Data Sharing Agreement Between the Colorado Department of Education (CDE) and the Colorado Department of Labor & Employment (CDLE)

This Data Sharing Agreement (Agreement) is entered into by and between the Colorado Department of Education (CDE), 201 E. Colfax Avenue Denver, CO 80203 and the Colorado Department of Labor and Employment (CDLE), 633 17th Ave, Suite 201 Denver, CO 80202, each individually a party and together the parties.

I. Scope of Agreement

CDE is a State Education Agency responsible for the implementation of education laws adopted by the State of Colorado. In fulfillment of law found in the Colorado Revised Statutes, CDE is charged with collecting and securely maintaining unit record data on students enrolled in the state's Local Education Agencies (LEAs). Every month, Current Employment Statistics (CES) surveys business establishments in order to produce estimates of employment, hours, and earnings data. CES data are compiled for all States, major metropolitan statistical areas (MSA), and the nation as a whole and broken down by industry according to the North American Industrial Classification System (NAICS). CES is a federal-state cooperative program funded by the Bureau of Labor Statistics (BLS). The mission of the Bureau of Labor Statistics (BLS) is to collect, process, analyze, and disseminate essential statistical data to the American public, the U.S. Congress, other Federal agencies, State and local governments, business, and labor. In order to maintain credibility and trust with our survey respondents, confidentiality protections for our data are essential. Protecting the confidentiality of data is central to accomplishing the BLS mission. When collecting data, the BLS makes a pledge of confidentiality to its respondents. This pledge varies depending on the context of each survey, but the standard BLS confidentiality pledge promises that data collected are used for statistical purposes only.

This Data Sharing Agreement applies to all data sharing between CDLE and CDE. Specific data to be shared are outlined in attached appendices, along with the purpose of data sharing, data ownership and conditions and/or regulations governing the usage of the shared data. Also in the appendix will be further requirements for shared data retention/destruction, and agency processes for implementing these actions.

II. Purpose

CDE and CDLE enter into an interagency agreement on or about April 15, 2015 to share and exchange Data for the purpose of improving educational practice and policy development. Details of data to be shared are outlined in attached Appendices. This Agreement is designed to be an umbrella agreement for all data sharing activities between CDE and CDLE. For specific use cases, i.e., detailed data requests for specific research purposes, the details shall be spelled out via an Appendix attached to this agreement. The appendix will include data requested, data

owners, information about relevant laws or guidelines to be followed, whether or not the use case requires data linking, and conditions around sharing and usage of the requested data.

This Agreement shall be used exclusively for the purposes of sharing Data with the intentions of using the Data for decision making, publishing, reporting, longitudinal analysis, educational research, and policy making, i.e., purposes under which the Family Education Rights and Privacy Act (FERPA) authorizes disclosure. CDE shall require the Data Consumer to demonstrate that the requested data will only be used for FERPA authorized purposes. CDLE shall require the Data Consumer to demonstrate that the requested data will only be used for authorized purposes as noted in the appendices. All Data sharing under this agreement will be shared following applicable regulations required by the State agency(s) [i.e. FERPA, CIPSEA, or others]. In the event that CDE shares data with CDLE and/or CDLE shares data with CDE, the same rules and regulations established under FERPA, State Rule, and other applicable laws shall apply.

Any data sharing under this agreement will comply with CDE's Information Security and Privacy Policy, dated February 2014 and as updated, thereafter.

All requirements for data management, handling and security listed herein shall apply equally to third party vendors performing services for named state agencies.

III. Definitions

Authorized User means an individual who has been granted the appropriate privileges and rights to access an information technology system and view the data contained within (as defined in the respective department's data sharing policy).

CIPSEA means the Confidential Information Protection and Statistical Efficiency Act. This statute prohibits disclosure or release, for non-statistical purposes, of information collected under a pledge of confidentiality. Under CIPSEA, data may not be released to unauthorized persons. Willful and knowing disclosure of protected data to unauthorized persons is a felony punishable by up to five years imprisonment and up to a $250,000 fine.

