



ADMINISTRATIVE POLICY STATEMENT

1 **Policy Title:** Data Governance

2 **APS Number:** 6010

APS Functional Area: **INFORMATION TECHNOLOGIES**

3

Brief Description: [The Data Governance Program serves to](#) ensure that data is managed as a material asset. ~~the~~[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: ~~TBD based on review process July 1, 2018~~ [July 1, 2024 \(Pending\)](#)

Approved by: ~~President Todd Saliman (Pending)~~ [President Bruce D. Benson](#)

Responsible University Officer: ~~Chair of Data Governance Executives Council~~ [Vice President of Administration](#)

Responsible Group/Office: ~~Data Governance Executives Council~~ [Office of the Vice President of Administration](#)

Policy Contact: data.governance@cu.edu [Chief Information Security Officer](#)

Supersedes: 6010 Data Governance, ~~July 1, 2018~~ [January 17, 2013](#)

Last Reviewed/Updated: ~~July 1, 2024~~ ~~TBD (Pending)~~ [July 1, 2018](#)

Applies to: University-wide

4

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

9

10 **I. INTRODUCTION**

11

12 The policy covers *university records and university information*; data ~~that is governed by where~~ federal or state [law or](#)
13 [regulations](#); ~~exists~~, and data ~~to which where~~ external contract requirements [apply](#) ~~exists~~ regardless ~~of where this~~ if the data
14 is stored, [processed or transmitted](#). ~~These items, together, will be defined as data assets, on a university-owned or~~
15 [managed system or on a third-party hosted service](#). ~~Excluded from the scope of this policy is intellectual property, that~~
16 is [considered](#), educational materials, ~~and there covered by APS1014~~.

17

18 **II. POLICY STATEMENT**

19

20 The [data governance](#) program shall be managed and monitored collaboratively ~~by by the data trustees, Data~~
21 [Governance Executives Council \(DGEC\) and all other applicable, in-force governance groups not mentioned here](#)
22 [within University Counsel, Chief Information Security Officer, data trustees, and Chief Information Officers](#). Roles
23 and responsibilities for data governance are as follows:
24
25
26

- 27 • Data governance executives are accountable for oversight of data governance activities across all data types and
 28 domains at their university. One data governance executive will be appointed for each campus and CU System.
 29 Data governance executives are appointed the president, chancellors, or their delegates and are typically senior
 30 administrative officers of the university. Data governance executives may also serve as data trustees.
 31
- 32 • Data governance executives provide cross-university guidance and leadership for the data governance program.
 33 DGEC works in partnership with data trustees to set direction, determine strategic priorities and identify
 34 appropriate objectives, and manage the progress of governance for all domains. Annually, DGEC will compile a
 35 summary report on the data governance structure's effectiveness and recommendations for improvement to IT
 36 Governance
 37
- 38 • Data trustees are accountable for managing, protecting, and ensuring the integrity and usefulness of university data.
 39 Data trustees ~~archave the primary~~ responsibility ~~for~~to ensure the university is following its policies and ~~is in~~
 40 compliance with federal and state laws and regulations. Data trustees, in consultation with ~~DGEC the Council of~~
 41 Data Trustees, shall identify the criticality and sensitivity of data. ~~Data trustees typically are associated with the~~
 42 ~~business functions of an organization rather than technology functions.~~ Data trustees are appointed by the
 43 president, chancellors, or their delegates and are typically an administrative officer of the university or departmental
 44 director. ~~The president or chancellor may choose to not identify a data trustee for certain data types given risk~~
 45 ~~decisions or administrative, research, or academic needs.~~
 46
- 47 • ~~Data stewards will often have data custodial responsibilities but are distinguished from custodians by delegated~~
 48 ~~decision-making authority from the data trustees, including identification of the criticality and sensitivity of data.~~
 49 ~~Data stewards actively participate in processes that establish business-context and quality definitions for data~~
 50 ~~elements. Data stewards are more likely to be associated with business functions than IT functions. Data custodians~~
 51 ~~typically have control over a data asset's disposition, whether stored (at rest), in transit, or during creation.~~
 52 ~~Custodians will often have modification or distribution privileges. Data custodians carry a significant~~
 53 ~~responsibility to protect data and prevent unauthorized use. Data custodians are often data providers to data user.~~
 54 ~~Data trustees or data stewards may also exercise custodial roles and responsibilities. Data custodians typically are~~
 55 ~~associated with IT units within the university, either central IT organizations or IT offices within academic and~~
 56 ~~administrative units.~~
 57
- 58 • Data custodians typically have control over a data asset's disposition, whether stored (at rest), in transit, or
 59 during creation. Custodians will often have modification or distribution privileges. Data custodians carry a
 60 significant responsibility to protect data and prevent unauthorized use. Data custodians often provide data to
 61 data users. Data trustees or data stewards may also exercise custodial roles and responsibilities. Data
 62 custodians typically are associated with IT units within the university, either central IT organizations or IT
 63 offices within academic and administrative units.
 64
- 65 • ~~Data stewards will often have data custodial responsibilities, but are distinguished from custodians by delegated~~
 66 ~~decision-making authority regarding the data. Data stewards may represent data trustees in policy discussions,~~
 67 ~~architectural discussions, or in decision-making forums. Data stewards actively participate in processes that~~
 68 ~~establish business context and quality definition for data elements. Data stewards are more likely to be associated~~
 69 ~~with business functions than IT functions.~~
 70
- 70 • To the degree that a data user creates university data and/or controls the disposition of university data, he or she has
 71 responsibility for the custodial care of that data. Data users share responsibility in helping data stewards and
 72 custodians manage and protect data by understanding and following ~~university~~ the IT and information privacy and
 73 security policies, ~~of the university related to data use.~~
 74

