

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## **Section**

1. DEFINITIONS
2. INTRODUCTION
3. SOURCES OF CONFIDENTIAL INFORMATION
4. LEGAL REQUIREMENTS
5. PROCEDURES
  - 5.1 Authorized Users
  - 5.2 Training of Authorized Users
  - 5.3 Access Eligibility Process
  - 5.4 Acknowledgement of Confidential Information
  - 5.5 Storage of Confidential Information
  - 5.6 Sharing of Confidential Information
  - 5.7 Destroying Confidential Information
  - 5.8 Breach of Confidentiality
6. SOURCES
7. ATTACHMENTS
  - 7.1 User Attestation Form
  - 7.2 Toolbox 2.0 Access Request Form

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## 1. DEFINITIONS:

### 1.1 Disclosure:

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

### 1.2 Authorized Users:

Defined as workforce investment system staff, consultants, or any other subcontracting entity, and include any other person having routine access to workforce investment system confidential information/data. These users must be identified on the appropriate entity's Confidential Information Authorized User List.

### 1.3 Confidential Information:

Any information that identifies or describes an individual or employer, including, but not limited to, name, social security number, ethnicity, age, date of birth, gender, home address, telephone number, physical description, family and household composition, domestic violence, education, medical / employment history, wages, Federal Employer Identification Number (FEIN), North American Industrial Classification System (NAICS) code, unemployment insurance payments or status, account information and/or financial matters. Confidential information also includes statements made by, or attributed to, the individual or any employer.

### 1.4 Partners or Partner Agencies:

Refers to any Missouri state agency as part of the Career Center system, besides the Division of Workforce Development (DWD). These include the Department of Labor and Industrial Relations (DOLIR), Family Support Division (FSD), Department of Corrections (DOC), Department of Elementary and Secondary Education (DESE), Office of Administration, Coordinating Board for Higher Education, Division of Vocational Rehabilitation, Information Technology Support Division (ITSD), Department of Health and Senior Services, Local Workforce Investment Boards and their contractor or subcontractor agencies. This includes agencies acting under the listed agencies' authority.

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## 2. INTRODUCTION

- 2.1 The public workforce investment system consists of DWD, local workforce investment boards (WIBs) and their contractors and sub-contractors, as well as partner agencies. All of these entities use various forms of confidential information in day-to-day operations.

The purpose of this plan is to identify sources of confidential information and to establish procedures for safe handling of this information so it is not accessed by unauthorized users. Maintaining confidential records is important for obvious reasons to the individual, including the prevention of identity theft.

Any WIB that has a Confidentiality and Information Security Plan must ensure the plan is in concurrence with this plan. Furthermore, the WIBs are responsible for ensuring that their contractors' (or any subcontractor's) confidentiality policies are in concurrence with this plan.

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## 3. SOURCES OF CONFIDENTIAL INFORMATION

3.1 Sources of confidential information in the workforce investment system include:

- 3.1.1 Customer individual record files (paper copy, Toolbox case files, etc.)
  - 3.1.1.1 This includes all eligibility documentation, as required by DWD Issuance 13-99, as amended, Technical Assistance Guidance on Documentation / Verification Systems for Title I of WIA.
- 3.1.2 Toolbox DWD Reports (Employment and Training Reports, assessment records, performance outcomes, etc.)
- 3.1.3 Mo Performs individual roster data (prepared by FutureWork Systems)
- 3.1.4 Unemployment Insurance (UI) wage records
- 3.1.5 Wage Record Interchange System (WRIS) data
- 3.1.6 U.S. Department of Labor Data Report and Validation Software (DRVS)
- 3.1.7 National Reporting System (NRS)

3.2 DWD oversees or operates various federal and state programs that collect confidential information on customers. In addition to these programs, the local workforce investment boards contract with service providers, who also must utilize confidential information in their operations. A customer's confidential information may be shared among various authorized users of partner agencies that coordinate services through the workforce investment system, provided it is the sole intention of sharing confidential information only to complete an employee's job duties in delivering authorized services to the customer or program participant.

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## 4. LEGAL REQUIREMENTS

- 4.1 The various programs and services offered through the local workforce system are covered by numerous state and federal legal provisions. (See Section 6 for a listing of some prominent legal provisions. This listing is not exhaustive and a variety of other civil and criminal implications may surround confidential information and/or identity theft and may apply to this plan. )

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## 5. PROCEDURES

### 5.1 Authorized Users

5.1.1 DWD Central Office staff that have access to confidential information include the Director, Assistant Director, Program Administrators, Central Office Managers, and their designated staff. Others with access may include staff from ITSD, the Performance and Research Unit, JobSTAT Unit, Skill Development Center – Technical Support and other staff designated by their supervisor, as well as federal program staff.