Data means the representation of facts as texts, numbers, graphics, images, sounds, or video. Facts are captured, stored, and expressed as Data.

Data Breach means unauthorized or unintentional exposure, disclosure, or loss of private public information, which may include personally identifiable information.

Data Consumer means an individual who receives, analyzes and reports results of data from the Data Provider. In the case of educational longitudinal data linking research, a researcher submitting a question would be the Data Consumer.

Data Governance means the oversight of data quality, data management, data policies, business process management, and risk management surrounding the handling of data, and includes a set

of processes that ensures that important Data assets are formally managed throughout the State Agency, department organization, or enterprise.

Data Governance Manager means the individual responsible for the implementation and oversight of the State Agency's data management goals, standards, practices, processes, and policies. Each Agency's Data Governance Manager is authorized, after following approved internal Data Governance policies, to approve the sharing and release of that Agency's or Program's data to entities outside of that Agency or Program.

Data Owner means a person having the responsibility and authority for an entrusted data resource. The Data Owner plays a key role in internal Data Governance within each State Agency or Early Childhood Program. The Data Owner takes ownership of the operational, technical, and informational management of the Data. The Data Owner knows how to use the data, to whom it can be released and the appropriate conditions and regulations that govern the use of the data.

Data Provider means the original collectors of the Data.

Data Steward means individuals who manage data elements and/or categories at various points in the data lifecycle.

Decision Making using Data means any instance where analysis of data and subsequent results are used to help make an educational, administrative, or other decision.

Educational Research means any research designed to address an educational goal, question, or issue.

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g, means the federal law that protects the privacy of students' personally identifiable information.

Demographic Data Set means a set of demographics that uniquely define a particular person.

K-12 means school education levels ranging from Kindergarten to high school graduation.

Linked Data means the resultant data set after two or more agencies' data have been linked through the link system.

Longitudinal Analysis means an analysis of data or a population over time.

Personal Identifiable Information (PII) includes, but is not limited to, all educator data including the educator's name, any unique identifier, and any other information that, alone or in combination, is linked or linkable to a specific individual.

Relevant Information to Strengthen Education (RISE); is the brand name applied to the outcomes that will be realized with the implementation of the SLDS Grant, and other data related initiatives.

Risk Assessment of Linked Data is a review conducted of the results of two or more pieces of data linked together by the RISE system to answer a specific educational question. The focus of the Risk Assessment is to determine the level of risk (related to a data breach) introduced by combining data. The individual data providers will participate in the Risk Assessment to help determine if the new data set may have unique regulations and conditions governing its release and use, that were not present prior to combining the data. The System Steward and Data Providers will agree on and carry out any additional security or steps that are required as a result of the Risk Assessment to ensure the integrity of the linked data, up to and including the decision not to release the linked data.

Role-Based Access means a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.

State Agency means each principal department within the executive branch, including each board, division, unit, office, or other subdivision within each department, each office or agency within the Governor's Office, each state-supported institution of higher education, and each local district junior college; except that State agency shall not include any department, agency, board, division, unit, office, or other subdivision of a department that does not collect unit records.

Statewide Longitudinal Data System (SLDS) means a federal grant program that has helped to propel the successful design, development, implementation, and expansion of K-12 longitudinal data systems to include early learning, post-secondary and workforce.

System Steward means the agency responsible for running and managing the "Link" data system (RISE). This generally refers to CDE. CDE will ensure that the provided data will be handled with care, following all applicable Colorado information security policies. When the Linked Data is produced from the RISE system, all involved Data Owners will participate in validation and risk assessments as defined in this agreement.

User means an individual with authorized access to and who uses a particular data system.

IV. Access Restrictions

A. The parties agree to use role-based access to ensure that only authorized individuals have access to Data.

B. The specific records to be released from CDE shall be subject to the consent of CDE's Data Governance Manager (or designated authority).

C. The specific records to be released from CDLE shall be subject to the consent of CDLE's Data Governance Manager (or designated authority as noted in the appendices).

