POLICIES OF THE COLORADO UNIVERSITY SYSTEM

POLICY FOR THE SYSTEM AND ALL INSTITUTIONS

Policy Title: Data Governance	
Effective Date: Original Effective Date: May 12, 2025 Last Revision: May 12, 2025	Category: Information Technology
Policy Owner: Vice President for Information Technology	Contacts: Division of Information Technology Phone: 970-491-5133

PURPOSE OF THIS POLICY

The purpose of this policy is to establish the Colorado State University System (System) Data Governance Program to ensure the formal management of data at the System and each of its Institutions.

APPLICATION OF THIS POLICY

This policy applies to all students, faculty, staff, contractors, consultants, affiliates, and any others granted use of Information Technology Resources or Data at the System or any of its Institutions.

EXCEPTIONS FROM THIS POLICY

The Data Governance Steering Committee and System Chief Information Officer must explicitly approve exceptions from this policy. The Data Governance Program Charter describes the process for how to request an exemption.

The System recognizes that Research Data requires specific and unique data management according to relevant laws, policies, regulations, standards, and specific funding agency requirements. Therefore, Research Data as subsequently defined are exempt from the Data Governance Program and this policy.

DEFINITIONS USED IN THIS POLICY

Data: Any information, regardless of electronic or printed form or location, which is created, acquired, processed, transmitted, or stored on behalf of the System or an Institution on an Information Technology Resource. This includes data created, acquired, processed, transmitted, or stored by the Institution in environments in which the Institution does not own or operate the

technology infrastructure.

Data Classification: The categorization of Data upon which the consistent application of access, privacy, and security standards is based. Classification levels are mutually exclusive. Classification of Data must be at the highest level based on the risks associated with improper use.

Data Governance Program: A set of activities coordinated by the Data Governance Steering Committee to provide clear practices and processes to support data quality, information awareness and literacy, compliance and regulatory requirements, data security and privacy, informed and strategic decision-making, interoperability and integration, transparency, and resource optimization at the System and its Institutions.

Data Handling: The actions Data Users should take to create, acquire, process, transmit, report, store, or destroy System or Institution Data in a privacy-protective and secure manner that aligns with the levels of Data Classification.

Data Lifecycle: The progression of stages in which a piece of information may exist between its original creation or collection and final archive or destruction.

Information Technology Resources: The facilities, services, technologies, and devices used to electronically create, acquire, process, transmit, or store System or Institutional Data. Information Technology Resources include, without limitation, computer labs, classroom technologies, computing and electronic devices and services, email, networks, servers, storage devices and systems, applications, software, telephones (including cellular), voice mail, fax transmissions, video, multimedia, and instructional materials.

Information Technology Resources also include, without limitation, applications used by the System or an Institution in hosted environments in which the System or Institution does not operate the technology infrastructure such as cloud and Software-as-a-Service (Saa-S), Platform-as-a-Service (PaaS), or any other connected/hosted device or service.

Institution(s): Institutions within the Colorado State University System including CSU Fort Collins, CSU Pueblo, and CSU Global are referred to collectively as the Institutions in this policy.

Personally Identifiable Information (PII): Any Data that can identify a specific individual, either directly or indirectly. This may be an individual variable or a combination of variables within a data set that allows for identification.

Principle of Least Privilege: Data should be made available only to those people, processes, or technologies that need them for a legitimate business purpose. Access should be role-based and restricted to the minimum amount of information and time required to accomplish an employee's business function.

Research Administration Data: Any data relevant to the management and operation of research

projects and the research enterprise. Examples include, but are not limited to, information about funding sources, project timelines, personnel involved, budget expenditures, compliance records, and progress reports about research projects.

Research Data: Research Data is the recorded factual information associated with research, including, but not limited to, all records necessary for the reconstruction and evaluation of the results of research, regardless of the form or medium on which the material is recorded (such as lab notebooks, photos, digital images, data files, data processing or computer programs (software), statistical records, etc.).

- Research Data do not include books, articles, papers, or other scholarly writings that are published or publicly presented; drafts of such scholarly writings; plans for future research; peer reviews; or communications with colleagues; although Research Data may be referenced or included within books, articles, papers, or other scholarly writings.
- Research Data do not include the Research Administration Data relevant to the management and operation of research projects and the research enterprise.
- Research Data do not include information collected for the formative or summative assessment/evaluation of educational programs or services.

