OLDC OREGON LONGITUDINAL DATA COLLABORATIVE

The mission of the Oregon Longitudinal Data Collaborative is to support objective analysis and reliable conclusions based on robust cross-sector, longitudinal education data.

SUBJECT:	Data Security Standards	**NUMBER**:	OLDC-STD-002
DIVISION:	Oregon Longitudinal Data Collaborative	**EFFECTIVE DATE**:	11/19/2019
APPROVED:	Approved by SLDS Executive Committee on 08/18/20		**Architectural Artifact**

Owner	Director, Oregon Longitudinal Data Collaborative
Status	Approved
Review Period	Annual
Revision History	

Version	Revision Date	Modified by	Change Summary
8/25/2016	1.0	D. Domagala	Document Initiation
10/3/2016	1.1	D. Domagala	Content Enhancements, still in draft form
10/10/2016	1.2	D. Domagala	Security Requirements section updates to include “solution” column
10/20/2016	1.3	M. Rebar	Revisions made to all document
11/21/2016	1.4	T. Brown	Revisions made to document
1/10/2017	1.5	T. Brown	Revisions made based upon CEdO feedback template
12/27/18	1.6	B. Tate	Updates made to reflect changes in data intake and program approach
9/9/19	1.7	B. Tate	Converted to Standards Template
9/19/19	1.8	B. Tate	Updated with feedback from Privacy Subcommittee
3/18/20	1.9	B. Tate	Updated introduction based on feedback from Privacy Subcommittee
6/15/20	2.0	B. Tate	Updated Standard 3 and 4/Removed Standard 6
9/16/22	2.1	B. Tate	Shift from SLDS to OLDC

STANDARDS:	It is the intent of the OLDC that data within the SLDS should be stored and used securely, and that these processes should be done in a standard and consistent manner. No action or process should deviate from the published standards without prior written approval by the SLDS Privacy Subcommittee. The Data Security Standards document outlines the functions and features the SLDS utilizes to protect the Personally Identifiable Information (PII) contained within it. This document is intended to provide a non-technical overview of security features and safeguards. Security methods and procedures are described, along with the

	planned approach to fully meet and exceed security requirements for the SLDS.
PURPOSE:	The Oregon Longitudinal Data Collaborative (OLDC) will ensure federal statues such as HIPAA and FERPA, and federal standards (such as those published by NIST and FIPS) protections are enforced and personally identifiable information is protected at rest and in transit. Access will only be granted to authorized and authenticated personnel. Where applicable, in accordance with FERPA, HIPAA and other legal requirements, database encryption will be applied to protect confidentiality of data at rest. Database access and administration privileges will be restricted to only those explicitly approved by the SLDS Governance Committees using role-base authorization and password authentication. Firewalls, anti-virus software, monitoring tools, and other existing security protections will be fully unitized, or installed as needed to meet the security guidelines SLDS Governance Committees. The SLDS will abide by all applicable security standards as outlined in Oregon's Enterprise Information Technology Policies. All data handled by contracted personnel will be handled securely and confidentially, in accordance with federal, state, Oregon Department of Education (ODE), Higher Education Coordination Commission (HECC), Oregon Employment Department (OED), Teacher Standards and Practices Commission (TSPC), and Oregon Enterprise Information Technology Policies.
SCOPE:	Standards related to data security for all data stored and utilized by OLDC
APPLICABILITY:	These standards apply to all data partner agencies as well as data requestors who want to use data provided by OLDC
ATTACHMENTS:	A. Laws and Standards
DEFINITIONS:	**Term**:
	Personally Identifiable Information: Personally identifiable data is data that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. **Data Partner Agency:** Agencies who actively share data with the Statewide Longitudinal Data System and participate in the governance of the system. Currently those agencies are: The Oregon Department of Education, the Higher Education Coordinating Commission, and the Employment Department. **Operational Data Store (ODS):** An ODS is a database designed to integrate data from multiple sources for additional operations on the data, for reporting, controls and operational decision support. **Master Data Management (MDM):** Master Data Management is a method used to define and manage the critical data of an organization to provide, with data integration, a single

