University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Data Governance

APS Number: 6010 **APS Functional Area:** **INFORMATION TECHNOLOGIES**

Brief Description:	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 handing of data poses a risk to the university it is necessary to define roles and responsibilities for certain types of data.
Effective:	July 1, 2018
Approved by:	President Bruce D. Benson
Responsible University Officer:	Vice President of Administration
Responsible Office:	Office of the Vice President of Administration
Policy Contact:	Chief Information Security Officer
Supersedes:	6010 Data Governance, January 17, 2013
Last Reviewed/Updated:	July 1, 2018
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*, data where federal or state regulations exists, and data where external contract requirements exists regardless if the data is stored on a university-owned or managed system or on a third-party hosted service. Excluded from the scope of this policy is intellectual property that is educational materials.

II. POLICY STATEMENT

The program shall be managed and monitored collaboratively by University Counsel, Chief Information Security Officer, *data trustees*, and Chief Information Officers. Roles and responsibilities for data governance are as follows:

- *Data trustees* are accountable for managing, protecting, and ensuring the integrity and usefulness of university data. *Data trustees* have the primary responsibility to ensure the university is following its policies and is in compliance with federal and state laws and regulations. *Data trustees*, in consultation with the Council of Data Trustees, shall identify the criticality and sensitivity of data. *Data trustees* typically are associated with the business functions of an organization rather than technology functions. *Data trustees* are appointed by the president, chancellors, or their delegates and are typically an administrative officer of the university or departmental director. The president or chancellor may choose to not identify a *data trustee* for certain data types given risk decisions or administrative, research, or academic needs.

- *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* are often data providers to *data user*. *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.

- *Data stewards* will often have data custodial responsibilities, but are distinguished from custodians by delegated decision-making authority regarding the data. *Data stewards* may represent *data trustees* in policy discussions, architectural discussions, or in decision-making forums. *Data stewards* actively participate in processes that establish business-context and quality definition for data elements. *Data stewards* are more likely to be associated with business functions than IT functions.

- To the degree that a *data user* creates university data and/or controls the disposition of university data, he or she has responsibility for the custodial care of that data. *Data user* share responsibility in helping *data stewards* and custodians manage and protect data by understanding and following the IT and information security policies of the university related to data use.

When university units create shared data repositories they take on responsibilities as *data custodians*. As such units must work with *data stewards* 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 without additional review by the appropriate *data steward*. When shared data repositories are created on third-party services, special care must be made to ensure that contracts or service agreements include appropriate security and privacy.

It is the responsibility of the *data steward* to understand business needs of the university unit and facilitate appropriate access to the required data. The *data steward* will also coordinate with the campus 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*.

Data stewards, in consultation with the appropriate Campus Information Security Officer or the Office of Information Security shall publish processes for requesting and monitoring access to data and periodically audit access to data. *Data stewards* shall, at least annually, provide the *data trustee* with information regarding the management, protection, and effectiveness of efforts to ensure the integrity and usefulness of university data. For example, how data is being used, identify data quality issues, and report on compliance issues.

The Chief Information Security Officer shall maintain and publish a list of identified *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 CISO will provide notice to the Counsel of Data Trustees to ensure the roles do not pose a risk to the university.

Each campus or division Chief Information Officer 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 data domains are identified, the appropriate Chief Information Officer and *data trustee* shall present the issues and recommendations to the CU IT Governance Board for resolution.

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 trustee* is a party or entity identified with and widely recognized to have primary authority and decision responsibility over a particular collection of university data. The Council of Data Trustees list is included on this page.
B. *Data custodian* is any party charged with managing a data collection for a *data trustee*.
C. *Data steward* is a party or entity possessing delegated authority to act on a *data trustee's* behalf.
D. *Data user* is any person or party that utilizes university data to perform his or her job responsibilities.

IV. HISTORY

- Originally approved January 1, 2013.
- The title of "IT Security Principals" was replaced with the title of "Information Security Officers" effective May 1, 2014.
- Revised 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.

V. KEY WORDS

Data, governance, information technology, compliance, risk, records, security.