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

December 18, 2014

The Honorable Martin O'Malley
Office of the Governor
100 State Circle
Annapolis, MD 21401

Dear Governor O'Malley,

Under the terms of Chapter 190 of the Acts of the General Assembly of 2010, the Governing Board of the Maryland Longitudinal Data System is required to submit an annual report to the Governor and the Maryland General Assembly.

On behalf of the Board, I am pleased to be given the opportunity to provide you with this report, which is enclosed, and hope that you find it useful and informative.

I am happy to address any questions you may have and look forward to continuing the work to fully develop and utilize a longitudinal data system for improved education and workforce policy decisions.

Sincerely,

Ross Goldstein
Executive Director

Enclosure

cc: President Thomas Miller
Speaker Michael Busch
Jared Billings, Office of the Governor
MLDS Governing Board
Caroline Boice, DLS
Nathan Bowen, DBM
Sarah Albert, DLS

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

A Report to the Governor and Maryland General Assembly

Regarding

The Development of the Maryland Longitudinal Data System & Center

December 2014

Contents

Introduction

The Maryland Longitudinal Data System (MLDS) is a statewide data system that contains student and workforce data. The MLDS was established pursuant to Chapter 190 of the Acts of the General Assembly of 2010. The MLDS draws on data from:

- The Maryland State Department of Education (MSDE);
- The Maryland Higher Education Commission (MHEC);
- The Maryland Department of Labor, Licensing and Regulation (DLLR); and
- Certain external data sources.

The MLDS will have the capacity to allow Maryland policy-makers, educators, and workforce development partners to improve their understanding and evaluation of the education and workforce development enterprise by providing a more transparent picture of the Maryland educational system and workforce outcomes through web-based data portals and in-depth research and studies.

The MLDS Governing Board is made up of 12 members. Seven of those members are designated by statute, including the Chancellor of the University System, the State Superintendent of Schools, the Secretary of Higher Education, the Secretary of the Department of Labor, Licensing, and Regulation, the President of Morgan State University, the Executive Director of the Maryland Association of Community Colleges, and the President of the Maryland Independent Colleges and Universities Association. The other five members are appointed by the Governor with the advice and consent of the Senate. One appointee must be a representative of local superintendents of schools and another must have expertise in large data systems and data security. The chair of the Governing Board is appointed by the Governor. See the attached Governing Board membership roster.

This Annual Report is a requirement under Education Article, §24-705, Annotated Code of Maryland, which requires the Governing Board to annually provide information to the Governor and General Assembly on the following:

1. An update on the implementation of the MLDS and activities of the MLDS Center;
2. List of all studies performed by the Center during the reporting period;
3. List of all currently warehoused data that are determined to be no longer necessary to carry out the mission of the Center;
4. Any proposed or planned expansion of data maintained in the database; and
5. Any other recommendation made by the Governing Board.

Implementation of the MLDS

Implementation of the System

System Development

The MLDS is fully developed and operational and has met the December 31, 2014 statutory deadline (*see* Education Article § 24-702(a), Annotated Code of Maryland). Although the system architecture is complete and staff are able to generate dashboards and have begun research, delays during system development prevented the Center from achieving the research and analysis output originally desired. However, with recent staff additions and steady gains in knowledge and expertise about the system, additional output is expected within the next 30 to 60 days.

The system development delays are a result of a variety of factors. First, this is a very complex system that required detailed planning and execution. Second, the decision to build all components in-house, instead of relying on off-the-shelf software applications, required additional development time. It should be noted that in the long run, the in-house development will save the State significant money by avoiding expensive software licensing fees. Finally, staffing the MLDS Center positions has been a challenge. For the most part the Center continued to function by utilizing contractual resources at MSDE. However, certain functions, such as data loading and web portal creation, came to a standstill at different points due to the unavailability of any staff or contractors. As described below, the Center has made significant strides in filling positions.

System Overview

The Center has created an internally managed environment using Dell servers, EMC Storage Area Network (SAN) and EMC AVAMAR enterprise storage solution and EMC VMWare. Below is a description of the components that make up the MLDS environment.

- TIBCO Managed File Transfer (MFT) software that provides data providers with a secure method of providing data files to the Center.
- An Oracle Warehouse Builder (OWB), which is a data extract, transform, and load (ETL) tool that is used to manage all data movement and transformation, through a fully automated process that removes the need to have staff involved in the process. It will take data provided on the MFT server, apply data quality steps to improve the data for processing, and to conform the data to standard codes used in the Master Database Management system.
- A Master Database Management (MDM) system has been constructed to perform identity resolution and to master key data. The MDM is a database system used to securely manage and maintain all personally identifiable information (PII) data, and is only accessible by the ETL service account. Identity data in the MDM is assigned a unique token and the associated identity information is then deconstructed, as an additional security precaution. No person is granted access to the MDM database, except through a special request that must be authorized by the Center's Executive Director or his acting agent, and only for a period not to exceed 24 hours.
- An Operational Data Store (ODS) accepts data from the ETL tool, along with the identity tokens (now de-identifiable data) from the MDM. The ODS does not contain any PII data and combines person and organization tokens from the MDM, along with person roles to form a combined identifier that represents a person's role at one or more organizations at any one time or over time (historical). This further abstraction of identifiers provides another layer of security. The combined identifier token is associated with data (e.g. enrollments, achievements, employment, assignments) in a way that allows easier analysis of data by researchers.
- A Data Warehouse (DW) database accepts data from the ETL tool (from the ODS), after it has been aggregated and the combined identifier token has been removed. This data is organized so that it can be easily used by Business Intelligence software.
- Oracle Business Intelligence Enterprise Edition (OBIEE) is the business intelligence (BI) software that reads data from the DW and uses the data to build cubes (multidimensional representations of data) that can be easily manipulated to produce dashboards and reports. OBIEE also uses a set of business rules to suppress data and enforce Family Educational Rights and Privacy Act (FERPA) compliance.
- Oracle WebCenter software is used to create web portals (websites) to communicate information.

WebCenter is used to present the dashboards and reports that are generated in OBIEE as well as other pertinent information relevant to the MLDS Center.

- The Center's new website has been implemented and contents are being posted. WebCenter integration has been configured for dashboards to be posted with dynamic data web portals.

Data Center - Hosting Location

The Center has changed the hosting location of the system from the Department of Public Safety and Correctional Services (DPSCS) to the Maryland State Department of Education (MSDE). In order to support the data system and web portals, new servers and software needed to be installed. The original plan had been to continue to have the system hosted at DPSCS. Hosting at DPSCS made sense during the initial development phase led by MSDE. At that time MSDE was simultaneously managing other projects, all of which were hosted at DPSCS. However, now that the system development is fully under the Center's control, the MSDE data center provides a better hosting solution because it is less expensive, more sustainable and offers greater control and access to the Center staff, but does not compromise security. Specifically, the following factors were considered:

1. Control - DPSCS provides a hosted solution versus the co-location model being presented by MSDE. With the MSDE model, the Center has full control over its environment, including installation and setup of the servers and ongoing operation and maintenance. Under the hosting model, DPSCS maintains the MLDS system in its environment. This means that servers, installation and certain design decisions would be determined by DPSCS, not the Center.
2. Cost - There are no direct hosting costs assessed to the Center with either option. However, there are other cost impacts that favor the MSDE option. DPSCS primarily requires its vendors to do the installation and maintenance work on all equipment within its data center. Having to rely on vendors increases the MLDS Center costs ($175/hr. labor cost) while also creating a situation where the Center's work is subject to DPSCS' schedule and resources. In comparison, MSDE is providing in-house resources to provide technical assistance as well as training and staff development.
3. Sustainability – MLDS Center was appropriated several full time positions to hire staff necessary to independently build and maintain the system. The goal is to ensure system sustainability. The MSDE hosting model will help achieve this goal of having a system maintained by staff instead of relying on vendors. MLDS Center staff resources will be able to work directly on any servers and/or data issues to resolve them in much quicker and timely manner.
4. Mobility – Should future needs require the Center to move its systems to another location, that process would be much easier to accomplish using the MSDE co-location model, because the system would not be integrated with or otherwise be a part of another system.
5. Security - One of the reasons that DPSCS was selected as the host for the data center was due to its robust security. After careful review, it was determined that the MSDE data center, which maintains personally identifiable student data, provides equivalent physical and network security at its data center.
    a. Network Security - Both MSDE and DPSCS use the same routers, switches, and firewalls. One advantage to MSDE is that it only requires the Center to maintain one level of user access control. The DPSCS model required a second layer of user access

controls, which would be more cumbersome to maintain and potentially less secure due to the interdependencies between the two layers of access control, and because more staff would have access to the security controls. Simply trying to keep access control upgrades and changes synchronized can require full time staffing positions.

b. Physical Security
   - Both facilities have 24/7 security guards (armed at DPSCS and unarmed at MSDE) who control access to the building that houses the data center.
   - Both facilities require authorized access to the server room via a key card.
   - Neither facility provides separate physical security for the Center equipment (*i.e.* a locked cage). This is an option that may be implemented at MSDE, if we determine it is necessary.
   - Cameras are installed in both facilities. DPSCS has cameras in the server room whereas MSDE has cameras at the entrance to the server room. The DPSCS camera installation is preferable and something MSDE would be willing to work with the Center to implement.
   - Both facilities have comparable cooling, conditioned power, virtual tape backup, and fire suppression capabilities.

Web portals and Dashboards

The Center will work on producing the following dashboards:

1. High School Graduates to Postsecondary (at State Level)
2. High School Graduates to Postsecondary (at State Level) by Gender, Race and Ethnicity
3. High School Graduates to Postsecondary by Postsecondary Institutions
4. High School Graduates to Postsecondary (by county)
5. High School Graduates to Postsecondary (by county) by Gender, Race and Ethnicity
6. High School Graduates to Postsecondary to Workforce (State Level)
7. High School Graduates to Postsecondary and Workforce (State Level)
8. High School Graduates to Workforce (State Level)
9. High School Graduates to Workforce (State Level) by Gender, Race and Ethnicity
10. Postsecondary to Workforce (State Level)
11. Postsecondary to Workforce (State Level) by Gender, Race and Ethnicity
12. High School Graduates to Workforce (County Level)
13. High School Graduates to Workforce (County Level) by Gender, Race and Ethnicity
14. Early Learning Workforce Retention

Implementation of the Center

Advisory Boards

Prior to the establishment of the Center, the *Information Technology Group* (iTech) and the *Intergovernmental Working Group* (IWG), met monthly to discuss plans for the system development and to help guide the Governing Board on policy matters, respectively. The Center has continued to utilize these groups and has worked to ensure their continuity by establishing a formal charter and outlining specific duties for each.

The Data Governance Advisory Board (Data GAB) is required by the *Data Security and Safeguarding Plan*. The Data GAB is a continuation of the *iTech Group*. The Data GAB meets monthly and has the following roles and responsibilities:

1. Reviewing the data inventory and collection schedule;
2. Monitoring data quality, including:
    a. Informing MLDS staff on limitations of data;
    b. Identifying potential differences between the uses of data; and
    c. Reviewing new portals;
3. Identifying data gaps and analyzing whether additional data collections are needed;
4. Identifying stakeholders and establishing decision rights and accountability;
5. Security oversight, including:
    a. Reviewing plans to implement the *Data Security and Safeguarding Plan;* and
    b. Providing input on meeting compliance with requirements;
6. Helping align initiatives by ensuring data collected is sufficient to meet research needs;
7. Ensuring data is used and maintained consistent with state and federal laws, regulations, and the Public Information Act; and
8. Identifying measures of success.

The membership of the Data GAB includes a data steward from each agency and the MLDS executive director and branch directors.

The Research and Policy Advisory Board is a continuation of the *Intergovernmental Working Group (IWG)*. To formalize the entity and clarify its roles and responsibilities, a more descriptive name and charter were established. The charter specifies that Research and Policy Advisory Board meets monthly and has the following roles and responsibilities:

1. Advising the MLDS staff on the Research Agenda, research plans, and prioritization;
2. Hearing from outside entities proposing additions to the agenda;
3. Commenting on research output, web portals, and other reports created by the MLDS Center;
4. Providing input on public communications and governance issues (i.e. regulations); and
5. Advising the Center on grant opportunities and possible partnerships.

The membership of the Research and Policy Advisory Board includes representatives of the Governing Board members, MLDS staff, and other key stakeholders appointed by the executive director.

Data Collection Schedule

The Center developed, and the Governing Board has approved, a *Data Collection Schedule* (attached). The schedule was developed in consultation with the Data Governance Advisory Board in order to ensure the schedules are feasible for the agencies. The schedule has a page for each of the agencies (MHEC, MSDE, and DLLR) and lists the specific data files to be provided. The schedule provides several steps for each data file.

1. A data collection window - the period of time during which the agency could begin to provide required data.
2. A final deadline for the data - to balance the flexibility of the collection window with a deadline

so the Center can plan its work.

3. A period of time for cross agency reconciliation where the Center and the agencies can work together on data matching and quality issues.
4. A deadline for the agencies to provide final sign off on the data.

The determination of whether specified data will be provided annually, quarterly, or otherwise depends on the data source and how often it is collected by the agency.

Regulations

Education Article § 24-706 requires the Center to adopt regulations to implement the law establishing the system and the Center. The following regulations have been created.

1. COMAR 14.36.01 - .03 (final)

   These regulations establish procedures for compliance with the Maryland Public Information Act (PIA), compliance with the Open Meetings Act, and addressing requests for correcting public records created and maintained by the MLDS Center. These three chapters follow the model regulations provided by the Office of the Attorney General.

2. COMAR 14.36.04 (final)

   These regulations establish an administrative procedure for managing requests for longitudinal data. A separate chapter for longitudinal data requests was created to clarify that such requests are distinct from a PIA request. The regulations establish requirements for:

   - The submission of a written request for longitudinal data on an application developed by the Center;
   - Completion of an affidavit specifying that data will not be used for commercial solicitation, marketing, or any form of financial gain;
   - The amount of time that the Center must respond to a request for longitudinal data;
   - Fees for providing the longitudinal data;
   - Ensuring that the disclosure of information is consistent with State and federal requirements to protect the privacy of student and workforce personally identifiable information; and
   - Referring a request for a non-longitudinal data (*i.e.* data that can be provided by only one of the agencies providing data to MLDS) to the appropriate agency.

3. COMAR 36.14.05 (proposed)

   These regulations formalize the current practices surrounding data collection. Specifically, the regulations require:

   - The inclusion of a data element in the data inventory, approved by the Governing Board, before collecting, using or warehousing the data;
   - Data collection pursuant to the schedule established by the Governing Board;
   - Data transmission pursuant to the method established by the Center; and
   - Data to be collected from MSDE, MHEC, or DLLR if the agencies are already collecting that data or agree to do so.

4. COMAR 36.14.06 (proposed)
   Education Article § 24-703(g), Annotated Code of Maryland, restricts access to the data in the MLDS to authorized staff of the Center. These regulations provide that authorized staff of the Center includes the employees of the Center and individuals authorized by the Executive Director to conduct research or to fulfill an information technology need. The regulations also specify that the number of staff must be restricted in number in order to maintain control over access and use and that staff must successfully complete a Criminal History Background Check and meet other security requirements.

