Type of Policy ■ *University* □ *Campus* □ *Department/Unit* □ Interim	**Data Governance** **Policy 3.237**
Business Management Policies	**Effective date:**

Policy History:	Approved by:	Resolution #	Date:
Approved			
Revised			
Responsible Office:	**Responsible Administrator:**	**Contact information:**	**Applies to:**
Vice Chancellor for Academic Affairs	Director of Institutional Effectiveness	937-769-1890	All employees

I. Introduction and Purpose

Data governance focuses on the management of the quality, consistency, usability, security, and availability of institutional data. The University's enterprise computer systems house vast amounts of data related to finances, students, and employees. The data in these systems are valuable institutional assets that support the University's mission and play an increasing role in developing and implementing the University's strategic goals.

To facilitate effective decision making, University data must be accessible, accurate, secure, and easily integrated across the University's enterprise systems. This policy authorizes a framework for ensuring that University data meet these criteria.

The purpose of this policy is threefold:

- Establish uniform data management standards for institutional data,
- Identify the shared responsibilities for assuring the integrity of institutional data, and
- Establish processes and procedures to assure that institutional data efficiently and effectively serve the needs of the University.

II. Scope of this Policy

The scope of this policy is limited to Institutional Data. For the purpose of this policy, Institutional Data is defined data in any form, location, or unit that meets one or more of the following criteria:

- It is subject to a legal obligation requiring the university to responsibly manage the data.
- 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.
- It is included in an official university report.
- It is clinical data or research data that is expressly identified as work for hire under the university's Intellectual Property Policy (5.503) and for which intellectual property rights is deemed to be held by the University.
- It is used to derive any data element that meets the above criteria.

Institutional Data includes the data housed in and retrieved from the University's enterprise systems as well as complementary systems that are supported by University IT and are managed by central University offices. University data may be used in University operations, institutional decision making, required reporting, official administrative reports, or may be shared with third parties.

This policy applies to

- All employees whose job responsibilities include inputting, safeguarding, retrieving, or using Institutional Data, and to those who supervise such individuals.
- The University and all of its campuses, schools, programs, institutes, and administrative and auxiliary units.
- All Institutional Data regardless of means or location of storage. Therefore, this policy applies to source data systems and data extracted from those source data systems, as well as data stored in any data repository.

The following types of data are excluded from the scope of this policy:

- Data in systems managed by the psychological services and counseling centers, which have their own data governance structure and information technology security infrastructure.
- Data provided to the University by external entities for research and other purposes, which are governed by the terms of the applicable data-sharing agreements.
- Data that are created by individual employees or departments for informal planning and administration, for which supplemental information technology systems are created and managed by departments.
- Data collected for the purposes of scholarly research that are not considered works for hire. The ownership of such data is governed by Intellectual Property Policy 5.503.

III. A. Guiding Principles

1. In order for the University to effectively manage and safeguard its Institutional Data, procedures must be in place to guide appropriate access to Institutional Data, ensure the security of Institutional Data, and provide a means to address procedural exceptions. It is necessary for all employees who deal with Institutional Data to be trained and informed about data security.
2. Role definitions of individuals with data responsibilities and of eligible users are necessary to support data integrity and security.
3. Sharing Institutional Data between academic and/or administrative units within the University should be facilitated where appropriate, subject to appropriate security restrictions as recommended by each Data Stewards and ratified by the Data Trustees.
4. Implementation of this policy will reinforce, wherever possible, a uniform set of definitions for commonly consumed data throughout the University.
5. Integration of Institutional Data across the University should be encouraged to foster data accuracy and uniformity, consistent with AU's institutional complexity, various data systems, and differing data formats. This should result in reduced duplication of data and greater data accuracy.
6. Institutional Data should be safeguarded to maintain the confidentiality and privacy of personally identified and personally identifiable information.

IV. Data Administration

A. University Ownership of Institutional Data

All Institutional Data are owned by Antioch University. As such, all members of the University community have the obligation to appropriately use and safeguard the asset, in all formats and in all locations.

B. Stewardship

Data stewardship is the accountability and responsibility for data and the processes that ensure effective control and use of data assets. Data stewardship includes, but is not limited to, establishing guidelines around the collection, analysis, reporting and use of Institutional Data; creating and managing core metadata; documenting rules and standards; managing data quality and integrity issues; and executing operational data governance activities.

The roles and responsibilities for safeguarding and classifying the Institutional Data assets are defined below in section V. Data Management Roles and Responsibilities.

C. Data Classification and Safeguarding

To ensure proper handling and sharing of data based on sensitivity and criticality of the information, data classifications and associated safeguards are addressed in the University's Information Security Policy (8.105) and are included by reference in this policy.

D. Access and Confidentiality

Generally, access to Institutional Data will be granted only to individuals who are employees, contracted employees, or volunteers of the institution and who need access to the data to perform assigned duties. Such access will be provided upon approval of the appropriate Data Steward and may require approval of a Data Trustee.