POLICY STATEMENT

The Colorado State University System has authority over the use of its Data as well as the Data of its Institutions and is the legal custodian of all those data. System and Institution Data are valuable assets, the use of which must be aligned with the System's strategic goals.

POLICY PROVISIONS

The System shall develop, document, periodically update, and implement policies, standards, procedures, guidelines, and training necessary to support an effective Data Governance Program to guide the strategic use, management, and reporting of System or Institution Data. The program shall ensure that Data are used in compliance with national, state, and local laws and regulations, applicable System and Institution policies, and relevant contractual obligations.

The Data Governance Program contains high-level elements outlined in this section. The Program Charter contains specific details.

A. Program Structure

The Data Governance Program shall be defined in the Program Charter, and shall address the following:

- Committee(s) and other groups that comprise the program, including meeting frequency, communications, and reporting requirements between them and to the System and its Institutions.

- Leadership (named or selected) for each committee and any other groups.
- Cross-functional representation from each Institution in committee(s) or other groups.

- Roles and responsibilities of each component of the program, including setting strategy, procuring, and administering resources, authoring and updating relevant policies, risk management, data management, procedures, and requirements for effective access to data, requirements for training, and communications related to the data environment.

B. Data Classifications

All Data must be classified at the highest level based on the risk of improper use and may have only one classification as levels are mutually exclusive. Access and use of Data is based on the Principle of Least Privilege and granted based on an individual's role within the System or Institution.

All Data Users are collectively responsible for the use and protection of all System and Institution data throughout its lifecycle. Data handling must comply with the System Information Security Policy and any other applicable System or Institutional policies, standards, procedures, or other guidance regarding data security and data privacy.

The System uses four data classification levels based on the nature of the data and the risks associated with improper use, which are set forth in this section.

Data Classification	Level 1 (Public)
Data Access	Data intended for broad use within the System or for public use.
Risk from Improper Use	Improper use of Level 1 Data results in low or no risk to the System, its Institutions, or individuals. Level 1 Data must be given normal security protection to prevent improper use.
Example Data	Examples of Level 1 Data include, but are not limited to, student Directory Information as defined by the Family Educational Rights and Privacy Act, course catalogs, financial audits, position vacancies with salary ranges, faculty education/degrees, and press releases.
Data Classification	Level 2 (Internal)
Data Access	Level 2 Data are intended for somewhat limited use within the System and/or any of its Institutions. Level 2 Data have controlled access mechanisms such as supervisor approval and may be distributed only in accordance with the Principle of Least Privilege.
Risk from Improper Use	Improper use of Level 2 Data results in moderate risk to the System, its Institutions, or individuals, including social, psychological, reputational, financial, and legal harm. Level 2 Data must be given heightened security protection to prevent improper use or disclosure.
Example Data	Examples of Level 2 Data include, but are not limited to, internal memos and other internal documents, draft reports or scholarly writings,

	marketing or other promotional information (before authorized release), floor plans, and embargoed rankings.
Data Classification	Level 3 (Confidential)
Data Access	Level 3 Data are intended for more limited use within the System and have controlled access mechanisms with additional data access controls, such as approvals from supervisors and Data Stewards. Level 3 Data or above should not be distributed to or accessed by agents outside the System on its behalf without explicit approval by the Data Governance Steering Committee.
Risk from Improper Use	Improper use of Level 3 Data results in considerable risk to the System, its Institutions, or individuals, including social, psychological, reputational, financial, and legal harm. Level 3 Data must be given high security protection to prevent improper use or disclosure.
Example Data	Examples of Level 3 Data include, but are not limited to, personnel records, donor information, passwords, assessment data, and any PII not classified as Level 4.
Data Classification	**Level 4 (Restricted)**
Data Access	Data intended for extremely limited use within the System and have strictly controlled access mechanisms. Secondary support from a supervisor and data trustees is also typically required.
Risk from Improper Use	Improper use of Level 4 Data results in severe risk to the System, its Institutions, or individuals, including civil and criminal penalties, loss of funding, and eliminating the ability for future funding or partnerships. Level 4 Data must be given the highest security protection to prevent improper use or disclosure.
Example Data	Examples of Level 4 Data include but are not limited to, biometric Data, Controlled Unclassified Information Data, Criminal Justice Information Services Data, individually identifiable financial information (e.g., bank account numbers, credit card/debit card numbers, account balances, etc.), government-issued identification and related numbers (e.g., passport, driver's license, national identification number, national identity card, Social Security Number, taxpayer identification numbers, visa numbers, etc.), and any other information with federal security compliance requirements.

