MARYLAND STATE LONGITUDINAL DATA SYSTEM (MLDS)

DATA SECURITY AND SAFEGUARDING PLAN

VERSION 2.0

December 13, 2013

Table of Contents

1 Introduction

1.1 Purpose

The Maryland Longitudinal Data System (MLDS) Data Security and Safeguard Plan identifies required policies and procedures to address safeguard requirements for the:

- Maryland Longitudinal Data System (MLDS);
- MLDS Center and the Data Center at which the MLDS is housed; and the,
- MLDS data governance process.

1.2 Background

The Maryland Education Article §24-702 establishes the MLDS, which is "… a statewide data system that contains individual-level student data and workforce data from all levels of education and the State's workforce." Section 24-704 outlines the minimally acceptable data security and safeguard requirements that are to be met prior to the system going operational and populated with live (versus non-sensitive test) data. Section 24-703 states that there will be a MLDS Center, which is an independent unit within the State government. The Center is responsible for conducting the business processes that are required "… to examine student progress and outcomes over time, including preparation for postsecondary education and the workforce." (§24-702 (b)(2)).

Researchers may use student or workforce data which has undergone anonymization or de-identification to conduct research. Section 9 contains definitions of these terms. Only employees of the MLDS Data Center are authorized to access the MLDS and to conduct this research.

The Data Security and Safeguarding Plan will be reviewed periodically and the resulting revisions will be documented in Section 10, Record of Revisions.

1.3 Data Security and Safeguard Policy Priorities

To ensure compliance with the intent of the legislation, data security and safeguard requirements are provided and are in accordance with the priorities stated in:

1. Authorized access and authentication for authorized access;
2. Privacy compliance standards;
3. Privacy and security audits;
4. Breach notification and procedures; and,
5. Data retention and disposition polices.

Additional policies and procedures will be developed as needed. Security and safeguard requirements address and are consistent with the requirements and guidance found in paragraph 1.6, References. The Governing Board and Center Executive Director are responsible for

managing risks to the MLDS project. This plan shall be reviewed on an annual basis to evaluate the effectiveness of the controls in managing MLDS risks.

1.4 Document Organization

The MLDS Data Security and Safeguards Program shall adopt a hierarchical approach to the development and implementation of policy and procedures, developing policy first and then procedures. The policy statements will reflect content from sources within paragraph 1.6. When possible, federal and publicly available sources will be used as the basis for the procedures and tailored to the specific needs of the MLDS Center and the MLDS.

The MLDS Data Security and Safeguard Plan is a living document and will contain the top level policy statements from which procedures will be developed. Appendices may be added as new policy requirements become known.

Section 2 describes the data governance process and associated security controls.

Sections 3 through 8 describe the planned data security and safeguard controls for the MLDS Center and the MLDS.

Section 9 contains terms and terminology relevant to the MLDS.

Section 10 contains Revision History.

Section 11 contains supporting documentation.

1.5 Roles and Responsibilities

The Maryland Longitudinal Data System Center shall:

- Oversee and maintain the warehouse of the MLDS data sets,
- Ensure routine and ongoing compliance with the federal Family Educational Rights and Privacy Act (FERPA), the federal Privacy Act, the federal Workforce Investment Act (WIA), the U.S. Department of Labor's rules governing confidentiality of State Unemployment Compensation information, and other relevant privacy laws, regulations, and policies,
- Provide data security, including the capacity for audit trails, and
- Perform regular audits for compliance with data privacy and security standards.

The Executive Director of the MLDS Center shall ensure the implementation of the requirements found within this Data Security and Safeguarding Plan.

1.6 References

Family Educational Rights and Privacy Act (FERPA) Legislation Act of 1974 (20 U.S.C. § 1232g; 34 CFR Part 99), FERPA Regulations. Retrieved from http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf

Federal Register, Family Educational Rights and Privacy (2011). Notice of Proposed Rule. Retrieved from https://www.federalregister.gov/articles/2011/04/08/2011-8205/family-educational-rights-and-privacy#p-3

Federal Register, 20 CFR 603 - FEDERAL-STATE UNEMPLOYMENT COMPENSATION (UC) PROGRAM; CONFIDENTIALITY AND DISCLOSURE OF STATE UC INFORMATION https://www.federalregister.gov/select-citation/2006/09/27/20-CFR-603

Maryland State Information Technology Security Policy and Standards. Retrieved from http://doit.maryland.gov/support/pages/securitypolicies.aspx

U.S. Department of Commerce, National Institute of Standards and Technology (2009). *Special Publication (SP) 800-53, Revision 3: Recommended Security Controls for Federal Information Systems and Organizations*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

U.S. Department of Commerce, National Institute of Standards and Technology (2012). *Special Publication (SP) 800-53, Initial Public Draft: Recommended Security Controls for Federal Information Systems and Organizations*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

U.S. Department of Commerce, National Institute of Standards and Technology (2010). *Special Publication (SP) 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

U.S. Department of Commerce, National Institute of Standards and Technology (2010). *Special Publication (SP) 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

U.S. Department of Education, Privacy Technical Assistance Center (2011). *Data Governance and Stewardship Checklist.* Retrieved from http://www2.ed.gov/policy/gen/guid/ptac/pdf/issue-brief-data-governance-and-stewardship.pdf

U.S. Department of Education, Privacy Technical Assistance Center (2011). *Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records*. Retrieved from http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601

U.S. Department of Education, Privacy Technical Assistance Center (2011*). Data Stewardship: Managing Personally Identifiable Information in Electronic Student Educations Records.* Retrieved from http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602

U.S. Department of Education, Privacy Technical Assistance Center (2011). *Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting.* Retrieved from http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011603

1.7 Review History

During the drafting and ongoing maintenance of this *Data Security and Safeguarding Plan*, the following review and consultation from data security experts has taken place:

1. Initial preparation by an independent consultant with expertise in data security;
2. Review by the Privacy and Technical Assistance Center of the U.S. Department of Education;
3. Review by the Maryland Department of Information Technology (DoIT);
4. Review and approval by the Chief Information Officer and Assistant Attorney General for the Maryland State Department of Education, Maryland Higher Education Commission, and Department of Labor, Licensing, and Regulation;
5. Review by information technology specialists at the University System of Maryland; and
6. Second review by the DoIT against relevant NIST security standards.

2 Data Governance Security

2.1 Goals and Objectives

This section describes how the MLDS Center will perform decision making regarding data retrieval, sharing, and use.

2.2 Data Governance Guiding Principles

The MLDS Center shall adhere to the following guiding principles.

a. **Security**. Data security shall inform all decisions and practices relating to system design, maintenance, and use.
   i. Anyone handling student or workforce data or with ability to access the information should be trained annually in the handling of sensitive information and in their responsibilities to monitor, detect, and report any security violations.
   ii. Data retrieval will be conducted at the times and in the manner specified in documented procedures and consistent with this *Data Security and Safeguarding Plan*.

b. **Privacy**. Privacy laws and policies shall be strictly applied to student and workforce data in the MLDS.

c. **Relevance**. Student and workforce data in the MLDS must be relevant and necessary for meeting the MLDS Center's purpose and mission.
   i. To ensure that all data is relevant and necessary, annual reviews of MLDS data will be conducted.
   ii. Reviews of data to determine relevance shall consider the functions and duties in Md. Ed. Art. §24-703(f), policy questions established by the Governing Board, and other requirements and projects assigned to the MLDS Center.

d. **Access.** Access to student and workforce data will be restricted to MLDS Center staff. In addition, student and workforce PII data will be further restricted to only those staff members who require access to manage the data matching and de-identification processes.

2.3 Roles and Data Protection Responsibilities

2.3.1 Executive Director, MLDS Center

The Executive Director shall oversee the functions and duties of the MLDS Center.

