Employment Security Department
WASHINGTON STATE

WorkSource System Policy
Employment System Administration and Policy

Washington envisions a nationally recognized fully integrated One-Stop system with enhanced customer access to program services, improved long-term employment outcomes for job seekers and consistent, high-quality services to business customers. In order to achieve this vision, Employment System Administration and Policy sets a common direction and standards for Washington's WorkSource system through the development of WorkSource system policies, information memoranda, and technical assistance.

Policy Number: 1021, Revision 2

To: Washington WorkSource System

Effective Date: 12/1/2022

Subject: Management Information System Access and Data Sharing, Disclosure, and Security Administration

1. **Purpose**:

To communicate Employment Security Department (ESD) and WIOA one-stop system partner roles and responsibilities related to data sharing, data disclosure, and security administration for the ESD's management information system (MIS) used by state and local administrators and service providers to oversee and deliver U.S. Department of Labor (DOL) funded WIOA one-stop system services.

2. **Background**:

ESD is responsible for (1) providing direction for MIS data sharing, data disclosure and security administration; (2) defining requirements for access to the MIS and its data; (3) defining roles and responsibilities for MIS data sharing, disclosure, and security administration; and (4) ensuring compliance with applicable laws, rules and policies that govern MIS data, which is required to be held private and confidential pursuant to RCW 50.13 and other applicable federal and state laws, rules, and guidance. Access to the MIS system and data must be limited to individuals whose currently assigned job duties justify a business need for access and those with access to MIS data must be informed on how to handle private and confidential information as specified in the procedures and terms of MIS data sharing contracts.

3. **Policy**:

a. Minimum Requirements for MIS Access

The following three conditions must be met before individuals are granted access to the MIS:

i. Individuals' agencies or organizations have signed effective contracts with LWDBs or ESD or directly with the U.S. Department of Labor identifying them as providers of WIOA-affiliated services; and
ii. Individuals' agencies or organizations have signed and effective MIS data sharing contracts with ESD; and
iii. Individuals have completed state-approved MIS training.

NOTE: ESD internal users are not impacted under conditions i. and ii., therefore must meet only the training requirement. (See definition section for internal users)

b. MIS Data Sharing Contracts

Each MIS data recipient is required to have a signed and effective MIS data sharing contract with ESD before access is granted to its employees. The data sharing contract must specify the business case for MIS access. Access must be requested to the ESD data-sharing unit by an approving authority of an LWDB.

c. Requests for Access to MIS Records

All requests from the public or subpoenas received by MIS data recipient for access to MIS records in accordance with RCW 42.56 or RCW 50.13 must be immediately reported to the MIS Security Administrator. The MIS data recipient must instruct the requester to submit the request in writing to:

Email: recordsdisclosure@esd.wa.gov
Phone: 844-766-8930
Fax: 866-610-9225
Mail: Records Disclosure Unit
Employment Security Department
PO Box 9046
Olympia, WA 98507-9046

The request will be processed by ESD's Records Disclosure Unit in accordance with published rules for release of information.

d. MIS Security Administration

The MIS Security Administration Unit is positioned in the Data Sharing office of ESD and protects MIS resources from unauthorized access or being compromised. The MIS Security Administration Unit has the following responsibilities:

i. Enforce the provisions of this policy at the local and state level.
ii. Monitor local level data sharing/disclosure requirements, including the activities of MIS Access Requesters.
iii. Provide general oversight, training, and support on data sharing and disclosure issues.
iv. Draft, negotiate, and ensure that valid MIS data sharing contracts are in place for every agency or organization that has MIS users.
v. Keep updated and accurate list of identified designated Access Requesters.
vi. Ensure that MIS access is revoked for users at such time that the data sharing contract for their agency or organization expires.

vii. Ensure that MIS access is granted only to users who work for an agency or organization that is party to a WorkSource Memorandum of Understanding (WorkSource Partner) or is an LWDB or ESD contractor for WIOA services.