Staffing

The MLDS Center is budgeted 15 positions (14 full-time and 1 part-time). As of the time of writing this report, the following eight positions are filled:

1. Executive Director
2. Executive Associate
3. Assistant Attorney General (part-time)
4. Systems Management Branch Director
5. Network Engineer
6. OBIEE Developer
7. OBIEE Analyst
8. ETL Developer

The duties of three additional positions are being fulfilled by contractors.

1. Senior System Developer - MLDS entered into a contract with the senior system developer who began the project at MSDE. This individual is the architect of the system and has already successfully completed a similar longitudinal data system for the State of Washington.
2. Database Engineer - Currently these duties are being completed by an MSDE contractor funded by MLDS Center. An active recruitment is under way.
3. Web Developer - The contract for this position ends in December. The contractor has applied for and has been selected to fill the state position.

There are three positions that are shared with the partner agencies (MLDS fully funds the positions, but fifty percent of each employee's time and duties is for the agency). The agencies are responsible for the recruitment. Currently all three are vacant. The MHEC and MSDE positions had been filled as of August 2013, but both employees received promotions within their respective agencies within the last three months. MSDE has selected an internal candidate to fill the position. MHEC did not have an in-house candidate and is conducting a recruitment to fill the vacancy. The DLLR shared position has never been filled, but an active recruitment is underway.

The role of the MSDE and MHEC shared positions have changed. They were both directors with supervisory authority over MLDS Center employees. While they will still play a critical role in the management and direction of the MLDS, they will no longer be in a supervisory role. Within MLDS, the shared positions do not make ideal supervisors because they are only involved in MLDS work fifty-percent of the time and because the MLDS employees that they would supervise are IT staff who are more effectively supervised and managed by full-time MLDS Center IT staff. A revised organization chart reflecting these changes is attached.

Finally, pursuant to the MOU with the University of Maryland, School of Social Work, a full-time research coordinator has been hired by the University to be funded by the MLDS Center. The Coordinator begins in January and will be responsible for:

- Designing and implementing advanced multivariate statistical analyses with large multi-level education and workforce data sets;
- Coordinating longitudinal education and workforce research activities;
- Supervising doctoral students on statistical methods; and
- Working in consultation with faculty members in the University of Maryland School of Social Work and College of Education (COE) and staff members of the MLDS Center.

In addition to the research coordinator, the Research Branch includes four doctoral students, who have been engaged in a variety of research and learning opportunities over the past year. There were two half-time doctoral fellows last academic year, and three this year (two half-time and one full-time). The students have helped identify and synthesize existing knowledge about research question topics, have been trained in the Oracle Business Intelligence tools that are used to query the database and create dashboards and reports, assisted in preparing and presenting in the monthly Research Series organized and hosted by the Research Team, contributed to conversations regarding data requirements to answer research questions, and have been involved in the recent initial access of the data systems and initial analyses with the data.

The Research Team also has many faculty now involved with the Center beyond the core faculty of Michael Woolley (SSW), Laura Stapleton (COE), and Terry Shaw (SSW). Robert Croninger (COE) was a presenter at has both presented one of the Research Series and contributed to the draft report on online education, which is part of the Center's first year Research Agenda (see below). Brenda Jones-Harden and Elisa Klein (both in the COE) and Gail Sunderman (Maryland Equity Project in the COE) all also sat on a Research Series panel and are helping to write a report on Early Childcare/Education workforce. Marvin Titus (COE) sat on a panel about workforce issues and is working with us on researching the transition from postsecondary education to the workforce. Finally, Lisa Berlin (SSW) contributed her expertise on early child development to a Research panel and we look forward to engaging her in the Center's research agenda in the future.

Interagency Agreements

This year the MLDS Center entered into interagency agreements with MSDE, MHEC, and DLLR regarding administrative agreements between the agencies including shared space and shared employees. These administrative MOUs went into effect as follows:

- MSDE – February 28, 2014
- MHEC – March 24, 2014
- DLLR – August 22, 2014

At the same time, the MLDS Center needed to update the existing "Interagency Data Sharing Agreement – Memorandum of Understanding Between the Maryland State Department of Education, Maryland Higher Education Commission, Maryland Department of Labor, Licensing and Regulation, and Maryland Longitudinal Data System Governing Board and Maryland Longitudinal Data Center" dated December 19, 2012 to include language consistent with updates to the Family Education Rights and

Privacy Act ("FERPA")(20 U.S.C. §1232g), and corresponding regulations (34 C.F.R. Part 99). The MLDS Center created a separate data sharing agreement for each of the partner agencies so that any additional language unique to the data being provided by those agencies and any additional State or Federal privacy laws related to those data sets could be addressed therein. The data sharing MOUs went into effect as follows:

- MSDE – April 9, 2014
- MHEC – April 2, 2014
- DLLR – August 6, 2014

The MLDS Center entered into a MOU with the University of Maryland, Baltimore concerning the research division of the MLDS Center and additional administrative items related to the location of Center staff within the University of Maryland, Baltimore School of Social Work. This agreement went into effect on February 7, 2014.

The MLDS Center is in the final phases of completing the MOU concerning the relocation of the MLDS Data Center from DPSCS to the Data Center at MSDE. This agreement will be completed by December 31, 2014.

Security

The Governing Board developed a detailed *Data Security and Safeguarding Plan* (DSSP) as required under Education Article § 24-704(g)(6)(iii) of the Annotated Code of Maryland (*see attached*). The MLDS Center has been working to implement and document all of the requirements established under the plan. A key aspect of the DSSP is ensuring that staff who access the data system are properly trained, notified of their security obligations and requirements, and have undergone a Criminal History Background Check. To meet these requirements, the following procedures and documentation (*included with the attached DSSP*) have been implemented.

1. *Rules of Security Behavior* - This form, which must be signed by staff, contains non-disclosure agreement requirements and also addresses other security related requirements including the following:
    - Training;
    - Acting in conformance with the DSSP;
    - Not sharing passwords;
    - Reporting risks or vulnerabilities;
    - Requirements for a Criminal History Background Check; and
    - Consequences for violating the rules which include:
        - Removal of system access;
        - Potential civil or criminal penalties; and
        - Employee disciplinary actions.
2. *Criminal History Background Investigations (CHBI)* - This document is a policy statement that establishes that the legal authority for the background investigations is pursuant to the State's Information Security Policy which states that security clearance is required for personnel who access a sensitive system (which the MLDS is). The CHBI policy also specifies that it is applicable to all employees and contractors - regardless of job classification. Finally, the CHBI

policy specifies what findings in a background investigation will result in a staff member not being granted access to the system. Those findings include any felony conviction or conviction in the last 10 years of a crime that qualifies as an infamous crime (such as treason, perjury, forgery, obstruction of justice or other misdemeanor involving dishonesty).

2. DSSP Acknowledgment Form - This is a form that staff must complete acknowledging receipt and review of the *Data Security and Safeguarding Plan*.
3. Security Training Requirements - This document outlines the required training staff must complete. There are two aspects to the training requirements. First is required security training, either through the State's *Security Mentor* Training Program (which includes ongoing training and certificates of completion) or through a Cyber Security Awareness training program available on the Department of Defense website. The second aspect to the training involves ensuring that staff understand the legal requirements surrounding educational data. These trainings include two FERPA online tutorials provided by the Privacy Technical Assistance Center (PTAC). Staff is looking for similar classes related to labor data.
4. *Temporary Staff Appointment Form* - Pursuant to State law, only staff of the MLDS Center is permitted access to the system. This form documents the process for appointing staff. Staff can only be appointed by the Branch Directors with the approval of the Executive Director. Currently, the only temporary staff are university researchers and the system development contractors.
5. *User System Access Request Form* - This form must be completed before access to the system is granted. In the first part of the form the requester provides a statement of business needs and his or her planned method of system access. The form states that the device that accesses the system must be limited to a device issued by the MLDS, partner agency, or university. Use of personal computing devices is prohibited. The network through which the system is accessed is either MSDE's internal network, or through a VPN over an external network (which must be a secure home or work network). Part two of the form is a series of confirmations that the requester has completed all of the security requirements and that his or her supervisor agrees with the access request. Part three of the form is completed by the system administrator who assigns the requester to a functional group that contains only the rights necessary to complete the stated business needs, and assigns an access duration date. Part four is final approval by the Executive Director.

Research Series

Last year the MLDS Center initiated a monthly *MLDS Center Research Series*. The *Series* is a lunchtime presentation and discussion on a MLDS-related research topic. The goal of the *Series* is to engage stakeholders in the education and workforce community in the research being conducted directly by the Center or significant research being conducted by other institutions and entities on related topics. The *Series* will also provide a useful forum for the researchers to interact with and receive input from educators and administrators on the research questions.

This year, the following presentations took place:

- February 2014 - Exploring Financial Aid Policy
- March 2014 - Panel Discussion on Workforce Issues
- April 2014 - LINKS Project: Lessons Learned from an Integrated Data System
- May 2014 - Panel Discussion on Early Childhood Education

- October 2014 - Online Education: Research, Theory and Practice
- November 2014 - Strategies for Missing Data in Education Research

Studies

Research Agenda

Research and studies undertaken by the Center are guided by the Research Agenda established by the Governing Board. The Research Agenda was updated this year to address concerns about the role of the Center to broaden the scope of the agenda. The revisions have been focused on a couple of areas. One area of revision was to make clear the nature of the Center's role. This was necessary to address concerns from the state agencies that the Center was not encroaching on their research domains. That led to the development of a preamble to the Research Agenda stating that the research agenda of the MLDS Center will focus on what happens to students before and after critical transitions and not on topics that could otherwise be researched by a single partner agency using its own data. The second area of revision was in developing research questions that address obvious gaps in the previously construed Research Agenda. The central additions were research questions focused on the workforce outcomes of students who do not attend postsecondary institutions, but rather go straight from high school to the work force. The revised Research Agenda is attached.

The Research Team has begun to work on the Research Agenda by conducting literature searches and synthesis of available knowledge about several of the Center research questions which will be critical parts of research reports. Researchers have developed drafts of such research syntheses across five of the Center research questions: 1) Early Childcare/Education Workforce, 2) Online education and whether data related to online education should be included in the Center's data, 3) The Efficacy of Developmental/Remedial Education programs in postsecondary education, 4) Financial Aid, and 5) Characteristics of postsecondary institutions that influence timeliness to degree completion. Once the Center has sufficient data to run analyses related to these topics, the reports will be completed.

In addition to the research and studies conducted by the Research Branch, the researchers have had to devote a good deal of time to system and web portal implementation and development issues.

1. Data Collection - To ensure the data collection was comprehensive the researchers went through the entire Common Education Standards (CEDS) data inventories for PK-12, postsecondary, and labor force (more than 5,000 variable elements) and coded what variables were needed in the MLDS Center to do the research required under the Research Agenda. The researchers also documented why those variables were needed, whether that was because a variable was a central factor to the mechanisms of a research outcome of interest, or a variable was a critical co-variate to such critical outcomes, or was needed as a tool in designing and implementing rigorous analyses.
2. Analytic Tools - Researchers have been working with the system development team to make the system accessible and responsive for research purposes. This includes obtaining and properly locating and loading needed analytic software needed and building within the system the needed access to create analytic datasets to be used in response to research questions.
3. Web Portal - The researchers are also an integral part of the process reviewing, revising, and refining dashboards for posting on the website for public access and consumption. The input from

the researcher is critically important to provide expertise in understanding how data are interpreted and best practices at informing the public on how to use (and not misuse) data. This integrated team approach will ensure comprehensive and meaningful information on the website.

Dual Enrollment Report

The Center submitted a report on Dual Enrollment to the Governor and General Assembly as required under Education Article § 24-703.1, Annotated Code of Maryland. The report provides the number of students who are dually enrolled, information about their enrollment, and various demographic information about the population.

Data Determined to be Unnecessary

At this time, no data has been determined to be unnecessary. However, there are elements in the data inventory that have been flagged for further review, and possible removal. However, staff wants to complete additional data analysis and dashboard development prior to making a proposal to the Governing Board to remove data.

In addition to the data in the MLDS, staff is also reviewing the data that is in the P20W system to determine whether it should be, maintained as a separate database, incorporated into the MLDS or purged. A recommendation will be made to the Governing Board in the next year.

Data Inventory

Md. Ed. Art. §24-701(f) defines the permissible types of student and workforce data that the MLDS may collect. Data that falls under that definition and is determined to be necessary to carry out the mission of the Center will be presented to the Governing Board for approval to be included in the data inventory. The *Data Inventory* (attached) represents the complete list of data that the MLDS Center will collect.

Recommendations

The accuracy of information reported by the Maryland Longitudinal Data System is of the utmost importance to the Governing Board and the Center. Accuracy is affected by the quality and completeness of the data received, the ability of the Center to match that data across sectors (early childhood, PK-12, higher education, and workforce), and the manner in which the information is presented to the public.

The Governing Board therefore recommends that the Center develop, for Board review and approval, a set of standards and protocols for assessing the accuracy of information reported to the public. The standards should include:

1. An assessment of whether the data relied upon for a report is sufficiently complete to support the information reported;
2. An assessment of whether the information presented can be reconciled against other sources;
3. Criteria for determining whether information based on incomplete data is appropriate to be reported; and
4. Methods for informing the public regarding the information published by the Center.

The Governing Board recommends that these standards and protocols be established prior to the release of public information from the MLDS.