2.3.2 Data Governance Advisory Board

a. The Executive Director shall periodically convene a Data Governance Advisory Board to:
   - Set direction for data quality
   - Monitor data quality
   - Report status for quality-focused initiatives
   - Identify stakeholders, establish decision rights, clarify accountability
   - Ensure protection of sensitive data
   - Align initiatives
   - Enforce regulatory, contractual, architectural, and compliance requirements
   - Identify measures of success

b. The Data Governance Advisory Board shall consist of:
   - A data steward from DLLR;
   - A data steward from MSDE;
   - A data steward from MHEC; and
   - The associate directors from the MLDS Center.

2.3.3 Data Management Staff The following three staff employees have specific responsibilities for data management as indicated below.

a. Associate Director for IT and Data Management Branch
   a. Coordinate all functions necessary to securely implement and maintain the MLDS system.
   b. Hire appropriate staff to fulfill the following functions.

b. Database Engineer
   i. Monitor data quality;
   ii. Protect sensitive data, and student or workforce data;
   iii. Identify risk;
   iv. Coordinate with stakeholders;
   v. Ensure consistent data usage and data definitions;
   vi. Report on data-related tasks or projects;
   vii. Monitor data to determine when no longer used or needed;
   viii. Maintain data inventory and dictionary

c. Application and Security Manager
   i. Assess risk or other impact of adding or acquiring additional data from existing or new external source and document assessment results
   ii. Add or modify existing controls, if required
   iii. Update system security plan;
   iv. Monitors the controls within this plan that are specific to privacy;
   v. Investigates and reports data breaches; and
   vi. Proves compliance with privacy and data governance policies.
   vii. Setup and maintain user accounts
   viii. Maintain the system, ensuring patches and settings are in alignment with this plan and relevant procedurs;
   ix. Troubleshoot problems and arrange for repairs
   x. Monitor system performance
   xi. Install software
   xii. Create backup and be able to recover the system

2.3.4 Staff

a. MLDS Center Staff shall abide by all Center policies governing privacy and security and ensure that these policies are consistently maintained.
b. The Executive Director shall ensure that each individual authorized as staff of the MLDS has completed the following:
   - Non-disclosure agreement;
   - Access Request Form;
   - When necessary, security background check; and
   - Written acknowledgement of receipt and review of this *Data Security and Safeguarding Plan*.

c. From time to time, staff, in addition to those individuals directly employed by the Center, may be needed to address the technical and research needs of the MLDS Center. In those instances, additional staff may be appointed by the Executive Director.

2.4 Data Quality and Integrity

The MLDS Center shall:

a. Confirm to the greatest extent practicable upon retrieval of student or workforce data , the accuracy, relevance, timeliness, and completeness of that information;
b. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information; and,
c. Document processes to ensure the integrity of student or workforce data through existing security controls.

2.5 Access Agreements – Data Sharing

The MLDS Center shall:

a. Ensure that individuals requiring access to MLDS (such are repair persons or employees) sign appropriate access agreements prior to being granted access; and
b. Review/update the access agreements annually or when major changes have occurred.

3 Authorized Access & Authentication Standard

3.1 Access Control Policy and Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented authorized access and authentication procedure that will limit access to the MLDS to authorized users. The procedure:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Facilitates the implementation of the authorized access and authentication policies and associated authorized access and authentication controls.

3.2 Account Management

a. The MLDS Center shall manage information system accounts, including:
    1) Identifying account types;
    2) Group or shared IDs are prohibited unless they are documented as "Functional IDs". Functional IDs are user accounts associated with a group or role that may be used by multiple individuals (e.g., Emergency Problem/Fix IDs) or that are associated with a particular production job process;
    3) Identifying authorized users of the information system and specifying access privileges (see paragraph 3.3 below). Direct access to data in the Maryland Longitudinal Data System shall be restricted to authorized staff of the Center;
    4) Ensuring each user has a unique user ID;
    5) Requiring approval from appropriate officials for requests to establish accounts;
    6) Establishing, activating, modifying, disabling, and removing accounts in a timely manner;
    7) Archiving inactive or terminated use accounts;
    8) Specifically authorizing and monitoring the use of temporary accounts;
    9) Notifying account managers when temporary accounts are no longer required and when MLDS users are terminated, transferred, or MLDS usage or need-to know/need-to-share changes;
    10) Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
    11) Validating system users who request reinstatement of user account privileges suspended or revoked by the MLDS;
    12) Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and

13) Reviewing accounts: (i) User accounts shall be reviewed quarterly, at a minimum; and (ii) Privileged accounts (e.g., system administrators, accounts with elevated access privileges) shall be reviewed semi-annually, at a minimum.

b. The MLDS Center shall employ automated mechanisms to support the management of MLDS accounts.
c. The MLDS shall, through automation:
    1) Terminate temporary and emergency accounts within 72 hours;
    2) Disable accounts which have been inactive after 90 days; and,
    3) Audit account creation, modification, disabling, and termination actions and notify, as required, appropriate individuals.

3.3 Account Types and Access Privileges

The MLDS Center shall define and manage account types and access privileges for the MLDS to include access to virtual machines or servers, the local area network and components, and the database.

3.4 Access Enforcement

The MLDS Center and the MLDS shall enforce approved authorizations for logical access to the system in accordance with applicable procedures.

3.5 Information Flow Enforcement

The MLDS shall enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable MLDS policy or procedures.

3.6 Separation of Duties

The MLDS Center shall:

a. Separate duties of individuals, to prevent harmful activity without collusion;
b. Document separation of duties; and,
c. Implement separation of duties through assigned MLDS access authorizations.

3.7 Least Privileged

The MLDS Center shall:

a. Employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with the MLDS mission and functions;
b. Explicitly authorize access to security functions (deployed in hardware, software, and firmware) and security-relevant information; and,
c. Require that users of MLDS accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other

system functions, and if feasible, audit any use of privileged accounts, or roles, for such functions.

3.8 Unsuccessful Login Attempts

The MLDS shall lock an account after four (4) consecutive unsuccessful access attempts within a fifteen (15) minute period by automatically locking that account for a minimum of 60 minutes. While the 60 minutes password count will be reset after 60 minutes, the account will remain locked until unlocked by an administrator.

3.9 System Use Notification

The MLDS shall:

a. Display an approved system use notification message or banner that identifies the system as the property of the Maryland State Government, before granting access to the system that provides privacy and security notices consistent with state and federal and state laws, directives, polices, or guidance. The text shall read:

> "Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of Maryland."

b. Maintain the system-use notification message/warning banner on the screen until the user takes explicit actions to log on to or further access the MLDS.

3.10 Concurrent Session Lock

The MLDS shall limit the number of interactive sessions as follows:

a. One (1) session for non-privileged authorized accounts (e.g., users);
b. Three (3) sessions are allowed for privileged accounts (e.g., system administrators, accounts with elevated access privileges); and,
c. Accounts used for automated processing by applications (e.g., database, service accounts) are not subject to the concurrent session limits above.

3.11 Session Lock

The MLDS shall implement a session lock at the operating system level that:

a. Initiates a session lock (e.g., screensaver) after 15 minutes of inactivity or upon receiving a request from the user (e.g., lock computer); and,
b. Prevents further access (e.g., password protected) to the system until the user reestablishes access using established identification and authentication procedures.