5.1.2 Local staff with access to confidential information includes workforce investment board members and staff, their contractors (20 CFR, Section 667.410 (a) (2)), One-Stop Site Managers (i.e., functional managers), partner agency staff, as well as local DWD 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 The Confidentiality and Information Security training will consist of an on-line PowerPoint tutorial and an associated test which will be made available through Alchemy SISTEM™. This training is designed to familiarize all users with privacy issues and guidelines for the use of confidential data maintained by DWD, local WIBs and their contractors, and partner agencies. All users will be required to take this training, pass a test, and sign the Confidential User Attestation Form (UAF—see Attachment 1) prior to requesting access to confidential information. This includes access to certain web sites or systems (such as Toolbox, UI Reporting, MoPerforms, DRVS, etc.) that contain confidential information.

5.2.2 System Access Request Forms for partner users must be signed by the immediate supervisor and the individual assigned to maintain the Confidential Information Authorized User List.

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## 5.3 Access Eligibility and Registry Process

- 5.3.1 DWD Skill Development Center (SDC) will be responsible for maintaining the Confidential Information Authorized User List composed of case management system and other on-line data systems users.
- 5.3.2 Local WIB Director and One-Stop Site Manager (OSSM) will oversee this process for their regions, including respective contractors, to ensure all partners (except local DWD staff) maintain the authorized user lists appropriately. This process should also be addressed in the local Memorandum of Understanding and the local Business Plan. DWD's Quality Assurance Unit may monitor compliance of this as part of the normal program monitoring process.
- 5.3.3 Supervisors of DWD authorized users will be responsible for ensuring that staff have been trained, and tested, and have submitted their Confidential UAF. The supervisor will submit completed Confidential UAFs to DED Human Resources for inclusion in employees' personnel files.

For partner agency staff, the Career Center OSSM will submit completed Confidential UAFs to the respective agency's personnel office contacts.

- 5.2.3 When posting names to the Confidential Information Authorized User List, the supervisor will also designate the types of information the user will be accessing (i.e., UI mainframe data [Sessions], Toolbox, and MoPerforms rosters).
- 5.2.4 DWD's Skill Development Center/Technical Support Unit will provide access (including requests from local WIBs) to authorized users.

## 5.4 Acknowledgement of Confidential Information

- 5.4.1 Customers accessing MissouriCareerSource.com are made aware that the information they submit:

*"(Is) only used for the specific purpose for which it is intended. We do not disclose, give, sell or transfer any personal information about our visitors, unless required for law enforcement or statute."*

Customers registering in-person with career center staff must also be reminded of this statement.

## Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

- 5.4.2 Paper copies of confidential information should be marked, “Confidential.”
- 5.4.3 E-mail and faxes are not considered secure transmissions for confidential information and have the ability 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 upon arrival. 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 E-mails and faxes must not contain a customer’s full social security number. Rather, the customer’s full name, with middle initial, followed by the last four digits of their social security number, the customer’s programmatic identification code, or the Toolbox application i.d. number, if applicable, will be used to protect their identity when providing communication documents.
- 5.4.5 Faxes and e-mails containing confidential information must include the statement below in the e-mail or on the fax cover sheet. The fax form available on WorkSmart has been updated to include this language.

**CONFIDENTIALITY STATEMENT:** This e-mail and any attachments are intended only for those to which 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 e-mail, you are hereby notified that any use, dissemination, or copying of this e-mail or the information contained in this e-mail 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.

Best practices suggest that a confidentiality tag line should be added to all email correspondence to guarantee that any intentional or unintentional reference to confidential client data is appropriately designated. The Division of Workforce Development will implement this by having all DWD staff add the above statement to their signature blocks. All Toolbox 2.0 users (including partners) must have a confidentiality tag line similar to the one above. To add the confidentiality statement to a signature block, reference appropriate Outlook or other software instructions.

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## 5.5 Storage of Confidential Information

- 5.5.1 Any confidential information that is in paper format will be stored in a secure location to prevent access from unauthorized users. A secure location could include a locked cabinet, room, or other secure means, with access only to staff who are authorized users.
- 5.5.2 Customer medical information needs to be stored in a separate secure location and noted in the customer's case file.
- 5.5.3 Confidential information stored electronically should have security programs put in place to prevent unauthorized users from accessing this information.
- 5.5.4 Confidential information should not be left unattended by the authorized users. Computers/computer screens should be "locked" (i.e., CTRL+ALT+DELETE) before leaving unattended. Authorized users should be conscious of information displayed on computer screens when interacting with unauthorized users.
- 5.5.5 Electronic media containing confidential information (i.e., diskettes, disk drives, CD-ROMs, tapes, etc.) must be properly secured (i.e., locked in a drawer or cabinet) to prevent unauthorized access.
- 5.5.6 When a staffing change occurs, it is the responsibility of the supervisor to ensure all confidential information is returned, and user access terminated as appropriate. This includes, but is not limited to, submitting an Access Request Form to DWD Skill Development Center/Technical Support to inactivate system access.