Attachments

1. Roster of Governing Board Members
2. Data Collection Schedule
3. MLDS Center Organizational Chart
4. Data Security and Safeguarding Plan
    - Rules of Security Behavior
    - Criminal History Background Investigation Policy
    - Security Training Requirements Policy
    - Temporary Staff Appointment Form
    - User System Access Request Form
5. Research Agenda
6. Data Inventory

Attachment 1 – Roster of Governing Board Members

1. Dr. William “Brit” Kirwan, Chancellor of the University System of Maryland (**Chairman**)

2. Dr. Lillian Lowery, State Superintendent of Schools

3. Ms. Catherine Shultz, Acting Secretary of Higher Education

4. Mr. Leonard Howie, Secretary of the Department of Labor, Licensing and Regulation

5. Dr. David Wilson, President of Morgan State University

6. Dr. Bernie Sadusky, Executive Director of the Maryland Association of Community Colleges

7. Tina Bjarekull, President of the Maryland Independent College and University Association

8. Dr. Renee Foose, Superintendent of Howard County Public Schools, (member representing local superintendents of schools)

9. Mr. Steven Rizzi, Vice President of PAR Government (member with expertise in large data systems and data security as required under §24-704(c))

10. Ms. Jennifer Strong Mullinex, Teacher with Howard County Public School

11. Mr. Jason Perkins-Cohen, Executive Director of the Job Opportunities Task Force

12. Mr. Brian Roberts, Change Management Specialist for the Montgomery County Government and parent of a public school student

Attachment 2

Maryland Longitudinal Data System Center

Data Collections 2014-2015

MSDE

Data Collection	Due Dates		Contact
End-of-Year Attendance (EOY Attendance)			Chandra Haislet
MSDE Data Verification Complete	July 17, 2015		
MLDS Center Collection Window	August 1, 2014	October 1, 2014	
Cross Agency Reconciliation	August 1, 2014	September 15, 2014	
Comment Window	September 15, 2014	October 1, 2014	
Linked Data Verification Complete	October 1, 2014		
Agency Sign off Due	October 1, 2014		
High School Status and Completers (HSSC)			Chandra Haislet
MSDE Data Verification Complete	September 15, 2014		
MLDS Center Collection Window	October 1, 2014	December 15, 2014	
Cross Agency Reconciliation	October 1, 2014	December 1, 2014	
Comment Window	December 1, 2014	December 15, 2014	
Linked Data Verification Complete	December 15, 2014		
Agency Sign off Due	December 15, 2014		
End-of-Year Student Course Grade Teacher (SCGT)			Chandra Haislet
MSDE Data Verification Complete	August 7, 2015		
MLDS Center Collection Window	August 15, 2015	October 15, 2015	
Cross Agency Reconciliation	August 15, 2015	October 1, 2015	
Comment Window	October 1, 2015	October 15, 2015	
Linked Data Verification Complete	October 15, 2015		
Agency Sign off Due	October 15, 2015		
College Board Assessments			Chandra Haislet
MSDE Data Verification Complete	October 1, 2014		
MLDS Center Collection Window	October 15, 2014	December 15, 2014	
Cross Agency Reconciliation	October 15, 2014	December 1, 2014	
Comment Window	December 1, 2014	December 15, 2014	
Linked Data Verification Complete	December 15, 2014		
Agency Sign off Due	December 15, 2014		
National Student Clearinghouse			Chandra Haislet
MSDE Data Verification Complete	October 1, 2014		
MLDS Center Collection Window	October 15, 2014	December 15, 2014	
Cross Agency Reconciliation	October 15, 2014	December 1, 2014	
Comment Window	December 1, 2014	December 15, 2014	
Linked Data Verification Complete	December 15, 2014		
Agency Sign off Due	December 15, 2014		

Maryland Longitudinal Data System Center

Data Collections 2014-2015

MHEC

Data Collection	Due Dates		Contact
Enrollment Information System (EIS) Summer Fall			Jon Enriquez
MHEC Data Verification Complete	January 15, 2015		
MLDS Center Collection Window	February 1, 2015	April 1, 2015	
Cross Agency Reconciliation	February 1, 2015	March 15, 2015	
Comment Window	March 15, 2015	April 1, 2015	
Linked Data Verification Complete	April 1, 2015		
Agency Sign off Due	April 1, 2015		
Enrollment Information System (EIS) Winter Spring			Jon Enriquez
MHEC Data Verification Complete	July 15, 2015		
MLDS Center Collection Window	August 1, 2015	October 1, 2015	
Cross Agency Reconciliation	August 1, 2015	September 15, 2015	
Comment Window	September 15, 2015	October 1, 2015	
Linked Data Verification Complete	October 1, 2015		
Agency Sign off Due	October 1, 2015		
Financial Aid Information System (FAIS)			Jon Enriquez
MHEC Data Verification Complete	February 15, 2015		
MLDS Center Collection Window	March 1, 2015	May 1, 2015	
Cross Agency Reconciliation	March 1, 2015	April 15, 2015	
Comment Window	April 15, 2015	May 1, 2015	
Linked Data Verification Complete	May 1, 2015		
Agency Sign off Due	May 1, 2015		
End of Term System (EOTS) Summer Fall			Jon Enriquez
MHEC Data Verification Complete	June 15, 2015		
MLDS Center Collection Window	July 1, 2015	September 1, 2015	
Cross Agency Reconciliation	July 1, 2015	August 15, 2015	
Comment Window	August 15, 2015	September 1, 2015	
Linked Data Verification Complete	September 1, 2015		
Agency Sign off Due	September 1, 2015		
End of Term System (EOTS) Winter Spring			Jon Enriquez
MHEC Data Verification Complete	November 15, 2015		
MLDS Center Collection Window	December 1, 2015	February 1, 2016	
Cross Agency Reconciliation	December 15, 2015	January 15, 2016	
Comment Window	January 15, 2016	February 1, 2016	
Linked Data Verification Complete	February 1, 2016		
Agency Sign off Due	February 1, 2016		
Degree Information System (DIS)			Jon Enriquez
MHEC Data Verification Complete	October 15, 2015		
MLDS Center Collection Window	November 1, 2015	January 1, 2016	
Cross Agency Reconciliation	November 1, 2015	December 15, 2015	
Comment Window	December 15, 2015	January 1, 2016	
Linked Data Verification Complete	January 1, 2016		
Agency Sign off Due	January 1, 2016		

Maryland Longitudinal Data System Center

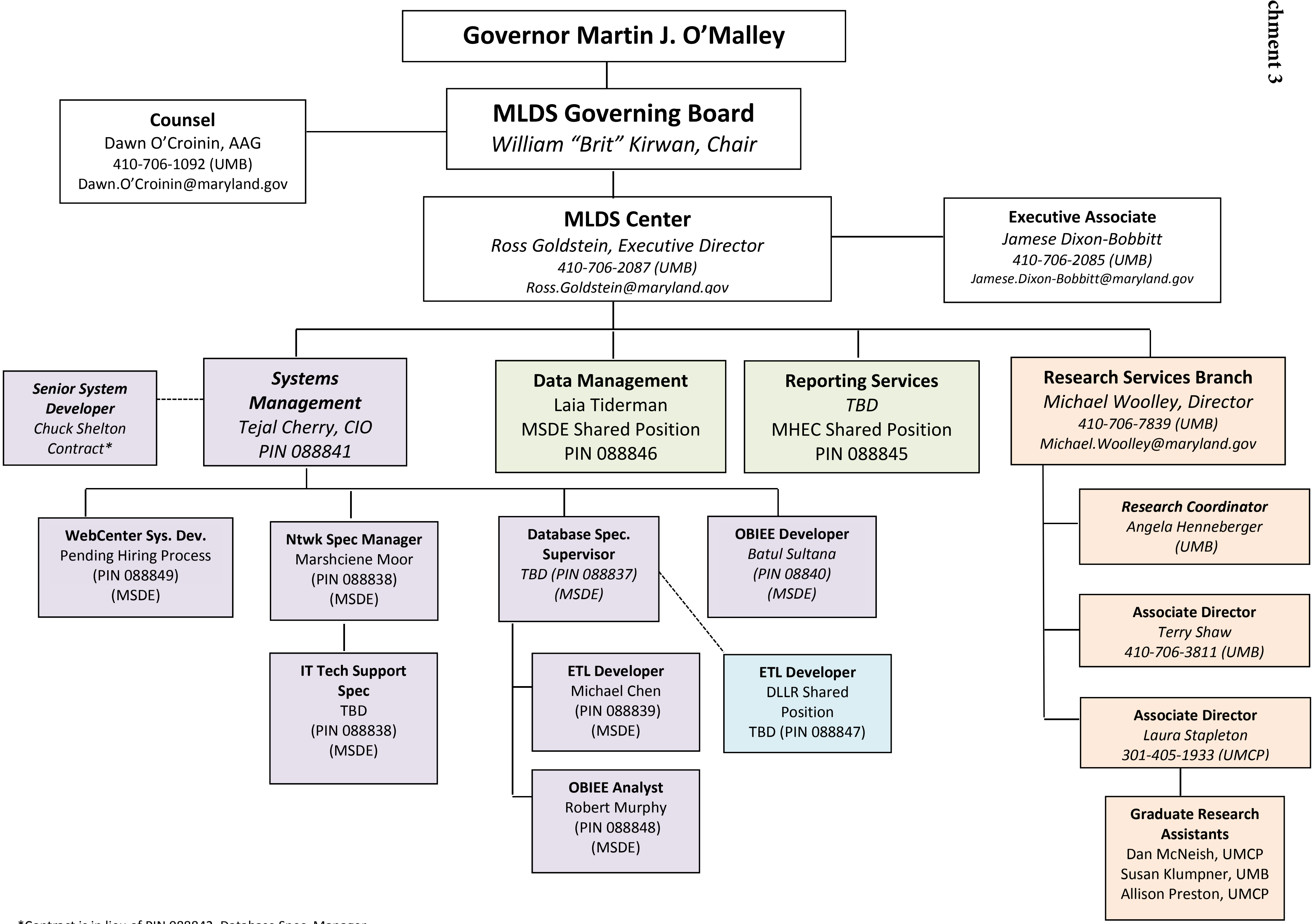
Data Collections 2014-2015

DLLR

Data Collection	Due Dates		Contact
UI Wage/Employer, GED, NEDP, Adult Education and Correctional Education Data Quarter 4			Donni Turner
DLLR Data Verification Complete	December 15, 2014		
MLDS Center Collection Window	March 15, 2015	May 15, 2015	
Cross Agency Reconciliation	March 15, 2015	May 1, 2015	
Comment Window	May 1, 2015	May 15, 2015	
Linked Data Verification Complete	May 15, 2015		
Agency Sign off Due	May 15, 2015		
UI Wage/Employer, GED, NEDP, Adult Education and Correctional Education Data Quarter 1			Donni Turner
DLLR Data Verification Complete	April 15, 2015		
MLDS Center Collection Window	June 15, 2015	August 1, 2015	
Cross Agency Reconciliation	June 15, 2015	July 15, 2015	
Comment Window	July 15, 2015	August 1, 2015	
Linked Data Verification Complete	August 1, 2015		
Agency Sign off Due	August 1, 2015		
UI Wage/Employer, GED, NEDP, Adult Education and Correctional Education Data Quarter 2			Donni Turner
DLLR Data Verification Complete	July 15, 2015		
MLDS Center Collection Window	September 15, 2015	November 1, 2015	
Cross Agency Reconciliation	September 15, 2015	October 15, 2015	
Comment Window	October 15, 2015	November 1, 2015	
Linked Data Verification Complete	November 1, 2015		
Agency Sign off Due	November 1, 2015		
UI Wage/Employer, GED, NEDP, Adult Education and Correctional Education Data Quarter 3			Donni Turner
DLLR Data Verification Complete	October 15, 2015		
MLDS Center Collection Window	December 15, 2015	February 1, 2016	
Cross Agency Reconciliation	December 15, 2015	January 15, 2016	
Comment Window	January 15, 2016	February 1, 2016	
Linked Data Verification Complete	February 1, 2016		
Agency Sign off Due	February 1, 2016		

Attachment 3

Maryland Longitudinal Data System (MLDS)



Governor Martin J. O'Malley

MLDS Governing Board
William "Brit" Kirwan, Chair

Counsel
Dawn O'Croinin, AAG
410-706-1092 (UMB)
Dawn.O'Croinin@maryland.gov

MLDS Center
Ross Goldstein, Executive Director
410-706-2087 (UMB)
Ross.Goldstein@maryland.gov

Executive Associate
Jamese Dixon-Bobbitt
410-706-2085 (UMB)
Jamese.Dixon-Bobbitt@maryland.gov

Senior System Developer
Chuck Shelton
*Contract**

Systems Management
Tejal Cherry, CIO
PIN 088841

Data Management
Laia Tiderman
MSDE Shared Position
PIN 088846

Reporting Services
TBD
MHEC Shared Position
PIN 088845

Research Services Branch
Michael Woolley, Director
410-706-7839 (UMB)
Michael.Woolley@maryland.gov

WebCenter Sys. Dev.
Pending Hiring Process
(PIN 088849)
(MSDE)

Ntwk Spec Manager
Marshciene Moor
(PIN 088838)
(MSDE)

IT Tech Support Spec
TBD
(PIN 088838)
(MSDE)

Database Spec. Supervisor
TBD (PIN 088837)
(MSDE)

OBIEE Developer
Batul Sultana
(PIN 08840)
(MSDE)

ETL Developer
Michael Chen
(PIN 088839)
(MSDE)

ETL Developer
DLLR Shared Position
TBD (PIN 088847)

OBIEE Analyst
Robert Murphy
(PIN 088848)
(MSDE)

Research Coordinator
Angela Henneberger
(UMB)

Associate Director
Terry Shaw
410-706-3811 (UMB)

Associate Director
Laura Stapleton
301-405-1933 (UMCP)

Graduate Research Assistants
Dan McNeish, UMCP
Susan Klumpner, UMB
Allison Preston, UMCP

*Contract is in lieu of PIN 088842, Database Spec. Manager.

Attachment 4

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)

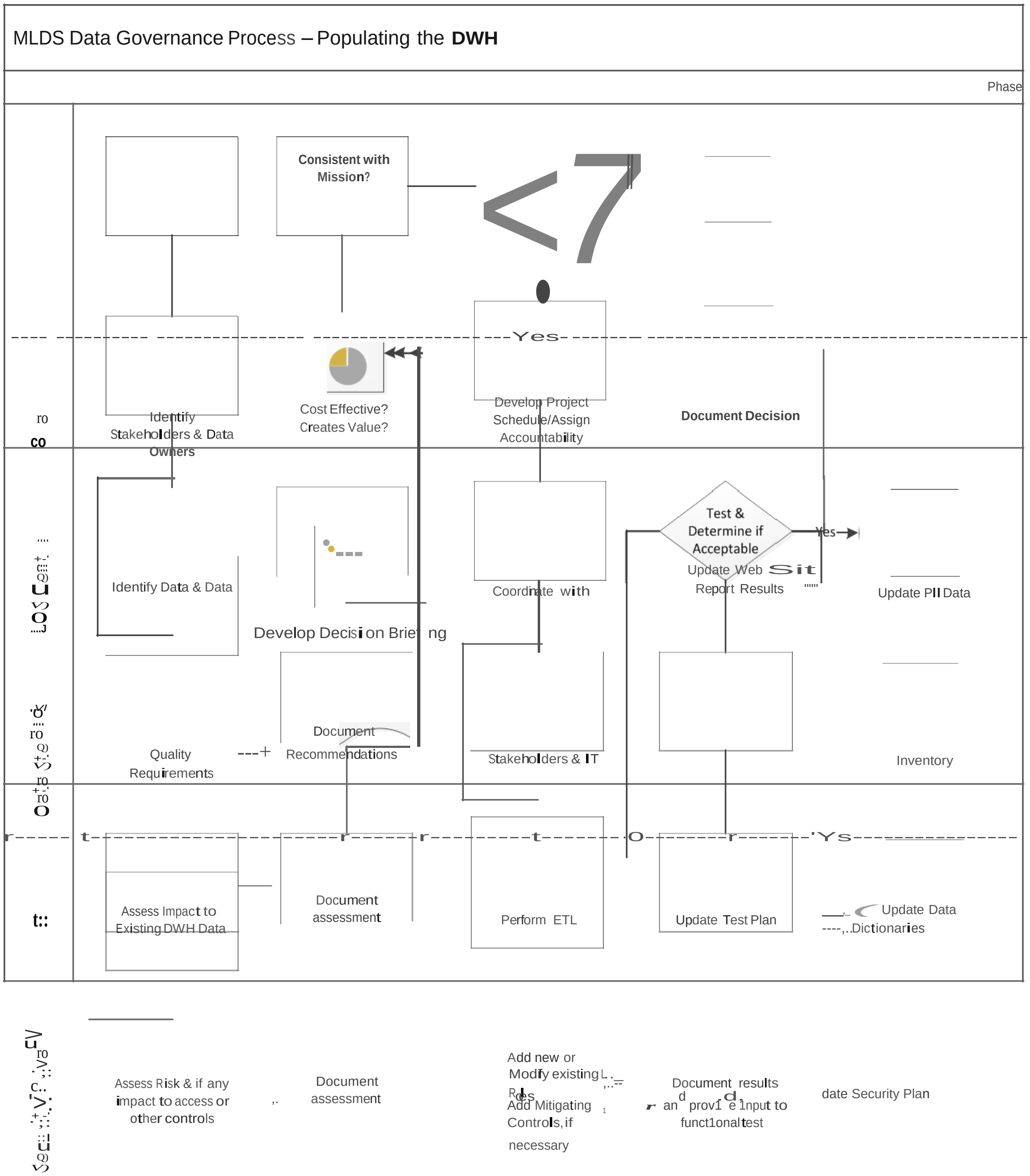
Workforce data -- data relating to: **(I)** Employment status; (2) Wage information; (3) Geographic location of employment; and (4) Employer information. (MD Education Article § 24-701)