3.12 Remote Access

The MLDS Center shall:

a. Document allowed methods of remote access to the MLDS;
b. Establish usage restrictions and implementation guidance for each allowed remote access method;
c. Monitor for unauthorized remote access to the MLDS;
d. Authorize remote access to the MLDS prior to connection;
e. Enforce requirements for remote connections to the MLDS;
f. Employ automate mechanisms to facilitate the monitoring and control of remote access methods;
g. Use cryptography to protect the confidentiality and integrity of remote access sessions. Encrypted remote access circuits shall comply with the encryption standards as outlined in FIPS 140-2;
h. Route remote accesses to the MLDS through a limited number of managed access control points;
i. Restrict the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs only, and only when an operational emergency exists, such as a breach or potential breach of the MLDS's security;
j. Continuously monitor for unauthorized remote connections to the MLDS and take appropriate action if an unauthorized connection is discovered;
k. Ensure that remote sessions for accessing security functions and security-relevant information employ additional security measures and are audited; and,
l. Disable networking protocols within the MLDS deemed to be non-secure, except for explicitly identified components in support of specific operational requirements.

3.13 Wireless Access

a. The MLDS Center shall:
    1) Establish usage restrictions and implementation guidance for wireless access in accordance with the Maryland Department of Information Technology Information Security Policy, version 3.0, Appendix D;
    2) Monitor for unauthorized wireless access to the MLDS;
    3) Authorize wireless access to the MLDS prior to connection;
    4) Enforce requirements for wireless connections to the MLDS; and,
    5) Monitor for unauthorized wireless connections to the MLDS, including scanning for unauthorized wireless access points, at least semi-annually, and take appropriate action if an unauthorized connection is discovered.
b. The MLDS shall protect wireless access to the system using authentication and encryption.

3.14 Access control for Mobile Devices

a. The MLDS Center shall:
   1) Establish usage restrictions and implementation guidance for MLDS Center laptop computers and other Portable Electronic Devices (PEDs) (e.g., PDAs, cellular phones);
   2) Document, monitor, and control access of laptop computers and other Portable Electronic Devices (e.g., PDAs, cellular phones) to the MLDS;
   3) Monitor for unauthorized connections of mobile devices to the MLDS;
   4) Enforce requirements for the connection of mobile devices to the MLDS;
   5) Disable MLDS functionality that provides the capability for automatic execution of code on removable media without user direction;
   6) Issue specially configured mobile devices to individuals traveling to locations that the MLDS Center deems to be of significant risk in accordance with internal policies and procedures;
   7) Apply approved inspection and preventative measures to mobile devices returning from locations that are deemed to be of significant risk in accordance with the State of Maryland policies and procedures;
   8) Restrict the use of writable, removable media within the MLDS. The use of removable media in the MLDS shall be prohibited when the owner of the media cannot be identified; and,
   9) Prohibit the use of privately owned portable electronic devices or removable media to process, store, or transmit MLDS information.

   Note: Examples of removable media include: USB memory sticks, external hard disk drives and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Personally owned equipment shall include all systems, devices, software, and media owned by an individual, but shall not include systems, devices, software, media that the MLDS Center has on a payment schedule or is leasing, or contractor-furnished IT equipment. Personally owned equipment, software and media (e.g., thumb drives, etc.) shall not be used to process, access, or store sensitive information, nor shall such equipment be connected to the MLDS directly or via a Virtual Private Network (VPN).

3.15 Use of State Agency and State Institution Data Systems

a. The MLDS Center shall establish terms and conditions, consistent with any trust relationships established with the state agencies and institutions providing data to the MLDS, allowing authorized individuals to access the MLDS for the purpose of transmitting student and workforce data.
b. The MLDS Center shall permit authorized individuals to access the MLDS to process, store, or transmit data only when the MLDS Center:

1) Can verify the implementation of required security controls on the state agency and state institution as specified in the MLDS Center's information security plan; or
2) Has an approved MLDS connection or processing agreement with the state agency or state institution system providing data to the MLDS.

3.16 User-Based Collaboration & Information Sharing

The MLDS Center shall define circumstances for using collaborative methods or tools by authorized MLDS users when these users are sharing information or data with other authorized MLDS users.

3.17 Identification & Authentication Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented identification and authentication procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among MLDS Center, and compliance; and
b. Facilitates the implementation of identification and authentication controls.

3.18 Identification and Authentication (Authorized Users)

The MLDS shall:

a. Uniquely identify and authenticate authorized users (or processes acting on behalf of authorized users);
b. Use multifactor authentication for network access to privileged accounts; and,
c. Use multifactor authentication for local access to privileged accounts.

3.19 Device-to-Device Identification and Authentication

a. The MLDS shall:
    1) Uniquely identify and authenticate devices before establishing a connection.
    2) Authenticate devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based. NOTE: Remote network connection is any connection with a device communicating through an external network (e.g., the Internet); and,
    3) Authenticate devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

b. The MLDS Center shall standardize, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.

3.20 Identifier Management

a. The MLDS Center shall manage MLDS identifiers for authorized users and devices by:

1) Receiving authorization from a designated MLDS Center official to assign a user or device identifier;
2) Selecting an identifier that uniquely identifies an individual or device;
3) Assigning the user identifier to the intended party or the device identifier to the intended device;
4) Preventing reuse of user or device identifiers;
5) Prohibiting the use of MLDS account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address);
6) Requiring that registration to receive a user ID and password include authorization by a supervisor, and be done in person before a designated registration authority; and,
7) Managing user identifiers by uniquely identifying the user.

b. The MLDS shall dynamically manage identifiers, attributes, and associated access authorizations.

3.21 Authenticator Management

a. The MLDS Center shall manage MLDS authenticators for authorized users and devices by:
   1) Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
   2) Establishing initial authenticator content for authenticators defined by the MLDS Center;
   3) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
   4) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
   5) Changing default content of authenticators upon MLDS installation;
   6) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
   7) Changing/refreshing authenticators ; and,
   8) Protecting authenticator content from unauthorized disclosure and modification; and
   9) Requiring users to take, and having devices implement, specific measures to safeguard authenticators.
      NOTE: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration.

b. The MLDS, for password-based authentication, shall:
   1) Enforce minimum password construction, usage and change requirements as follows:

a) The password must not be the same as the user id;
b) Passwords must never be displayed on the screen;
c) Change temporary passwords at the first logon;
d) Passwords must be a minimum of eight (8) characters and consist of mixed alphabetic, numeric, and special characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters;
e) Passwords must not contain leading or trailing blanks;
f) Force change of user passwords every 90 days;
g) Password reuse must be prohibited by not allowing the last 20 passwords to be reused with a minimum password age of at least 48 hours;
h) Where possible, users should be prohibited from only changing/or adding one (1) character to their previous password (i.e., users should be prohibited from using passwords that are similar to their previous password);
i) State issued login credentials (username & password) shall not to be used for ancillary 3rd party services (online Web accounts, e-mail, e-commerce, etc.)
j) Passwords older than the expiry date must be changed before any other system activity is performed;
k) User ids associated with a password must be disabled or locked after 60 days of inactivity; and,
l) When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established.

2) Encrypt passwords in storage and in transmission.

c. The MLDS, for PKI-based authentication (if PKI is in use), shall:
1) Validate certificates by constructing a certification path with status information to an accepted trust anchor;
2) Enforce authorized access to the corresponding private key; and
3) Map the authenticated identity to the user account.

d. The MLDS Center shall require that the registration process to receive authenticators be carried out in person before a designated registration authority with authorization by a designated MLDS Center official (e.g., a supervisor).

3.22 Authenticator Feedback

The MLDS shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

3.23 Cryptographic Module Authentication

The MLDS shall use mechanisms for authentication to a cryptographic module that meets the requirements of Federal Information Processing Standard (FIPS) Pub 140-2.

3.24 Personnel Categorization

The MLDS Center shall:

a. Assign a sensitivity/risk level designation for all positions (employee and contractor);
b. Establish screening criteria for individuals filling these positions; and
c. Review and revise position sensitivity/risk level designations at a minimum annually or when position descriptions are rewritten.