## 5.6 Sharing of Confidential Information

- 5.6.1 Sharing confidential information is a necessity to operate the programs mentioned in Section 2 of this plan. Any user utilizing this information will need to be an authorized user.
- 5.6.2 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.
- 5.6.3 When requested in writing by law enforcement for investigative purposes, confidential information will be shared. However, the user receiving the request

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

must follow procedures outlined in the DWD Media and Legislative policy, found on the Internet at <https://worksmart.ded.mo.gov>.

## 5.7 Destroying Confidential Information

- 5.7.1 When paper copies of confidential information are no longer needed, documents should be disposed of according to applicable state and federal retention guidelines, and using appropriate methods (i.e., shredded on site, placed in a locked receptacle for shredding later, and otherwise ensuring it is not accessible to others, etc.) to maintain confidentiality.
- 5.7.2 Per state policy, electronic documents and emails are archived and cannot be destroyed.

## 5.8 Breach of Confidentiality

- 5.8.1 Any disclosure of confidential information (whether careless, accidental, or intentional) to unauthorized individuals is considered a breach. Unauthorized modification or deletion of information, or other violations of procedures listed in this plan, are also considered breaches. Information regarding a confidential information security breach is, on its own, confidential information and is not to be shared with anyone other than the immediate supervisor. Such actions may result in disciplinary, civil, or criminal, action.
- 5.8.2 If the breach involves information from DWD or a partner agency (see Section 1.4), the user who discovered the breach must notify the supervisor immediately, but not later than two (2) business days. It is then the supervisor's responsibility to ensure notification is provided to the agency's appropriate up-line management.
- 5.8.3.1 If a breach occurs within DWD, the DWD Director (or assigned designee) will be responsible for notifying the partner agency acting as the source of information compromised.

If the breach occurs within a partner agency, the Director from the partner agency is responsible to notify the partner agency that was the source of information compromised. (i.e., DWD or other agency listed in Section 1.4)

## Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

- 5.8.4 If a breach occurs, the agency acting as the customer point of contact and source of information will be responsible for notifying the individual of the breach.

If the notifying agency is acting under the authority of DWD, the DWD Director (or assigned designee) will be involved in the customer notification process.

- 5.8.5 The U.S. Department of Labor's Training and Employment Notice #26-07, Job Bank Security Fraud Awareness, dated January 23, 2008, provides a list of resources individuals and organizations may use regarding prevention and reporting of cyber crimes. Individuals who suspect or know they have been the victim of a cyber crime can file a report at <http://www.ic3.gov/>. This website is the Internet Crime Complaint Center, which is a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance. DWD will comply with the criminal complaint procedures and promote the best practices outlined in this notice.

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

## 6. SOURCES

6.1 Below is a list of state and federal legal provisions that may affect the programs and services offered through the local workforce investment system. This list should not be considered all inclusive. This listing is not exhaustive and a variety of other civil and criminal implications may surround confidential information or identity theft and may apply to this plan. )

- 6.1.1 State Code of Conduct Policy SP-13.
- 6.1.2 U.S. Department of Labor's Training and Employment Notice #26-07, *Job Bank Security Fraud Awareness*, dated January 23, 2008
  - The purpose of this document is to increase awareness of potential threats to Personally Identifiable Information (PII) and other types of data stored in state job bank data systems and to inform states and local areas about resources for job bank fraud prevention and reporting.
- 6.1.3 Revised Statutes of Missouri, Chapter 288, Section 250, Title XVIII, Labor and Industrial Relations
- 6.1.4 Missouri's Safe at Home Act (2007)
- 6.1.5 Title III of the Social Security Act (SSA)
  - Statutory Confidentiality and disclosure requirements by this agency and use of Social Security number.
- 6.1.6 The Federal Unemployment Tax Act (FUTA)
  - Statutory Confidentiality and disclosure requirements.
- 6.1.7 Public Health Service Act (PHSA)
  - Provisions on the use of data by the National Center for Health Statistics.
- 6.1.8 The Health Insurance Portability and Accountability Act (HIPA)
  - Permits health insurance shopping by consumers and protects individuals by limitations on how health information may be used and privacy implications.
- 6.1.9 The Family Educational Rights and Privacy Act (FERPA)

# Workforce Development System Confidentiality and Information Security Plan



Effective September 1, 2008

- Protects the privacy interests of students and parents of students who are minors with respect to their personal education records.

6.1.10 The Family Medical Leave Act (FMLA)

6.1.11 Freedom of Information Act (FOIA)

6.1.12 The Open Records Act (Sunshine Act)

6.1.13 The Age Discrimination in Employment Act

6.1.14 Title IV of the Civil Rights Act of 1964

6.1.15 Workforce Investment Act (WIA) - Requires the states to measure their progress in services by using “quarterly wage records, consistent with State law.”

6.1.16 Any confidential information management regulations.

6.1.17 Any regulations and rules of Federal Personnel Law Governing Federal Employee’s Behavior.