10 Record of Revisions

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

11 Background Information

11.1 Data Governance Workflow


MLDS Data Governance Process – Populating the DWH
Phase
Consistent with Mission?
Yes
Identify Stakeholders & Data Owners
Cost Effective? Creates Value?
Develop Project Schedule/Assign Accountability
Document Decision
Test & Determine if Acceptable
Yes
Update Web Site
Report Results
Identify Data & Data
Develop Decision Briefing
Coordinate with
Update PII Data
Quality Requirements
Document Recommendations
Stakeholders & IT
Inventory
Yes
Assess Impact to Existing DWH Data
Document assessment
Perform ETL
Update Test Plan
Update Data Dictionaries
Assess Risk & if any impact to access or other controls
Document assessment
Add new or Modify existing Roles
Add Mitigating Controls, if necessary
Document results and provide input to functional test
date Security Plan

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

Rules of Security Behavior for MLDS Center Staff

This form must be completed and filed with the MLDS Center Executive Associate within 5 days of becoming staff of the Center. Please read this document carefully. After reviewing the document, please sign and date. You must sign and date this in the presence of a current MLDS staff member. The staff member will serve as your witness and must sign on the appropriate line. If you are unable to have a staff member serve as a witness, a notary can serve as your witness.

Name: ______________________ Affiliation: ______________________

Address ______________________ City, State ZIP ______________________

Phone: ______________________ Email: ______________________

For purposes of this document:

1. "Confidential information" means:
    a. Any information about the data system, including database design or schematics that are proprietary or if disclosed could compromise system security;
    b. Education data that contains personally identifiable information, de-identified individual records, or aggregate records that may be identifiable based on the size or uniqueness of the population; or
    c. Workforce data that reveals the name, address, social security number, or any other identifying particular of an individual or employer or could foreseeably be combined with other publicly available information to reveal such particulars.
2. "Data System" means all hardware and software that constitutes the Maryland Longitudinal Data System, including the Master Data Management System, the Operational Data Store, the Data Warehouse, storage devices, and other components.
3. "MLDS Center staff" includes the following types of individuals regardless of whether they are paid by the Center:
    a. A contractual or permanent employee of the MLDS Center;
    b. An individual approved by the Executive Director to serve as a MLDS Center staff member for a specified time and duration; and
    c. A contractor or vendor.

MLDS Center staff shall:

1. Complete all required security training within 10 business days of:
    a. Being hired or starting a staff appointment;
    b. The assignment of additional training by the Executive Director; or
    c. Each anniversary of being hired or starting a staff appointment;
2. Review the MLDS Center *Data Security and Safeguarding Plan* and act in conformity with that plan and documents referenced therein;
3. Consistent with the *Policy for Conducting Criminal History Background Investigations*, submit to all necessary Criminal History Background Investigations and receive authorization before having access to sensitive or confidential information, materials or equipment;
4. Not share passwords or provide unauthorized access to the data system;
5. Not disclose any confidential information;

6. Not make written notes about confidential data;
7. Only access confidential information on a computer and at a location that has been pre-approved by the MLDS Center Executive Director and consistent with the *Data Security and Safeguarding Plan* and documents referenced therein;
8. Not download confidential information from the data system unless required for research analysis and done pursuant to a procedure pre-approved by the MLDS Center Executive Director and consistent with the *Data Security and Safeguarding Plan* and documents referenced therein;
9. Not discuss confidential information with any person other than appropriate MLDS Center staff; and
10. Report any actual or potential risk or vulnerability that may compromise the security of confidential information to the MLDS Center Executive Director or a Branch Director.

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

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

Printed Name of Employee Signature Date

Printed Name of Witness Signature Date

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

Policy for Conducting Criminal History Background Investigations

Purpose

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

Legal Authority

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

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

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

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

Background

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

Applicability

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

Policy

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

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

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

Required Security Training for MLDS Center Staff

August 8, 2014

Under the *Rules of Security Behavior* MLDS Center staff members agree to complete all required security training within 10 business days of:

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

Classes

□ Security Awareness – staff will be assigned one of the following:

- Security Awareness Training by Security Mentor ® (staff will be emailed information for logging on and taking the training program).

  or

- Cyber Security Awareness training for Department of Defense Employees*. The course may be found at http://iase.disa.mil/eta/cyberchallenge/launchPage.htm. There are several options listed. Please make sure to select the top option for Department of Defense Employees. Please note that this course should be taken using Windows Internet Explorer. Other browsers may have trouble producing the certificate of completion.

□ FERPA 101* course located at http://ptac.ed.gov. You will be required to create a login and password in order to take the course. The prompt for login will appear once you click on the course name.

□ FERPA 201* course located at http://ptac.ed.gov. You will be required to create a login and password in order to take the course. The prompt for login will appear once you click on the course name.

** Provide a copy of the certificates of completion to Jamese Dixon-Bobbitt.*

Reference Materials and Resources for Review

- Family Education and Privacy Act (20 U.S.C. §1232g) and regulations (34 CFR Part 99).

- Privacy Technical Assistance Center (PTAC) provides resources for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems.
  - Data Governance Checklist
  - FERPA Exceptions Summary
- Federal-State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information (20 CFR 603).
- *Maryland State Information Technology Security Policy and Standards*

- U.S. Department of Commerce, National Institute of Standards and Technology (NIST)
  - *Recommended Security Controls for Federal Information Systems and Organizations* - (SP 800-53, Revision 4)
  - *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* – *(SP* 800-53A*)*
  - *Guide to Protecting the Confidentiality of Personally Identifiable Information* - (Special Publication (SP 800-122)

- NCES Publications
  - *Concepts and Definitions for Privacy and Confidentiality in Student Education Records*
  - *Managing Personally Identifiable Information in Electronic Student Educations Records*.
  - *Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting*

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

Temporary Staff Appointment

A temporary staff appointment may only be made by a MLDS Center Branch Director as necessary to assist in the work of the Center. A temporary staff appointment is necessary for an individual who is not an MLDS Center PIN employee and who will be working directly with the longitudinal data system maintained by the Center. In addition, like all other MLDS Center employees, the temporary staff member will have to sign the Rules of Security Behavior, complete a criminal history background check, review and comply with the Data Security and Safeguarding Plan, and complete required security training.

Appointee: ____ **Affiliation:** ________________________

Appointed by: ___________________________________ ___________________________________
Branch Director Signature

Term: *(beginning)* ______________________ *(ending)* ______________________

Reason for appointment:

□ Research Services

□ IT Support Services

□ Other: ______________________

Approved by: ____
Ross Goldstein, Executive Director

Version 1.0

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

User Access Request Form

Part 1. Requester

Name: ______________________________________ Affiliation: _________________________

Email: ______________________________________ Phone: ____________________________

Status: [] MLDS Center PIN Employee

[] ~~Temporary~~ Staff Appointment - __________________________
Appointment End Date

Name of supervisor or branch director who appointed you: ________________________________

Business Need for Access to System*

*Access will be restricted to only what is expressly needed for the person to fulfill the stated business needs. Accordingly, please provide a complete description of the business need to ensure the appropriate access is established.

Based on the business needs described above, please select the access most applicable for you:

- □ Application developer access - all server environments and all data
- □ Researcher access - Operational Data Store, Data Warehouse, and OBIEE Cubes only
- □ Developer access - Operational Data Store and Data Warehouse only
- □ Analyst access - OBIEE Cubes only
- □ Network Administrator Access

Method of System Access

Hardware: (check all that apply)

[] Desktop computer issued by: ____

[] Laptop computer issued by: ____

[] Tablet computer issued by: ____

Network: (check all that apply)

[] Internal – MSDE

[] External – MSDE Wireless Network

[] External – Research Institution LAN

[] External – Research Institution Wireless Network

[] External – Home LAN

[] External – Home Wireless Network

Users may only access the MLDS with the computers and via the networks indicated on this form. If the user has indicated that he or she will be using a wireless network, the user will be required to provide the system administrator with the type of security set-up applied to that network.

Requested Access Duration

Beginning: _____________________ Ending: _______________________

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

____ _______________________
Requester's Signature Date

Part 2. Confirmations

Security

The Requester has completed all of the following security requirements:

- □ The Requester is staff of the MLDS Center.
- □ The Requester has completed the Rules of Security Behavior.
- □ The Requester has had a Criminal History Background Check and does not have a history that would prohibit him/her from obtaining system access.
- □ The Requester has completed all required security training.

____ _______________________
Jamese Dixon-Bobbitt Date

Supervisor Review

I agree that the stated business needs are accurate and the requested access duration is necessary for the requester to carry out the assigned duties.

____ _______________________
Supervisor or Branch Director Date

Part 3. System Administrator

Check all of the functional user groups and access privilege necessary for this user.

□ Management	□ Read Only	□ Read/Write
□ System Support	□ Read Only	□ Read/Write
□ DBA Group	□ Read Only	□ Read/Write
□ VMWare Administration Group	□ Read Only	□ Read/Write
□ OBIEE Administration Group	□ Read Only	□ Read/Write
□ OBIEE Developer Group	□ Read Only	□ Read/Write
□ Researcher Group	□ Read Only	□ Read/Write
□ OWB Administration Group	□ Read Only	□ Read/Write
□ OWB Developer Group	□ Read Only	□ Read/Write
□ WebCenter Administration Group	□ Read Only	□ Read/Write
□ WebCenter Internal Group	□ Read Only	□ Read/Write
□ WebCenter Public Group	□ Read Only	□ Read/Write
□ LDAP Administration Group	□ Read Only	□ Read/Write
□ WebMethods Administration Group	□ Read Only	□ Read/Write

Assigned Access Duration: ____________________ to _____________________
Beginning Ending

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

____ ________________________
System Administrator Date

Final Approval

Executive Director: ______________________________________ Date: ___________________________

MARYLAND LONGITUDINAL DATA SYSTEM CENTER RESEARCH AGENDA

The Maryland Longitudinal Data System (MLDS) provides the ability to examine student preparation, progress and outcomes over time, across PreK-12, postsecondary education and training, and the workforce. Establishing the Research Agenda is the duty of the MLDS Governing Board (see Ed. Art. § 24-704(g)(5), Annotated Code of Maryland). This revised Research Agenda reflects the Governing Board's commitment to longitudinal analyses of critical education and workforce transitions and outcomes. Accordingly, the research agenda of the MLDS Center will focus on what happens to students before and after critical transitions and not on topics that could otherwise be researched by one partner agency using its own data.

To that end, all research analyses, and therefore research reports intended to inform policy and programming, will utilize data from at minimum two of the three partner agencies providing data to the MLDS Center:

1) Maryland State Department of Education;
2) Maryland Higher Education Commission; and
3) Department of Labor, Licensing, and Regulation.

For example, all analyses of the postsecondary readiness, access, persistence and completion will be examined, when available, in the context of the academic experiences, achievement, and life circumstances of Maryland students in the PreK-12 education system and/or prior workforce experiences. Similarly, all analyses of the workforce transition or outcomes will be conducted in the context of the academic experiences, achievement, and life circumstances of Marylanders, which may include PreK-12 data, postsecondary education or training data, or both, as well as prior workforce experiences.

The Center research analyses may also include data from sources other than these three agencies as the Center grows and the sources of data expand.

Finally, all research analyses of each of the following research questions will include examinations of how results vary by different critical student subgroups and backgrounds (which is MLDS – Question 15). Such subgroups and backgrounds, for example, include: 1) race or ethnicity, 2) gender, 3) socioeconomic status, 4) language, 5) ability, and 6) setting.

A. Postsecondary Readiness and Access

1. Are Maryland students academically prepared to enter postsecondary institutions and complete their programs in a timely manner? (MLDS – Q1 – P20W priority)
2. What percentage of Maryland high school exiters go on to enroll in Maryland postsecondary education? (MLDS– Q2)
3. What percentage of Maryland high school exiters entering college are assessed to need to take developmental courses and in what content areas? (MLDS – Q3 – P20W priority)
4. Which financial aid programs are most effective in improving access and success (i.e., retention and graduation) for Maryland students?(MLDS – Q9 – P20W priority)
5. Assess the need for inclusion of online education data. (SLDS Grant Q5.2)

B. Postsecondary Completion

6. How likely are students placed in developmental courses to persist in postsecondary education and transfer and/or graduate? (MLDS – Q4)
7. Are community college students able to transfer within the state to 4-year institutions successfully and without loss of credit? (MLDS – Q5 – P20W priority)
8. What are the differences in performance, retention, and graduation, including time to degree, of students who initially matriculate at a Maryland community college and transfer to a Maryland 4-year institution versus those who initially matriculate at a Maryland 4-year? (MLDS Q7)
9. What are the differences in performance, retention and graduation, including time to degree, of students beginning in dual enrollment programs, at 2-year institutions and at 4-year institutions? (MLDS Q8)
10. What are the characteristics of 2-year institutions that are allowing students to persist most effectively and either graduate or transfer? (MLDS Q10)
11. Which 4-year institutions are graduating students most effectively and in the timeliest fashion? (MLDS Q11)

C. Workforce Outcomes

12. What happens to students who start at community colleges and do not go on to 4-year institutions? (MLDS Q6)
13. What are the educational and labor market outcomes for individuals who use federal and state resources to obtain training at community colleges or other postsecondary institutions? (MLDS Q12)
14. What economic value do noncredit community college credentials have in the workplace? (MLDS Q13)
15. Are exiters of Maryland colleges successful in the workforce? (MLDS Q9 – P20W priority)
16. Assess STEM post-graduate student state and regional job acceptance and retention. (SLDS Grant Q5.1)
17. Assess training and retention of early childhood workforce in Maryland. (SLDS Grant Q5.3)
18. What are the workforce outcomes for Maryland students who earn a high school diploma (via high school graduation or GED®) but do not transition to postsecondary education or training? (new)
19. What are the workforce outcomes for Maryland high school students who complete Career Technical Education coursework, who either enter the workforce directly or also obtain postsecondary education or training? (new)
20. What are the workforce outcomes of Maryland high school non-completers? (new)

MARYLAND STATE LONGITUDINAL DATA SYSTEM (MLDS)

DATA INVENTORY

DECEMBER 18, 2014

Table of Contents

1. Overview

The Maryland Longitudinal Data System (MLDS) data warehouse blends select P-12, postsecondary, and workforce data to analyze Maryland student trends in college and career readiness. The MLDS Governing Board is required to submit an Annual Report under Md. Ed. Art. §24-704(g)(6) to create an inventory of individual student and workforce data Approved to be maintained in the system and generally serves to inform the general public about the contents of the MLDS database.