3.25 Personnel Screening

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. All MLDS Center employees shall sign a confidentiality agreement upon accepting employment with the MLDS Center.

3.26 Personnel Termination

a. The MLDS Center shall require departing employees to return all forms of media used to gain system access to MLDS Center media, personal electronic devices, keys, identification (ID) cards, proxy cards, and any other MLDS Center property on their last workday.
b. Unfriendly termination (fired or resignation) involves the removal of an employee under involuntary or adverse conditions (e.g., engaging in unauthorized activities). Given the potential for adverse consequences during unfriendly termination, the MLDS Center shall at a minimum, include the following in unfriendly termination procedures (Note: Unfriendly termination (fired or resignation) involves the removal of an employee under involuntary or adverse conditions (e.g., engaging in unauthorized activities) and may result in adverse consequences):
    1) Immediate termination of MLDS access;
    2) Retrieval of MLDS Center property (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes);
    3) Briefing on the continuing responsibilities for confidentiality and privacy; and
    4) Retaining access to MLDS Center information and the MLDS formerly controlled by the terminated individual.
c. The MLDS Center shall conduct an exit interview with a departing employee, after an employee is notified of termination, but before their departure, to ensure all out processing/exit actions are completed and all MLDS Center property and equipment is returned.

3.27 Personnel Transfer

The MLDS Center shall implement and maintain procedures to ensure appropriate system accesses are revoked for employees/contractors who leave the MLDS Center, are reassigned to other duties, on extended leave, or are under disciplinary actions.

a. Logical and physical access authorizations to the MLDS and MLDS Center facilities shall be reviewed when personnel are reassigned or transferred to other positions within the MLDS Center.

b. Transfer or reassignment actions shall be initiated within five (5) business days of the formal transfer action.

3.28 Contract and Service Providers

a. The MLDS Center shall:
    1) Establish personnel security requirements including security roles and responsibilities for contractor or service providers (for example, Data Center contractor or service employees, hosting center contractor or service employees) ;
    2) Require contractors and service providers to comply with personnel security policies and procedures of the organization (for example, Data Center contractor or service employees, hosting center contractor or service employees);
    3) Document personnel security requirements; and
    4) Monitor provider compliance.
b. The MLDS Center shall require contractor and service providers to notify the Information Security Officer of the MLDS Center of any personnel transfers or terminations of any contractor or service employees working at any MLDS Center facilities with credentials, badges, or MLDS privileges within 24 hours.

3.29 Personnel Sanctions

The MLDS Center shall employ a formal sanctions process, as set forth in relevant state laws, for personnel failing to comply with established information security policies and procedures.

4 Privacy Compliance Standard

4.1 Privacy Program

The MLDS Center shall:

a. Assign an employee as the Privacy Officer accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the retrieval, use, maintenance, sharing, and disposal of student or workforce data.
b. Develop, disseminate, review, and update annually a formal, documented privacy compliance procedure that:
    1) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2) Facilitates the implementation of the privacy compliance policy and associated privacy controls
c. Monitor federal and state privacy laws and policy for changes that affect the privacy program; and,
d. Allocate budget and staffing resources to implement and operate the MLDS privacy program.

4.2 Privacy Impact and Risk Assessment

The MLDS Center shall:

a. Establish a privacy risk assessment process that assesses privacy risk to individuals resulting from the retrieval, sharing, storing, transmitting, and use of student or workforce data; and,
b. Conduct a Privacy Impact Assessment (PIA) for the MLDS in accordance with applicable state law and federal privacy laws.

4.3 Privacy Requirements for Contractors and Service Providers

The MLDS Center shall:

a. Establish privacy roles and responsibilities for contractors and service providers;
b. Require any contractors or service providers who may require temporary access, for purpose of repairs or emergencies, to the MLDS to sign a confidentiality agreement; and
c. Include privacy requirements in MLDS Center contracts and other acquisition-related documents.

4.4 Privacy Awareness

The MLDS Center shall:

a. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
b. Administer basic privacy training at least annually and targeted, role-based privacy training for personnel having responsibility for student or workforce data or for activities that use this data, at least annually; and
c. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually.

4.5 Privacy Notice

The MLDS Center shall provide a privacy notice that reflects the MLDS legislative requirements:

a. Direct access to data in the Maryland Longitudinal Data System shall be restricted to authorized staff of the Center.
b. The Center may only use de-identified data in the analysis, research, and reporting conducted by the Center.
c. The Center may only use aggregate data in the release of data in reports and in response to data requests.
d. 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.
e. 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.

4.6 Dissemination of Privacy Program Information

The MLDS Center shall:

a. Ensure that the public has access to information about its privacy activities and is able to communicate with its Privacy Officer; and
b. Ensure that its privacy practices are publicly available through organizational websites or otherwise.

4.7 Use Limitation of Student or Workforce Data

a. Student or workforce data is a specific type of sensitive information that the MLDS shall receive from sources, such as the Maryland Department of Labor, Licensing, and Regulation, State Department of Education and the Maryland Higher Education Commission.
b. The MLDS Center shall use student or workforce data internally only for the authorized purpose(s) as identified in the legislative language (see paragraph 4.5 above);
c. All MLDS employees shall be responsible for protecting any student and workforce data that they may have in their possession, whether the student and workforce data is in paper form or in MLDS-owned computer equipment and the MLDS.

d. Student or workforce data shall only be viewed by those authorized employees within the MLDS Center as having a "need to know" or requires access to the information, in the performance of their duties.
e. Sensitive information, such as user accounts and passwords, and student or workforce data that is stored or transmitted by computer equipment (such as laptops and memory storage devices) shall be encrypted.
f. Sensitive Information, such as such as user accounts and passwords, student or workforce data shall not be posted to internal or external websites.
g. No information containing sensitive or student or workforce data shall be placed into an employee's calendar (e.g., Outlook, etc.).

4.8 Inventory of Student or Workforce Data

The MLDS Center shall:

a. Identify the student or workforce data that are relevant and necessary to accomplish the legally authorized purpose of the data retrieval;
b. Limit the retrieval and retention of the student or workforce data to the minimum elements identified for the purposes
c. Conduct an initial evaluation of student or workforce data holdings and establish and follow a schedule for regularly reviewing those holdings at least semi-annually to ensure that the student or workforce data continues to be necessary to accomplish the legally authorized purpose for which it was collected;
d. Establish, maintain, and update an inventory that contains a listing of all MLDS subsystems identified as retrieving, using, or maintaining student or workforce data; and
e. Provide each update of the student or workforce data inventory to the Center Executive Director or information security official to support the establishment of information security requirements.

4.9 Complaint Management

The MLDS Center shall:

a. Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.
b. Respond to complaints, concerns, or questions from individuals within 30 business days.

4.10 Privacy Monitoring

The MLDS Center shall inspect semi-annually, and monitor as near real time as feasible, privacy controls and internal privacy procedures, to ensure effective implementation.

5 Auditing Standard for Privacy & Data Security

5.1 Auditing and Accountability Procedure

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented audit and accountability procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the audit and accountability policy and associated audit and accountability controls.

5.2 Auditable Events

The MLDS Center shall:

a. Determine, based on a risk assessment, that the MLDS is capable of auditing events as identified in the Maryland Department of Information Technology Information Security Policy, version 3.0, paragraph 7.1;
b. Coordinate the security audit function with other organizational entities (for example, Office of Legislative Audits, security consultants, Department of Information Technology, internal auditors) requiring audit related information to enhance mutual support and to help guide the selection of auditable events;
c. Provide a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;
d. Determine, based on current threat information and ongoing assessment of risk, what events are to be audited within the MLDS; and,
e. Review and update the list of identified auditable events at a minimum annually;
f. Include execution of privileged functions in the list of events to be audited by the MLDS. Note: In this context, privileged functions consist of commands executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

5.3 Content of Audit Records

The MLDS shall:

a. Produce audit records that contain sufficient information, at a minimum, to establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event; and,
b. Include detailed information in the audit records for audit events identified by type, location, or subject.

