partner, or contractor is not disclosable to the customer.

6.3 In keeping with Section 552a(c) of the Privacy Act of 1974, as amended, an accounting of all disclosures of any confidential record to any person or agency (including the customer) must be kept for a period of five years, or the life of the customer's record, whichever is longer. This accounting should include the name and address of any requestor as well as the date, nature, and purpose of each disclosure request. Denied requests and the cause for denial must be included in this accounting. The statewide electronic case-management system may be used for this purpose.

[52] OWD Issuance 09-2105-Change 1, "Statewide Service Notes Policy," December 23, 2015. (This right is also established by the Privacy Act of 1974, as amended, Pub. Law 93-579 [5 U.S.C. 552a(d)], with which subrecipients must comply.

[53] Missouri State law also provides that "upon receipt of a written request from a claimant or his or her authorized representative, the [Division of Employment Security] shall supply information previously submitted to the division by the claimant, the claimant's wage history, and the claimant's benefit payment history." RSMo 288.250.

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 not exhaustive. Varieties of civil and criminal provisions surround confidential information or identity theft and may apply to this Plan.

- Federal laws
  - Workforce Innovation and Opportunity Act, Pub. L. 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.
  - The Family Educational Rights and Privacy Act of 1974 (FERPA), Pub. Law 93-380, August. 21, 1974 (20 U.S.C. 1232g)—Protects the privacy interests of students and parents of students who are minors with respect to their personal education records. FERPA is reinforced by Missouri State law,[54] which prescribes substantial civil monetary penalties for violation of the confidentiality of certain education records and student privacy.
  - Section 504 of the Rehabilitation Act of 1973, "Nondiscrimination under Federal Grants," Pub. Law 93-112 [29 U.S.C. 701 et seq.] as amended, including amendments made by the ADA Amendments Act of 2008, Pub. Law 110-325 [42 U.S.C. 12101 et seq.] and implementing regulations at 29 CFR part 32.
  - The Privacy Act of 1974, as amended, Pub. Law 93-579 [5 U.S.C. 552a]. Principally addresses the contents and disclosure procedures for records kept by federal agencies, as well as individuals' access to those records. However, some federal awards and grants require recipient's assurances to abide by certain requirements or procedures in the Act.
  - Pub. Law 105-318, "Identity Theft Assumption and Deterrence Act" [18 U.S.C. 1028].
  - The Federal Information Security Modernization Act of 2014 (FISMA), Pub. Law 113-283 [44 U.S.C. Chapter 35]. FISMA became law after passage of WIOA. Its information-security provisions apply specifically to federal operations and assets. However, some federal awards and grants may require a recipient's contractual assurances to abide by certain requirements or procedures in the Act.
  - The Federal Funding Accountability and Transparency Act of 2006 (FFATA),[55] as amended by the Digital Accountability and Transparency Act of 2014 (DATA Act),[56] specifies federal standards for data elements for public accountability and transparency purposes.
  - The Consolidated Appropriations Act of 2016[57] stipulates that no federal funds may be used to maintain or establish a computer network unless such network blocks the viewing, downloading, and exchanging of pornography. That is, the creation or maintenance of any network without appropriate content filters is a disallowed cost.

[54] RSMo 161.096.5.
[55] Pub. Law 110-252.
[56] Pub. Law 113-101.
[57] Pub. Law 114-113, Section 521(a), December 18, 2015.

- Federal regulations
  - Uniform Guidance for Federal Awards, 2 CFR 200.303, "Internal controls," and 2 CFR 200.337, "Restrictions on public access to records."
  - Uniform Guidance for Federal Awards, 2 CFR 200.113, "Mandatory disclosures."
  - 20 CFR Part 603, "Confidentiality and Disclosure of State UC Information";
  - 34 CFR Part 99, "Family Educational Rights and Privacy";
  - 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?"

- Federal guidance and standards
  - U.S. Department of Labor, Employment and Training Administration, Training and Employment Guidance Letter (TEGL) 5-08, "Policy for Collection and Use of Workforce System Participants' Social Security Numbers," November 13, 2008.
  - The protection, use, and release of personal information under the Vocational Rehabilitation (VR) program, which is one of the core programs under WIOA, are governed by 34 CFR 361.38, listed above. In addition to these VR program-specific confidentiality requirements, VR agencies also must consider FERPA and UC confidentiality requirements when accessing confidential UC information in wage records and PII from education records. On August 23, 2016, DOL and ED issued joint guidance authorizing matching of PII in education records, vocational rehabilitation records, and wages records used for administering UC. (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").
  - National Institute of Standards and Technology (NIST), FIPS Pub 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.
  - OMB, Revision of OMB Circular A-130, Managing Federal Information as a Strategic Resource (Washington, D.C.; July 28, 2016).
  - 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 *(see Attachment 4)*.
  - U.S. Department of Education "Data Breach Response Checklist," PTAC-CL, September 2012.
  - U.S. Department of Education, Departmental Directive OM:6-107, April 15, 2008, "External Breach Notification Policy and Plan."
  - National Institute of Standards and Technology, FIPS Pub 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

- Missouri State laws
  - Revised Statutes of Missouri, Chapter 288, Section 250, Title XVIII, DOLIR; also Chapter 407, Section 407.1500,"Merchandising Practices" (requires customer PII-breach notification, including PII held by governmental agencies).
  - Missouri's Safe at Home Act (2007) RSMo 589.660–589.683, provides for strict address confidentiality for program participants who are experiencing domestic abuse or have similar reasons for relocation to secure locations.
  - 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."

- DHEWD/OWD Policies
  - DHEWD "Acceptable Computer Use Policy," August 28, 2019.
  - DHEWD "Personal Accountability and Conduct" policy, August 28, 2019.
  - Applicable OWD Policy Issuances are available at https://jobs.mo.gov/dwdissuances

CONFIDENTIAL INFORMATION USER ATTESTATION FORM

I understand that in the course of my employment with the Missouri Office of Workforce Development, Local Workforce Development Board, subrecipient, or partner agency, I will receive or become aware of information that is sensitive or confidential. This information may be written, electronic, or verbal, and come from a variety of sources. I understand that I am not to access sensitive or confidential information unless it is necessary in order for me to complete my job responsibilities. I further understand that the Missouri Office of Workforce Development's policy on Confidentiality and Information Security applies to information I may inadvertently hear or see that does not directly involve me in an official capacity. I acknowledge that I must protect all sensitive or confidential information.

I understand that in the performance of my duties I may be requested to provide sensitive or confidential information to others. I agree to hold in confidence and not to disclose any sensitive or confidential information to any person, including employees of state, federal, or local governments, except to those who have an official business reason for the information. Should I have questions regarding the proper handling and disclosure of confidential or sensitive information, I will immediately notify my supervisor for further clarification and direction prior to releasing the information.

If I willfully and knowingly disclose such information in any manner to any person or agency not entitled to receive information, I understand that I may be subject to adverse action, including corrective or disciplinary action, or possibly, civil or criminal personal liability.

I acknowledge that I have received the mandatory training, passed the exam, and have read, understand, and will adhere to the Missouri Office of Workforce Development's Confidentiality and Information Security Plan and the above requirements.

Signature_____

Print Name _____

Employer of Record_____

Date Signed_____