This document provides the complete inventory of data and is organized by domain. Domains include Workforce, Postsecondary, K12 and external data sources such as the Integrated Postsecondary Education Data System (IPEDS) and U.S. Census Bureau (Census).

Data elements in the MLDS database are mapped to the Common Education Data Standards (CEDS Version 4.0) when possible. CEDS represents a national, collaborative effort to develop voluntary, common data standards across the P-20W pipeline and provides nationally recognized naming conventions and definitions. Where data cannot be mapped to CEDS 4.0 standards, alternate domain, entity, and element names are provided, if applicable.

Data Entities and Data Elements identified with Approval Status of ‘Approved’ are Approved for approval by the MLDS Governing Board for collection by the MLDS Center.

Approved data elements are included in the Data Inventory with an Availability date that the data is expected to be available to the MLDS. Data elements with no Availability date are already included in the MLDS.

Source indicates the origin of the data for the specific Domain. This may be the name of the data collection administered by the agency or the table name. The source is specific to the agency providing the data to the MLDS.

Data Loaded and Active provides an indication of the status of the data element within the MLDS. Further explanation for Inactive data elements is provided in the Comments.

Additional columns specific to the domain are included to provide greater meaning and understanding of the data elements.

The MLDS Center staff appreciates the continued collaboration of staff at DLLR, MSDE and MHEC, the Data Advisory Group members, and the Research and Policy Board members.

Workforce

Workforce domain data is provided to the MLDS from the Department of Labor, Licensing and Regulation (DLLR).

2. Workforce Data Entities

The following Workforce domain data entities are approved or Approved for inclusion in the MLDS Data Inventory:

- Quarterly Employment
- W Employer
- W Person
- Adult Education

3. Workforce Data Elements

The following Workforce domain data elements are approved or Approved for inclusion in the MLDS Data Inventory:

Workforce Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
NA	W Employer	Agency Source System Identification Name	Approved		UI_Tax	MDM	Active	
1156	W Employer	Organization Type	Approved		UI_Tax	ODS, MDM	Active	
631	W Employer	Organization Name	Approved		UI_Tax	ODS, MDM	Active	
1071	W Employer	EIN: Federal Employer Identification Number	Approved		UI_Tax	MDM	Active	
1071	W Employer	Maryland State Employer Account Number	Approved		UI_Tax	MDM	Active	
1064	W Employer	NAICS Code	Approved		UI_Tax	ODS	Active	
269	W Employer	Address Line 1	Approved		UI_Tax	ODS	Active	
40	W Employer	Address City	Approved		UI_Tax	ODS	Active	
267	W Employer	Employer State	Approved		UI_Tax	ODS	Active	
214	W Employer	Employer Zip Code	Approved		UI_Tax	ODS	Active	
214	W Employer	Employer Zip Code Plus Four	Approved		UI_Tax	ODS	Active	
NA	W Employer	Liability Date	Approved		UI_Tax	ODS	Active	
NA	W Person	Agency Source System Identification Name	Approved		UI_Claimant	MDM	Active	
1071	W Person	Social Security Number (SSN)	Approved		UI_Claimant	MDM	Active	
115	W Person	Claimant First Name	Approved		UI_Claimant	MDM	Active	
184	W Person	Claimant Middle Name	Approved		UI_Claimant	MDM	Active	

Workforce Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
172	W Person	Claimant Last Name	Approved		UI_Claimant	MDM	Active	
NA	W Person	Date of Birth	Approved		UI_Claimant	MDM	Active	
NA	W Person	Telephone Number	Approved		UI_Claimant	MDM	Inactive	This data element will not be used and/or loaded
NA	W Person	Gender	Approved		UI_Claimant	MDM	Active	
NA	W Person	Race	Approved		UI_Claimant	MDM	Active	
NA	W Person	Address Line 1	Approved		UI_Claimant	MDM	Inactive	Staging Area for matching, will use for matching in ODI
NA	W Person	Address Line 2	Approved		UI_Claimant	MDM	Inactive	
NA	W Person	City	Approved		UI_Claimant	MDM	Inactive	
990	W Person	State	Approved		UI_Claimant	MDM	Inactive	
NA	W Person	Zip Code	Approved		UI_Claimant	MDM	Inactive	
NA	W Person	Zip Code Plus Four	Approved		UI_Claimant	MDM	Inactive	
NA	Quarterly Employment	Agency Source System Identification Name	Approved		Quarterly Wage File	MDM	Active	
259	Quarterly Employment	Employee Social Security Number	Approved		Quarterly Wage File	MDM	Active	
NA	Quarterly Employment	Employee Name Validation	Approved		Quarterly Wage File		Inactive	This data element will not be used and/or loaded
NA	Quarterly Employment	Employer Maryland Account Number	Approved		Quarterly Wage File	MDM	Active	
NA	Quarterly Employment	Wage Year and Quarter	Approved		Quarterly Wage File	ODS	Active	

Workforce Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
989	Quarterly Employment	Wage Amount	Approved		Quarterly Wage File	ODS	Active	
NA	Quarterly Employment	Employer Name	Approved		Quarterly Wage File	ODS	Active	
NA	Quarterly Employment	Employer Address	Approved		Quarterly Wage File	ODS	Active	
NA	Quarterly Employment	Employer Address Line 1	Approved		Quarterly Wage File	ODS	Active	
NA	Quarterly Employment	Employer Address Line 2	Approved		Quarterly Wage File	ODS	Active	
NA	Quarterly Employment	Employer Address Line 3	Approved		Quarterly Wage File		Inactive	This data element will not be used and/or loaded
40	Quarterly Employment	Employer City	Approved		Quarterly Wage File	ODS	Active	
267	Quarterly Employment	Employer State	Approved		Quarterly Wage File	ODS	Active	
214	Quarterly Employment	Employer Zip Code	Approved		Quarterly Wage File	ODS	Active	
214	Quarterly Employment	Employer Zip Code Zone	Approved		Quarterly Wage File	ODS	Active	
NA	Quarterly Employment	Employer Zip Code Bar Code	Approved		Quarterly Wage File		Inactive	This data element will not be used and/or loaded

Workforce Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
NA	Quarterly Employment	Employer Zip Code Carrier Code	Approved		Quarterly Wage File		Inactive	This data element will not be used and/or loaded
NA	Quarterly Employment	Employer Phone Number	Approved		Quarterly Wage File	ODS	Inactive	
172	W Person	Name (FIRST NAME, MIDDLE NAME, LAST NAME, GENERATIONAL SUFFIX)	Approved	2015	GED	MDM	Active	
269	W Person	Address (ADDRESS LINE1, ADDRESS LINE 2, CITY, STATE, ZIP CODE, ZIP +4)	Approved	2015	GED	MDM	Active	
33	W Person	If Awarded Diploma (GED award date)	Approved	2015	GED	MDM, ODS	Active	
1071	W Person	Social Security Number (SSN)	Approved	2015	GED	MDM	Inactive	This data is being prepared by DLLR and has not been transmitted yet.
33	W Person	Date of Birth	Approved	2015	GED	MDM	Inactive	
255	W Person	Gender	Approved	2015	GED	MDM	Inactive	
NA	W Person	Test Date	Approved	2015	GED	MDM, ODS	Inactive	
21	W Person	Subject/ Module	Approved	2015	GED	ODS	Inactive	
115	AE Student	First Name	Approved	2015	NEDP	MDM	Inactive	
184	AE Student	Middle Name	Approved	2015	NEDP	MDM	Inactive	
172	AE Student	Last Name	Approved	2015	NEDP	MDM	Inactive	
1071	AE Student	Date Of Birth	Approved	2015	NEDP	MDM	Inactive	
33	AE Student	Social Security Number (SSN)	Approved	2015	NEDP	MDM	Inactive	
NA	AE Student	NEDP Diploma Site	Approved	2015	NEDP	ODS	Inactive	
NA	AE Student	Diploma Number	Approved	2015	NEDP		Inactive	

Workforce Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
81	AE Student	Diploma Date	Approved	2015	NEDP	ODS	Inactive	This data is being prepared by DLLR and has not been transmitted yet.
115	AE Student	First Name	Approved	2015	Correctional Education	MDM	Inactive	
184	AE Student	Middle Name	Approved	2015	Correctional Education	MDM	Inactive	
172	AE Student	Last Name	Approved	2015	Correctional Education	MDM	Inactive	
1071	AE Student	Social Security Number (SSN)	Approved	2015	Correctional Education	MDM	Inactive	
NA	AE Student	Age	Approved	2015	Correctional Education		Inactive	
301, 34, 20, 16, 192, 974	AE Student	Race	Approved	2015	Correctional Education	MDM	Inactive	
783	AE Student	If Awarded Certificate	Approved	2015	Correctional Education	ODS	Inactive	
115	AE Student	First Name	Approved	2015	Adult Education	MDM	Inactive	
184	AE Student	Middle Name	Approved	2015	Adult Education	MDM	Inactive	
172	AE Student	Last Name	Approved	2015	Adult Education	MDM	Inactive	
1071	AE Student	Social Security Number (SSN)	Approved	2015	Adult Education	MDM	Inactive	

Workforce Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
33	AE Student	Date Of Birth	Approved	2015	Adult Education	MDM	Inactive	This data is being prepared by DLLR and has not been transmitted yet.
1288	AE Student	Name of Instructional Program	Approved	2015	Adult Education	MDM	Inactive	
255	AE Student	Gender	Approved	2015	Adult Education	MDM/ODS	Inactive	

PK12

PK12 domain data is provided to the MLDS from the Maryland State Department of Education (MSDE).

4. PK12 Data Entities

The following PK12 domain data entities are approved or Approved for inclusion in the MLDS Data Inventory:

- Assessments
- EL Organization
- EL Staff
- K12 Class/Section
- K12 Course
- K12 Organization
- K12 School
- K12 Staff
- K12 Student
- LEA
- PS Institution
- PS Student

5. PK12 Data Elements

The following PK12 domain data elements are approved or Approved for inclusion in the MLDS Data Inventory:

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
131	K12 School	Grades Offered	Approved		School Data Set	ODS /MDM	Active	
242	K12 School	School Type	Approved		School Data Set	ODS /MDM	Active	
181	K12 School	Magnet or Special Program Emphasis School	Approved		School Data Set	ODS /MDM	Active	
39	K12 School	Charter School Indicator	Approved		School Data Set	ODS /MDM	Active	
710	K12 School	Charter School Type	Approved		School Data Set	ODS /MDM	Active	
533	K12 School	School Operational Status	Approved		School Data Set	ODS /MDM	Active	
257	K12 School	Shared Time Indicator	Approved		School Data Set	ODS /MDM	Active	
284	K12 School	Title I Program Type	Approved		School Data Set	ODS	Active	
497	K12 School	First Instruction Date	Approved		School Data Set	ODS	Active	
496	K12 School	Days In Session	Approved		School Data Set		Inactive	Not yet loaded
1156	LEA	Organization Type	Approved		School Data Set	ODS	Active	

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
1066	LEA	Address Type for Organization	Approved		School Data Set	ODS	Active	
19	LEA	Address Apartment Room or Suite Number	Approved		School Data Set	ODS	Active	
40	LEA	Address City	Approved		School Data Set	ODS	Active	
1209	LEA	County ANSI Code	Approved		School Data Set	ODS	Active	
97	K12 Student	Enrollment Entry Date	Approved		Attendance	ODS	Inactive	Not yet loaded
714	K12 Student	Kindergarten Program Participation Type	Approved		Attendance	ODS	Inactive	Not yet loaded
94	K12 Student	Enrollment Status	Approved		Attendance	ODS	Inactive	Not yet loaded
100	K12 Student	Entry Grade Level	Approved		Attendance	ODS	Inactive	Not yet loaded
99	K12 Student	Entry Type	Approved		Attendance	ODS	Inactive	Not yet loaded
107	K12 Student	Exit Date	Approved		Attendance	ODS	Inactive	Not yet loaded
1210	K12 Student	Exit Grade Level	Approved		Attendance	ODS	Inactive	Not yet loaded
110	K12 Student	Exit or Withdrawal Type	Approved		Attendance	ODS	Inactive	Not yet loaded
108	K12 Student	Exit or Withdrawal Status	Approved		Attendance	ODS	Inactive	Not yet loaded
46	K12 Student	Cohort Year	Approved		Attendance	MDM/ODS	Inactive	Not yet loaded
584	K12 Student	Cohort Graduation Year	Approved		Attendance	MDM/ODS	Inactive	Not yet loaded
138	K12 Student	High School Diploma Type	Approved		Attendance	ODS	Active	