5.4 Audit Storage Capacity

The MLDS Center shall allocate audit record storage capacity based on the types of auditing to be performed and the audit processing requirements, and configure auditing to reduce the likelihood of such capacity being exceeded.

5.5 Response to Audit Processing Failure

The MLDS Center shall:

a. Alert the MLDS Information Security Officer in the event of an audit processing failure; and,
b. Implement additional actions in accordance with the MLDS Incident Response Procedures.

5.6 Audit Review Analysis, and Reporting

The MLDS Center shall:

a. Review and analyze MLDS audit records, on a routine basis (daily or weekly), for indications of inappropriate or unusual activity, and report findings to the MLDS Information Security Officer; and
b. Adjust the level of audit review, analysis, and reporting within the MLDS when there is a change in risk to MLDS operations, assets, individuals, based on law enforcement information, intelligence information, or other credible sources of information; and,
c. Integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

5.7 Audit Reduction and Report Generation

The MLDS shall provide:

a. An audit reduction and report generation capability, which does not alter original audit records. Note: An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements. and for after-the-fact investigations of security incidents; and,
b. The capability to automatically process audit records for events of interest based on selectable, event criteria as identified in applicable state policy.

5.8 Time Stamps

The MLDS shall:

a. Use internal system clocks to generate time stamps for audit records, and,
b. Synchronize internal information system clocks at a minimum quarterly.

5.9 Protection of Audit Information

The MLDS shall protect audit information and audit tools from unauthorized access, modification, and deletion.

5.10 Non-Repudiation

The MLDS shall achieve non-repudiation by protecting against an individual falsely denying having performed a particular action.

5.11 Audit Record Generation

The MLDS shall, in accordance with the Maryland Department of Information Technology Information Security Policy, version 3.0, and the MLDS Incident Response procedures:

a. Provide audit record generation capability for auditable events within the MLDS components;
b. Allow a designated organizational personnel to select which auditable events are to be audited by specific components of the system;
c. Generate audit records for auditable events; and,
d. Compile audit records into a system-wide (logical or physical) audit trail that is time-correlated.

5.12 Audit Record Retention

The MLDS Center shall retain audit records for the lesser of three (3) years or until the Office of Legislative Audits completes the audit of the entity to:

a. Enable the recreation of computer related accesses to both the operating system and to the application wherever confidential information is stored;
b. Provide support for after-the-fact investigations of security incidents; and
c. Meet regulatory and organizational information retention requirements.

6 Breach Notification Procedures

6.1 Breach Notification Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented breach notification procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the breach notification policy and associated breach notification controls.

6.2 Privacy Reporting

The Executive Director, MLDS Center, shall develop, disseminate, and update reports to the Governing Board at least semi-annually to demonstrate accountability with specific statutory and regulatory privacy program mandates.

6.3 Privacy Incident Response

The MLDS Center shall provide an organized and effective response to any privacy incident involving student or workforce data in accordance with the Incident Response Plan, as described in paragraph 8.6 of this document.

7 Data Retention and Disposition Standard

7.1 Data Retention and Disposition Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented data retention and disposition procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the data retention and disposition standard and associated data retention and disposition controls.

7.2 Data Retention and Disposal

The MLDS Center shall:

a. Retain student or workforce data in accordance with Maryland Education Article §24-702(c), which states, "The linkage of the student data and workforce data for the purpose of the MLDS shall be limited to no longer than 5 years from the date of latest attendance in any educational institution in the State."
b. Dispose of, destroy, erase, and/or anonymize the student or workforce data, regardless of the method of storage in accordance with a state-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
c. Use state-approved methods to ensure secure deletion or destruction of student or workforce data (including originals, copies, and archived records).
d. Configure the MLDS to record the date student or workforce data is retrieved or updated and when the student or workforce data is to be deleted. .

8 General Controls

8.1 Information Integrity

8.1.1 Malicious Code

a. The MLDS Data Center shall:
   1) Employ malicious code protection mechanisms at MLDS entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
   2) Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with MLDS Center configuration management policy and procedures;
   3) Configure malicious code protection mechanisms to:
      i. Perform monthly scans of the MLDS and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with MLDS Center security policy; and
      ii. Block malicious code, with notification to the user, in response to malicious code detection; and
   4) Centrally manage malicious code protection mechanisms.

b. The MLDS shall:
   1) Automatically update malicious code protection mechanisms (including signature definitions); and,
   2) Prevent non-privileged users from circumventing malicious code protection capabilities.

8.1.2 MLDS Monitoring

The MLDS Data Center shall monitor the MLDS to detect attacks and indicators of potential attacks.

8.1.3 Security Alerts, Advisories, and Directives

The MLDS Center shall:

a. Receive information system security alerts, advisories, and directives from designated external organizations (for example, Department of Information Technology (DoIT), regional, or national security organizations) on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to MLDS employees; and
d. Implement security directives in accordance with established time frames.

8.2 Security Awareness and Training Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented awareness and training procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the awareness and training policy and associated awareness and training controls.

8.2.1 Security Awareness

The MLDS Center shall ensure that all authorize users (to include MLDS Center employees, contractors) receive security awareness training within five business days of being employed by the MLDS Center, if he/she has not received awareness training within the past twelve months. Security awareness training shall be provided to all MLDS authorized users:

a. As part of initial training for new users;
b. When required by MLDS changes; and
c. At least annually thereafter.

8.2.2 Security Training

The MLDS Center shall provide role-based, security-related training to those MLDS Center employees who have significant security responsibilities relevant to the MLDS. This includes the MLDS Executive Director, Security Specialist, Network Administrator, Systems Administrator, Database Administrator (DBA), Programmer/Systems Analyst, Systems Designer/Systems Developer, and help desk personnel. The training shall be oriented to the individual's role and operational security responsibilities. This training shall be administered:

a. Before authorizing access to the MLDS or performing assigned duties;
b. When there are significant changes to the MLDS environment or procedures; and,
c. At least annually thereafter.

8.2.3 Security Training Records

The MLDS Center shall:

a. Document and monitor individual MLDS security training activities; and
b. Retain training records for a period of three (3) years.

8.3 System Security Assessment and Authorization

8.3.1 Security Assessments

a. The MLDS Center shall develop and employ a security assessment plan that describes the scope of the assessment, including:
    1) Security controls and control enhancements under assessment;

2) Assessment procedures to be used to determine security control effectiveness;
3) Assessment environment, assessment team, and assessment roles and responsibilities; and,
4) The results of all security assessments shall be documented in a security assessment report.

b. The MLDS Center shall include announced assessments as part of its security control assessments on an annual basis. These assessments may consist of, but are not limited to the following assessment types:
1) In-depth monitoring;
2) Malicious user testing;
3) Penetration testing; and
4) Red team exercises.

8.3.2 MLDS Connections

The MLDS Center shall:

a. Document MLDS connections through an Interconnection Security Agreement (ISA) and associated security requirements for each connection, the interface characteristics, security requirement, and the nature of the information communicated;
b. Monitor MLDS connections, verifying enforcement of security requirements.
c. Apply adequate countermeasures before connecting any equipment to the MLDS; and, ;
d. Establish any interconnections between MLDS and state agency and state institution systems providing data to the MLDS through controlled interfaces.