V. Re-disclosure of Data

A. Without authorization from the Data Governance Manager (or designated authority) of the Data Provider, the Data Consumer may only further disclose data in an aggregate form that does not allow the identification of individuals. Prior to such disclosure, the Data Consumer shall inform the Data Governance Manager who will have a reasonable opportunity to review the proposed disclosure, to confirm that the aggregate disclosure does not allow the identification of individuals.

B. There shall be no disclosure of individual level data to government agencies outside of the state.

VI. Data Provider Duties

A. The Data Provider shall maintain ownership of the Data.

B. The Data Provider maintains ownership in the case of third party vendors who may house agency Data off-site as a part of the longitudinal data linking process.

C. The Data Provider shall ensure that no identifying information is transmitted through unsecured unencrypted connections.

VII. Data Consumer Duties

A. The Data Consumer maintains a stewardship role for the preservation and quality of the Data.

B. The Data Consumer shall not retain any right, title or interest in any of the Data furnished by the Data Provider.

C. The Data Consumer is required to have a written agreement with any third party vendor who receives or uses PII to ensure the vendor will not further use or disclose the Data.

D. The Data Consumer may use and disclose Data as permitted in this agreement and only in a manner that does not violate state, or federal privacy regulations adopted by the Data Providing Agency.

E. The Data Consumer shall implement appropriate safeguards to prevent use or disclosure of Data not authorized by this agreement.

F. The Data Consumer agrees to abide by all applicable federal and State laws and regulations, including FERPA, CIPSEA and others as specified in attached appendices.

G. The Data Consumer shall ensure that the Data are kept in a secured environment (commensurate with level of data sensitivity) at all times and that only Authorized Users have access.

H. The Data Consumer shall promptly report to the Data Provider any use or disclosure of the Data of which the Data Consumer becomes aware that is not provided for or permitted in this agreement.

I. The Data Consumer shall permit the Data Provider to investigate any such report and to examine the Data Consumer's premises, records and practices. The Data Consumer agrees to abide by the resulting notification procedures outlined by the Data Provider in the event of a breach.

J. Data Consumer shall comply with CDE's "Data Security Assurances" found at http://www.cde.state.co.us/cdereval/dataprivacyandsecurity, and also attached as Addendum 1 to this Agreement, the terms of which are incorporated verbatim with this reference.

VIII. System Steward Duties

A. The System Steward maintains a stewardship role for the preservation and quality of the Data.

B. The System Steward shall manage the RISE system, and ensure the integrity and safety of the Data at all times.

C. The System Steward shall implement appropriate safeguards to prevent use or disclosure of Data not authorized by this agreement and the attached appendices.

D. The System Steward agrees to abide by all applicable state and federal laws and regulations, including FERPA, CIPSEA and others as specified in attached appendices.

E. The System Steward shall ensure that the Data are kept in a secured environment at all times while under their control and that only authorized users have access.

IX. Release of Linked Data to Consumer

The result of linking different agencies' (e.g., CDE and CDLE) data sets is a new data set that potentially has unique regulations and conditions governing its release and use.

A. Prior to release of linked data, the System Steward will classify the linked data according to risk of data breach. This could include evaluating based on means of release, or on likelihood of identifying Personally Identifiable Information from the linked data (or violating other regulations that apply to the linked data).

B. Based on the above classification, if PII will be released, a full Risk Assessment shall be conducted prior to release. The following questions shall be asked:

1. Does the linked data meet the original request and can it be used how the Data Consumer planned?
2. What conditions and/or regulations apply to the linked data?
3. Does usage of the linked data pose a high risk of breaching those regulations?
4. Have reasonable and appropriate steps been taken to reduce the risk of breach during the actual transfer of data to the Data Consumer?
5. How will the data be protected at rest and in transit.
6. Others as required.

C. Results of the Risk Assessment shall be provided to Data Providers for review

D. Based on the results of the Risk Assessment and recommendations from Data Providers, the System Steward shall apply additional constraints as necessary to the usage of the linked data. Options shall at a minimum include:

1. Require Data Consumer to destroy data after 6 months (or less if the risk is determined to be high), with accompanying proof of destruction submitted to System Steward,
2. The System Steward must follow-up after specified time period to review results of data usage by Data Consumer; and
3. Data Consumer must demonstrate that no PII was released to additional third parties,
4. Others as required.