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
93	K12 Student	End of Term Status	Approved		Attendance		Inactive	Not yet loaded
530	K12 Student	Promotion Reason	Approved		Attendance		Inactive	Not yet loaded
531	K12 Student	Non-promotion Reason	Approved		Attendance		Inactive	Not yet loaded
202	K12 Student	Number of Days in Attendance	Approved		Attendance		Inactive	Not yet loaded
201	K12 Student	Number of Days Absent	Approved		Attendance		Inactive	Not yet loaded
325	K12 Student	Participation in School Food Service Programs	Approved		Attendance	ODS	Inactive	Not yet loaded
149	K12 Student	Homelessness Status	Approved		Attendance	ODS	Inactive	Not yet loaded
147	K12 Student	Homeless Serviced Indicator	Approved		Attendance	ODS	Inactive	Not yet loaded
590	K12 Student	Program Participation Start Date	Approved		Attendance	ODS	Inactive	Not yet loaded
591	K12 Student	Program Participation Exit Date	Approved		Attendance	ODS	Inactive	Not yet loaded
570	K12 Student	Limited English Proficiency Exit Date	Approved		Attendance	ODS	Inactive	Not yet loaded
NA	K12 Student	Life Status	Approved		Attendance	ODS	Active	
115	K12 Staff	First Name	Approved		Staff	MDM	Inactive	Not yet loaded
184	K12 Staff	Middle Name	Approved		Staff	MDM	Inactive	Not yet loaded
172	K12 Staff	Last or Surname	Approved		Staff	MDM	Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
121	K12 Staff	Generation Code or Suffix	Approved		Staff	MDM	Inactive	Not yet loaded
206	K12 Staff	Other Name	Approved		Staff	MDM	Inactive	Not yet loaded
1070	K12 Staff	Staff Member Identifier	Approved		Staff	MDM	Inactive	Not yet loaded
33	K12 Staff	Birthdate	Approved		Staff	MDM	Inactive	Not yet loaded
255	K12 Staff	Sex	Approved		Staff	ODS, MDM	Inactive	Not yet loaded
16	K12 Staff	American Indian or Alaska Native	Approved		Staff	ODS, MDM	Inactive	Not yet loaded
20	K12 Staff	Asian	Approved		Staff	ODS, MDM	Inactive	Not yet loaded
34	K12 Staff	Black or African American	Approved		Staff	ODS, MDM	Inactive	Not yet loaded
192	K12 Staff	Native Hawaiian or Other Pacific Islander	Approved		Staff	ODS, MDM	Inactive	Not yet loaded
301	K12 Staff	White	Approved		Staff	ODS, MDM	Inactive	Not yet loaded
144	K12 Staff	Hispanic or Latino Ethnicity	Approved		Staff	ODS, MDM	Inactive	Not yet loaded
1068	K12 Staff	Local Education Agency Identifier	Approved		Staff	MDM	Inactive	Not yet loaded
1069	K12 Staff	School Identifier	Approved		Staff	MDM	Inactive	Not yet loaded
645	K12 Staff	Teaching Assignment Start Date	Approved		Staff	ODS	Inactive	Not yet loaded
646	K12 Staff	Teaching Assignment End Date	Approved		Staff	ODS	Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
87	K12 Staff	Education Staff Classification	Approved		Staff	ODS	Inactive	Not yet loaded
525	K12 Staff	Primary Assignment Indicator	Approved		Staff	ODS	Inactive	Not yet loaded
622	K12 Staff	Classroom Position Type	Approved		Staff	ODS	Inactive	Not yet loaded
220	K12 Staff	Professional Educational Job Classification	Approved		Staff	ODS	Inactive	Not yet loaded
558	K12 Staff	Special Education Staff Category	Approved		Staff	ODS	Inactive	Not yet loaded
264	K12 Staff	Special Education Teacher	Approved		Staff	ODS	Inactive	Not yet loaded
283	K12 Staff	Title I Program Staff Category	Approved		Staff	ODS	Inactive	Not yet loaded
71	K12 Staff	Credential Type	Approved		Staff	ODS	Active	
277	K12 Staff	Teaching Credential Basis	Approved		Staff	ODS	Inactive	Not yet loaded
302	K12 Staff	Years of Prior Teaching Experience	Approved		Staff	ODS	Inactive	Not yet loaded
141	K12 Staff	Highest Level of Education Completed	Approved		Staff	ODS	Inactive	Not yet loaded
142	K12 Staff	Highly Qualified Teacher Indicator	Approved		Staff	ODS	Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
207	K12 Staff	Paraprofessional Qualification Status	Approved		Staff	ODS	Inactive	Not yet loaded
32	K12 Staff	Staff Compensation Base Salary	Approved		Staff	ODS	Inactive	Not yet loaded
589	K12 Staff	Faculty and Administration Performance Level	Approved		Staff	ODS	Inactive	Not yet loaded
67	K12 Course	Course Title	Approved		SCGT	ODS	Inactive	Not yet loaded
55	K12 Course	Course Identifier	Approved		SCGT	ODS	Inactive	Not yet loaded
56	K12 Course	Course Code System	Approved		SCGT	ODS	Inactive	Not yet loaded
517	K12 Course	Course Description	Approved		SCGT	ODS	Inactive	Not yet loaded
246	K12 Course	Secondary Course Identifier	Approved		SCGT	ODS	Inactive	Not yet loaded
247	K12 Course	Secondary Course Level	Approved		SCGT	ODS	Inactive	Not yet loaded
248	K12 Course	Secondary Course Subject Area	Approved		SCGT	ODS	Inactive	Not yet loaded
57	K12 Course	Course Credit Units	Approved		SCGT	ODS	Inactive	Not yet loaded
58	K12 Course	Course Credit Value	Approved		SCGT	ODS	Inactive	Not yet loaded
137	K12 Course	High School Course Requirement	Approved		SCGT	ODS	Inactive	Not yet loaded
448	K12 Course	Instruction Language	Approved		SCGT	ODS	Inactive	Not yet loaded
518	K12 Course	Core Academic Course	Approved		SCGT	ODS	Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
1385	K12 Course	K12 Course Grade Level	Approved		SCGT	ODS	Inactive	Not yet loaded
1386	K12 Course	K12 End of Course Requirement	Approved		SCGT	ODS	Inactive	Not yet loaded
978	K12 Class/ Section	Class Section Identifier	Approved		SCGT	ODS	Inactive	Not yet loaded
251	K12 Class/ Section	Session Begin Date	Approved		SCGT	ODS	Inactive	Not yet loaded
253	K12 Class/ Section	Session End Date	Approved		SCGT	ODS	Inactive	Not yet loaded
252	K12 Class/ Section	Session Designator	Approved		SCGT	ODS	Inactive	Not yet loaded
448	K12 Class/ Section	Instruction Language	Approved		SCGT	ODS	Inactive	Not yet loaded
517	K12 Class/ Section	Course Description	Approved		SCGT	ODS	Inactive	Not yet loaded
1385	K12 Class/ Section	K12 Course Grade Level	Approved		SCGT		Inactive	Not yet loaded
90	K12 Class/ Section	Prior to Secondary Course Identifier	Approved		SCGT	ODS	Inactive	Not yet loaded
1159	K12 Class/ Section	Prior to Secondary Course Subject Area	Approved		SCGT	ODS	Inactive	Not yet loaded
247	K12 Class/ Section	Secondary Course Level	Approved		SCGT		Inactive	SCED course level
246	K12 Class/ Section	Secondary Course Identifier	Approved		SCGT	ODS	Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
248	K12 Class/ Section	Secondary Course Subject Area	Approved		SCGT	ODS	Inactive	Not yet loaded
61	K12 Class/ Section	Course Level Characteristic	Approved		SCGT		Inactive	Not yet loaded
72	K12 Class/ Section	Credit Type Earned	Approved		SCGT		Inactive	Not yet loaded
60	K12 Class/ Section	Course Grade Point Average Applicability	Approved		SCGT		Inactive	Not yet loaded
1071	K12 Class/ Section	Student Identifier	Approved		SCGT	MDM	Active	
1075	K12 Class/ Section	Student Identification System	Approved		SCGT		Inactive	Not yet loaded
97	K12 Class/ Section	Enrollment Entry Date	Approved		SCGT	ODS	Inactive	Not yet loaded
125	K12 Class/ Section	Grade Level When Course Taken	Approved		SCGT		Inactive	Not yet loaded
182	K12 Class/ Section	Marking Period Name	Approved		SCGT	ODS	Inactive	Not yet loaded
124	K12 Class/ Section	Grade Earned	Approved		SCGT	ODS	Inactive	Not yet loaded
1070	K12 Class/ Section	Staff Member Identifier	Approved		SCGT	ODS	Active	
1074	K12 Class/ Section	Staff Member Identification System	Approved		SCGT		Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
526	K12 Class/ Section	Assignment Start Date	Approved		SCGT	ODS	Inactive	Not yet loaded
527	K12 Class/ Section	Assignment End Date	Approved		SCGT	ODS	Inactive	Not yet loaded
648	K12 Class/ Section	Teaching Assignment Role	Approved		SCGT	ODS	Inactive	Not yet loaded
28	Assessments	Assessment Title	Approved		Assessments	ODS	Inactive	Not yet loaded
29	Assessments	Assessment Type	Approved		Assessments	ODS	Inactive	Not yet loaded
21	Assessments	Assessment Academic Subject	Approved		Assessments	ODS	Inactive	Not yet loaded
177	Assessments	Assessment Level for Which Designed	Approved		Assessments		Inactive	Not yet loaded
26	Assessments	Assessment Purpose	Approved		Assessments		Inactive	Not yet loaded
415	Assessments	Assessment Type Administered to Children With Disabilities	Approved		Assessments	ODS	Inactive	Not yet loaded
369	Assessments	Assessment Subtest Score Metric Type	Approved		Assessments		Inactive	Not yet loaded
933	Assessments	Assessment Family Short Name	Approved		Assessments		Inactive	Not yet loaded
932	Assessments	Assessment Family Title	Approved		Assessments	ODS	Inactive	Not yet loaded
24	Assessments	Assessment Form Name	Approved		Assessments		Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
366	Assessments	Assessment Form Number	Approved		Assessments		Inactive	Not yet loaded
1185	Assessments	Assessment Form Accommodation List	Approved		Assessments		Inactive	Not yet loaded
1187	Assessments	Assessment Form Intended Administration End Date	Approved		Assessments		Inactive	Not yet loaded
1068	Assessments	Local Education Agency Identifier	Approved		Assessments	ODS	Active	
1069	Assessments	School Identifier	Approved		Assessments	ODS	Active	
573	Assessments	Proficiency Status	Approved		Assessments		Inactive	Not yet loaded
245	Assessments	Assessment Subtest Result Score Value	Approved		Assessments		Inactive	Not yet loaded
126	Assessments	Grade Level When Assessed	Approved		Assessments		Inactive	Not yet loaded
383	Assessments	Assessment Accommodation Category	Approved		Assessments		Inactive	Not yet loaded
1016	Assessments	Assessment Registration Retest Indicator	Approved		Assessments		Inactive	Not yet loaded
228	Assessments	Reason Not Tested	Approved		Assessments		Inactive	Not yet loaded
717	Assessments	Assessment Performance Level Identifier	Approved		Assessments		Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
718	Assessments	Assessment Performance Level Label	Approved		Assessments		Inactive	Not yet loaded
418	Assessments	Assessment Performance Level Lower Cut Score	Approved		Assessments	ODS	Inactive	Not yet loaded
419	Assessments	Assessment Performance Level Upper Cut Score	Approved		Assessments	ODS	Inactive	Not yet loaded
269	EL Organization	Address Street Number and Name	Approved		CCATS	ODS	Active	
269	EL Organization	Address Apartment Room or Suite Number	Approved		CCATS	ODS	Active	
40	EL Organization	Address City	Approved		CCATS	ODS	Active	
267	EL Organization	State Abbreviation	Approved		CCATS	ODS	Active	
214	EL Organization	Address Postal Code	Approved		CCATS	ODS	Active	
19	EL Organization	Address County Name	Approved		CCATS	ODS	Active	
1209	EL Organization	County ANSI Code	Approved		CCATS	ODS	Active	
NA		Country Code	Approved		CCATS	ODS	Active	
279	EL Organization	Telephone Number	Approved		CCATS		Inactive	Not yet loaded
865	EL Organization	State Licensed Facility Capacity	Approved		CCATS		Inactive	Not yet loaded
828	EL Organization	Early Learning Program Licensing Status	Approved		CCATS		Inactive	Not yet loaded

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
348	EL Organization	Initial License Date	Approved		CCATS		Inactive	Not yet loaded
354	EL Organization	Authorized Hours Per Day	Approved		CCATS		Inactive	Not yet loaded
355	EL Organization	Authorized Days Per Week	Approved		CCATS		Inactive	Not yet loaded
115	EL Staff	First Name	Approved		CCATS	MDM	Active	
184	EL Staff	Middle Name	Approved		CCATS	MDM	Active	
172	EL Staff	Last or Surname	Approved		CCATS	MDM	Active	
121	EL Staff	Generation Code or Suffix	Approved		CCATS	MDM	Active	
1070	EL Staff	Staff Member Identifier	Approved		CCATS	MDM	Active	
269	EL Staff	Address Street Number and Name	Approved		CCATS	ODS	Inactive	Not yet loaded
19	EL Staff	Address Apartment Room or Suite Number	Approved		CCATS	ODS	Inactive	Not yet loaded
40	EL Staff	Address City	Approved		CCATS	ODS	Inactive	Not yet loaded
267	EL Staff	State Abbreviation	Approved		CCATS	ODS	Inactive	Not yet loaded
214	EL Staff	Address Postal Code	Approved		CCATS	ODS	Inactive	Not yet loaded
190	EL Staff	Address County Name	Approved		CCATS	ODS	Active	
50	EL Staff	Country Code	Approved		CCATS	ODS	Active	
279	EL Staff	Telephone Number	Approved		CCATS	ODS	Inactive	Not yet loaded
33	EL Staff	Birth date	Approved		CCATS	MDM	Active	
255	EL Staff	Gender	Approved		CCATS	MDM	Active	
16	EL Staff	American Indian or	Approved		CCATS	MDM	Active	

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
		Alaska Native						
20	EL Staff	Asian	Approved		CCATS	MDM	Active	
34	EL Staff	Black or African American	Approved		CCATS	MDM	Active	
192	EL Staff	Native Hawaiian or Other Pacific Islander	Approved		CCATS	MDM	Active	
301	EL Staff	White	Approved		CCATS	MDM	Active	
144	EL Staff	Hispanic or Latino Ethnicity	Approved		CCATS	MDM	Active	
343	EL Staff	Degree or Certificate Type	Approved		CCATS	ODS	Active	
141	EL Staff	Highest Level of Education Completed	Approved		CCATS	ODS	Inactive	Not yet loaded
347	EL Staff	Employment Status	Approved		CCATS	ODS	Inactive	Not yet loaded
213	EL Staff	Employment Position	Approved		CCATS	ODS	Inactive	Not yet loaded
346	EL Staff	Position Start Date	Approved		CCATS	ODS	Inactive	Not yet loaded
795	EL Staff	Position End Date	Approved		CCATS	ODS	Inactive	Not yet loaded
1072	K12 Organization	LEA	Approved	2015	NSC	MDM	Inactive	This data is being prepared by MSDE and has not been transmitted yet.
1069	K12 School	School	Approved	2015	NSC	ODS	Inactive	
1071	K12 Student	State Assigned Student Identifier (SASID)	Approved	2015	NSC	MDM	Inactive	
1072	K12 Student	Local Education Agency Identifier	Approved	2015	NSC	MDM	Inactive	

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
1072	K12 Student	Last Name	Approved	2015	NSC	MDM	Inactive	This data is being prepared by MSDE and has not been transmitted yet.
115	K12 Student	First Name	Approved	2015	NSC	MDM	Inactive	
184	K12 Student	Middle Name	Approved	2015	NSC	MDM	Inactive	
121	K12 Student	Generational Suffix	Approved	2015	NSC	MDM	Inactive	
33	K12 Student	Date of Birth	Approved	2015	NSC	MDM	Inactive	
1210	K12 Student	Student's Grade	Approved	2015	NSC		Inactive	
255	K12 Student	Gender	Approved	2015	NSC	MDM	Inactive	
144	K12 Student	Ethnicity	Approved	2015	NSC	MDM	Inactive	
301, 34, 20, 16, 192, 974	K12 Student	Race	Approved	2015	NSC	MDM	Inactive	
259	K12 Student	Social Security Number	Approved	2015	NSC	MDM	Inactive	
243	K12 Student	Academic Year	Approved	2015	NSC	ODS	Inactive	
1242	K12 Student	Special Education Status	Approved	2015	NSC	ODS	Inactive	
180	K12 Student	Limited English Proficiency Status	Approved	2015	NSC	ODS	Inactive	
92	K12 Student	Participation in School Food Service Programs	Approved	2015	NSC	ODS	Inactive	
281	K12 Student	Title I	Approved	2015	NSC	ODS	Inactive	
577	K12 Student	ADA Status	Approved	2015	NSC	ODS	Inactive	
185	K12 Student	Migrant Status	Approved	2015	NSC	ODS	Inactive	
110	K12 Student	Exit or Withdrawal Type	Approved	2015	NSC	ODS	Inactive	