8.3.3 Plan of Action and Milestones – System Level

The MLDS Center shall:

a. Develop a Plan of Action and Milestones (POA&M) to document the planned remedial actions to correct weaknesses or deficiencies noted during the initial assessment of the security controls and when necessary, to reduce or eliminate known vulnerabilities in the system;
b. Update existing POA&Ms on an annual basis, at a minimum, based on the findings from security controls assessments, security impact analyses, and monitoring activities;

8.4 Configuration Management

8.4.1 Configuration Management Plan and Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented configuration management plan and change control procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and

b. Facilitates the implementation of configuration management and change control policy and associated configuration management controls.

8.4.2 Baseline Configuration

a. The MLDS Center shall develop, document, and maintain under configuration control, a current baseline configuration of the MLDS and associated software or hardware components, including communications and connectivity-related aspects of the systems. The baseline configuration shall:
   1) Provide information about the components of the MLDS and each component's technology (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with the current version numbers and patch information), network topology, and logical placement within the MLDS architecture.
   2) Use only legal and licensed (including open source, shareware, and freeware licenses, etc.) software (including operating system, databases, applications, etc.) shall be used or installed on MLDS. and,
b. The MLDS Center shall review and update the baseline configuration of the MLDS:
   1) When required due to significant changes to more than 25% of the baseline; and
   2) As an integral part of the MLDS component installations and upgrades.
c. The MLDS Center shall retain older versions of baseline configurations to support rollback.

8.4.3 Configuration Change Control

The MLDS Center shall:

a. Determine the types of changes to the MLDS that are configuration controlled;
b. Review proposed configuration controlled changes to the MLDS and approve;
c. Disapprove such changes with explicit consideration for security impact analyses;
d. Document approved configuration controlled changes to the MLDS;
e. Retain and review records of configuration controlled changes to the MLDS;
f. Audit activities associated with configuration controlled changes to the MLDS;
g. Coordinate and provide oversight for configuration change control activities through a configuration control board; and,
h. The MLDS Center shall test, validate, and document changes to the MLDS before implementing the changes in the production environment.

8.4.4 Configuration Settings

The MLDS Center shall, throughout the MLDS's lifecycle, and in accordance with MLDS security policies:

a. Establish and document mandatory baseline configuration settings for IT products employed in the MLDS using security configuration checklists (e.g., DISA Security

Technical Implementation Guide (STIG), NSA hardening guides, Center for Internet Security (CIS) security benchmark guides) that reflect the most restrictive mode consistent with operational requirements;

b. Implement and enforce the established configuration settings;
c. Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the MLDS based on explicit operational requirements; and,
d. Monitor and control changes to the configuration settings.

8.4.5 Least Functionality

a. The MLDS Center shall configure the MLDS to provide only essential capabilities and disable or remove any unnecessary or non-secure functions, ports, protocols, and/or services. The MLDS shall:
    1) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software on the MLDS; and
    2) Review and update the list of authorized software on a semi-annual basis.
b. The MLDS Center shall:
    1) Review the MLDS semi-annually to identify unnecessary and non-secure functions, ports, protocols, and services; and
    2) Disable functions, ports, protocols, and services within the MLDS deemed to be unnecessary or non-secure.

8.4.6 MLDS Component Inventory

a. The MLDS Center shall develop, document, and maintain an inventory of MLDS components that:
    1) Accurately reflects the MLDS;
    2) Is consistent with the authorization boundary of the MLDS;
    3) Is at a level of granularity deemed necessary for tracking and reporting, as requirements defined within this section for the MLDS components;
    4) Includes all MLDS-defined information deemed necessary to achieve effective property accountability; and
    5) Is available for review and audit by designated MLDS officials.
b. The MLDS Center shall maintain a current and updated inventory of MLDS components as an integral part of component installations, removals, and MLDS updates. The inventory management system shall include, at a minimum:
    a) Manufacturer
    b) Model Number
    c) Serial Number
    d) IP Address
    e) MLDS Barcode
    f) Hostname

g) Function
h) Software License number
i) Interconnections
j) System/Component Information
k) System/Component Owner

c. The MLDS Center shall:
   1) Employ automated mechanisms annually to detect the addition of unauthorized components/devices into the MLDS; and,
   2) Disable network access by such components/devices or notify designated MLDS personnel of unauthorized components/devices.
d. The MLDS Center shall include in property accountability information for the MLDS components, a means for identifying individuals (e.g. position, name and/or role), who are responsible for administering those components.
e. The MLDS Center shall verify that all components within the physical boundary of the MLDS are either inventoried as a part of the system or recognized by another system as a component within that system.

8.5 Contingency Planning

8.5.1 Contingency Planning Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented contingency planning procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of contingency planning policy and associated contingency planning controls.

8.5.2 MLDS Recovery and Reconstitution

The MLDS Center shall:

a. Provide for the recovery and reconstitution of the MLDS to a known state after any disruption, compromise, or failure;
b. Implement transaction recovery for systems that are transaction-based; and,
c. Provide compensating security controls for circumstances that can inhibit recovery and reconstitution to a known state/configuration.

8.5.3 Contingency Plan

The MLDS Center shall:

a. Develop and maintain a contingency plan that:
   1) Identifies essential functions and associated contingency requirements;

2) Provides recovery objectives, restoration priorities, and metrics;
3) Addresses contingency roles, responsibilities, assigned individuals with contact information;
4) Addresses eventual, full MLDS restoration without deterioration of the security measures originally planned and implemented; and
5) Is reviewed and approved by the MLDS Center Executive Director.

b. Plan for the resumption of essential functions as soon as feasible after contingency plan activation, and as defined within the MLDS recovery strategy.

8.5.4 Contingency Training, Plan Testing, and Exercises

a. All MLDS and MLDS Data Center personnel shall be trained in their roles and responsibilities in executing the contingency plan with respect to the MLDS and provided refresher training at least annually.
b. The MLDS Center shall:
   1) Test the contingency plan for the MLDS to determine the effectiveness of the plan and the MLDS Center's readiness to execute the plan;
   2) Review the contingency plan test results; and
   3) Initiate corrective actions.

8.5.5 Alternate Storage Site

The MLDS Center shall:

a. Establish an alternate storage site including necessary agreements to permit the storage and recovery of MLDS backup information;
b. Identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards; and,
c. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions, as required.

8.5.6 MLDS Backup

The MLDS Data Center shall:

a. Conduct backups of user-level information contained in the MLDS at least weekly;
b. Conduct backups of system-level information contained in the MLDS at least daily;
c. Conduct backups of MLDS documentation including security-related documentation at least monthly;
d. Protect the confidentiality and integrity of backup information at the storage location - The media shall be marked with the highest level of sensitivity;
e. Restrict access to backup media to authorized personnel only; and,
f. Test backup information to verify media reliability and information integrity at least semi-annually.

8.6 Incident Response

8.6.1 Incident Response Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented incident response procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the incident response policy and associated incident response controls.

8.6.2 Incident Response Training, Testing, and Exercises

The MLDS Center shall:

a. Train personnel in their incident response roles and responsibilities with respect to the MLDS;
b. Provide incident response refresher training at least annually; and,
c. Test and/or exercise the incident response capability for the MLDS at least annually to determine the incident response effectiveness and document the results.

8.6.3 Incident Handling

The MLDS Center shall:

a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinate incident handling activities with contingency planning activities;
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures and implements the procedures accordingly; and,
d. Employ automated mechanisms, when available, to support the incident handling process.

8.6.4 Incident Monitoring

The MLDS Center shall track and document MLDS security incidents.

