FEEDBACK

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~~ are 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~~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, 2018~~TBD (Pending)
Approved by:	~~President Bruce D. Benson~~President Todd Saliman (Pending)
Responsible University Officer:	~~Vice President of Administration~~Chair of Data Governance Executives Council
Responsible Office:	~~Office of the Vice President of Administration~~Data Governance
Policy Contact:	~~Chief Information Security Officer~~data.governance@cu.edu
Supersedes:	6010 Data Governance, ~~January 17, 2013~~July 1, 2018
Last Reviewed/Updated:	~~July 1, 2018~~TBD (Pending)
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 exist~~s~~;, and data where external contract requirements exist~~s~~ regardless of where this data is stored, processed, or transmitted~~if the data is stored on a university-owned or managed system or on a third-party hosted service~~. *University records* are any form of recorded information, regardless of physical characteristics, that is created, received, maintained, or legally filed in the course of university business. 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,~~ the *data trustees,* Data Governance Executives Council, and the IT Governance Group~~*data trustees*, and Chief Information Officers~~. Roles and responsibilities for data governance are as follows:

A. The Data Governance Executives Council (DGEC) provides cross-university guidance and leadership for the data governance program. It is comprised of one *data governance executive* from 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. The chair(s) is elected by consensus of the DGEC. At least annually, the Data Governance Executives Council will compile 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.

B. *Data governance executives* are accountable for oversight of data governance activities across all data types and domains at their university. They work in partnership with *data trustees* to set direction, determine strategic priorities and identify appropriate objectives, and manage the progress of data governance for all domains. When data management issues or risks regarding data overlaps between multiple campuses are identified, the appropriate *data governance executive* and *data trustee*(s) shall present the issues and recommendations to the Data Governance Executives Council for resolution.

~~B.~~C. *Data trustees* are accountable for managing, protecting, and ensuring the integrity and usefulness of university data. *Data trustees* ~~have the primary responsibility~~are primarily responsible 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~~Data Governance Executives Council, shall identify the criticality and sensitivity of data. Individual *data trustees* may delegate this responsibility to a Data Stewardship Council or *data steward.* *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.~~

D. *Data stewards* will often have data custodial responsibilities but are distinguished from *data custodians* by their decision-making authority regarding the data, as delegate by the *data trustee 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.

~~C.~~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 over data assets in their purview. *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 custodians* oversee the deployment of appropriate policies, which may include data maintenance of operational transactional data systems, data quality assurance using definitions provided by data stewards, integration of data with internal and external data systems, applying system upgrades, internal audit reporting, risk identification, and remediation of system issues that may affect the confidentiality, integrity, or availability of data. *Data custodians* typically are associated with IT units within the university, either central IT organizations or IT offices within academic and administrative units.

~~D. *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.~~

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

The Chair of the Data Governance Executives Council shall maintain and publish a list of identified *data executives*, *data trustees* and *data stewards* for specific data types on the Data Governance Program website. Where a single individual maintains multiple roles (e.g., *data trustee* and *data steward*) the Chair of the Data Governance Executives

Council will provide notice to the Data Governance Executives Council to ensure the roles do not pose a risk to the university.

~~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 System Office of Information Security shall ~~publish~~ establish processes for requesting and monitoring access to data, in accordance with existing CU policies, procedures, and standards. ~~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.~~

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 of approved usage 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.

The CU Data Governance Procedure Statement and Operating Model, published on the Data Governance Program website, provide an escalation pathway for Data Governance and Management conflict or issue resolution. For example, decisions made by Data Stewards may be appealed to the Data Governance Executives Council, who will bring together the appropriate stakeholders to inform, make, and enforce the final decision. Final decision-making responsibility rests with the Council of Data Governance Executives, who are accountable to the IT Governance Process should they be unable to come to resolution on their own.

Each campus and System Administration shall adopt the Data Governance Program and may create campus-specific policies, standards, and procedures to meet special campus needs, if 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 a party or entity appointed to be accountable for oversight of data governance activities across all data types and domains at their campus.

~~A.~~B. *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, and holds the responsibilities outlined in ~~APS 6010~~section II.C. The Council of Data Trustees list is included on this page.

~~B.~~C. *Data custodian* is any party charged with managing a data collection for a *data trustee*, and holds the responsibilities outlined in ~~APS 6010~~section II.E.

~~C.~~D. *Data steward* is a party or entity possessing delegated authority to act on a *data trustee's* behalf, and holds the responsibilities outlined in ~~APS 6010~~section II.D.

E. *Data user* is any person or party that utilizes university data to perform ~~his or her~~their job responsibilities, and holds the responsibilities outlined in ~~APS 6010~~section II.F.

~~D.~~F. *University records* are any form of recorded information, regardless of physical characteristics, that is created, received, maintained, or legally filed in the course of university business.

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; TBD (Pending).

~~V. KEY WORDS~~

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