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 1
To: Washington WorkSource System
Effective Date: December 3, 2021

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

b. MIS Data Sharing Contracts

Each MIS data recipient is required to have a signed and effective MIS data sharing contract with ESD or an LWDB before access is granted to its employees. The data sharing contract must specify the business case for MIS access and must include all of the provisions noted below. Sub-state requests must be requested to the ESD data-sharing unit by an approving authority of an LWDB.

c. General Provisions to be Included in All MIS Data Sharing Contracts

The ESD standard MIS data sharing contract must be used for all MIS data sharing contracts between MIS data recipient(s) and ESD. Contracts are subject to approval by the MIS Security Administrator and the ESD Contracts Office. The MIS Security Administrator must obtain signed approval from the owning division's designated Data Owner(s) before approving data sharing contracts.

d. 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.

e. MIS Security and Data Sharing Administrator

The MIS Security and Data Sharing Administrator is positioned in the Data Sharing unit of ESD. The MIS Security and Data Sharing Administrator 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, support and technical assistance 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. Monitor and verify employment status of Access Requesters;
vi. Work with ESD Regional Directors and LWDB Directors to identify designated Access Requesters.
vii. Ensure that MIS access is immediately revoked for users at such time that the data sharing contract for their agency or organization expires.
viii. Ensure that MIS access is granted only to users who work for an agency or organization that is party to a WorkSource Memorandum of Agreement (WorkSource Partner) or is an LWDB or ESD contractor for WIOA services.

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

f. MIS – Security Administration

The Security Administration is to protect the MIS resources from unauthorized access or being compromised. Both the Employment Connections Division (EC) of ESD and the LWDB Directors will designate the MIS Access Requesters to ensure oversight of the responsibilities for local Security Administration.

g. EC Responsibilities – Security Administration

i. Designate local MIS Access Requesters who have authority to request user access to the MIS and its data.
ii. Enforce the provisions of this policy at the local and state level.
iii. Ensure that all users complete state-approved MIS training.
iv. Ensure that staff submit Non-Disclosure agreements in MIS once access is granted.
v. Provide local level oversight, support and technical assistance.
vi. Verify employment status of ESD staff;
vii. Verify employment status of ESD Access Requesters;
viii. Designate an Access Reqeuster for ESD Central Office staff.
ix. Ensure by monitoring that separated MIS user access are deactivated timely.
x. Notify ESD's data sharing unit through the request form (see "Procedure to Add/Change/Disable User Access" below) when users need to be added, changed or disabled.

h. LWDB Responsibilities - Security Administration

i. Designate local MIS Access Requesters who have authority to request user access to the MIS and its data.
ii. Enforce the provisions of this policy at the local and state level.
iii. Ensure that all users complete state-approved MIS training.
iv. Ensure that local MOU and Data Sharing agreements are in place prior to requesting access for users.
v. Ensure staff submit Non-Disclosure agreements in MIS once access is granted.
vi. Provide local level oversight, support and technical assistance.
vii. Enforce security rules and policy at the local level.
viii. Ensure by monitoring that local separated MIS user access are deactivated timely.
ix. Report system abuse and security breaches to the MIS Security Administrator.
x. Notify ESD's data sharing unit through the request form (see "Procedure to Add/Change/Disable User Access" below) when users need to be added, changed or disabled.

MIS Security Administration ensures compliance with all applicable statutes, laws, rules and policies related to MIS security.

i. MIS Access Requester

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 within their Workforce Development Areas (WDAs). Upon submitting requests to add new users, MIS Access Requesters must certify that the following conditions have been met:

i. Users have completed required training;
ii. Users profiles and office assignments requested are appropriate, based on business needs and approved by user's supervisor; and
iii. Once access has been granted, users have signed and dated non-disclosure agreements.

MIS Access Requesters must submit requests to the data sharing unit to have users 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 disabled, if possible.

All requests for MIS access from other agencies or private source must go through the Security and Data Sharing Administrator to ensure proper documentation has been completed.

j. MIS Access Management

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

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

k. Procedure to Add/Change/Disable User Access

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

l. 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 duly authorized ESD representatives.

m. 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 that entity's officers, directors, officials, trustees, employees and/or agents including students and volunteers unless otherwise stated in the MIS data sharing contract.

Management Information System (MIS) – The ESD automated client tracking, accountability and reporting system used by the 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 ITSD to recieve all access requests tor MIS users added, removed or modified.

MIS Access Requester – An individual designated by a Regional Director, Field Administrator or LWDB authority to submit requests to ESD to have MIS users added, removed or modified.

MIS Data Recipient – A WorkSource partner (including ESD), LWDB, or WIOA contractor/grantee that is authorized to have access to or receives MIS data.

MIS Security Administration – Responsibilities to protect the MIS resources from unauthorized access or being compromised.

MIS Security and Data Sharing Administrator – An individual appointed by ESD to enforce the provisions of this policy and carry out other responsibilities identified in the 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 Abuse – IT abuse describes willful or negligent unauthorized activity that affects the availablity, confidentiality or integrity of the information technology resources.

MIS State-Approved Training - MIS Basic training is designed for new users to gain access to the ETO system. It can be delivered by the ESD lead trainer or by a local area trainer. 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, or Workfirst. Program specific training is done by the Program Operators or by your local area subject matter experts.

Non-ESD WorkSource Partner – An entity that is a party to a local WorkSource Memorandum of Understanding (MOU) and is performing WorkSource services and includes that entity's officers, directors, officials, trustees, employees and/or agents including students and volunteers unless otherwise stated in the MIS Data Sharing Contract.

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 unless otherwise stated in the MIS Data Sharing Contract.

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
- Add/Change/Disable User Request Form

6. **Supersedes:**

   - WorkSource System Policy 1021 – WorkSource Integrated Technology (WITS) Data Sharing, Disclosure, and Security Administration
   - ESD Administrative Policy 0030 - SKIES Data Sharing, Data Disclosure, and Security Administration

7. **Website:**

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

8. **Action:**

   LWDBs and their contractors, as well as Employment Security Regional Directors, must distribute this policy broadly throughout the system and ensure that WorkSource System staff are in complaince 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 Other Inquiries To:

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