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
108	K12 Student	Exit or Withdrawal Status	Approved	2015	NSC	ODS	Inactive	This data is being prepared by MSDE and has not been transmitted yet.
107	K12 Student	Exit or Withdrawal Date	Approved	2015	NSC	ODS	Inactive	
545	K12 Student	High School Diploma Flag	Approved	2015	NSC	ODS	Inactive	
892	K12 Student	High School Certificate Flag	Approved	2015	NSC	ODS	Inactive	
893	K12 Student	High School Program Completion	Approved	2015	NSC	ODS	Inactive	
NA		Record Found Flag	Approved	2015	NSC		Inactive	
NA		Collection Date	Approved	2015	NSC		Inactive	
NA		Collection Type	Approved	2015	NSC		Inactive	
NA		Search Date	Approved	2015	NSC		Inactive	
166	PS Institution	College Code	Approved	2015	NSC	ODS	Inactive	
167	PS Institution	College Branch	Approved	2015	NSC	ODS	Inactive	
204	PS Institution	College Name	Approved	2015	NSC	ODS	Inactive	
267	PS Institution	College State	Approved	2015	NSC	ODS	Inactive	
178	PS Institution	College Type Code	Approved	2015	NSC	ODS	Inactive	
48	PS Institution	Collge Public Flag	Approved	2015	NSC	ODS	Inactive	
NA		College Sequence	Approved	2015	NSC		Inactive	
98	PS Student	College Enrollment Begin Date	Approved	2015	NSC	ODS	Inactive	
107	PS Student	Collge Enrollment End Date	Approved	2015	NSC	ODS	Inactive	
96	PS Student	College Enrollment Status Code	Approved	2015	NSC	ODS	Inactive	

PK12 Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
1312	PS Student	College Class Level	Approved	2015	NSC	ODS	Inactive	This data is being prepared by MSDE and has not been transmitted yet.
43	PS Student	Enrollment Major 1	Approved	2015	NSC	ODS	Inactive	
43	PS Student	Enrollment CIP 1	Approved	2015	NSC	ODS	Inactive	
43	PS Student	Enrollment Major 2	Approved	2015	NSC	ODS	Inactive	
43	PS Student	Enrollment CIP 2	Approved	2015	NSC	ODS	Inactive	
NA	PS Student	College Graduate Flag	Approved	2015	NSC		Inactive	
344	PS Student	College Graduate Date	Approved	2015	NSC	ODS	Inactive	
342	PS Student	Degree Title	Approved	2015	NSC	ODS	Inactive	
342	PS Student	Degree Major 1	Approved	2015	NSC		Inactive	
342	PS Student	Degree CIP 1	Approved	2015	NSC	ODS	Inactive	
342	PS Student	Degree Major 2	Approved	2015	NSC		Inactive	
342	PS Student	Degree CIP 2	Approved	2015	NSC	ODS	Inactive	
342	PS Student	Degree Major 3	Approved	2015	NSC		Inactive	
342	PS Student	Degree CIP 3	Approved	2015	NSC	ODS	Inactive	
342	PS Student	Degree Major 4	Approved	2015	NSC		Inactive	
342	PS Student	Degree CIP 4	Approved	2015	NSC	ODS	Inactive	
110	PS Student	High School Exit Tupe	Approved	2015	NSC	ODS	Inactive	
NA		MD College Concurrent Enrollee	Approved	2015	NSC	ODS	Inactive	

Postsecondary

Postsecondary domain data is provided to the MLDS from the Maryland Higher Education Commission (MHEC).

6. Postsecondary Data Entities

The following Postsecondary domain data entities are approved or Approved for inclusion in the MLDS Data Inventory:

- PS Institution
- PS Student

7. Postsecondary Data Elements

The following Postsecondary domain data elements are approved or Approved for inclusion in the MLDS Data Inventory:

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
46	PS Institution	Collection Year	Approved		MHEC_9	ODS	Active	
NA	PS Institution	Collection Term	Approved		MHEC_9	ODS	Active	
745	PS Institution	Tuition - Published	Approved	Future	MHEC_9	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
746	PS Institution	Tuition Unit	Approved	Future	MHEC_9	ODS	Inactive	
753	PS Institution	Price of Attendance	Approved	Future	MHEC_9	ODS	Inactive	
NA	PS Student	Geographic Origin	Approved	Future	MHEC_9	MDM	Inactive	
79	PS Student	Dependency Status	Approved	Future	MHEC_9	MDM	Inactive	
NA	PS Student	Tuition Status	Approved	Future	MHEC_9	MDM	Inactive	
NA	PS Student	Commuter Status	Approved	Future	MHEC_9	MDM	Inactive	
NA	PS Student	Father's Educational Attainment	Approved	Future	MHEC_9	MDM	Inactive	
NA	PS Student	Mother's Educational Attainment	Approved	Future	MHEC_9	MDM	Inactive	
265	PS Student	SAT Math Score	Approved	Future	MHEC_9	ODS	Inactive	
265	PS Student	SAT Verbal Score	Approved	Future	MHEC_9	ODS	Inactive	
NA	PS Student	ACT English Score	Approved	Future	MHEC_9	ODS	Inactive	
NA	PS Student	ACT Math Score	Approved	Future	MHEC_9	ODS	Inactive	
NA	PS Student	ACT Reading Score	Approved	Future	MHEC_9	ODS	Inactive	
NA	PS Student	ACT Science Reading Score	Approved	Future	MHEC_9	ODS	Inactive	
NA	PS Student	ACT Composite Score	Approved	Future	MHEC_9	ODS	Inactive	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
265	PS Student	SAT Writing Score	Approved	Future	MHEC_9	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
265	PS Student	Admission Test Flag	Approved		MHEC_9		Inactive	
NA	PS Student	Term Credit Hours Attempted	Approved		MHEC_9	ODS	Active	
NA	PS Student	Term Native Credit Hours Earned	Approved		MHEC_9	ODS	Active	
35	PS Student	Commuter Status	Approved		MHEC_9		Inactive	This data is being prepared by MHEC and has not been transmitted yet
NA	PS Student	Expected Family Contribution	Approved		MHEC_9		Inactive	
753	PS Student	Cost of Attendance	Approved		MHEC_9		Inactive	
113	PS Student	Aid Category Award Code	Approved		MHEC_9		Inactive	
112	PS Student	Aid Category Award Amount	Approved		MHEC_9		Inactive	
NA	PS Student	Adjusted Gross Income	Approved		MHEC_9		Inactive	
166	PS Student	OPEID (FICE + 2),	Approved		MHEC_9	MDM	Active	
18	PS Student	External Credits Awarded	Approved		MHEC_9		Inactive	This data is being prepared by MHEC and has not been transmitted yet.
NA	PS Student	Teacher Candidate	Approved		MHEC_9		Inactive	
166	PS Student	OPEID (FICE + 2)	Approved		MHEC_9	MDM	Active	
1075	PS Student	School Identification System	Approved		IPEDS		Inactive	This data is being prepared by MHEC and has not been transmitted yet.

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
NA	PS Student	High School Code (College Board)	Approved		MHEC_9	MDM	Active	
117	PS Student	First Time Flag,	Approved		MHEC_9		Inactive	This data is being prepared by MHEC and has not been transmitted yet.
46	PS Student	Collection Year,	Approved		MHEC_9	ODS	Active	
727	PS Student	Collection Term	Approved		MHEC_9	ODS	Active	
166	PS Student	OPEID(FICE + 2)	Approved	2014	MHEC_4	MDM	Active	
214	PS Student	Application Zip Code	Approved	2014	MHEC_4	MDM	Active	
214	PS Student	Application Zip Code + 4	Approved	2014	MHEC_4	MDM	Active	
NA	PS Student	Current Zip Code	Approved	2014	MHEC_4	MDM	Active	
NA	PS Student	Current Zip Code + 4	Approved	2014	MHEC_4	MDM	Active	
297	PS Student	Residency Code	Approved	2014	MHEC_4	MDM	Active	
43	PS Student	Degree Sought	Approved	2014	MHEC_4	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
727	PS Student	Term Attendance	Approved	2014	MHEC_4	ODS	Inactive	
1308	PS Student	Distance Education Enrollment	Approved	2014	MHEC_4		Inactive	
NA	PS Student	Distance Education Location	Approved	2014	MHEC_4		Inactive	
NA	PS Student	High School Graduation Date	Approved	2014	MHEC_4	ODS	Active	
NA	PS Student	High School GPA	Approved	2014	MHEC_4	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
166	PS Student	Sending OPEID (FICE)	Approved	2014	MHEC_4	MDM	Active	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
NA	PS Student	Freeze Flag	Approved	2014	MHEC_4		Inactive	This data is being prepared by MHEC and has not been received yet.
259	PS Student	Identification Number (SSN)	Approved	2014	MHEC_2	MDM	Active	
NA	PS Student	Identification Number Type	Approved	2014	MHEC_2	MDM	Active	
1071	PS Student	SASID	Approved	2014	MHEC_2	MDM	Active	
NA	PS Student	Program Taxonomy	Approved	2014	MHEC_2	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
NA	PS Student	First Major Link	Approved	2014	MHEC_2	ODS	Inactive	
NA	PS Student	Cumulative GPA	Approved	2014	MHEC_2	ODS	Inactive	
NA	PS Student	Cumulative Native Credits Earned	Approved	2014	MHEC_2	ODS	Inactive	
NA	PS Student	Cumulative Degree Credits Hours Awarded	Approved	2014	MHEC_2	ODS	Inactive	
NA	PS Student	Entry Year	Approved	2014	MHEC_2	ODS	Inactive	
NA	PS Student	Reverse Transfer Flag	Approved	2014	MHEC_2	ODS	Inactive	
NA	PS Student	Credit Hours Required to Earn Award	Approved	2014	MHEC_2	ODS	Inactive	
NA	PS Student	Gender	Approved	2014	MHEC_2	MDM	Active	
299	PS Student	US Citizenship	Approved	2014	MHEC_2	MDM	Active	
144	PS Student	Hispanic/ Latino Ethnicity	Approved	2014	MHEC_2	MDM	Active	
301	PS Student	White	Approved	2014	MHEC_2	MDM	Active	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
34	PS Student	Black/African American	Approved	2014	MHEC_2	MDM	Active	
20	PS Student	Asian	Approved	2014	MHEC_2	MDM	Active	
16	PS Student	American Indian/ Native Alaskan	Approved	2014	MHEC_2	MDM	Active	
192	PS Student	Native Hawaiian/ Pac. Is.	Approved	2014	MHEC_2	MDM	Active	
727	PS Student	Collection Term	Approved	2014	MHEC_5	ODS	Active	
46	PS Student	Collection Year	Approved	2014	MHEC_5	ODS	Active	
166	PS Student	OPEID(FICE + 2)	Approved	2014	MHEC_5	MDM	Active	
259	PS Student	Identification Number (SSN)	Approved	2014	MHEC_5	MDM	Active	
NA	PS Student	Identification Number Type	Approved	2014	MHEC_5	MDM	Active	
NA	PS Student	SASID	Approved	2014	MHEC_5	MDM	Active	
NA	PS Student	Term Native Credit Hours Registered	Approved	2014	MHEC_5	ODS	Active	
NA	PS Student	Term Native Degree Credit Hours Attempted	Approved	2014	MHEC_5	ODS	Active	
127	PS Student	Term GPA	Approved	2014	MHEC_5	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
NA	PS Student	Cumulative Native Credit Hours Earned	Approved	2014	MHEC_5	ODS	Active	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
NA	PS Student	Cumulative GPA	Approved	2014	MHEC_5	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
NA	PS Student	Cumulative Credit Hours Awarded	Approved	2014	MHEC_5	ODS	Inactive	
NA	PS Student	Term Academic Standing	Approved	2014	MHEC_5	ODS	Inactive	
727	PS Student	Collection Term	Approved	2014	MHEC_3	ODS	Active	
46	PS Student	Collection Year	Approved	2014	MHEC_3	ODS	Active	
166	PS Student	OPEID(FICE + 2)	Approved	2014	MHEC_3			
259	PS Student	Identification Number (SSN)	Approved	2014	MHEC_3	MDM	Active	
NA	PS Student	Identification Number Type	Approved	2014	MHEC_3	MDM	Active	
1071	PS Student	SASID	Approved	2014	MHEC_3	MDM	Active	
727	PS Student	Collection Term	Approved	2014	MHEC_6	ODS	Active	
46	PS Student	Collection Year	Approved	2014	MHEC_6	ODS	Active	
166	PS Student	OPEID(FICE + 2)	Approved	2014	MHEC_6	MDM	Active	
259	PS Student	Identification Number (SSN)	Approved	2014	MHEC_6	MDM	Active	
1075	PS Student	Identification Number Type	Approved	2014	MHEC_6	MDM	Active	
1071	PS Student	SASID	Approved	2014	MHEC_6	MDM	Active	
255	PS Student	Gender	Approved	2014	MHEC_6	ODS	Active	
363	PS Student	Financial Aid Application Status	Approved	2014	MHEC_6		Inactive	This data is being prepared by MHEC and has not been transmitted yet.
96	PS Student	Fall Attendance	Approved	2014	MHEC_6		Inactive	
96	PS Student	Spring Attendance	Approved	2014	MHEC_6		Inactive	
1415	PS Student	Family Size	Approved	2014	MHEC_6	ODS	Active	
299	PS Student	US Citizenship	Approved	2014	MHEC_6	ODS	Active	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
144	PS Student	Hispanic/Latino Ethnicity	Approved	2014	MHEC_6	ODS	Active	
301	PS Student	White	Approved	2014	MHEC_6	ODS	Active	
34	PS Student	Black/African American	Approved	2014	MHEC_6	ODS	Active	
20	PS Student	Asian	Approved	2014	MHEC_6	ODS	Active	
16	PS Student	American Indian/ Native Alaskan	Approved	2014	MHEC_6	ODS	Active	
192	PS Student	Native Hawaiian/ Pac. Is.	Approved	2014	MHEC_6	ODS	Active	
259	PS Student	Social Security Number (SSN)	Approved	2014	MHEC_7	MDM	Active	
115	PS Student	First Name	Approved	2014	MHEC_7	MDM	Active	
184	PS Student	Middle Name	Approved	2014	MHEC_7	MDM	Active	
1072	PS Student	Last Name	Approved	2014	MHEC_7	MDM	Active	
121	PS Student	Generational Suffix	Approved	2014	MHEC_7	MDM	Active	
243	PS Student	School Year	Approved	2014	MHEC_7	ODS	Active	
178	PS Institution	Organization Level	Approved	2014	MHEC_7	ODS	Active	
191	PS Institution	Organization Long Name	Approved	2014	MHEC_7	ODS/MDM	Active	
1487	PS Institution	Organization Short Name	Approved	2014	MHEC_7	ODS/MDM	Active	
1069	PS Institution	Local School ID	Approved	2014	MHEC_7	MDM	Active	
NA	PS Institution	MHEC State Identification Code (SIC)	Approved	2014	MHEC_7	ODS	Active	
269	PS Institution	Address Line 1	Approved	2014	MHEC_7	ODS	Active	
19	PS Institution	Address Line 2	Approved	2014	MHEC_7	ODS	Active	
40	PS Institution	City	Approved	2014	MHEC_7	ODS	Active	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
267	PS Institution	State	Approved	2014	MHEC_7	ODS	Active	
214	PS Institution	Zip Code	Approved	2014	MHEC_7	ODS	Active	
1209	PS Institution	County	Approved	2014	MHEC_7	ODS	Active	
727	PS Student	Collection Term	Approved	*Pending – 2016 Target	MHEC_1	ODS	Active	
46	PS Student	Collection Year	Approved	*Pending – 2016 Target	MHEC_1	ODS	Active	
166	PS Student	OPEID(FICE + 2)	Approved	*Pending – 2016 Target	MHEC_1	MDM	Active	
1502	PS Student	Course Subject	Approved	*Pending – 2016 Target	MHEC_1	ODS	Active	
1314	PS Student	Course Number	Approved	*Pending – 2016 Target	MHEC_1	ODS	Active	
1315	PS Student	Section Number	Approved	Pending – 2016 Target	MHEC_1	ODS	Active	
96	PS Student	Full-time or Part-time Status Instructor	Approved	*Pending – 2016 Target	MHEC_1	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
346	PS Student	Date of Initial Employment of Instructor	Approved	*Pending – 2016 Target	MHEC_1	ODS	Inactive	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
730	PS Student	Principal Occupational Assignment of Instructor	Approved	*Pending – 2016 Target	MHEC_1	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
739	PS Student	Academic Tenure Status of Instructor	Approved	Pending – 2016 Target	MHEC_1	ODS	Inactive	
NA	PS Student	Highest Degree Attained by Instructor	Approved	Pending – 2016 Target	MHEC_1	ODS	Inactive	
277	PS Student	Appointment Status of Instructor	Approved	Pending – 2016 Target	MHEC_1	ODS	Inactive	
NA	PS Student	Remedial Math	Approved	Pending – 2016 Target	MHEC_1	ODS	Inactive	
NA	PS Student	Remedial English	Approved	Pending – 2016 Target	MHEC_1	ODS	Inactive	
NA	PS Student	Remedial Reading	Approved	Pending – 2016 Target	MHEC_1	ODS	Inactive	
1308	PS Student	Instruction Type	Approved	Pending – 2016 Target	MHEC_1	ODS	Inactive	
NA	PS Student	Instructional Location	Approved	Pending – 2016 Target	MHEC_1	ODS	Inactive	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
NA	PS Student	Collection Term	Approved	Pending – 2016 Target	MHEC_8	ODS	Active	
NA	PS Student	Collection Year	Approved	Pending – 2016 Target	MHEC_8	ODS	Active	
166	PS Student	OPEID(FICE + 2)	Approved	Pending – 2016 Target	MHEC_8	MDM	Active	
259	PS Student	Identification Number (SSN)	Approved	Pending – 2016 Target	MHEC_8	MDM	Active	
1075	PS Student	Identification Number Type	Approved	Pending – 2016 Target	MHEC_8	MDM	Active	
1071	PS Student	SASID	Approved	Pending – 2016 Target	MHEC_8	ODS	Active	
1502	PS Student	Course Subject	Approved	Pending – 2016 Target	MHEC_8	ODS	Active	
1314	PS Student	Course Number	Approved	Pending – 2016 Target	MHEC_8	ODS	Active	
1315	PS Student	Section Number	Approved	Pending – 2016 Target	MHEC_8	ODS	Active	