8.6.5 Incident Reporting

The MLDS Center shall:

a. Require MLSD Center employees and contractor personnel to report suspected security incidents to the MLDS Center Information Security Officer within twenty-four hours;
b. Report security incident information to the Governing Board, the Maryland Department of Information Technology (DoIT), MSDE, DLLR, MHEC, and to law enforcement officials, if applicable; and,
c. Incorporate an automated capability to assist in reporting of security incidents.

8.6.6 Incident Response Assistance

The MLDS Center shall provide an incident response support resource (e.g., helpdesk or assistance group) to offer advice and assistance to MLDS Center staff for handling and reporting of security incidents.

8.6.7 Incident Response Plan

The MLDS Center shall:

a. Develop an incident response plan that:
   1) Provides the MLDS Center with a roadmap for implementing its incident response capability;
   2) Describes the structure of the incident response capability;
   3) Provides a high-level approach for how the incident response capability fits into the overall MLDS Center;
   4) Meets the unique requirements of the MLDS Center, which relate to its mission, size, structure, and functions;
   5) Defines reportable incidents;
   6) Provides metrics for measuring the incident response capability within the MLDS Center;
   7) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8) Is reviewed and approved by designated officials within the MLDS Center.
b. Distribute copies of the incident response plan to authorized MLDS Center incident response personnel and MLDS Center business units;
c. Review the incident response plan at a minimum on an annual basis;
d. Revise the incident response plan to address system and MLDS Center changes or problems encountered during plan implementation, execution, or testing; and
e. Communicate incident response plan changes to authorized MLDS Center incident response personnel and MLDS Center.

8.7 Maintenance

8.7.1 Maintenance Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented maintenance procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the maintenance policy and associated maintenance controls.

8.7.2 Controlled Maintenance

a. The MLDS Center shall:
    1) Schedule, perform, document, and review records of maintenance and repairs on MLDS components in accordance with manufacturer or vendor specifications and/or MLDS Center requirements;
    2) Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
    3) Require that a designated MLDS Center official explicitly approve the removal of any MLDS system components from the MLDS Center or the Data Center facilities for off-site maintenance or repair;
    4) Sanitize equipment to remove all information from associated media prior to removal from MLDS Center or Data Center facilities for off-site maintenance or repairs; and
    5) Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
b. The MLDS Center shall maintain maintenance records for the MLDS that include:
    1) Date and time of maintenance;
    2) Name of the individual performing the maintenance;
    3) Name of escort, if necessary;
    4) A description of the maintenance performed; and
    5) A list of equipment removed or replaced (including identification numbers, if applicable).

8.7.3 Maintenance Tools

The MLDS Center shall:

a. Approve, control, monitor the use of, information system maintenance tools;
b. Check all media containing diagnostic and test programs for malicious code before the media is used in the maintenance or troubleshooting of the MLDS; and,
c. Prevent the unauthorized removal of maintenance equipment by one of the following:
    1) Verifying that there is no MLDS Center or MLDS information contained on the equipment;
    2) Sanitizing or destroying the equipment;
    3) Retaining the equipment within the facility; or
    4) Obtaining an exemption from a designated a MLDS Center official explicitly authorizing removal of the equipment from the facility.

8.7.4 Non-Local Maintenance

The MLDS Center shall:

a. Authorize, monitor, and control non-local maintenance and diagnostic activities;

b. Allow the use of non-local maintenance and diagnostic tools only as necessary and when no other alternative is available;
c. Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
d. Maintain records for non-local maintenance and diagnostic activities;
e. Terminate all sessions, maintenance ports, and network connections when nonlocal maintenance is completed;
f. Audit non-local maintenance and diagnostic sessions. Designated MLDS Center personnel shall review the maintenance records of the sessions;
g. Document, in the security plan for the MLDS, the installation and use of non-local maintenance and diagnostic connections; and,
h. Require that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or
i. Remove the component to be serviced from the MLDS and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to MLDS Center information) before removal from MLDS Center or Data Center facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the MLDS.

8.7.5 Maintenance Personnel

The MLDS Center shall:

a. Establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel;
b. Ensure that personnel performing maintenance on the MLDS have required access authorizations or designate MLDS Center personnel with required access authorizations and technical competence deemed necessary to supervise MLDS maintenance when maintenance personnel do not possess the required access authorizations; and
c. Limit access to system software and hardware to authorized personnel.

8.7.6 Timely Maintenance

The MLDS Center shall obtain maintenance support and/or spare parts for failed MLDS components and/or key information technology components within a period consistent with recovery time objectives.

8.8 Media Protection

8.8.1 Media Protection Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented media protection procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of media protection and is consistent with the Maryland Department of Information Technology Information Security Policy, version 3.0, paragraph 6.5.

8.9 Physical and Environmental Protection

8.9.1 Physical and Environmental Protection Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented physical and environmental protection procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

8.9.2 Physical Access Authorizations

The MLDS Center shall:

a. Develop and keep current a list of personnel with authorized access to MLDS facilities where the MLDS and data reside (except for those areas within the facility officially designated as publicly accessible);
b. Issue authorization credentials (e.g., badges, identification cards, and smart cards); and,
c. Review and approve the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.

8.9.3 Physical Access Control

The MLDS Center and Data Center shall:

a. Enforce physical access authorization for all physical access points (including designated entry/exit points) to the facility where the MLDS resides (excluding those areas within the facility officially designated as publicly accessible);
b. Verify individual access authorizations before granting access to a facility;
c. Control entry to facilities containing the MLDS, using physical access devices and/or guards;
d. Secure keys, combinations, and other physical access devices;
e. Inventory physical access devices at a minimum annually;
f. Change combinations and keys at least annually and when keys are lost, combinations are compromised, or individuals who have access are transferred, terminated, or no longer require access;
g. Implement access controls for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times. Access controls shall be:

1) Based on the level of risk; and
2) Sufficient to safeguard assets against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

h. Enforce physical access authorization to the MLDS independent of the physical access controls for the facility in which it is located; and,
i. Ensure all physical access points to facilities where the MLDS resides is guarded and/or alarmed and monitored 24 hours per day, 7 days per week, commensurate with identified risk.

8.9.4 Access Control for Transmission Medium

The MLDS Center and Data Center shall ensure physical access to MLDS distribution and transmission lines is controlled.

8.9.5 Access Control for Output Devices

The MLDS Center and Data Center shall control physical access to the MLDS output devices (e.g., monitors, printers) to prevent unauthorized individuals from obtaining the output.

8.9.6 Monitoring Physical Access

The MLDS Center and Data Center shall ensure:

a. Physical access to the MLDS is monitored to detect and respond to physical security incidents;
b. Physical access logs are reviewed semi-annually; and,
c. Monitoring for real-time physical intrusion alarms and surveillance equipment.

8.9.7 Visitor Control

The MLDS Center and Data Center shall:

a. Ensure control of the physical access to the MLDS by authenticating visitors before authorizing access to the facility (e.g., access roster) where the MLDS resides other than areas designated as publicly accessible. Note: Escort access to a MLDS facility requires the non-MLDS personnel (e.g., visitor) to be accompanied by an authorized MLDS or DPSCS employee and their activity to be monitored within the facility. The escort shall have the escorted person(s) in view or be situated as such the escorted person(s) cannot leave the escorted area without being seen.
b. Ensure all visitors:
    1) Sign-in upon entering the facility;
    2) Be escorted; and
    3) Sign-out when exiting the facility.

8.9.8 Access Records

The MLDS Center & Data Center shall:

a. Maintain visitor access records/logs to facilities where the MLDS resides (except for those areas within the facility officially designated as publicly accessible). Access logs shall be reviewed by designated personnel at least monthly to identify and remedy suspicious activity; and,
b. Maintain a record of all physical access, both of visitors and authorized individuals.

