MISSOURI Career Center
Where talent and opportunities meet
www.MissouriCareerSource.com

NEMO WORKFORCE INVESTMENT BOARD • 111 E. Monroe • Paris, Missouri 65275 • (660) 327-5125 • Fax (660) 327-5128
www.nemowib.org

MEMORANDUM

TO: NEMO WIB Employees and Subcontractors

FROM: Brandi Glover, Executive Director

SUBJECT: Confidentiality and Confidential User Attestation

The NEMO Workforce Investment Board has adopted DWD Issuance 01-2008, Change 2 regarding Workforce Development System Confidentiality and Information Security Plan as its Confidentiality policy. The NEMO WIB requires that all employees of the NEMO WIB and all employees of NEMO WIB subcontractors adhere to DWD Issuance 01-2008, Change 2.

The NEMO WIB requires all employees and employees of subcontractors, that access confidential information, to complete the DWD Confidentiality and Information Security training & test, and sign the Confidential User Attestation. The Confidential User Attestation should be placed in the individual's personnel file.

If you have any questions regarding confidentiality, please contact the WIB office.

DWD Issuance 01-2008, Change 2

Issued: September 15, 2011
Effective: September 15, 2011

Subject: **Workforce Development System Confidentiality and Information Security Plan, Breach of Toolbox Data Confidentiality Update**

1. Purpose: The purpose of this Issuance Change is to update all appropriate data users, and their supervisors, regarding the breach of Toolbox data confidentiality.

2. Background: The Department of Economic Development Acceptable Computer Use Policy governs the use of State systems and applies to all Department of Economic Development (DED) employees and **all DED system users.**

   Pursuant to the DED Acceptable Computer Use Policy, The Division of Workforce Development (DWD) has amended its Workforce Development System Confidentiality and Information Security Plan to include a section regarding Breach of Toolbox Data Confidentiality which is attached. Future trainings regarding compliance with the Confidentiality and Information Security Plan shall include a discussion of the breach of Toolbox data confidentiality.

3. Substance: The Workforce Development System Plan (**Attachment 1**) identifies sources of confidential information and authorized users, including training for these users. The Plan also includes procedures for the storage, sharing and discarding of confidential information and basic information for handling breaches of confidentiality.

4. Action: The Workforce Development System Confidentiality and Information Security Plan with the Breach of Toolbox Data Confidentiality addendum should be distributed to all potential data users from the local Workforce Investment Boards (LWIB), subrecipients, and partner agencies and their supervisors, so that they become familiar with its content.

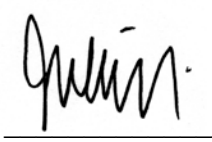
   Any LWIB that maintains its own confidentiality plan should ensure that their plan is in concurrence with the Workforce Development System Confidentiality and Security Plan, as amended through this Issuance. Also, LWIBs are responsible for ensuring that their subrecipients' confidentiality policies are in concurrence with same.

6. Contact: Direct questions or comments regarding this Issuance to the Skill Development Center-Technical Training unit at dwdtraining@ded.mo.gov.

7. Reference: Department of Economic Development Acceptable Computer Use Policy

8. Rescissions: No Rescissions.

9. Attachments: (1) Workforce Development System Confidentiality and Information Security Plan (Section 5.9, Breach of Toolbox Data Confidentiality).



Julie Gibson
Director

Authority: DWD Issuance 01-2008, 09/01/08; DWD Issuance 01-2008 C1, 02/01/11

Workforce Development System
Confidentiality and Information Security Plan

Section:

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 /disability related or 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 (LWIB) and their contractor or subcontractor agencies. This includes agencies acting under the listed agencies' authority. Partner agency refers to organizations and requirements of WIA Section 121.

1.5 Medical Information:

Any information, whether oral or recorded in any form or medium that relates to the past, present, or future mental or physical health or condition of an individual or the provision of medical services to an individual.

1.6 Disability Related Information:

Any information, whether oral or recorded in any form or medium, that relates to a physical or mental impairment of an individual that substantially limits one or more major life activities of that individual.

2. INTRODUCTION

The public workforce investment system consists of DWD; LWIBs and their contractors and sub-contractors; and 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 LWIB that has a Confidentiality and Information Security Plan must ensure the plan is in concurrence with this Plan. Furthermore, the LWIBs are responsible for ensuring that their contractors' (or any subcontractors' and partner agencies') confidentiality policies are in concurrence with this Plan.

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 13-1999, 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 LWIBs 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.

4. LEGAL REQUIREMENTS

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.)

5. PROCEDURES

5.1 Authorized Users :

5.1.1 DWD Central Office staff that have access to confidential information include the Director, Assistant Directors, 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, and federal program staff.

5.1.2 Local staff with access to confidential information includes LWIB members and staff, their contractors (20 CFR, Section 667.410 (a) (2)), Functional Leaders, partner agency staff, and 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 the Skill Development Center-Technical Support unit. This training is designed to familiarize all users with privacy issues and guidelines for the use of confidential data maintained by DWD, LWIBs 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 7. Forms) prior to requesting access to confidential information. This includes access to certain websites or systems (such as Toolbox, UI Reporting, MO Performs, 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.

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 LWIB Director and Functional Leader 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 monitoring process.

5.3.3 Supervisors of DWD authorized users will be responsible for ensuring that staff have been trained, tested, and have submitted their Confidential UAF. The supervisor will submit completed Confidential UAFs to DED Human Resources for inclusion in employees' personnel file.

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

5.3.4 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).

5.3.5 DWD's SDC/Technical Support unit (TSU) will provide access (including requests from LWIBs) 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.

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 (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 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 e-mail correspondence to guarantee that any intentional or unintentional reference to confidential client data is appropriately designated. DWD will implement this by having all DWD staff add the above statement to their signature blocks. All Toolbox 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.