Final agreement on additional constraints shall be documented in the Appendix, and signed by the Providers, the Requestors and System Steward as appropriate,* prior to *release of Linked Data.

X. Data Accuracy

The Data provided are the best and most complete documentation available. CDE and CDLE do not ensure 100% accuracy of all records and fields. Some data fields, including those that are not used, may contain incorrect or incomplete Data. CDE and CDLE will report any systematic problems with the Data identified in linked data sets to the data owner. Data that has been manipulated or re-processed by either CDE or CDLE is the responsibility of the user.

XI. Confidentiality

A. The parties agree to protect Data and information according to acceptable standards and no less rigorously than they protect their own confidential information. Personal Identifying Information will not be reported or made public.

B. All Data sharing shall be performed in accordance with the requirements of FERPA. FERPA Section 1232g(b)(1)(F) provides that education records and personally identifiable information may be released without student or parental consent to "organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administrating predictive tests, administering student aid programs, and improving instruction, if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations."

C. Additionally, CDE shall comply with any agency or program specific laws or regulations outlined in C.R.S. Title 22, and CDLE shall comply with any agency or program specific laws or regulations outlined in C.R.S. Title 26, that govern the sharing of protected information.

D. All State Agencies and vendors agree to abide by all federal regulations, including FERPA and CIPSEA regarding the Data specified in the appendices.

E. CDE and CDLE shall not disclose, release, reveal, show, sell, rent, lease, loan or otherwise grant access to PII and/or any Data derived or extracted, to any individual who does not need the Data to complete their work assignment as required by their job responsibilities within the scope of this agreement. This includes reports, written or oral presentations, written analysis, study articles or any similar documents containing Data.

XII. Non-Financial Understanding

This Agreement is a non-financial understanding between CDE and CDLE. No financial obligation by or on behalf of either of the parties is implied by a party's signature at the end of this Agreement. The terms of any financial liability that arises from data processing activities carried out in support of the responsibilities covered herein must be negotiated separately and to the mutual satisfaction of the parties. The legal authority for data sharing for specified purposes conveyed by this Agreement cannot be used to support a subsequent claim of implied agreement to financial obligation.

XIII. Data Retention

A. Data Consumers agree to safely maintain Data while conducting the research (or work scope) specified in the Agreement. All unnecessary records shall be purged within 4

years from the time it was released to the Data Consumer, or sooner if it has been determined there is no longer an educational purpose or potential research value. Records shall either be returned to the Data Provider or destroyed in a secure manner. Data retention policies shall comply with the Colorado State Archives Records Management Manual for State Government Agencies http://www.colorado.gov/dpa/doit/archives/rm/rmman/index.htm.

B. Any additional data retention/destruction requirements unique to a particular use case will be described in detail in the relevant Appendix.

C. Any external party housing Data on behalf of one of the parties agrees to the same standards, restrictions, and conditions of this agreement.

XIV. Data Governance Plan

Both parties agree to have in place a Data Governance plan with support and participation from across their organizations that detail the organization's policies and procedures to protect privacy and data security, including ongoing management of data collection, processing, storage, maintenance, use and destruction. Please see Addendum 2 to this agreement, for the minimums required to satisfy CDEs requirements for a Data Governance Plan. If the Data Governance program is unique to a particular division or unit within CDLE, the associated governance policies and procedures may be identified within the applicable appendix.

