MLDS Center

Maryland Longitudinal Data System

Better Data • Informed Choices • Improved Results

# Staff Authorization and Access

(Version 6 – October 20, 2022)

**Maryland Longitudinal Data System Center**
550 West Baltimore Street
Baltimore, MD 21201
www.MLDSCenter.Maryland.gov
MLDS.Center@Maryland.gov
410-706-2085

**Table of Contents**

## Overview

This document provides the procedures and forms for staff authorization and access to the Maryland Longitudinal Data System. The document also outlines the required rules of security behavior to ensure the security and privacy of the data in the system.

## Legal Requirements

1. Ed. Art. § 24-703 (g)

   *(1) Direct access to data in the Maryland Longitudinal Data System shall be restricted to authorized staff of the Center.*
   *(2) The Center may only use de–identified data in the analysis, research, and reporting conducted by the Center.*
   *(3) The Center may only use aggregate data in the release of data in reports and in response to data requests.*
   *(4) Data that may be identifiable based on the size or uniqueness of the population under consideration may not be reported in any form by the Center.*
   *(5) The Center may not release information that may not be disclosed under the federal Family Educational Rights and Privacy Act and other relevant privacy laws and policies.*

2. COMAR 14.36.06.

   *.01 Authorized staff include State employees and individuals authorized by the Executive Director. The executive director may only authorize individuals to serve as staff of the Center who are necessary to carry out the mission of the Center. The number of authorized staff shall be restricted in number for the purpose of maintaining control over access to the system. Generally, authorized staff are researchers and information technology experts and technicians.*

   *.02 Requires staff to have a State and federal criminal history background check within 5 business days of starting as staff of the Center. An individual is deemed to have an unsatisfactory criminal history background if the individual has been convicted of a felony of any nature or, within the last 10 years, has been convicted of a crime that qualifies as an infamous crime under Maryland law.*

   *.03 Requires staff to comply with rules of security behavior, receive and review the MLDS Data Security and Safeguarding Plan, and periodically take security and privacy training classes. The executive director shall remove staff member's access for failure to comply with these requirements.*

# Procedure

**Note:** All signatures will be collected electronically using DocuSign. Accordingly, you will need to provide all required information on this form and then email it unsigned to Jamese Dixon-Bobbitt (Jamese.Dixon-Bobbitt@maryland.gov). She will review the form to ensure that it is complete and then circulate it to you and the other required signatories.

**Provide Applicant Information**

| | |
|---|---|
| **Name**[1] | |
| **Affiliation** | |
| **Address** | |
| **City, State Zip** | |
| **Phone** | |
| **Email** | |

**Required Steps**

1. Review - *Rules of Security Behavior*
2. Review *Policy for Conducting Criminal History Background Investigations* and Complete the Background Investigation (not required for view only access)
3. Complete required Security Training for MLDS Center Staff (not required for view only access)
4. Complete required FERPA Training
5. Review - *Acknowledgement of Receipt and Review of Required Documents* (not required for view only access)
6. Review and Sign – *Department of Labor Confidentiality Certification Form* (Appendix B) (not required for view only access)
7. Complete and Sign – *User Access Form* (not required for view only access)
8. Final Authorization Approval

[1] If the name you provide is different from the name on your Driver's License or other official identification card, please note that you will be required to provide that name when completing your criminal history background investigation. If your name is different, please email ross.goldstein@maryland.gov to notify him of the fact that the name that will appear on the criminal history background investigation report is different from the name on this form.

# Rules of Security Behavior for Authorized Staff of the MLDS Center

For purposes of this document:

1. "Authorized staff of the Center" includes the following types of individuals regardless of whether they are paid by the Center:
    a. State employees (permanent or contractual) of the MLDS Center;
    b. A researcher authorized by the Executive Director, pursuant to COMAR 14.36.06, to serve as a MLDS Center staff member for a specified time and duration;
    c. An information technology contractor or vendor authorized by the Executive Director pursuant to COMAR 14.36.06; and
    d. A researcher or data analyst from a data sharing partner agency.
2. "Confidential information" means:
    a. Any information about the data system, including the data dictionary and any documentation with information about database design or schematics that are proprietary or if disclosed could compromise system security;
    b. Any data that contains personally identifiable information,[2] de-identified individual records,[3] or aggregate information that may be identifiable based on the size or uniqueness of the population or could foreseeably be combined with other publicly available information to reveal identifiable information.
3. "Data System" means all hardware and software that constitutes the Maryland Longitudinal Data System, including the Master Data Management System, the Operational Data Store, the Data Warehouse, virtual machines, and other components.