Postsecondary Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	Database	Data Loaded and Active	Comments
58	PS Student	Course Hours	Approved	Pending – 2016 Target	MHEC_8	ODS	Active	
57	PS Student	Course Hour Type Flag	Approved	Pending – 2016 Target	MHEC_8	ODS	Inactive	This data is being prepared by MHEC and has not been transmitted yet.
NA	PS Student	Entry-Level Credit-Bearing Math	Approved	Pending – 2016 Target	MHEC_8	ODS	Inactive	
NA	PS Student	Entry-Level Credit-Bearing English	Approved	Pending – 2016 Target	MHEC_8	ODS	Inactive	
1299	PS Student	Course Outcome	Approved	Pending – 2016 Target	MHEC_8	ODS	Inactive	

External Domains

External domain data is acquired by the MLDS from the Integrated Postsecondary Education Data System (IPEDS) and U.S. Census Bureau (Census).

8. IPEDS Data Entities

The following IPEDS domain data entities are approved or Approved for inclusion in the MLDS Data Inventory:

- Financial Aid
- Institutional Characteristics
- PS Institution
- Tuition

9. IPEDS Data Elements

The following IPEDS domain data elements are approved or Approved for inclusion in the MLDS Data Inventory:

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
NA	PS Institution	Collection Year	Approved	2015	IPEDS	Academic Year	ODS	Inactive
NA	PS Institution	Organization Level	Approved	2015	IPEDS	Level of Institution	ODS	Inactive
NA	PS Institution	Organization Long Name	Approved	2015	IPEDS	Institution/Group name in TCS Online	ODS/MDM	Inactive
NA	PS Institution	Organization Short Name	Approved	2015	IPEDS	Institution Name	ODS/MDM	Inactive
1069	PS Institution	Local School ID	Approved	2015	IPEDS	Unit ID	ODS	Inactive
NA		Parent Organization Identifier	Approved	2015	IPEDS	Unit ID Linchpin	ODS/MDM	Inactive
NA	PS Institution	MHEC State Identification Code (SIC)	Approved	2015	IPEDS	ANSI code	ODS	Inactive
40	PS Institution	City	Approved	2015	IPEDS	City	ODS	Inactive
267	PS Institution	State	Approved	2015	IPEDS	State	ODS	Inactive
214	PS Institution	Zip Code	Approved	2015	IPEDS	Zip	ODS	Inactive
NA	PS Institution	Organization Type	Approved	2015	IPEDS	Sector of Institution	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Control	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
NA	Institutional Characteristics		Approved	2015	IPEDS	Geographic Region	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Carnegie Classification 2005	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Carnegie Classification 2005 (Collapsed)	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Carnegie Classification 2005 by Sector	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Land grant institution status	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Historically Black College or University status	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Hispanic Serving Institution status	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of applicants	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of applicants - male	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of applicants - female	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of admissions	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of admissions - male	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of admissions - female	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of first-time degree/certificate-seeking	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
						undergraduates		
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of first-time degree/certificate-seeking male undergraduates	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Total number of first-time degree/certificate-seeking female undergraduates	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Number of first-time degree/certificate-seeking applications received	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Number of first-time degree/certificate-seeking students admitted	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Number of first-time, full-time degree/certification-seeking enrolling full-time	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Number of part-time first-time degree/certificate-seeking students enrolled	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Number of first-time degree/certificate-seeking students submitting ACT scores	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Percentage of first-time degree/certificate-seeking students submitting ACT scores	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
NA	Institutional Characteristics		Approved	2015	IPEDS	Number of first-time degree/certificate-seeking students submitting SAT scores	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Percentage of first-time degree/certificate-seeking students submitting SAT scores	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	SAT Math 25th percentile score	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	SAT Math 75th percentile score	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	SAT Critical Reading 25th percentile score	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	SAT Critical Reading 75th percentile score	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	Regional Compact	ODS	Inactive
NA	Institutional Characteristics		Approved	2015	IPEDS	HECA Index	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Number of full-time first-time degree/certificate-seeking undergraduates receiving any aid	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Percentage of full-time first-time	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
						degree/certificate-seeking undergraduates receiving any aid		
NA	Financial Aid		Approved	2015	IPEDS	Number of full-time first-time degree/certificate-seeking undergraduates receiving federal grants	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Percentage of full-time first-time degree/certificate-seeking undergraduates receiving federal grants	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Average amount of federal grants received by full-time first-time degree/certificate-seeking undergraduates	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Number of full-time first-time degree/certificate-seeking undergraduates receiving state/local grants	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Percentage of full-time first-time degree/certificate-seeking undergraduates receiving state/local grants	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Average amount of state/local grants received	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
						by full-time first-time degree/certificate-seeking undergraduates		
NA	Financial Aid		Approved	2015	IPEDS	Number of full-time first-time degree/certificate-seeking undergraduates receiving institutional grants	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Percentage of full-time first-time degree/certificate-seeking undergraduates receiving institutional grants	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Average amount of institutional grants received by full-time first-time degree/certificate-seeking undergraduates	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Number of full-time first-time degree/certificate-seeking undergraduates receiving student loans	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Percentage of full-time first-time degree/certificate-seeking undergraduates receiving student loans	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
NA	Financial Aid		Approved	2015	IPEDS	Average amount of student loans received by full-time first-time degree/certificate-seeking undergraduates	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - number of full-time first-time degree/certificate-seeking undergraduates	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - students in cohort as percentage of total undergraduates	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - number of students in cohort in-district	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - percentage of students in cohort in-district	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - number of students in cohort in-state	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - percentage of students in cohort in-state	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - number of students in cohort out-of-state	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - percentage of students in cohort out-of-state	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - number of students in cohort residence unknown	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Fall cohort - percentage of students in cohort residence unknown	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Total number of undergraduate students (fall count)	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Year cohort - number of full-time first-time degree/certificate-seeking undergraduates	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Year cohort - percentage of total unduplicated count of all full-time first-time degree/certificate-seeking undergraduates	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Year cohort – unduplicated count of total undergraduate students	ODS	Inactive
NA	Financial Aid		Approved	2015	IPEDS	Revenue from federal appropriations and federal, state, and local grants and contracts	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
NA	Tuition		Approved	2015	IPEDS	Institution has hospital	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-district average tuition for full-time undergraduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-district required fees for full-time undergraduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-district tuition and fees for full-time undergraduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-state average tuition for full-time undergraduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-state required fees for full-time undergraduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-state tuition and fees for full-time undergraduates (Sticker price)	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	Out-of-state average tuition for full-time undergraduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	Out-of-state required fees for full-time undergraduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	Out-of-state tuition and fees for full-time undergraduates	ODS	Inactive

IPEDS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availability	Source	IPEDS Label	Database Name	Data Loaded and Active
NA	Tuition		Approved	2015	IPEDS	In-district average tuition full-time graduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-district required fees for full-time graduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-district tuition and fees for full-time graduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-state average tuition full-time graduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-state required fees for full-time graduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	In-state tuition and fees for full-time graduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	Out-of-state average tuition full-time graduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	Out-of-state required fees for full-time graduates	ODS	Inactive
NA	Tuition		Approved	2015	IPEDS	Out-of-state tuition and fees for full-time graduates	ODS	Inactive

10. CENSUS Data Entities

The following CENSUS domain data entities are approved or Approved for inclusion in the MLDS Data Inventory:

- Address

11. CENSUS Data Elements

The following CENSUS domain data elements are approved or Approved for inclusion in the MLDS Data Inventory:

CENSUS Data Elements

CEDS Global ID	Entity	Element Name	Approval Status	Availibility	Source	CENSUS Label	Database Name	Data Loaded and Active
NA			Approved	2015	Census Bureau	Census Region	ODS/MDM	Inactive
NA	Address	State Abbreviation	Approved	2015	Census Bureau	State Code	ODS/MDM	Inactive
NA	Address	Country Code	Approved	2015	Census Bureau	State Abbreviation	ODS/MDM	Inactive
NA	Address		Approved	2015	Census Bureau	City Code	ODS/MDM	Inactive
NA	Address	Address City	Approved	2015	Census Bureau	City Name	ODS/MDM	Inactive
NA	Address	County ANSI Code	Approved	2015	Census Bureau	County Code	ODS/MDM	Inactive
NA	Address		Approved	2015	Census Bureau	County Name	ODS/MDM	Inactive
NA	Address	Latitude	Approved	2015	Census Bureau	Latitude	ODS/MDM	Inactive
NA	Address	Longitude	Approved	2015	Census Bureau	Longitude	ODS/MDM	Inactive

12. *Supporting Information*

For more information on the MLDS Center please visit the MLDS Center website at www.mldscenter.org.

For additional support on CEDS 4.0 Data Standards visit ceds.ed.gov.

13. *Contributors and Change History*

Date	Description/Reason for change	Authors/Contributors	Version
07/25/2012	Initial Draft	John Bruns	1.0
09/1/2012	Revision of content, addition of tables	John Bruns, Rob London	1.0
10/2/2013	Revision of content, addition of person, organization data elements; mapping to CEDS workforce elements added	John Bruns	2.0
10/29/2013	Added CEDS 4.0 details and data elements planned for the MLDS Master Data Management system	John Bruns	2.0
10/31/2013	Review and update	Chandra Haislet	2.0
11/1/2013	Updates to sections 2.0-5.0	Ross Goldstein	2.1
11/1/2013	Inactive CEDS 4.0 elements removed from Appendix B	John Bruns	2.2
11/15/2013	Active and Approved elements added to Appendix B and C; reserved elements removed	John Bruns	2.3
11/20/2013	Removed Appendices related to elements by policy question and system source; added active and Approved elements; denoted elements not mapped to CEDS 4.0	John Bruns	2.4
11/25/2013	Defined Approved elements as those approved by agencies for submission; removed Approved elements not approved	John Bruns	2.5
12/13/2013	All "Approved" data elements in Version 2.5 marked as active following MLDS Board approval	John Bruns	2.6
1/4/2014	Initial Draft of CEDS Elements	John Bruns (MSDE)	3.1
1/31/2014	Research Request of CEDS Elements	Mike Woolley (UMB)	3.1
2/28/2014	Availability of Data Alignment – K12	Janice Johnson (MSDE)	3.2
2/28/2014	Availability of Data Alignment – Workforce	Donni Turner (DLLR)	3.2
2/28/2014	Availability of Data Alignment – Postsecondary	Andrew Nichols (MHEC)	3.2
3/13/2014	Approved Items for Inventory	Chandra Haislet (MLDS Center)	3.3

Date	Description/Reason for change	Authors/Contributors	Version
5/28/2014	Availability of Data Alignment – Postsecondary	Jon Enriquez (MHEC)	3.4
6/2/2014	Approved Items for Inventory (Data Gab)	Chandra Haislet (MLDS Center)	3.5
6/6/2014	Availability of Data Alignment – Early Learning	Phil Koshkin (ECH)	3.6
6/6/2014	Additional Postsecondary Data	Jon Enriquez (MHEC)	3.7
6/9/2014	Availability of Data Alignment – Workforce	Donni Turner (DLLR)	3.8
12/8/2014	Availability of Data Alignment – Governing Board Meeting 12/16/2014	Laia Tiderman (MLDS Center)	4.0
12/18/2014	Proposed Data Elements Approved by the Governing Board 12/16/2014	Laia Tiderman (MLDS Center)	4.1