COVER PAGE & NOTE: The following Guide for Internal Use & Access of Institutional Data is posted to the Draft and Revised for review purposes.

Upon final approval of the Updated Institutional Data Management Policy, this Guide will be posted to the University's Data Governance website and linked in the Institutional Data Management Policy.

GUIDE FOR INTERNAL USE & ACCESS OF INSTITUTIONAL DATA

- Supported Policy: IT 13.10.050 – *Institutional Data Management*.
- Issued by Information Technology – Enterprise Application Services (IT EAS), the Data Governance Committee, and the Office of Institutional Research & Analysis (IRA)
- Date: February 9, 2026

PURPOSE OF THIS GUIDE

This Guide has been developed to support implementation of University Policy IT 13.10.050 - *Institutional Data Management* to guide University employees in the responsible use and access of Institutional Data.

FOUNDATIONAL PRINCIPLES

- Access to University Institutional Data carries responsibilities and obligations.

- Data Users must protect Institutional Data from inappropriate disclosure, use, or storage at all times, considering the level of risk associated with various types of data as outlined in University Policy IT 13.10.051 – *Data Classification*, and respecting the privacy and confidentiality of individuals whose data may be accessed.

- Institutional Data must be used only for University business purposes and in ways consistent with the mission of the University.

- Data Users granted access to Institutional Data must comply with all applicable University policies, guidelines, and standards, as well as state and federal laws and regulations, including but not limited to:
  - HIPAA
  - FERPA
  - HEA
  - federal human subjects research regulations
  - GLBA
  - PCI DSS
  - Privacy laws such as GDPR and the Colorado Privacy Act

- Use of Institutional Data for non-business purposes, improper disclosure, or inappropriate data storage may result in loss of data access and corrective action up to and including termination of employment.sup

INFORMATION SECURITY TRAINING

All Data Users must complete the University's Information Security Trainings before submitting any Data Use Request.

IT Security Essentials

Security Awareness

Cybersecurity Online Training

FERPA

See: https://catalogue.du.edu

REQUESTING ACCESS

Submitting a Data Use Request

1. Data Users must submit Data Use Requests to Institutional Research & Analysis (IRA) institutionalresearch@du.edu or to the appropriate Data Steward using the approved written Data Use Request Form.

2. If a request is approved in whole or in part, the Data Custodian (as defined in University Policy IT 13.10.050 - *Institutional Data Management*) is responsible for performing all technical steps required to grant access.

3. If a request is denied in whole or in part, the Data Steward(s) must provide the Data User with a timely written explanation of the reason(s) for denial.

DATA GOVERNANCE STEERING COMMITTEE

Data Governance Committee is led by Director of Institutional Research.

The Steering Committee includes representatives from the Provost's Office, IT, Compliance and Risk Management, University Finance, Registrar, Advancement, the Data Domain Chairs, and Institutional Research.

Responsibilities of the Steering Committee include:

1. Developing and updating this Guide
2. Appointing Data Stewards
3. Establishing data definitions, classifications, risks, and standards
4. Proposing data management and disclosure policies
5. Reviewing data use processes and request forms
6. Developing or sourcing data security and data use training
7. Determining first level appeals for data use requests
8. Evaluating and documenting system components, data assets, and their use
9. Coordinating subcommittees or task forces as needed

DATA TRUSTEES

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.

Each Data Trustee will appoint a Data Domain Chair for their applicable Data Domain. The Data Domain Chair will serve on the Data Governance Steering Committee.

Data Trustee	Data Domain	Data Domain Chair
Senior Vice Chancellor for Business and Financial Affairs	Financial/Administrative	Assistant Vice Chancellor for University Financial Services
Senior Vice Provost for Research and Sponsored Programs	Research	Senior Vice Provost for Research and Sponsored Programs
Senior Vice Chancellor for Advancement	External Relations	Executive Director of Strategic Analytics
Provost and Executive Vice Chancellor	Student/Educational Records	Registrar

DATA STEWARDS

Data Stewards are data owners, administrators, and leaders representing University departments or units (e.g., Registrar, Director(s) in the Office of Human Resources, Research Compliance Officer, Library Director). Their responsibilities include developing and implementing:

1. Data Use Request Processes and Forms – written processes and request forms for Institutional Data in their area, reviewed by the Steering Committee.

2. Written decision criteria for determining whether a Data Use Request will be granted, consistent with University policy and this Guide.

3. Data Use Request Forms requiring, at minimum:
   a. Description of the data requested
   b. Intended use of the data
   c. Locations and systems where the data will be stored
   d. Security classification(s) of requested data
   e. Justification for requesting high risk data
   f. Certification of required data security training
   g. Supervisor approval

APPEALS

Users may appeal a denial to the Steering Committee with Supervisor approval.

1. If a Data User's request is denied in whole or in part, they may submit an appeal to the Data Governance Steering Committee with permission from their Supervisor.

2. Appeal forms must include the original written justification for denial.

3. The Steering Committee (in consultation with the Office of General Counsel) shall:

   - confer with all Data Stewards involved in the original decision,
   - document in writing the basis for sustaining or denying the appeal, and
   - deliver this documentation to the Data User in a timely manner.

COMPLIANCE

1. Allegations that a Student has violated the Institutional Data Management policy (the “Policy”) will be referred to the Office of Student Rights & Responsibilities ("SRR") for consideration of action under the Honor Code.

2. Allegations that an Employee has violated the Policy will be referred to Human Resources & Inclusive Community for investigation and to determine appropriate corrective action.

3. If a user of Institutional Data is found to have violated the Policy, the University may:

    a. Suspend or terminate the individual's use of University information technology resources;
    b. Impose Outcomes for Students through the SRR process as set forth in the Honor Code;
    c. Impose corrective action on Employees.

In addition, users of Institutional Data may face civil or criminal liability under federal, state, or local laws, regulations, or ordinances.

DEFINITIONS

“Data User” means an individual University employee who accesses Institutional Data to perform assigned duties and is responsible for safeguarding access privileges and securing the data.

“Institutional Data” means data in any form, location, or unit that meets one or more of the following:

1. It is subject to a legal obligation requiring responsible management;
2. It is substantive and relevant to major University administrative functions;
3. It is included in an official University report;
4. It is clinical or research data meeting the definition of “Work” under University Policy ORSP 2.40.010 – *Intellectual Property*; or
5. It is used to derive any data element meeting the above criteria.