Each Party has the right to conduct audits or other monitoring of the other Party's Data Governance policies, procedures, and systems. If, through these monitoring activities, vulnerability is found, the breaching Party must take timely appropriate action to correct or mitigate any weaknesses discovered. The Requestor's current data security policies and procedures are not posted on an externally facing website but will be provided to CDE prior to the signature of this Agreement and annually thereafter and must include the minimum security policies and procedures set forth below:

A. Privacy and Security Policy
B. Privacy and Security Board and Officer
C. Management Oversight
D. Sanctions for Violations
E. Reporting Potential Problems in Privacy and Security
F. Incident Response and Incident Response Mitigation
G. Privacy and Security Training
H. Access Control, Minimum Necessary Access and Verification for Access to Sensitive Data
I. Password Management
J. Transmitting Sensitive Information

K. Log-in Monitoring
L. Workstation Security Configuration
M. Faxing
N. Device and Media Control
O. Computer Monitor Copier Printer Locations
P. Securing Materials with Identifying Information
Q. Encryption
R. Authorizations for Personal Health Information, if applicable
S. Permitted Uses and Disclosures of PHI, if applicable
T. HIPAA Status, if applicable
U. Business Associate Status, if applicable
V. Designating Sensitive Information
W. Risk Assessments
X. Information Risk Management
Y. Change Control
Z. Audit and Evaluation

XV. Unauthorized Uses, Disclosures or Breaches

A. In the event a Data Breach occurs as a result of Data sharing, the Data Consumer shall be responsible for notifying CDE and/or CDLE and working with the respective agencies' Data Governance Managers (or delegates as noted in the appropriate Appendix) in contacting and informing the individuals who may have been affected by the security breach. Data Consumers may not contact such individuals prior to notification of CDE and/or CDLE management.

B. The Data Consumer shall permit the Data Provider to investigate any such report and to examine the Data Consumer's premises, records and practices. The Requestor agrees to abide by the resulting notification procedures outlined by the Data Provider in the event of a breach.

C. Should a person not comply with this agreement, he/she may subject himself/herself to disciplinary action, including, but not limited to, termination of access authorization.

D. Failure to comply with this policy may result in denial of access or any actions deemed "inappropriate dissemination of student or staff data" may result in a penalty as defined in the following section of Colorado Revised Statutes, 6-1-716.

E. CDE and the CDLE shall make a good faith effort to identify any use or disclosure of confidential Data not authorized by this agreement.

F. If there are costs associated with notifying individuals whose personally identifiable information has been compromised or any other damages resulting from the release of the

Data, the compensating party shall depend on determined fault for the initial Data breach. If CDE is responsible for the breach, CDE shall compensate for communication and damages. If CDLE is responsible for the breach, CDLE shall compensate for communication and damages.

XVI. Survival

The respective rights and obligations of parties shall survive the termination of this Agreement with respect to Data previously shared.

XVII. Data Requests

The parties shall follow the agreed-upon Data governance rules and policies for security and privacy found at: https://www.cde.state.co.us/dataprivacyandsecurity. CDE and CDLE will hold Data Owners and Data Governance Managers accountable to ensure their Data is handled by the authorized individuals necessary to achieve the stated purposes, while still conforming to all regulations and security policies.

XVIII. Data Owners

The Data Owners, System Steward, and Consumers shall ensure that access to the original Data covered by this Agreement shall be limited to eligible divisions of CDLE and CDE and the minimum number of individuals necessary to achieve the purposes stated in this Agreement.

XVIX. Effective Date and Term

This Agreement shall take effect upon its signing by all parties. This Agreement may be amended at any time by mutual agreement of all parties. All parties will conduct an independent review of this Agreement on an annual basis. This Agreement shall remain in effect until terminated by written notification from one party to another.

XX. Signatures

To further the collection and analysis of Colorado educational Data, CDE, represented by the Interim Commissioner of Education for Colorado, and CDLE, represented by Executive Director CDLE, Ellen Golombek, agree to the cooperative sharing of data between the two agencies pursuant to the conditions set forth herein.

Signature: Katy Anthes *Date:* 6/28/16

Katy Anthes, Ph.D.

