MLDS Center

Maryland Longitudinal Data System

Address 550 West Baltimore Street
Baltimore, MD 21201
Phone 410-706-2085
Email mlds.center@maryland.gov
Website www.MLDSCenter.org

Memorandum

TO: MLDS Governing Board

FROM: Tejal Cherry, Chief Information Officer

DATE: December 8, 2025

SUBJECT: MLDS Data Security and Safeguarding Plan (DSSP)

Purpose
In accordance with state law (see Education Article § 24-704(g)(6)(iii), Annotated Code of Maryland) the MLDS Center Governing Board is required to establish and maintain a comprehensive *Data Security and Safeguarding Plan* (DSSP) prior to incorporating any individual data into the MLDS. The original DSSP developed by the Governing Board has been in place since the initial implementation and development of the MLDS. Since that time there have been a lot of changes to the system and its operations and management. One important change is the role the Department of Information Technology plays in managing the system's security profile. In addition, Center staff have implemented security operations that are not reflected in the DSSP. Accordingly, staff, with the help of a security systems technical writer and input from DoIT, revised the DSSP.

A copy of the revised DSSP is attached herein. ***Please note that the DSSP is a confidential document and should not be distributed.***

Background
The revision process included a comprehensive review of:

1. The DSSP and related documents,
2. The role of DoIT's enterprise system management;
3. The Center's current system security procedures and operations; and
4. The State of Maryland Information Technology Security Manual.

The new DSSP is designed to align with the security and privacy control families outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 and is consistent with the Maryland Department of Information Technology (DoIT) Information Technology Security Manual v1.2. It incorporates appropriate technical, administrative and physical safeguards to protect personally identifiable information (PII) and other sensitive data in accordance with state regulations and applicable federal standards. Full adherence to this plan supports a secure data environment and promotes trust in the governance of longitudinal data assets.

The DSSP was presented to the CyberSecurity Subcommittee on November 5, 2025 by Ms. Tejal Cherry, MLDS Center CIO. Ms. Cherry provided an in depth review of the revised plan. The Subcommittee was supportive of the revised DSSP.

Summary
The MLDS Center adheres to the following principles:

1. Security First: Data security shall guide all decisions and practices related to system design, maintenance, and use. Data retrieval shall be performed in accordance with documented procedures and must align with the requirements of this DSSP.
2. Privacy Compliance: Strict adherence to applicable privacy laws and policies shall govern the handling of student and workforce data within the MLDS.
3. Data Relevance: Data collected is vetted and approved through a defined data inventory and data governance process.
4. Restricted Access: Access to student and workforce data shall be strictly limited to authorized staff of the Center. Access to PII data is restricted to members of the ETL team and system administrator, whose responsibility it is to perform data matching. Research and reporting does not require access to PII data within the MDM environment.
5. Alignment with MLDS Center Mission: The purpose of the MLDSC is to generate timely and accurate information about student performance that can be used to improve the State's education system and guide decision makers at all levels.

Priorities

To ensure compliance with state law, the DSSP requirements are consistent with the priorities stated in the State of Maryland Department of Information Technology (DoIT) Information Technology Security Manual, including:

1. A detailed user access authorization process;
2. Privacy compliance standards;
3. Privacy and security audits; and
4. Incident management and disaster recovery procedures.

Action

We request the Governing Board approve the revised version of the DSSP.