I. INTRODUCTION

The policy covers university records and university information, data that is governed by federal or state law or regulations exists, and data to which external contract requirements apply exists 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. These items, together, will be defined as data assets. 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 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 University Counsel, Chief Information Security Officer, the data trustees, Data Governance Executives Council, and the IT Governance Group. 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**. 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.

A-B. The **Data Governance Executives Council (DGEC)** provides 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. 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-C. **Data trustees** are accountable for managing, protecting, and ensuring the integrity and usefulness of university data. **Data trustees** have primary responsibility for ensuring the university is following its policies and is in compliance with federal and state laws and regulations. **Data trustee**, in consultation with the DREC, 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 delegated decision-making authority from the **data trustees**, including identification of the criticality and sensitivity of data regarding the data, as delegated 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 definitions 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 responsible to data users. **Data custodians** 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.

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, they 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 university IT and security policies of the university related to data use.

The Chair of the Data Governance Executives’ Council (DGEC) shall maintain and publish a list of identified data stewards, data trustees, and data stewards for specific data types on the Data Governance Program website. The list will also identify the classification of specific data types. Where a single individual maintains multiple roles (e.g., data trustee (steward) and data steward (custodian)), the Chair of the Data Governance Executives’ Council (DGEC) will provide notice to the Data Governance Executives’ Council (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 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.

Each campus Data Governance Executive shall be responsible for providing data management guidance to data stewards 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 steward(s) shall present the issues and recommendations to the DGEC. 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.

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 or the System Office of Information Security, shall publish, establish processes for requesting and monitoring access to data, in accordance with existing CU Data Classification and 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 the appropriate data stewards and 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, special care must be made to ensure that 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 website 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 Data Governance Executives Council (DGEC), who will bring together all the appropriate stakeholders to inform, make, and enforce the final decision. Final decision-making responsibility rests with the Council of Data Governance Executives (DGEC), who are 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 create campus-specific policies, standards, and procedures to meet unique campus needs, provided, 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 an individual party or entity 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 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. CU System data trustees and/or campus data trustees are identified on this page. The Council of Data Trustees list is included on this page.

C. Data custodian is any party individual charged with managing a data collection for a data trustee, and holds the responsibilities outlined in APS 6010.

D. Data steward is an individual party or entity possessing delegated authority to act on a data trustee's behalf, and holds the responsibilities outlined in APS 6010. Trustees may delegate specific roles to a steward to act on their behalf.

E. Data user is any individual person or party that utilizes university data to perform his or her job responsibilities, and holds the responsibilities outlined in APS 6010.

F. IT Governance is defined as described in https://www.cu.edu/it-gov/about. 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. RELATED RESOURCES

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

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: July 1, 2024 (Pending).

V. KEY WORDS

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