Interim Commissioner of Education

Colorado Department of Education

Signature: _____ *Date:* 6/27/16

Ellen Golombek

Executive Director

Colorado Department of Labor & Employment

APPENDIX A – Occupational Employment Statistics

Business Use Case

This use case describes the process whereby the CDE provides educator information to the Colorado Department of Labor and Employment (CDLE) for the purposes reporting employment statistics to the Federal Reserve Bureau of Labor Statistics. The mission of the Bureau of Labor Statistics (BLS) is to collect, process, analyze, and disseminate essential statistical data to the American public, the U.S. Congress, other Federal agencies, State and local governments, business, and labor.

The Federal Reserve / Bureau of Labor Statistics uses the data for the purpose of monitoring employment and unemployment statistics to help to examine trends in job growth for the nation and for different geographic areas, industries and occupations. In addition the data provides additional insight into the pay and benefit statistics about the well-being of American workers and families.

The gathering of employee statistics falls under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA). This statute prohibits disclosure or release, for non-statistical purposes, of information collected under a pledge of confidentiality. Under CIPSEA, data may not be released to unauthorized persons. Willful and knowing disclosure of protected data to unauthorized persons is a felony punishable by up to five years imprisonment and up to a $250,000 fine.

The Occupational Employment Statistics (OES) program is the only comprehensive source of regularly produced occupational employment and wage rate information for the U.S. economy, as well as States, the District of Columbia, Guam, Puerto Rico, the Virgin Islands, all metropolitan areas and divisions, and balance-of-State areas for each State, for complete geographic coverage. The OES program produces employment and wage estimates by non-farm industry for the full Standard Occupational Classification (SOC) system, which includes over 800 detailed occupations. Uses of the data include evaluating current and historical employment and wages by industry, occupation, and geographic area; foreign labor certification; projecting occupational demand for the Nation and States; vocational planning; estimating social security receipts, and as an input to calculating reimbursement rates for Medicare and Medicaid providers; identifying science, technology, engineering and mathematics (STEM) related occupations for the National Science Foundation; calculating occupational injury rates; as an input to the President's Pay Agent report; and industry skill and technology studies. The OES portions of the BLS public website generate some of the highest levels of activity among all program areas. In addition, OES data are the foundation of the industry-occupation matrix used in the Employment Projections (EP) program to produce national occupational projections. OES employment and wage data are used throughout the Occupational Outlook Handbook (OOH) and related career publications, as well as in similar products produced by the SWAs for State and local areas. • In FY 2016, the SWAs, in cooperation with the BLS, will collect employment and

wage information from semi-annual sample panels of approximately 200,000 establishments, for a total of 400,000 for the year. Respondents provide data for a payroll period that includes the 12th day of the survey month.

Participating Agencies

The **Colorado Department of Education** (CDE) will be sharing data with the **Colorado Department of Labor and Employment** (CDLE)

Data Required from (Agency) – Data Providers

Annual educator staff or sometimes referred to as human resources data.

Conditions under which data may and may not be linked and shared

Educator data will be extracted from the CDE Data Warehouse repository for the most recently reported school district staff or human resources collections. The CDLE provides the educator data along with other occupational data to the Federal Bureau of Labor and Statistics through a separate process on an annual basis. The Bureau of Labor Statistics, its employees, agents, and partner statistical agencies, uses the information provided for statistical purposes only and will hold the information in confidence to the full extent permitted by law. In accordance with the Confidential Information Protection and Statistical Efficiency Act of 2002 (Title 5 of Public Law 107-347) and other applicable Federal laws, your responses will not be disclosed in identifiable form without your informed consent.

For the purpose of the above business use case, the roles of data consumer and authorized user shall be limited to the below identified data owners and data consumers. CDE and CDLE may identify additional staff as Authorized Users in writing for review and consideration. CDLE includes as data consumers Barbara Wills and Ralph Longobardi of the CDE educator data.

The role of Data Governance Manager for CDE is Marcia Bohannon for this agreement, and the role of Data Governance Manager for CDLE is a shared responsibility between Alexandra Hall, the Chief Economist, Colorado Department of Labor and Employment and Ralph Longobardi, Occupational Employment Statistics Program Manager, Colorado Department of Labor and Employment for the interim period. After the establishment of a formal Data Governance Manager at CDLE, that staff will assume the responsibilities outlined in the definitions section and in accordance with roles and responsibilities as assigned by CDLE.