The Chair of 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 DGEC 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

82 ~~review by the appropriate *data steward*. When shared data repositories are created on third-party services, special care~~
 83 ~~must be made to ensure that contracts or service agreements include appropriate security and privacy.~~

84
 85 Each campus *Data Governance Executive* shall be responsible for providing data management guidance to *data trustees*
 86 and establishing appropriate data governance structures. When data management issues or risks regarding data overlaps
 87 between multiple campuses are identified, the campus *Data Governance Executive* and the campus *data trustee(s)* shall
 88 present the issues and recommendations to the DGEC. It is the responsibility of the *data steward* to understand business
 89 needs of the university unit and facilitate appropriate access to the required data. The *data steward* will also coordinate
 90 with the campus Information Security Officer to ensure that adequate security controls are identified and implemented.
 91 Should the *data steward* have questions regarding the legitimacy of the university unit's business need the *data steward*
 92 shall validate the need with the *data trustee*.

93
 94 It is the data steward's responsibility to understand the university unit's business needs and facilitate appropriate access
 95 to the required data. The *data steward* will also coordinate with the campus or system Information Security Officer to
 96 ensure that adequate security controls are identified and implemented. Should the *data steward* have questions regarding
 97 the legitimacy of the university unit's business need, the *data steward* shall validate the need with the *data trustee and*
 98 *Data Governance Executive*.

99
 100 ~~*Data stewards*, in consultation with the appropriate cCampus or system Information Security Officer ~~or the Office of~~~~
 101 ~~Information Security shall establishpublish processes for requesting and monitoring access to data, in accordance~~
 102 ~~with CU Data Classification and CU policies, procedures, and standards, and periodically audit access to data. *Data*~~
 103 ~~*stewards* shall, at least annually, provide the *data trustee* with information regarding the management, protection,~~
 104 ~~and effectiveness of efforts to ensure the integrity and usefulness of university data. For example, how data is being~~
 105 ~~used, identify data quality issues, and report on compliance issues.~~

106
 107 When university units create shared data repositories, they take on responsibilities as *data custodians*. As such, units
 108 must work with the appropriate *data trustee(s)* to ensure that they understand external regulatory and university policy
 109 compliance requirements. *Data custodians* may not extend the use of university data beyond the initial scope without
 110 additional review by the appropriate delegated *data steward*. When shared data repositories are created on third-party
 111 services, contracts or service agreements must include appropriate security and privacy provisions, which are covered
 112 separately through procurement processes that may differ by campus. [Check the Procurement Service Center website
 113 for up-to-date links on the procurement process]

114 ~~The Chief Information Security Officer shall maintain and publish a list of identified *data trustees* and *data stewards* for~~
 115 ~~specific data types. The list will also identify the classification of specific data types. Where a single individual~~
 116 ~~maintains multiple roles (e.g., *data steward* and *data custodian*) the CISO will provide notice to the Counsel of Data~~
 117 ~~Trustees to ensure the roles do not pose a risk to the university.~~

118
 119 The CU Data Governance Procedure Statement and Operating Model, published on the Data Governance Program
 120 website, provide an escalation pathway for data governance and management conflict or issue resolution. For example,
 121 decisions made by *data stewards* with data management implications crossing multiple campuses may be appealed to
 122 the DGEC, who will bring together all appropriate stakeholders to inform the final decision. Final decision-making
 123 responsibility rests with the DGEC, who is accountable to the IT Governance Process should DGEC be unable to come
 124 to a resolution on their own.

125
 126 Each campus and System Administration shall adopt the Data Governance Program and may establish campus-specific
 127 policies, standards, and procedures to meet unique campus needs, provided they do not conflict with the requirements in
 128 the Data Governance Program or require systemwide resources.

129 ~~Each campus or division Chief Information Officer shall be responsible for providing data management guidance to~~
 130 ~~*data trustees* and establishing appropriate data governance structures. When data management issues or risks regarding~~
 131 ~~data overlaps between multiple data domains are identified, the appropriate Chief Information Officer and *data trustee*~~
 132 ~~shall present the issues and recommendations to the CU IT Governance Board for resolution.~~

133
 134
 135 **III. DEFINITIONS**

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

139
 140 A. *Data governance executive* is an individual appointed to be accountable for oversight of data governance
 141 activities across all data types and domains at their campus.

142 ~~A-B.~~ *Data trustee* is an ~~individual party or entity identified with and widely recognized~~ to have primary
 143 authority and decision responsibility over a particular collection of university data. [CU System data trustees and/or](#)
 144 [campus data trustees are identified on this page.](#)~~The Council of Data Trustees list is included on this page.~~

145 ~~B-C.~~ *Data custodian* is an ~~individual y party~~ charged with managing a data collection for a ~~data trustee~~*trustee*.

146 ~~C-D.~~ *Data steward* is an ~~individual party or entity~~ possessing delegated authority to act on a *data trustee's* behalf.
 147 [Trustees may delegate specific roles to a steward to act on their behalf.](#)

148 E. *Data user* is any individual~~person or party~~ that utilizes university data to perform his or her job
 149 responsibilities.

150 ~~D-F.~~ *IT Governance* is defined as described in <https://www.cu.edu/it-gov/about>

151
 152 **IV. HISTORY**

- 153 • Originally approved January 1, 2013.
- 154 • The title of “IT Security Principals” was replaced with the title of “Information Security Officers” effective May 1,
 155 2014.
- 156 • Revised July 1, 2018.
- 157 • July 9, 2018: Removed reference to APS 2006 for the definition of university record. That definition is now
 158 included in the APS Glossary of Terms.

160
 161 **V. KEY WORDS**

162 Data, governance, information technology, compliance, risk, records, security.
 163
 164