UNIVERSITY OF DENVER	**UNIVERSITY OF DENVER POLICY MANUAL INSTITUTIONAL DATA MANAGEMENT**	
Responsible Department: Vice Chancellor for Information Technology **Recommended By:** Provost and Executive Vice Chancellor, Senior Vice Chancellor for Business and Financial Affairs, Vice Chancellor for Information Technology **Approved By:** Chancellor	**Policy Number** IT 13.10.050	**Effective Date** 1/11/2023

I. INTRODUCTION

The University owns all institutional data (as defined below). The University adopts this Policy to establish uniform data management standards for institutional data and identify the shared responsibilities of members of the University community for: i) protecting the integrity of institutional data, and ii) utilizing institutional data to serve the decision-making needs of the University.

II. POLICY OVERVIEW

A. The value of data as an institutional resource is increased through its widespread and appropriate use. Conversely, the value of data is diminished through misuse, misinterpretation, or unnecessary restrictions on access.

B. The University grants permission to access institutional data to eligible employees and designated appointees of the University for legitimate University purposes.

C. Users of institutional data must:
1. access data only for conducting University business;
2. respect the confidentiality and privacy of individuals whose records are accessed;
3. safeguard and maintain the confidentiality and privacy of personally identified and personally identifiable information;
4. observe ethical restrictions that apply to the data; and
5. abide by applicable laws, regulations, policies and procedures with respect to access, use, disclosure, retention, and/or disposal of the data.

D. Users of institutional data must not:
1. disclose data to others except as required by their job responsibilities;
2. use data for their own or others' personal gain or profit; or

3. access data to satisfy personal curiosity.

E. IT - Enterprise Application Services ("IT-EAS") is responsible for partnering with Data Trustees in the development of procedures to meet the objectives embodied in this Policy.

III. PROCESS OVERVIEW

A. DATA ADMINISTRATION

1. University Ownership.

All institutional data is owned by the University. All members of the University community have the obligation to appropriately use and safeguard institutional data in all formats and in all locations.

2. Stewardship.

Roles and responsibilities for safeguarding and classifying institutional data are defined in subparagraph C below (Data Management Roles and Responsibilities).

B. DATA CLASSIFICATION

In accordance with University Policy IT 13.10.51 – *Data Classification,* institutional data is categorized as Public, Internal, Confidential, or Restricted.

C. DATA MANAGEMENT ROLES AND RESPONSIBILITIES

1. *Data Trustee*: Data Trustees are University officials who have planning and policy-making responsibilities for institutional data and for the establishment of operational processes to collect and record data in accordance with University business rules. The Data Trustees, as a group, are responsible for overseeing the establishment of institutional data management procedures, and for the assignment of data management accountability.

2. *Data Steward*: Data Stewards are typically operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for the transactional systems. Data Stewards are appointed by the respective Data Trustee. The Data Steward is responsible for implementing this Policy and the applicable procedures established by the Data Trustee(s), specifying best practices, and identifying adequate resources that enable Data

Custodians to implement best practices. Data Stewards are the first escalation point for problem resolution.

3. *Data User*: Data Users are individuals who access institutional data to perform their assigned duties. Data Users are responsible for safeguarding their access privileges, for the use of the institutional data in conformity with all applicable University policies, and for securing such data.

4. *Data Custodian*: Data Custodians are information technology experts assigned to each transactional and reporting system which maintains institutional data. Data Custodians oversee the safe transport and storage of data, establish and maintain the underlying infrastructure, set security measures, and perform activities required to keep the data intact and available to users.

In addition, Data Custodians are responsible for working with Data Stewards to develop automated processes which identify erroneous, inconsistent, or missing data. Data Custodians work with data support groups, the Office of Institutional Research & Analysis, and Data Stewards to resolve data issues.

D. ACCESS AND CONFIDENTIALITY

1. Access to University institutional data is based on the business needs of the applicable unit.

2. Data Users will be granted secure access to view or query institutional data on a “need to know” basis for the purposes of performing legitimate administrative, research, academic and other official responsibilities pertaining to the mission of the University. Examples include, but are not limited to, planning, decision making, and official reporting.

a. The "need to know" basis exists when certain conditions are met, including, but not limited to:

i. The institutional data is needed to improve services to faculty, staff, students, and other University constituents.

ii. Access to institutional data increases the understanding, usefulness, and ease of use of the data, and/or maximizes efficiency of human, physical, and digital resources.

iii. Integration of institutional data with other data and information or applications increases the value of the institutional data to those who may use it.

b. Curiosity does not constitute a "need to know." Access to institutional data for academic research and inquiry may be approved subject to privacy rules and regulations, and appropriate institutional review.

c. Access to institutional data will be granted subject to best practices for data and information management and analysis and should minimize duplication of data and information capture, storage, maintenance, and retrieval.