	point of reference. **Active Directory (AD):** Active Directory is a Microsoft product that consists of several services that run on Windows Server to manage permissions and access to networked resources. **SLDS:** Statewide Longitudinal Data System, the data system OLDC uses to import agency data, match it at an individual level and make that matched data available for reporting and research.
STANDARD 1:	Data Transfer Security
KEY FEATURES:	• Data Partner Agencies provide data with through an automated set of routines, which will pull data from source systems into the Operational Data Store on a scheduled basis, or by providing data manually through a secure means. Data transfers (whether automatic or manual) take place over an internal, secure network supported by Enterprise Information Services (EIS). • Only authorized system administrators, as determined by SLDS Privacy Subcommittee, have access to the data files, the loading routines, and the ODS data structures. Enterprise Information Services (EIS) administers the secure network used to transmit the data and files. Personally Identifiable Information from ODE, TSPC, HECC and OED is securely housed within the Operational Data Store, in order to longitudinally match those individuals across state systems.
STANDARD 2:	Data Matching Security
KEY FEATURES:	• The Operational Data Store (ODS) securely houses personally identifiable student data from data partner agencies. This data is processed through a match engine (powered by Informatica software) using pre-defined match rules. • Once a match is determined, all state data for that matched student is de-identified and assigned a randomly generated system identifier as it is loaded into a secure longitudinal data warehouse.
STANDARD 3:	Data Visualization Security
KEY FEATURES:	• De-identified records for Oregon students are stored in secure databases on virtual machines running on physical hardware within the State Data Center. Authorized personnel from Enterprise Information Services (EIS) have physical access to the database servers. • Authorized administrators have system access to the databases. • Researchers and analysts authorized by the SLDS Research Subcommittee have access to the de-identified longitudinal information provided by OLDC. • Requestors are allowed to access data extracts provided by OLDC through any tool

	of choice. They have to complete a data structure training to help educate them on how the data is stored within the system (see SLDS-POL-001 System Access for details). • The SLDS Research Subcommittee will thoroughly review and explicitly approve any longitudinal reports before being publicly available. Public reports are aggregated or suppressed at a cell level to avoid potential identification of individual students. Suppression rules of the data partner agencies are utilized and in the case of multi-agency data the most restrictive rules are applied. • Current suppression rules: o Oregon Department of Education (ODE) ▪ If counts are shown, suppress counts of 5 or fewer (less than 6). ▪ If percentages are shown, suppress 5% or less and 95% or greater. o Higher Education (HECC) ▪ If counts are shown, suppress 9 or fewer (count). ▪ If percentages are shown, suppress based on counts of 9 or fewer. o Workforce (OED) ▪ Suppress data if there are fewer than three (3) records for any data point.
STANDARD 4:	Informatica Security
KEY FEATURES:	• Users and groups of users who have been given access to the various services either directly or through the use of predefined roles. Account management within Informatica allows for configuration of Maximum Login Attempts and locking out individual users (including users with the Administrator role). Three failed login attempts within two minutes result in account lockout. • Accounts will be reviewed annually to ensure inactive users are removed.
STANDARD 5:	Master Data Management Security
KEY FEATURES:	• Security for Master Data Management (MDM) is established by configuring users within the MDM Hub Master Database or by synchronizing groups with an LDAP service. These users or groups are then granted permissions directly or by role to various objects and services. • Account management within MDM is accomplished using a Global Password Policy where a maximum number of failed logins is configured. Three failed login attempts within two minutes result in account lockout.

