



ADMINISTRATIVE POLICY STATEMENT

Policy Title: Data Governance

APS Number: 6010

APS Functional Area: **INFORMATION TECHNOLOGIES**

Brief Description: The Data Governance Program serves to ensure that data is managed as a material asset. The university has established a data governance program with the goals of ensuring that data provides value, meets compliance requirements, and risks are managed appropriately. Given that poor handling of data poses a risk to the university, it is necessary to define roles and responsibilities for certain types of data.

Effective: July 1, 2024

Approved by: President Todd Saliman

Responsible University Officer: Chair of Data Governance Executives Council

Responsible Office: Data Governance Executives Council

Policy Contact: data.governance@cu.edu

Supersedes: July 1, 2018, Data Governance

Last Reviewed/Updated: July 1, 2024

Applies to: Universitywide

Reason for Policy: Define roles and responsibilities to enable the university to exercise positive control over the processes and methods used to handle data and assure that university employees and administrative processes have appropriate access to reliable, authentic, accurate, and timely data. Data governance authority rests ultimately with the president and chancellors; this policy defines roles and responsibilities to assist the president and chancellors.

I. INTRODUCTION

The policy covers *university records* and *university information*; data that is governed by federal or state law or regulations; and data to which external contract requirements apply regardless of where this data is stored, processed, or transmitted. These items, together, will be defined as data assets. Excluded from the scope of this policy is intellectual property, that is considered educational materials, and they are covered by [APS 1014 – Educational Property That is Educational Materials](#).

II. POLICY STATEMENT

The data governance program shall be managed and monitored collaboratively by the *data trustees*, Data Governance Executives Council (DGEC) and all other applicable, in force governance groups not mentioned here within. Roles and responsibilities for data governance are as follows:

- A. *Data governance executives* are accountable for oversight of data governance activities across all data types and domains at their university. One *data governance executive* will be appointed for each campus and CU System. *Data governance executives* are appointed by the president, chancellors, or their delegates and are typically senior administrative officers of the university. *Data governance executives* may also serve as *data trustees*.

- B. *Data governance executives* provide cross-university guidance and leadership for the data governance program. DGEC works in partnership with *data trustees* to set direction, determine strategic priorities and identify appropriate objectives, and manage the progress of governance for all domains. Annually, DGEC will compile a summary report on the data governance structure's effectiveness and recommendations for improvement to *IT Governance*.
- C. *Data trustees* are accountable for managing, protecting, and ensuring the integrity and usefulness of university data. *Data trustees* are responsible for ensuring the university is following its policies and complies with federal and state laws and regulations. *Data trustees*, in consultation with DGEC, shall identify the criticality and sensitivity of data. *Data trustees* are appointed by the president, chancellors, or their delegates and are typically an administrative officer of the university or departmental director.
- D. *Data stewards* will often have data custodial responsibilities but are distinguished from *custodians* by delegated decision-making authority from the *data trustees*, including identification of the criticality and sensitivity of data. *Data stewards* actively participate in processes that establish business-context and quality definitions for data elements. *Data stewards* are more likely to be associated with business functions than IT functions.
- E. *Data custodians* typically have control over a data asset's disposition, whether stored (at rest), in transit, or during creation. Custodians will often have modification or distribution privileges. *Data custodians* carry a significant responsibility to protect data and prevent unauthorized use. *Data custodians* often provide data to *data users*. *Data trustees* or *data stewards* may also exercise custodial roles and responsibilities. *Data custodians* typically are associated with IT units within the university, either central IT organizations or IT offices within academic and administrative units.
- F. To the degree that a *data user* creates university data and/or controls the disposition of university data, they have responsibility for the custodial care of that data. *Data users* share responsibility in helping *data stewards* and *custodians* manage and protect data by understanding and following university IT and information privacy and security policies.

The Chair of the DGEC shall maintain and publish a list of identified *data executives*, *data trustees* and *data stewards* for specific data types. The list will also identify the classification of specific data types. Where a single individual maintains multiple roles (e.g., *data steward* and *data custodian*) the Chair of DGEC will provide notice to the DGEC to ensure the roles do not pose a risk to the university.

Each campus *Data Governance Executive* shall be responsible for providing data management guidance to *data trustees* and establishing appropriate data governance structures. When data management issues or risks regarding data overlaps between multiple campuses are identified, the campus *Data Governance Executive* and the campus *data trustee(s)* shall present the issues and recommendations to the DGEC.

It is the *data steward's* responsibility to understand the university unit's business needs and facilitate appropriate access to the required data. The *data steward* will also coordinate with the campus or system Information Security Officer to ensure that adequate security controls are identified and implemented. Should the *data steward* have questions regarding the legitimacy of the university unit's business need, the *data steward* shall validate the need with the *data trustee* and *Data Governance Executive*.

Data stewards, in consultation with the appropriate campus or system Information Security Officer shall establish processes for requesting and monitoring access to data, in accordance with [CU Data Classification and CU policies, procedures, and standards](#).

When university units create shared data repositories, they take on responsibilities as *data custodians*. As such, units must work with the appropriate *data trustees(s)* to ensure that they understand external regulatory and university policy compliance requirements. *Data custodians* may not extend the use of university data beyond the initial scope of approved usage without additional review by the appropriate delegated *data steward*. When shared data repositories are created on third-party services, contracts or service agreements must include appropriate security and privacy provisions, which are covered separately through procurement processes that may differ by campus. (Check the [Procurement Service Center](#) for up-to-date links on the procurement process.)

The CU Data Governance Procedure Statement and Operating Model, published on the Data Governance Program website, provides an escalation pathway for Data Governance and Management conflict or issue resolution. For

example, decisions made by *Data Stewards* with data management implications crossing multiple campuses may be appealed to the DGEC, who will bring together all appropriate stakeholders to inform the final decision. Final decision-making responsibility rests with the DGEC, who is accountable to the [IT Governance Process](#) should DGEC be unable to come to a resolution on their own.

Each campus and System Administration shall adopt the Data Governance Program and may establish campus-specific policies, standards, and procedures to meet unique campus needs, provided they do not conflict with the requirements in the Data Governance Program or require systemwide resources.

III. DEFINITIONS

Italicized terms used in this Administrative Policy Statement (APS) are defined in the [APS Glossary of Terms](#) or are defined in this section.

- A. *Data governance executive* is an individual appointed to be accountable for oversight of data governance activities across all data types and domains at their campus.
- B. *Data trustee* is an individual appointed to have primary authority and decision responsibility over a particular collection of university data. CU System data trustees and/or campus data trustees are identified on this [page](#).
- C. *Data custodian* is an individual charged with managing a data collection for a *data trustee*.
- D. *Data steward* is an individual possessing delegated authority to act on a *data trustee's* behalf. Trustees may delegate specific roles to a steward to act on their behalf.
- E. *Data user* is any individual that utilizes university data to perform their job responsibilities.
- F. *IT Governance* is defined as described in <https://www.cu.edu/it-gov/about>

IV. RELATED RESOURCES

- Data Governance Website – <http://www.cu.edu/data-governance>

V. HISTORY

- Adopted: January 1, 2013.
- Revised: May 1, 2014 - The title of “IT Security Principals” was replaced with the title of “Information Security Officers”); July 1, 2018; July 9, 2018 (Removed reference to APS 2006 for the definition of university record. That definition is now included in the APS Glossary of Terms); July 1, 2024.
- Last Reviewed: July 1, 2024.