3. In order that the proper controls are applied, it is the responsibility of each person accessing institutional data to:
a. Know the classification of the system being used.
b. Know the type of institutional data being used.
c. Follow the appropriate security measures.
d. Consult the related policies for further information.

E. TRAINING

The Data Trustees are responsible for establishing required training for individuals that manage Institutional Data, as appropriate to their role.

F. INTEGRITY, VALIDATION, AND CORRECTION

1. Institutional data must be safeguarded and managed in all formats and media (e.g., print and digital), at all points of access, and across all University systems through coordinated efforts and shared responsibilities.

2. Each Data Trustee, in conjunction with the appropriate Data Steward, shall be responsible for developing a plan for their functional area to assess the risk of erroneous or inconsistent data and indicate how such institutional data, if found, will be corrected.

3. IT-EAS will assist each functional area to develop and implement processes for identifying and correcting erroneous or inconsistent data.

G. EXTRACTION, MANIPULATION, AND REPORTING

Extraction, manipulation, and reporting of institutional data must be done only for University business purposes, or subject to terms of use as otherwise approved by the appropriate Data Steward. Personal use of institutional data, in any format and at any location, is prohibited. All data users are expected to be familiar with and conform to the University Policy 13.10.010 – *Use of Computer and Network Systems*.

1. Non-Identifiable Aggregate Data.

Units needing aggregate constituent data may obtain these data from IRA or by request. IRA will only provide aggregate data that protect the identity of individuals. Unless obtained directly from the IRA website, any

University data being reported to an external entity must be reviewed by IRA prior to reporting.

2. Identifiable, Individual-Level University Constituent Data.

Access to identifiable, individual-level campus constituent data must serve to answer an assessment/evaluation need for the University. University constituents include, but are not limited to:

a. Students (prospective and current)
b. Faculty members
c. Staff members
d. Administrators
e. Alumni and friends of the University

When a University unit determines a need for identifiable, individual-level constituent data to which it does not currently have access, they must contact the appropriate office (*see* the IRA for links to offices responsible for specific categories of data). The appropriate office will consult with the IRA and other campus offices as necessary, to determine whether the data are needed as part of the unit's assessment/evaluation needs.

3. Data access related to individual research interests or class projects.

a. University constituents may obtain identifiable, individual-level constituent data for purposes of their own research interests or class projects (in the case of students) only if approved by IRA. Aggregate data may be used for these projects and requests can be made to IRA for aggregate data not readily available on the website. IRA reserves the right to refuse a request when the aggregate data are not for public consumption.

b. Students partnering with campus units on the assessment/evaluation projects as part of a class project may access identifiable, individual-level constituent data only if approved by IRA, but may access aggregate data as determined by the assessment/evaluation project lead.

H. DATA RETENTION AND DESTRUCTION

Institutional data may reside in University records, be used to produce University records, or itself constitute University records, and as such, must be managed in accordance with approved records retention and disposition schedules consistent with University Policy RISK 1.10.025 – *Records Management*.

I. COMPLIANCE

Failure to comply with this Policy may result in sanctions relating to the individual's use of University information technology resources, termination of employment or student disciplinary proceedings, as applicable, and/or civil or criminal liability.

IV. DEFINITIONS

A. "Access to institutional data" refers to the permission to view or query institutional data.

B. "Best practices" means accepted management and access procedures that Data Custodians and Data Users follow to ensure security, accessibility, and integrity of Institutional Data. Best practices change as technology, procedural improvements, and the nature of the data change. Because best practices are subject to change, they will be described in documented procedures that reference this Policy.

C. "Data administration" is the function of applying formal guidelines and tools to manage the University's information resource.

D. "Eligible employees" are faculty and staff holding full-time appointments at the University, or other employees specifically designated as eligible to access institutional data by the head of their department, division, or school.

E. "Designated appointees" are non-employees holding an appointment with the University (ex. academic no-pay) that are authorized as eligible to access institutional data by the head of their department, division, or school.

F. "Institutional Data" (or information) is data in any form, location, or unit that meets one or more of the following criteria:

1. It is subject to a legal obligation requiring the University to responsibly manage the data;
2. It is substantive and relevant to the planning, managing, operating, documenting, staffing or auditing of one or more major administrative functions or multiple organizational units of the University;
3. It is included in an official University report;
4. It is clinical data or research data that meets the definition of "Work" under University Policy ORSP 2.40.010 - *Intellectual Property;* or
5. It is used to derive any data element that meets the above criteria.

V. RESOURCES

A. Request Data from the Office of Institutional Research & Analysis ("IRA")

B. University Policy IT 2.10.080 – *Information Security*.

C. University Policy IT 13.10.015 – *Security Awareness and Training*

D. University Policy IT 2.30.065 – *Data Breach Protocol*

E. University Policy IT 13.10.51 – *Data Classification*

F. IT policy - Data Security Standards

G. IT policy - Access Management

Revision Effective Date	**Purpose**