MLDS Center staff shall:

1. Comply with the training requirements specified in the *Required Security and Privacy Training for MLDS Center Staff (page 9);*
2. Review the MLDS Center *Data Security and Safeguarding Plan* and act in conformity with that plan and documents referenced therein;
3. Review MLDS Center data sharing agreements with data sharing partners and act in conformity with the data use, data security and confidentiality requirements established in those agreements;
4. Consistent with the *Policy for Conducting Criminal History Background Investigations (page 6)*, submit to all necessary Criminal History Background Investigations and receive authorization before having access to confidential information;
5. Not share passwords or provide unauthorized access to the data system;
6. Not disclose any confidential information;
7. Not make written notes about confidential data;

[2] Personally identifiable information includes an individual's name, Social Security number, driver's license number, state identification number, or other individual identification number such as a passport number, an Individual Taxpayer ID, or a financial or other account number.

[3] De-identified individual records are individual student or worker records that have been stripped of personally identifiable information. This includes all records in the MLDS operational data store.

8. Only access the data system on a computer and network that has been pre-approved by the MLDS Center CIO in the *User Access Form* and in a manner consistent with the *Data Security and Safeguarding Plan* and documents referenced therein;
9. Not download, copy (including a screenshot), or in any way distribute or use confidential information from the data system;
10. Ensure that all data tables and other information requested for release from the system:
    - Contain only aggregate results from de-identified data;
    - Have been suppressed consistent with the Center's requirements; and
    - Have been reviewed and approved for release[4] by the Executive Director, or the Executive Director's designee;
11. Not discuss confidential information with any person other than appropriate MLDS Center staff; and
12. Report any actual or potential risk or vulnerability that may compromise the security of confidential information to the MLDS Center Executive Director or a Branch Director.

I have read and understand these rules of security behavior and that they are applicable even when my staff appointment with the MLDS Center has concluded. I also understand that violation of any applicable rule:

- Will immediately result in temporary or permanent termination of data system access;
- May give rise to criminal and/or civil penalties under Criminal Law Article §§ 7-203, 7-302 and 8-301 of the Annotated Code of Maryland, and 20 CFR Part 603, and other State and Federal laws;
- May result in disciplinary action as defined in State Personnel & Pensions Article § 11-104 of the Annotated Code of Maryland; and
- Other disciplinary actions as provided under applicable rules.

Printed Name: _____ Signature: _____ Date: _____

[4] Unless otherwise instructed, information approved for release from the system will be sent to the staff member by the Executive Director, or the director's designee.

# Policy for Conducting Criminal History Background Investigation

## Purpose

The purpose of this policy is to provide a standard for the use and application of Criminal History Background Investigations (CHBI) by the Maryland Longitudinal Data System Center (MLDS Center).

## Legal Authority

Pursuant to §§ 3-401 through 3-413 and 3-701 through 3-705 of the State Finance and Procurement Article, the Department of Budget and Management Office of Information Technology is required to develop an *Information Technology Security Policy and Standards (*ITSPS*)*. Specifically, section 8.5 of the ITSPS states:

> Security clearances are required for personnel as determined by the system sensitivity and data classification designation. Agencies will ensure that an appropriate background investigation (e.g., CJIS, State Police) has been completed on personnel as necessary. Agencies will maintain personnel clearance information on file.

In other words, the ITSPS requires agencies to ensure sufficient security clearance for employees who use systems that are deemed by the agency as sensitive.

The data system is deemed sensitive because the MLDS Center's authorizing statute discusses the need for the Center to provide data security and restrict access to the data to authorized staff of the Center. Md. Code, Ed. Art., §24-703. Section 24-704 also discusses the provisions for protecting privacy and security of the data to be housed by the MLDS Center, and tasks the Governing Board of the Center with developing a detailed data security and safeguarding plan to include standards for authorized access and authentication for authorized access.

## Background

The *Rules of Security Behavior* requires authorized staff and contractors of the MLDS Center to submit to all necessary background checks and receive authorization before having access to sensitive, confidential, or trademark specific information, materials, or equipment. These background checks are necessary to ensure that the MLDS Center is taking necessary and reasonable steps to protect the confidential student and workforce data contained within the Maryland Longitudinal Data System and to ensure compliance with all State and federal confidentiality, privacy and data security laws. The Maryland Longitudinal Data System Data Security and Safeguarding Plan (Version 2.0, December 13, 2013) contains two provisions relevant to background checks on staff, §2.3.4(b) and §3.2.5. Specifically, §3.2.5 provides that "The MLDS Center shall screen all employees and contractors before authorizing access to the MLDS, at a minimum a criminal background check will be performed."

## Applicability

The Data Security and Safeguarding Plan (DSSP) requires a criminal history background investigation on all employees and contractors of the MLDS Center, regardless of job classification.

## Policy

The Executive Director of the MLDS Center shall request a CHBI for all full-time, part-time, permanent, temporary and contract employees of the MLDS Center in accordance with the Data Security and Safeguarding Plan. The Executive Director shall request the CHBI after any such employee has accepted an offer of employment, but prior to any such employee accessing the Maryland Longitudinal Data System, in a period not to exceed sixty (60) days from commencement of employment with the MLDS Center.