Improper release, maintenance, or disposal of Institutional Data may be damaging to the college community and exposes Antioch University to significant risk and possible legal action. Those granted access to college data must comply with the following guidelines.

1. Maintenance of data must strictly adhere to the policies and procedures of the University. Data may not be altered or changed except in the usual course of business.

2. Data may not be released to third parties or others at the University who do not have access to the data without the consent of the appropriate Data Steward.

3. Any release of data must always be done in compliance with FERPA and HIPAA regulations.

4. Access to and use of data is restricted to the scope of an individual's work. Data should not be viewed or analyzed for purposes outside of official business.

5. Data Users, as defined below, may not grant access to data. If data need to be shared with others, the appropriate data steward needs to authorize access to those data. All security and computer use policies must be adhered to (see Acceptable Use of Electronic Resources Policy #8.101, Email Use Policy #8.103, and Information Security Policy #8.105).

V. Data Management Roles and Responsibilities

Several roles and responsibilities govern the management of, access to, and accountability for institutional data.

<u>Data Governance Committee</u>

This committee is co-chaired by the University Director of Institutional Effectiveness and the University Director of Academic Affairs is composed of Data Stewards from across all functions of the University. The Data Governance Committee is responsible for the following tasks:

- Establish data stewards for each data element and confirm processes are in place to ensure data is being accurately recorded.
- Create and oversee processes and procedures by which all external reports are reviewed for completeness and accuracy before they are released.
- Work with stakeholders to assess the need for additional data elements and determine the best location for those elements to be stored.

- Establish and maintain policies governing user access to institutional data that follow best practices and are compliant with federal and state regulations.
- Adopt, communicate, and oversee implementation of University-wide standards for data administration aspects of business processes, data definitions, data dictionaries, data warehouse elements, and business intelligence tools.
- Engage in priority-setting and policy setting as related to the above.
- Recommend and coordinate structures and subcommittees to work on specific data issues; invite other individuals to participate on the Committee as needed.

Data Trustees

Data Trustees are members of the University Leadership Council or their designees who have planning, policy-level, and management responsibility for data within their functional areas. By understanding the planning needs of the institution, they are able to anticipate how data will be used to meet institutional needs. Data Trustees approve and implement policy and administrative decisions that promote data quality, security, integration, and alignment.

Data Stewards

Data Stewards are University employees who have direct operational-level responsibility for the management of one or more types of institutional data. Data stewards are responsible for implementing data standards, monitoring data quality, and handling inquiries about data. Data stewards safeguard the data from unauthorized access and abuse through established security and authorization procedures and educational programs. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access. Data Stewards are assigned by the Data Trustees and are generally directors or managers.

Data Custodians

Data Custodians are business analysts, subject matter experts or technical professionals responsible for the management and operation of institutional data sources. They are responsible for acquiring, validating, maintaining, storing and processing required data to ensure accessibility, reliability, and timeliness for data consumers. Custodians also participate in setting data governance priorities.

Data Users

Data Users are University employees or other University affiliates who have been granted access to Institutional Data in order to perform assigned duties or in fulfillment of assigned roles or functions within the University.

The organizational scheme for Data Trustees and Data Stewards by administrative data area is presented below:

Institutional Area	Data Trustee	Data Steward
Academic Affairs	Vice Chancellor for Academic Affairs and University Provost	Assistant Vice Chancellor for Student Success
Accreditation	Vice Chancellor for Academic Affairs and University Provost	Director of Accreditation and Academic Compliance
Institutional Research	Vice Chancellor for Academic Affairs and University Provost	University Director of Institutional Effectiveness
Student Success	Vice Chancellor for Academic Affairs and University Provost	Assistant Vice Chancellor for Student Success
Library Services	Assistant Vice Chancellor for Student Success	Library Systems Supervisor
Student Academic Records	Assistant Vice Chancellor for Student Success	University Registrar
Admissions	Vice Chancellor for Enrollment Management	Director of Admissions Director of Enrollment Services
Financial Aid	Vice Chancellor for Enrollment Management	Director of Financial Aid
Student Accounts	Vice Chancellor for Finance/CFO	Director, Student Accounts
Advancement & Alumni Relations	Vice Chancellor for Finance/CFO	Director, Donor Relations
Finance and Budget Planning	Vice Chancellor for Finance	Controller Financial Systems Analyst
Human Resources	University Counsel	Chief Human Resources Officer
Information Services	Chief Information Officer	Director of Administrative Applications

Policy Cross Reference

Intellectual Property	Policy #5.503
Acceptable Use of Electronic Resources	Policy #8.101
Email Use Policy	Policy #8.103
Information Security Policy	Policy #8.105
Datatel Administrative Software Policy	Policy #8.111