Policy 10.13
Institutional Data Management

Responsible Official: Provost and Executive Vice President for Academic Affairs
Administering Division/Department: General Policies
Effective Date: April 15, 2014
Last Revision: August 02, 2018

Policy Sections:

Overview

Emory University defines itself as an ethically engaged institution driven by inquiry, and as such the integrity and accuracy of data from and about the university are matters of core concern. Institutional Data measures and description of the university and its operations are valuable assets in support of the university's teaching, research, and public service missions. This policy outlines a data management framework designed to maintain the quality of Institutional Data and promote and safeguard the appropriate and effective use of Institutional Data.

Applicability

This policy applies only to Institutional Data that is academic/administrative data of Emory University, including but not limited to certain faculty and student data. This policy does NOT apply to any clinical, patient, or other data of Emory Healthcare, Inc. and/or any clinical units of Emory University, nor does it apply to any data concerning medical research or human subjects.

Each academic and academic/administrative support unit responsible for providing university data under this policy for internal and/or external reports shall establish a process for overseeing the integrity of the data reported.

Policy Details

10.13.1: General Principles

Proper Use: Emory policy prohibits all who work with Institutional Data from knowingly falsifying or fabricating data or destroying or deleting data unless such data are subject to destruction or deletion under an applicable record retention policy. Data should be destroyed or deleted in accordance with applicable record retention policies (http://policies.emory.edu/5.21). Data must be maintained in accordance with any and all applicable policies concerning security and confidentiality of the data. Personal use of Institutional Data, including derived data, is prohibited. Institutional Data must not be accessed or manipulated for personal gain, or out of personal interest or curiosity.

Shared Resources: Institutional Data are a university resource that may be used and relied upon by many users. Sharing information across academic and administrative units should be facilitated where appropriate.

Integrity and Security: Data integrity and security begin with the person or office creating the data, and are the

continuing and shared responsibility of all who access and use them.Institutional Data must be protected and managed at all levels to ensure their integrity. Institutional Data should be safeguarded to maintain the confidentiality and privacy of personally identifiable information and must be protected against systematic errors, loss, and security breaches.

Data Definitions: A sustained data administration function should reinforce a set of definitions for commonly used data, with the understanding that there may be multiple valid definitions for variables with different institutional contexts (e.g., first-year student).

Sources of Information: When there is no single metric or source of information, the use of multiple sources of information across the University should be encouraged to foster data accuracy.

10.13.2**:** Data Management Roles and Responsibilities

See Data Flow Chart.

Emory University is the owner of all Institutional Data. Individual units or departments have responsibilities for particular elements and/or aspects of the data. All members of the Emory Community have the obligation to protect and appropriately use Institutional Data.

University Data Authority is assigned to the Executive Vice President with administrative oversight of the Institutional Data in question (e.g., Faculty and student data -- the Provost and Executive Vice President for Academic Affairs, financial data -- the Executive Vice President for Business and Administration, and health care systems data -- the Executive Vice President for Health Affairs).

- The University Data Authority is the institutional authority on all matters pertaining to the integrity and use of the university's Institutional Data and ensures that the university has adequate policies, procedures and practices in place to support its needs for information.
- The University Data Authority or delegate appoints members to the Data Advisory Committee.
- The University Data Authority may commission outside parties to review any unit’s compliance with its defined process and data integrity.

The **Data Advisory Committee** (DAC) is a representative body of Data Trustees and Data Stewards from University academic and administrative support units. The Data Advisory Committee is charged with the development and on-going review of the operational effectiveness of data management policies and procedures and makes recommendations to Data Trustees for improvement or change.

- The DAC is responsible for developing and maintaining a Data Dictionary.
- The DAC provides support for the development of procedures and practices to ensure data integrity and mediates any disputes that may arise.
- The DAC is chaired by the Associate Vice Provost for Academic Planning who is responsible for maintaining archives of committee recommendations.
- The DAC ensures regular communication with academic and administrative units, Data Custodians, and Data Users about data management policies and procedures.

The **Office of Institutional Research** (OIR) is the designated office of official data collection and reporting of Institutional Data for Emory University.

- The OIR provides university administrators with information that supports institutional strategic planning, policy formation, and decision making.
- The director of the OIR is responsible for working with the appropriate Data Stewards to develop definitions of commonly used terms such as "faculty," "enrolled student," “department,” “employee,” or “project”.
  - The OIR, working with the appropriate Data Stewards, defines how official University metrics are calculated and collaborates with work groups responsible for the operational systems which store Institutional Data.
  - The OIR will promptly report any data discrepancies and inconsistencies identified in the course of its work to the appropriate Data Steward for resolution.
- The OIR maintains an archive of external reports submitted by Data Stewards on behalf of the University.

Data Trustees are senior university administrators who have policy-making and planning responsibilities for university data.

- Data Trustees are responsible for appointing Data Stewards and assigning data management roles for their units.
- Data Trustees set priorities for external reporting for their academic or administrative units.

Data Stewards are university administrators with direct operational responsibility for one or more types of Institutional Data. Individual units or departments have stewardship responsibilities for particular elements and/or aspects of the data.