The MIS Security Administration Unit is responsible for ensuring compliance with all applicable laws, rules and policies related to data sharing, disclosure, and MIS security administration.

e. MIS Access Requester

Division Directors, Regional Directors, Administrators and LWDB Directors have the authority to designate the Local MIS Access Requesters to ensure oversight of the responsibilities for local Security Administration.

Only designated MIS Access Requesters have authority to submit requests to have MIS users added, changed, or disabled (See “Procedure to Add/Change/Disable User Access” below). All MIS Access Requesters are responsible for submitting MIS user access requests for the offices within their Workforce Development Areas (WDAs). Upon submitting requests to add new users, MIS Access Requesters must certify that the minimum requirements in section 3.a. has been met.

i. Responsibilities of Local Access Requesters

1) Enforce the provisions of this policy.
2) Ensure that all users complete state-approved MIS training prior to requesting MIS access.
3) Verify requested default office assignment, users’ profiles, and any additional office assignments are appropriate, based on business needs and approved by user’s supervisor.
4) Ensure that the local MOU has been signed by the partner and Data Sharing agreements are in place prior to requesting access for user.
5) Ensure that users electronically sign non-disclosure agreements in MIS once access is granted.
6) Provide local oversight and support.
7) Ensure by monitoring, that separated MIS users’ access are deactivated timely.
8) Report system misuse and security breaches to the MIS Security Administrator.

ii. Responsibilities of Internal Central Office Access Requesters

1) Ensure that all users complete state-approved MIS training prior to requesting MIS access.
2) Verify requested default office assignment, users’ profiles, and any additional office assignments are appropriate, based on business needs and approved by user’s supervisor.
3) Ensure that users electronically sign non-disclosure agreements in MIS once access is granted.
4) Ensure by monitoring, that separated MIS users’ access are deactivated timely.
5) Report system misuse and security breaches to the MIS Security Administrator.

ESD Internal Central Office Access Requesters are assigned within divisions of ESD.

f. MIS Procedure to Add/Change/Disable User Access

ESD will provide an access request form, that designated MIS Access Requesters can use to transmit information needed to process requests to add, change or disable MIS users. Requests will be reviewed and verified that all conditions for MIS access have been met. Upon approval of requests, users will be added, changed, or disabled in the MIS as requested, and MIS Access Requesters and users will receive notification of the actions taken.

MIS Access Requesters must submit requests to the MIS Security Administration Unit at Datasharingsupport@esd.wa.gov to have users added, changed or disabled who no longer have business needs to access the MIS (e.g., resignation, retirement, termination, end of projects) at least 24 hours before the effective date that access is to be disabled, if possible.

g. MIS Access Management

The MIS Access Management Unit is positioned in the Information Technology Services Division (ITSD) of ESD, and has the following responsibilities:

i. Process all approved and completed requests for user access.
ii. Assign user logon IDs and remove users from the system on receipt of complete and authorized requests from MIS Access Requesters.

h. MIS Monitoring and Audit

The MIS, its data, and security administration procedures at the state and local levels are subject to audit by ESD's Internal Audit Unit and the State Auditor's Office and monitoring by authorized ESD representatives.

i. Sanctions

Violation of this policy may result in revocation of access to the MIS in accordance with the "Termination of Access" provision in the MIS data sharing contract. Misuse or unauthorized release of records, or information considered private and confidential by any person or organization, may subject the individual or organization to sanctions under the state's WIOA Title I Policy 5406 and civil penalties and other applicable sanctions under RCW 50.13 and other applicable federal and state laws, rules, and guidance.

4. Definitions:

Local Workforce Development Board (LWDB) – An entity authorized under WIOA Section 107 that includes entity's officers, directors, officials, trustees, employees and/or agents including students and volunteers unless otherwise stated in the WIOA Memorandum of Understanding (MOU).