Table of Required Data and Ownership:

No.	Data	From	Source System	Data Owner

No.	Data	From	Source System	Data Owner
1.	School Year	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
2.	Organization Code	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
3.	Edid	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
4.	Last Name	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
5.	First Name	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
6.	Middle Name	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
7.	Gender Code	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
8.	School Code	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
9.	Emp Status Code	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
10.	Contract Days	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
11.	Hours Per Day	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
12.	Hourly Pay Rate	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
13.	Base Salary	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
14.	Jobclass Code	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
15.	Subject Area Code	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
16.	Program Area Code	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
17.	Mode Fte	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
18.	Yrs Principal This School	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
19.	Grade Level Infant	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
20.	Grade Level Prek	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
21	Grade Level K	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
22.	Grade Level 1st	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager

No.	Data	From	Source System	Data Owner
23.	Grade Level 2nd	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
24.	Grade Level 3rd	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
25.	Grade Level 4th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
26.	Grade Level 5th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
27.	Grade Level 6th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
28.	Grade Level 7th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
29.	Grade Level 8th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
30.	Grade Level 9th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
31.	Grade Level 10th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
32.	Grade Level 11th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager
33.	Grade Level 12th	CDE	CDE Data Warehouse	Jan Petro, K-12 Data Governance Manager

CDLE, in order to facilitate the data sharing outlined in this Appendix and comply with the practices outlined in the Agreement, must put in place interim data governance practices until such time that formal governance may replace the below outlined procedures.

A. Data Governance: At a minimum and in conjunction with the established clearance process for interagency agreements, CDLE will convene the above identified data owner, Occupational Employment Statistics Program Manager, and any other subject matter expert deemed necessary to review all data sharing requests. The recommendations from this body shall accompany the formal request through the clearance process to the Chief Economist, Colorado Department of Labor and Employment and the Occupational Employment Statistics Program Manager, Colorado Department of Labor and Employment, and only after the request has completed clearance shall linked data sets be shared.

B. Please see the attached APPENDIX N – CONFIDENTIAL NATURE OF BLS RECORDS. This document establishes the Data Governance policies the CDLE must follow when utilizing the occupational statistics data.

C. Risk Assessment: CDLE will reconvene the above identified interim governance group, and any subject matter experts deemed necessary, to review the linked data and any results generated by CDE to consider potential risks. The risk assessment process shall mirror that described in the Agreement section IX, items A-E, and as needed include collaboration with the Data Steward and Data Governance processes established within CDE.

Regulations that Apply

- PII (34 CFR Part 99, section 99.3)

Additional Constraints, as required by Section IX, entitled "Release of Linked Data to Requestor"

Signatures

To further the collection and analysis of Colorado educational Data, CDE, represented by the Interim Commissioner of Education, and CDLE represented by the Department of Labor and Employment and Director, Office of Labor Market Information, agree to the cooperative sharing of data between the two agencies pursuant to the conditions set forth herein.

Signature: Katy Anthes *Date:* 6/28/16

Katy Anthes, Ph.D.
Interim Commissioner of Education
Colorado Department of Education

Signature: Paul Schacht *Date:* 6/23/16

Paul Schacht
Director, Office of Labor Market Information
Colorado Department of Labor and Employment

ADDENDUM 1 – Data Security Assurances

Overview

The Colorado Department of Education is required by law to collect and store student and educator records, and takes seriously its obligations to secure information systems and protect the privacy of data collected, used, shared and stored by the Department. In the event that Personally Identifiable Information (PII) must be shared with other entities, there is a very strict set of policies and standards that must be followed, and may be found at the following link: http://www.cde.state.co.us/cdereval/approvalprocessdocs

CDE's standards include requirements for protecting CDE data at rest and in transit within an environment at least as secure as protections in place at CDE. Those requirements are summarized in this document below.