- Data Stewards are appointed by the respective Data Trustees.
- Data Steward responsibilities include, but are not limited to:

    - Determining data access in the administrative unit;
    - Creating and managing processes to ensure data integrity;
    - Certifying analysis and published reports;
    - Certifying data entered in University storage systems.
- Data Stewards, in collaboration with Data Trustees, are responsible for approving the unit's participation in external surveys and for overseeing the integrity of data collected, managed and reported by the unit.
    - Data Stewards develop and maintain an inventory of external surveys submitted by the unit.
- Data Stewards work with the OIR to ensure that Institutional Data elements are properly defined and common shared data standards and structures are identified, documented and made available to all users.
- Data Stewards perform regular assessments of procedures designed to ensure data integrity and evaluate the effectiveness of the specific check points.
- Data Stewards submit an annual report to the DAC on compliance with data management policies and procedures.
- Data Stewards train all Data Custodians and Data Users in the structure, definitions, and use of Institutional Data, as well as relevant University and academic or administrative unit data policies.

Data Custodians are academic or administrative unit employees responsible for data management.

- Data Custodians are responsible for data management activities such as the creation, storage, maintenance, cataloguing, use, dissemination and disposal of data as well as any data administration activities assigned to them by the data stewards.
- Data custodians must ensure that procedures are in place to carry out policies and comply with standards approved by the university.

Data Users are unit employees or community members who access university data to perform their assigned duties.

- Data Users are responsible for complying with the Institutional Data policies outlined in this document, and for following procedures established by data custodians.
- Since data may cross functional lines, data used by any one Data User may have different data managers and data stewards.

10.13.3**:** Data Administration

Accessibility -- Access to University data should enhance the ability of the University to achieve its mission. Wherever possible, Institutional Data should be made available to all members of the University who have a legitimate business need for the data for academic, research or administrative purposes.

Training -- All Data Users must receive training in the structure and definitions of Institutional Data as well as relevant policies prior to accessing data.

Privacy and Confidentiality -- Data Users must respect the privacy of individuals whose records they may access (Statement of Confidentiality: http://policies.emory.edu/4.79). No subsequent disclosure of personal information contained in files or databases may be made. Disclosure is understood to include (but is not limited to) verbal references or inferences, correspondence, memoranda and sharing of electronic files. Institutional Data must be stored in such a way as to ensure that the data are secure, and that access is limited to authorized users (Information Technology Conditions of Use: http://policies.emory.edu/5.1). When electronic data are no longer required for administrative, legal or historical reasons, it should be deleted in such a way that recovery is not possible (Confidentiality and Release of Information about Students -- Retention Recommendations http://policies.emory.edu/8.3#13).

Data Extraction, Manipulation, and Reporting -- Every data user must recognize that Institutional Data and information derived from it are potentially complex. It is the responsibility of every Data User to understand the data that they use, and to guard against making misinformed or incorrect interpretations of data or misrepresentations of information. Where appropriate, the Data Steward should be consulted when information is used or reported outside of the Data User's functional unit. Where appropriate, the Data Steward should be consulted when information is used or reported outside of the Data User's functional unit.

Data Integrity -- Institutional Data must be protected and managed at all levels to ensure their integrity. Employees who identify inaccurate, inconsistent or unreliable data should notify the appropriate Data Steward within 5 business days. The Data Steward shall within five business days document the error and correct the data and/or refer the problem to the Director of OIR and the appropriate Data Trustee. Problems may also be reported anonymously through the Emory Trust Line 1-888-550-8850 or Emory Trust Line Online at https://www.mycompliancereport.com/EmoryTrustLineOnline.

Sanctions:

Failure to comply with this policy may have legal consequences and may result in:

- Suspension or termination of access;
- Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy.

Definitions

Data Classifications: Emory University groups data into four categories – internal data, public data, confidential data and restricted data. See the Disk Encryption Policy for descriptions of these categories, http://policies.emory.edu/5.12.

Data Dictionary is a reference resource containing key data elements and structures as well as algorithms for defining University metrics. The Data Dictionary should be accessible to all Data Users and included in training.

Data Integrity is defined as the accuracy, completeness, consistency, reliability, and timeliness of Institutional Data:

Accuracy -- data are free from errors

Completeness -- all values are present

Consistency -- data satisfy a set of definitions or constraints that are applied and maintained in the same manner across reports

Reliability -- independent custodians or users obtain consistent results when applying the same definitions or constraints

Timeliness – data are available when required

Data Management includes obtaining, defining, cleaning, archiving, and documenting data.

Institutional Data are defined as all data created, collected, maintained, recorded, managed, or used by University employees in the performance of official job duties to understand and describe the institution and its activities. These data do not include healthcare or faculty research data.

Related Links

- Current Version of This Policy: http://policies.emory.edu/10.13
- Example of Emory University's Data Flow (https://policies.emory.edu/uploads/Data%20users%20flow%20chart%2031.pdf)
- Records Retention Policy (http://policies.emory.edu/5.21)
- Disk Encryption Policy (http://policies.emory.edu/5.12)
- Statement of Confidentiality (http://policies.emory.edu/4.79)
- Information Technology Conditions of Use (http://policies.emory.edu/5.1)
- Confidentiality and Release of Information about Students-Retention Recommendations (http://policies.emory.edu/8.3#13)
- Emory Trust Line Online (https://www.mycompliancereport.com/EmoryTrustLineOnline)
- (http://)

Contact Information

Subject	Contact	Phone	Email
Institutional Data Management	Nancy G. Bliwise	(404)727-4170	nbliwis@emory.edu

Revision History

- Version Published on: May 09, 2017
- Version Published on: May 09, 2017
- Version Published on: Feb 12, 2015
- Version Published on: Jun 12, 2014 *(Original Publication)*