8.9.9 Power Equipment and Power Cabling

The MLDS Data Center shall protect power equipment and power cabling for the MLDS from damage and destruction.

8.9.10 Emergency Shutoff

The MLDS Data Center shall:

a. Provide the capability of shutting off power to the MLDS or individual system components in emergency situations;
b. Place emergency shutoff switches or devices in a location near the MLDS or system components to facilitate safe and easy access for personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

8.9.11 Emergency Power

The MLDS Data Center shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the MLDS in the event of a primary power loss.

8.9.12 Emergency Lighting

The MLDS Center and Data Center shall employ and maintain an automatic emergency lighting system that activates in the event of a power outage or a disruption of emergency exit/evacuation route areas.

8.9.13 Fire Protection

a. The MLDS Data Center shall employ and maintain fire suppression and detection devices/systems (e.g., sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors) for the MLDS that are supported by an independent energy source.
b. The MLDS Center & Data Center shall ensure detection and suppression systems are automatically activated in the event of a fire and provide notification of the activation to emergency responders.
c. The MLDS Data Center shall employ an automatic fire suppression capability for the MLDS when the facility is not staffed on a continuous basis.

8.9.14 Temperature and Humidity Controls

The MLDS Data Center shall:

a. Maintain temperature and humidity levels within facilities where the MLDS resides at acceptable levels; and

b. Monitor temperature and humidity levels daily.

8.9.15 Water Damage Protection

The MLDS Data Center shall protect the MLDS from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

8.9.16 Delivery and Removal

The MLDS components, entering and exiting a facility, shall be controlled, recorded, maintained, and authorized by MLDS Center or Data Center personnel.

8.9.17 Alternate Work Site

The MLDS Center shall:

a. Employ management, operational, and technical information system security controls as defined within this policy at alternate work sites;
b. Assess the effectiveness of security controls at alternate work sites; and
c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.
d. Ensure that individuals within the MLDS Center employ appropriate information system security controls while at alternate work sites.

8.9.18 Location of MLDS Components

The MLDS Center and Data Center shall position MLDS components within the Data Center to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

8.10 Risk Assessment

8.10.1 Risk Assessment Procedures

The MLDS Center shall develop, disseminate, review, and update annually a formal, documented risk assessment procedure that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, and compliance; and
b. Facilitates the implementation of the risk assessment policy and associated risk assessment controls.

8.10.2 Risk Assessment

The MLDS Center shall:

a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the MLDS and the information it processes, stores, or transmits;
b. Document risk assessment results in system security plans and risk assessment plans;
c. Review risk assessment results at least annually; and
d. Update risk assessments at least every three (3) years or whenever there are significant changes to the MLDS or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the MLDS.

Note: Examples of significant changes to the MLDS that should have a technical risk assessment updated include, but are not limited to: (i) Installation of a new or upgraded operating system, middleware component, or application; (ii) Modifications to system ports, protocols, or services; (iii) Installation of a new or upgraded hardware platform or firmware component; or (iv) Modifications to cryptographic modules or services.

8.10.3 Vulnerability Scanning

The MLDS Data Center shall:

a. Scan for vulnerabilities in the MLDS and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1) Enumerating platforms, software flaws, and improper configurations;
    2) Formatting and making transparent, checklists and test procedures; and
    3) Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from security control assessments;
d. Remediate legitimate vulnerabilities;
e. Employ vulnerability scanning tools that include the capability to readily update the MLDS vulnerabilities to be scanned; and
f. Update the MLDS, if appropriate, when new vulnerabilities are identified and reported.

8.10.4 Rules of Behavior

The MLDS Center shall:

a. Establish and make available to all MLDS authorized users, the rules that describe their responsibilities and expected behavior with regard to information and MLDS usage; and,
b. Ensure all users sign a statement indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to information and the MLDS.

8.11 Security Program Management

8.11.1 Senior Information Security Officer

The MLDS Center Director shall appoint an information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

8.11.2 Information Security Resources

The MLDS Center Director shall ensure that information security resources are available for expenditure as planned.

8.11.3 Plan of Action and Milestones – Program Level

The MLDS Center shall implement a process for ensuring that plans of action and milestones for the security program and the MLDS are maintained and shall document the remedial information security actions to mitigate risk to MLDS Center operations, assets, and individuals.

8.11.4 MLDS Inventory

The MLDS Center shall develop and maintain an inventory of the MLDS hardware and software components.

8.11.5 Information Security Measures of Performance

The MLDS Center shall develop, monitor, and report on the results of information security measures of performance to the Governing Board on a semi-annual basis.

9 **Terms and Terminology** (Note: Not all terms below are used in this document)

Adult – an individual who is age 18 or older

Adult Education – same meaning as adult education and literacy activities - services or instruction below the postsecondary level for individuals--

a. who have attained 16 years of age;
b. who are not enrolled or required to be enrolled in secondary school under State law; and
c. who--
    (i) lack sufficient mastery of basic educational skills to enable the individuals to function effectively in society;
    (ii) do not have a secondary school diploma or its recognized equivalent, and have not achieved an equivalent level of education;
    (iii) are unable to speak, read, or write the English language.

Anonymization – The act of permanently and completely removing personal identifiers from data, such as converting personally identifiable information found within the student or workforce data into aggregated data. Anonymized data is data that can no longer be associated with an individual in any manner.

Apprentice – a worker 16 years old or older, who has entered into a voluntary written agreement with a sponsor who has agreed to teach the worker a skilled trade under terms defined in MD Regulations 2.04 and2.05.

Breach – an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.

Correctional Education Service – a continuum of structured education, workforce training, and transition services to incarcerated students that will prepare the student to enter Maryland's workforce

Data Governance – a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.

Data Steward – A person delegated the responsibility for managing a specific set of data resources (Authority: ISOIEC 11179)

Dates of attendance –

(a) The term means the period of time during which a student attends or attended an educational agency or institution. Examples of dates of attendance include an academic year, a spring semester, or a first quarter.

(b) The term does not include specific daily records of a student's attendance at an educational agency or institution. (Authority: 20 U.S.C. 1232g (a)(5)(A))

De-Identification – Involves the removal of personally identifying information in order to protect student or workers privacy. De-identified data may not necessarily be anonymized data, but may be data that can be re-associated with personally identifiable student or workforce data at a later time.

Direct Identifiers – Information that relates specifically to an individual, such as the individual's residence, including for example, name, address, social security number, or other identifying number or code, telephone number, or email address.

Disclosure – To permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record. (Authority: 20 U.S.C. 1232g(b)(1) and (b)(2))

Indirect Identifiers – Information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator and other descriptors.

Record – Any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche. (Authority: 20 U.S.C. 1232g)

State Assigned Student Identifier (SASID) – identifying information assigned to each student by a local education agency based on the identifier system developed by the State Department of Education or an institution of higher education, if the student has not been assigned an identifier by a local education agency

Sensitive data – Information or data that carries the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose student data, or workforce data was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains this data.

Student Data – data relating to student performance and includes: (i) State and national assessments; (ii) Course-taking and completion; (iii) Grade point average; (iv) Remediation; (v) Retention; (vi) Degree, diploma, or credential attainment; (vii) Enrollment; and (viii) Demographic data. **Student data does not include:** (i) Juvenile delinquency records; (ii)

Criminal and CINA records; (iii) Medical and health records; and (iv) Discipline records. (MD Education Article § 24-70 I)

Workforce data -- data relating to: **(I)** Employment status; (2) Wage information; (3) Geographic location of employment; and (4) Employer information. (MD Education Article § 24-701)

10 Record of Revisions

Revision	Date	Section	Description
1.0	8/30/2012		Initial Draft

11 Background Information

11.1 Data Governance Workflow