Management Information System (MIS) – The ESD automated client tracking, accountability and reporting system used by the Department of Labor (DOL) funded WorkSource (one-stop) service delivery system to support the delivery and management of WIOA employment and training services.

MIS Access Management – The unit designated by ESD to implement all access requests tor MIS users added, changed, or disabled.

MIS Access Requester – An individual designated by a Division Director, Regional Director, Field Administrator or LWDB Director authorized and responsible for management and submission of requests to ESD to have MIS users added, changed, or disabled.

MIS Data Recipient – A WorkSource partner, LWDB, or WIOA contractor/grantee that has an MIS data sharing agreement authorizing access to the MIS.

MIS Internal Users –A person employed by ESD, where the position is assigned to central office and uses the MIS system for administrative or oversight functions.

MIS Security Administration – The Data Sharing office is responsible for verification and authorization of MIS access and agreements in accordance with local, state, and federal laws while enforcing the provisions and responsibilities identified in this policy.

MIS Security Breach – A security breach is any incident that results in unauthorized access to computer data, applications, networks, or devises. It results in information being accessed without authorization.

MIS System Misuse – Described as willful or negligent unauthorized activity that affects the availability, confidentiality or integrity of MIS data and access.

MIS State-Approved Training - MIS Basic training designed for new users to gain access to the state MIS. It can be delivered by the ESD lead trainer, or by a local area trainer or the online ETO basic /refresher training videos posted to WPC https://wpc.wa.gov/tech/ETO-refresher-training. It covers ETO basic functionality, where resources are located on the Workforce Professional Center (WPC) site and an overview of WorkSource Washington (WSWA). It does not cover program specific training such as, Workforce Innovation Opportunity Act (WIOA) Title I-B programs, Trade Adjustment Assistance (TAA), Veterans, RESEA or WorkFirst. Program specific training is done by the Program Operators or by your local area subject matter experts.

Memorandum of Understanding (MOU) – A formal agreement(s) developed and executed by the LWDB and partners, with agreement of local CEO(s), relating to the operation of the one-stop delivery system. It further define(s) roles, responsibilities, and the flow of services to be provided by one-stop partner programs in the local WDA and ensure(s) the successful integration and implementation of partner programs in the one-stop system. See policy 1013 Revision 4, One-Stop Memorandum of Understanding.

WIOA Contractor – An entity that has a contract to provide DOL funded WIOA employment and training services and includes the Contractor's officers, directors, officials, trustees, employees and/or agents including students and volunteers.

5. **References**:

- RCW 50.13 - Records and Information - Privacy and Confidentiality
- RCW 50.13.060 - Access to records or information by governmental agencies
- RCW 42.56.070 – Documents and indexes to be made public
- Public Law 113-128, Workforce Innovation and Opportunity Act of 2014
- Governor's Executive Order 003 on Public Record Privacy Protection
- Privacy Act of 1974
- Social Security Act
- ETO Add Change User Form

- 20 CFR 603
- Policy 1013 Revision 4, One-Stop Memorandum of Understanding

6. **Supersedes**:

   WorkSource System Policy 1021 Revision 1 – Management Information System Access and Data Sharing, Disclosure, and Security Administration dated December 3, 2021

7. **Website**:

   https://wpc.wa.gov/policy/state/worksource

8. **Action**:

   Local Workforce Development Boards and their contractors as well as ESD Regional Directors must distribute this policy broadly throughout the system to ensure that WorkSource System staff are familiar with its content and requirements.

9. **Attachments**:

   None

Direct Inquiries To:

MIS Data Sharing Unit
Employment Security Department
PO Box 9046
Olympia, WA 98507-9046
Datasharing@esd.wa.gov

Direct Policy Inquiries To:

Employment System Administration and Policy
Employment System Policy and Integrity Division
Employment Security Department
P.O. Box 9046
Olympia, WA 98507-9046
SystemPolicy@esd.wa.gov