C. Training

No request for Data access will be granted for Level 2-4 Data without appropriate training. Processes for requesting data access and completing training for each level are described in the Data Governance Program Charter.

ROLES AND RESPONSIBILITIES

All individuals to whom this policy applies are responsible for becoming familiar with and following this policy.

Data Trustees: A Data Trustee is responsible for the subset of System or Institution Data to which they have been assigned oversight.

- These individuals have compliance responsibility for their designated data set(s);
- They appoint and maintain accountability for one or more Data Stewards for their designated data set(s);
- Trustees ensure Data Stewards are appropriately trained for their roles;
- They support the objectives and operation of the CSU System Data Governance Program;
- They promptly review and approve/deny Data access requests forwarded by their Data Stewards.

Data Stewards: Data Stewards are designated by and accountable to Data Trustees. Data Stewards are responsible for working collaboratively together in operational tasks and as defined in the Data Governance Program, to promote a culture that embraces the responsible use and handling of System or Institution Data throughout its lifecycle. The Data Steward must attend required training appropriate to their designated data set(s) before being authorized to function as a Data Steward and participate regularly in management of and coordination and communication with their Data Users.

- Data Stewards are responsible for the appropriate classification of the Data within their designated Institution data set(s);
- They share knowledge of appropriate Data use, Data quality, and management procedures;
- They communicate process or definitional changes that may affect systems or analytics relating to specific Data elements;
- These individuals maintain oversight of the Data Users under their authority by understanding their business needs for Data access, promptly reviewing and approving or denying requests for Data access from potential Data Users, and informing Data Trustees when responsibilities or job duties have changed such that a Data User's access to System or Institution Data should be revoked. They will maintain a current list of Data Users under their authority that will include data access and revocation dates.
- Data Stewards ensure Data Users have the knowledge, expertise, and ability to access, manipulate, and generate high-quality reports from System or Institution Data. This includes oversight of training materials, processes, and completion for their designated Institution data set(s).

Data Users: Data Users are all students, faculty, staff, contractors, consultants, affiliates, and any others granted use of Information Technology Resources or Data at the System or any of its Institutions. They are granted permission to access Data by their Data Steward, as approved by the appropriate Data Trustee(s).

Data Users must:

- Complete training on the appropriate definition, access, storage and use of data sets and centrally managed enterprise reporting tool(s).
- Adhere to the Principle of Limited Privilege accessing only the minimum amount of Data required to perform their business functions.
- Access Data only in their conduct of official System or Institution business, and in ways consistent with furthering the System or Institution mission of education, research, and public service.
- Preserve the confidentiality and privacy of individuals whose records they may access.
- Observe any ethical restrictions that apply to the data to which they have access.
- Abide by applicable laws, regulations, standards, and policies regarding access, use, disclosure, retention, and/or disposal of information.

Data Users must NOT:

- Disclose data to others except as required by their job responsibilities and approved by their Data Steward.
- Use Data for their own or others' personal gain or profit.
- Access Data to satisfy personal curiosity.
- Store Data in any manner that violates existing university policies.
- Share passwords to access data.

COMPLIANCE WITH THIS POLICY

Assistance with policy compliance is provided by the Division of Information Technology.

Failure to comply with this policy may result in disciplinary action in accordance with applicable Institution disciplinary policies.

REFERENCES

The Division of IT provides a variety of information regarding Data protection that is useful in the implementation of this policy.

The CSU System maintains the most current copy of all System policies.

- Acceptable Use Policy
- IT Security Policy

Additional relevant policies and statutes:

- Colorado Open Records Act (CORA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Colorado State Records Retention Schedule
- Americans with Disabilities Act (ADA)
- Family Educational Rights and Privacy Act (FERPA)
- The Electronic Communications Privacy Act of 1986 (ECPA)
- Federal Trade Commission (FTC) Red Flags Rule
- Gramm Leach Bliley Act (GLBA)
- Colorado State University Research Data Policy
- Intellectual Property—Copyrights and Patents
- General Data Protection Regulation

APPROVALS

Policy Owner

Colorado State University System

Brandon Bernier, Vice President of Information Technology and Chief Information Officer

By: /x/

Date: 5/12/2025

Legal Review

Colorado State University System

Office of General Counsel

Jason L. Johnson, Deputy General Counsel

By: /x/
Date: 5/11/2025

FINAL APPROVAL:

Colorado State University System

Anthony A. Frank, Chancellor

By: /x/
Date: 5/11/2025