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 and disability related information should be stored in a separate, secure location; and the location of the medical and disability related information should be noted in the customer's main 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 SDC/TSU 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 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 e-mails 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 following the discovery of the breach. It is then the supervisor's responsibility to ensure notification is provided to the agency's appropriate up-line management.

5.8.3 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).

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 (USDOL) Training and Employment Notice #26-07, Job Bank Security Fraud Awareness, dated January 23, 2008, provides a list of resources that 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.

5.9 Breach of Toolbox Data Confidentiality:

5.9.1 The Department of Economic Development Acceptable Computer Use Policy governs the use of State systems and applies to all Department of Economic Development (DED) employees and **all DED system users**. This policy cannot be modified by a supervisor's statement or conduct.

5.9.2 Each DED system user is responsible for all computer/Internet use associated with his or her assigned User ID. It is prohibited for a DED system user to use another person's User ID and confidential Password. A DED system user MUST NOT give his or her User ID and/or Password to any other individual, and must guard against unauthorized access to their assigned equipment.

5.9.3 If a breach of Toolbox data confidentiality occurs, including the sharing of Toolbox Password and Log-In, any Toolbox user who has violated the confidentiality policy shall have their access to Toolbox immediately removed. The breach of confidentiality will be assessed. For DWD employees, the appropriate employment action will be taken. Action steps include a written reprimand, suspension, or termination. A letter outlining the incident will be provided to DED Human Resources (HR) for any DWD employee affected, and a copy of that letter maintained in the employee's personnel file. Those Toolbox users who are not DWD employees will also have a letter outlining the incident sent to the LWIB Chair, with a copy to the Chief Local Elected Official (CLEO) for local disciplinary action as appropriate. Access to Toolbox will be re-instated

only after compliance with the policy is re-determined (viewing the confidentiality PowerPoint and re-taking the Confidentiality Test.)

5.9.4 Upon the second individual incident and confirmed breach of Toolbox data confidentiality, including the sharing of Toolbox Password and Log-In, any Toolbox user who has violated the confidentiality policy shall have their access to Toolbox immediately removed. The breach of confidentiality will be assessed. For DWD employees, the appropriate employment action will be taken. Action steps include a written reprimand, suspension, or termination. A letter outlining the incident will be provided to DED HR for any DWD employee affected, and a copy of that letter maintained in the employee's personnel file. Those Toolbox users who are not DWD employees will also have a letter outlining the incident sent to the LWIB Chair, with a copy to the CLEO for local disciplinary action as appropriate. Access to Toolbox will not be re-instated any sooner than two (2) full weeks from the date of the letter; and only after once again complying with the confidentiality requirements.

5.9.5 Upon the third incident of confirmed breach of Toolbox data confidentiality, including the sharing of Toolbox Password and Log-In, any Toolbox user who has violated the confidentiality policy shall have their access to Toolbox immediately removed. DWD employees will be terminated from employment. Non-DWD employees will be permanently removed from Toolbox access and a third letter outlining the incident sent to the CLEO with a copy to the LWIB Chair for local disciplinary action as appropriate.

5.9.6 **Whistleblower Clause:** All DED employees and DED system users are encouraged to report any potential breach of confidentiality through their respective lines of supervision. If you feel that reporting any issue might adversely impact your job, you can report directly to Roger Baugher (roger.baugher@ded.mo.gov), at DWD Central Office. Any reported incident will be investigated by DWD Central Office staff, and will be held in strictest confidence until the results are conclusive.

5.10 Medical and Disability Related Information:

Medical and disability related information, identified in the Workforce Development System Confidentiality and Information Security Plan, Section 5.5-

Storage of Confidential Information, shall be maintained in a separate, secure location, different from participants or employees' main file. Local Workforce Investment Boards (WIB), partner agency staff, and the Division of Workforce Development (DWD) will take measures to ensure, with the support of Information and Technical Services Division (ITSD), that all medical and disability related information collected, will be treated consistent to all other information identified as "confidential" within the policy, with the exception that medical and disability related information must be kept "confidential and separate" from the main file; whether information is maintained with paper or electronic copy. Electronic files must be password-protected and hard files must be kept in a secure, locked location.

Under 5.5 – Storage of Confidential Information, Subsection 5.5.2, "Customer medical and disability related information must be stored in a separate, secure location; and the location of the medical and disability related information must be noted in the customer's main file."

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

The revisions to this policy, (DWD Issuance 01-2008) including any attachments, will be made effective immediately and all Next Generation Career Center (NGCC) participants and employees, including DWD, WIB Staff, partner agency staff, and subrecipients, shall be provided the authority to carry out the revision required by this notice.

In addition to the rules applied under Section 5.8, Breach of Confidentiality, this policy addendum is subject to the corrective actions and sanctions procedures found in DWD Issuance 07-2010.

Direct all inquiries or comments to Juanita Davis Reynolds, State EO Officer, at (573) 751-2428 or e-mail juanita.reynolds@ded.mo.gov.

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 USDOL'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, DOLIR.

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 SSN.

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).

- 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."

6.1.15a Workforce Investment Act (WIA) Section 188 and Section 504 of the Rehabilitation Act of 1973, as Amended.

6.1.16 Any confidential information management regulations.

6.1.17 Any regulations and rules of Federal Personnel Law Governing Federal Employee's behavior.

7. Forms:

CONFIDENTIAL USER ATTESTATION FORM

I understand that in the course of my employment with the Missouri Division of Workforce Development, local Workforce Investment Board, subcontractor, 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 Division 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 to not 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 Division of Workforce Development's Confidentiality and Information Security Plan and the above requirements.

Signature_____

Print Name_____

Date Signed_____