If the CHBI indicates that the employee or contract employee has been convicted of a felony of any nature or any crime which qualifies as an infamous crime (including treason, felony, perjury, forgery, obstruction of justice and misdemeanors involving dishonesty) under Maryland law, whether felony or misdemeanor occurring within ten (10) years of the date of hire, the employee may be terminated or denied system access.

## Required Notification: Noncriminal Justice Applicant's Privacy Rights

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for employment or a license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below. All notices must be provided to you in writing. These obligations are pursuant to the Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, and Title 28 Code of Federal Regulations (CFR), 50.12, among other authorities.

- You must be provided an adequate written FBI Privacy Act Statement (dated 2013 or later) when you submit your fingerprints and associated personal information. This Privacy Act Statement must explain the authority for collecting your fingerprints and associated information and whether your fingerprints and associated information will be searched, shared, or retained.
- You must be advised in writing of the procedures for obtaining a change, correction, or update of your FBI criminal history record as set forth at 28 CFR 16.34.
- You must be provided the opportunity to complete or challenge the accuracy of the information in your FBI criminal history record (if you have such a record).
- If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the employment, license, or other benefit based on information in the FBI criminal history record.
- If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding this process may be obtained at https://www.fbi.gov/services/cjis/identity-history-summary-checks and https://www.edo.cjis.gov.
- If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI by submitting a request via https://www.edo.cjis.gov. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)
- You have the right to expect that officials receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime

Prevention and Privacy Compact Council.

## Privacy Act Statement

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety. (This privacy act statement is located on the back of the FD-258 fingerprint card. As of 03/03/2018.)

# Required Security and Privacy Training for MLDS Center Staff

The *Rules of Security Behavior* require staff members to agree to complete all required security training within 10 business days of:

1. Being hired or starting a staff appointment; or
2. The assignment of additional training requirements.

## Classes

1. Security Awareness Training – the MLDS Center CIO will assign staff either:
   - Monthly security awareness training provided by the Maryland Department of Information Technology;

     ***Or***
   - Department of Defense Cyber Awareness Challenge*

2. FERPA 101**– Staff will be required to create a login and password in order to take the course. The prompt for login will appear once you click on the course name. Please select the FERPA 101 course - *For Colleges and Universities* or *For Local Education Agencies* - that is most relevant to your area of work.

3. FERPA 201** – Staff will be required to create a login and password in order to take the course. The prompt for login will appear once you click on the course name.

4. Additional security and privacy training or information may be provided in writing or presented at staff meetings.

* https://public.cyber.mil/training/cyber-awareness-challenge/

** https://studentprivacy.ed.gov/content/online-training-modules

# Acknowledgement of Receipt and Review of Required Documents

Each MLDS staff member is provided* with a copy of the following documents to ensure the staff member is fully aware of security, privacy and data use limitations.

1. **Data Security and Safeguarding Plan** (DSSP). The DSSP identifies required policies and procedures that govern all aspects of the security of the MLDS, including IT systems, user access, data governance, and staff conduct. Each staff member plays a critical role in the security of the system and therefore an understanding of the DSSP by each staff member is required.

2. **Data Sharing Agreements** with partner agencies:
    a. Maryland State Department of Education;
    b. Maryland Department of Labor;
    c. Maryland Higher Education Commission;
    d. Motor Vehicle Administration;
    e. Maryland Department of Juvenile Services; and
    f. Maryland Department of Human Services.

3. **Memoranda of Understanding - MLDS Center and the University of Maryland, Baltimore (2021-2023);**

I,_____, staff of the MLDS Center, acknowledge that I have received and reviewed the above referenced documents.

_____

Signature (Date)

*All referenced documents are posted to the MLDS Center Website.
https://mldscenter.maryland.gov/internal/NewHiredocs.html

# Maryland Department of Labor - Confidentiality Certification Form (Appendix B)

I understand that I will or may be exposed to certain confidential information from records maintained by the Maryland Department of Labor, Division of Unemployment Insurance (Labor), which have been released to my employer pursuant to an Agreement and/or Memorandum of Understanding ("Agreement"). Such information, hereinafter referred to as "Confidential UI Data" may include, but is not limited to: names; addresses; social security numbers; wages; employment data; and unemployment insurance ("UI") benefit information which are private and confidential and may not be disclosed to others. I acknowledge and agree to abide by the following standards for the receipt and handling of Confidential UI Data:

A. I shall not disclose my username (if applicable), password (if applicable), or any other information needed to access Confidential UI Data maintained by Labor to any party nor shall I give any other individual access to this information.

B. If I should become aware that any other individual, other than an authorized employee, agent, contractor, or subcontractor of my employer, may have obtained or has obtained access to my username, password or other information needed to access records maintained by Labor, I shall immediately notify Labor.