In addition to the policies that govern these steps, a formal Data Sharing Agreement must be in place between CDE and any entity receiving CDE data, prior to any data sharing. Data Sharing Agreements and what they contain are explained in more detail at

http://www.cde.state.co.us/cdereval/checklistforpiiagreements

This document outlines the minimum data environment that must be in place at an external entity prior to receiving any PII from CDE, for all vendor contracts executed or renewed after the date of this agreement.

Assurances Required to Accept CDE Data

Data Consumers receiving PII from CDE must incorporate the following requirements:

- ✓ Strong access control must be in place. All data must be at a minimum protected with a complex password, workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended. Passwords must be confidential and sharing of passwords is prohibited, must not be written down or stored in an insecure location, and periodically changed and not reused or a reasonable time period.
- ✓ Unused and terminated user accounts must be disabled and/or deleted immediately; account inactivity must be periodically assessed for potential stale accounts.
- ✓ Care must be exercised in inadvertently sharing data on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.

- ✓ Systems must be in place for logging and monitoring access and use of data.
- ✓ At a minimum, annual intrusion penetration/vulnerability testing will be implemented.
- ✓ Laptop/mobile device password locks and full disk/storage encryption are required.
- ✓ Data at rest on central computing systems must be encrypted; any backup, backup media, removable media, tape or other copies must also be encrypted, and not used to transport data.
- ✓ Mandatory annual Security awareness training on how to handle PII is required.
- ✓ Appropriate endpoint security anti-virus and anti-malware software must be installed and maintained on computers accessing or processing PII.
- ✓ Transmitting data must occur via a secure method such as Secure File Transfer Protocol (SFTP) or comparable and never sent via email or transported on removable media.
- ✓ Physical security in buildings housing PII, along with controlled physical access to buildings and/or data centers.
- ✓ Ability to suppress small N-sizes for aggregated student data reports is required.
- ✓ After prescribed use is concluded, data disposal policies must apply for cleaning up all data. This includes secure scrubbing and securely overwriting data from storage, or physically destroying the storage media.
- ✓ Devices used to copy or scan hard copies of data must have encrypted storage and have storage devices appropriately scrubbed when equipment is retired. Hard copy containing PPI is discouraged and must be physically secured, not left unattended, and physically destroyed.
- ✓ All data processing systems, servers, laptops, PCs, and mobile devices must be regularly scanned and have all security patches applied in a timely manner.
- ✓ Data stored in cloud based systems must be protected in the same manner as local data, as described throughout this document. Use of free cloud based services is prohibited, and secondary encryption must be used as appropriate to protect data in cloud storage.
- ✓ Cloud environments, when employed, must be fully documented and open to CDE inspection and verification.

- ✓ Access to cloud based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

Questions

Questions about the Information Security and Privacy Policy at the Colorado Department of Education should be directed to Marcia Bohannon, Chief Information Officer, at Bohannon_m@cde.state.co.us and/or Corey Kispert, Information Security Officer, at Kispert_C@cde.state.co.us.

ADDENDUM 2 – Minimum Data Governance Requirements for Data Sharing with CDE

Requirements

- Agency-established person to act as authorized representative for any CDE data that is shared.
- Identified data owners for any data that interfaces with or is linked to CDE data.
- One person (Data Governance Manager) identified to coordinate data owners/stewards responsible for data that might interface with or is linked to CDE data, and who defines the rules and policies that apply to any data sets containing CDE data. This can be the same person as the authorized rep as described in the first bullet point. Ideally, this person should have meetings with other related data owners to facilitate data management and data security. Additional tasks for this person and/or group include:
  - Define minimum data management rules from which to operate
  - Review and approve data requests that could impact any CDE data
  - Define, implement and monitor security policies required to protect the CDE data (and linked data set) at rest and in transit
  - Define, implement and monitor access controls required to ensure that those with access are trained in FERPA and methods of data protection
  - Ensure that local information security requirements meet or exceed CDE's requirements as laid out in CDE's Data Security Assurances, included in this agreement as Addendum 1.
- Minimum required documentation is as follows:

All of the above items must be documented and available to all personnel with access to or reason to work with CDE shared data. This should also be made available to CDE.