STANDARD 6:	Data Encryption
KEY FEATURES:	• All data within the local network will have encryption enabled. All data transfers will be done over encrypted protocols. At no time will the data be transmitted or stored in an unencrypted fashion.
STANDARD 7:	Unit Record Auditing
KEY FEATURES:	• Unit record auditing is configured on all databases holding or potentially housing personally identifiable information (PII). This can be used to determine when a record was last updated, and by whom. • Logging will be enabled for specific functions or commands within the system, such as downloading data.
STANDARD 8:	Security Testing
KEY FEATURES:	• OLDC will coordinate and perform an IT risk assessment at least annually and document the testing performed with the findings. • Document and review annually the process to accomplish research, analysis and evaluations and the process to share data findings with data partner agencies to ensure they are secure and update/review as needed. • Document and map the infrastructure that contains the data and review the documentation on an annual basis with agencies to ensure system compatibility and optimal system operation. Update and revise as needed. • Run vulnerability scans annually or as needed and document findings. Share findings with agencies and create a mitigation plan to track resolution of risk. • Regularly monitor those persons with access to PII to determine whether the job responsibilities of those persons continue to require access, and will immediately remove access for any person who is determined to no longer need such access. OLDC will notify the SLDS Privacy Subcommittee that access has been terminated.

Exhibit A – Laws and Standards

The Agencies shall adhere to privacy and confidentiality policies identified through the Oregon SLDS Governance Committee, Federal, and State laws and statutes. The SLDS Program Team will follow the security standards in place with the Office of the State Chief Information Officer (OSCIO) at a minimum. The SLDS Program is following the National Center for Educational Statistics (NCES) best practices and recommendations. This list of laws and statutes for reference is not all, inclusive. In addition to the identified laws/statutes, technology best practices for secure data transfer and data storage will also be employed as such technology advances.

All Parties shall comply with the following laws and standards:

- Privacy Act of 1974: Defines, and provides for the security and privacy of, personal data maintained by the federal government.
- Privacy Protection Act of 1980 (PPA)
- Computer Security Act of 1987: Increases the protection requirements for Privacy Act data and other sensitive federal information; requires a security plan for each computer system that contains sensitive federal information.
- E-Government Act of 2002, Title V, subtitle A, Confidential Information Protection mandates the protection of individually identifiable information that is collected by any federal agency for statistical purposes. Unauthorized disclosure of these data is a class E felony.
- Education Sciences Reform Act of 2002: Mandates the protection of individually identifiable information about students, their families, and schools that is collected and disseminated by IES. Unauthorized disclosure of these data is a class E felony.
- Family Educational Rights and Privacy Act of 1974 (FERPA)
- Oregon Consumer Identity Theft Protection Act of 1970 (ORS 646A et seq.)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Individuals with Disabilities Education Act (IDEA) of 1975
- Applicable Oregon privacy statutes (e.g., ORS 84, 182, 187, 326, 336, 581)
- Applicable State of Oregon Laws
- Applicable Federal Laws
- Other statutes may apply under certain circumstances, such as the Computer Fraud and Abuse Act of 1986, which makes it a felony to gain unauthorized access to a computer system containing federal data, or to abuse the access one has, with the purpose of doing malicious destruction or damage.
- Oregon SLDS Program Information Security plan
- OSCIO security standards: http://www.oregon.gov/das/OSCIO/Pages/SecurityGuidance.aspx
- ETS security standards
- NISTIR 7298 Glossary of Key Information Security Terms
- DAMA-DMBOK – Data Management Book of Knowledge
- ISO/IEC JTC 1 – Information Technology
- Department of Administrative Services Policies (e.g., 107-004)
- As a hosted client of the Oregon State Data Center (SDC), annual risk assessments will be conducted of the data system integrity, which is in compliance with the DAS State Standards. Data classifications for each environment (data assets) within the Oregon SLDS will be maintained as part of the security requirements for data integrity.
- National Center for Education Statistics SLDS in “Technical Brief 3 Statistical Methods for Protecting Personally identifiable Information in Aggregate Reporting”