C. I will not share with anyone any other information regarding access to Confidential UI Data records maintained by Labor unless I am specifically authorized by Labor.

D. I will not request access to any social security numbers or wage data unless such access is necessary for the performance of my official duties.

E. I will not disclose any Confidential UI Data to any parties who are not authorized to receive such information (including but not limited to relatives, friends, etc.) except in the form of reports containing only aggregate statistical information compiled in such a manner that it cannot be used to identify the individual(s) involved.

F. I shall retain Confidential UI Data only for that period of time necessary to perform my duties or to comply with the purposes set forth in the Agreement. Thereafter, I shall either arrange for the retention of such information consistent with federal record retention requirements or delete or destroy such data.

G. I have either been trained in the proper use and handling of Confidential UI Data or I have received written standards and instructions in the handling of such data. I shall comply with all confidentiality safeguards contained in such training, written standards, or instructions, including but not limited to: a) protecting the confidentiality of my username and password; b) securing computer equipment, disks, and offices in which wage record data may be kept; and c) following procedures for the timely disposal, destruction or deletion of Confidential UI Data.

H. I understand that if I violate any of the confidentiality provisions set forth in the written standards, training, and/or instructions I have received, my user privileges may be immediately suspended or terminated. I further acknowledge that applicable state law may provide that any individual who discloses Confidential UI Data in violation of state law or regulation may be subject to a fine and/or a period of imprisonment and dismissal from public service. I have been instructed that if I should violate the provisions of the law, I may receive one or more of these penalties.

I. Should I have any questions concerning the handling or disclosure of Confidential UI Data, I shall immediately notify Labor and be guided by advice given by Labor regarding the handling of Confidential UI Data.

Employee Signature:_____ Date: _____

Employee Name (printed): _____

# User Access Form

**User Profile**

| IT/Admin | Job Title | Reason for Access/Project | |
|---|---|---|---|
| MLDS Center PIN Employee | | | |
| Contractor | | | |
| Other | | | |
| **Research/Reporting** | **Affiliation** | **Role (PI, student*, etc.)** | **Project (if applicable)** |
| MLDS Center Research Branch Member | | | |
| External Researcher | | | |
| Agency Partner | | | |
| Other | | | |

**Students must also provide the name of their supervising faculty member*

Please indicate the type of access you are requesting. The final determination about the type of access will be made by the MLDS Center CIO.

| X | Access Type | Description |
|---|---|---|
| | Information Technology Staff | Assigned by CIO |
| | Administrative or Legal | File access |
| | Researcher Full | Access to ODS |
| | Researcher Partial | Access to designated ODS tables |
| | Researcher Restricted | Access to an analytic data set developed by MLDS Center data Analyst |
| | View Only | No system access, but allowed to view pre-suppressed materials through a screen share |

**Connection**

Please list each computer and network that you will use to connect to the MLDS (provide one line for each computer and network below. You may only use the computer(s) and network(s) indicated on this form. An exception may only be granted by the MLDS Center CIO.

| **Computer (Personal or Work – indicate name institution)** | **I confirm that the computer complies with anti-virus requirements (sign below)** |
|---|---|
| | |
| | |

| **Network provider (name of home ISP or work)** | **I confirm that the network is encrypted and password protected (sign below)** |
|---|---|
| | |
| | |

**Requested Access Duration***

| **Begin Access** | **End Access** |
|---|---|
| | |

**MLDS Center will make the final determination on when system access may begin and when it will end.*

I understand that I must remain in compliance with the *Rules of Security Behavior* and training and requirements and may only access the MLDS as indicated above.

Requester's Signature _____ Date _____

# Authorization

1. **Administrative Review** - The Requester has completed all of the following requirements:
   - Rules of Security Behavior
   - Acknowledgement of Receipt and Review of Required Documents
   - The Requester has had a Criminal History Background Check and does not have a history that would prohibit him/her from obtaining system access.
   - The Requester has completed all required security training.

_____

Executive Associate Date

2. **Supervisor Review** - The stated business needs are accurate and the requested access duration is necessary for the requester to carry out the assigned duties.

_____

Supervisor or Branch Director Date

3. **System Administrator Access Determination** – List all of the functional user groups and access privilege necessary for this user.

| |
|---|
| |

Assigned Access Duration: _____ (Beginning) to _____ (Ending)

The assigned user groups and access privileges and the access duration represent the least privileged access necessary for this user to complete the business needs stated above.

_____

System Administrator Date

## Final Approval

Since this applicant has met all of the requirements laid out in this document, is a researcher or information technology expert or technician, and is necessary to carry out the mission of the Center, I authorize the applicant to be staff of the Center and to have access to the system as approved by the System Administrator.

_____ _____

Executive Director Date