3.237 Data Governance

Type of Policy ■ ***University*** □ ***System***	**Data Governance** **Policy 3.237**
Business Management Policies	**Effective date:** **September 3, 2024**

Policy History:	**Approved by:**	**Resolution #**	**Date:**
Approved	**Chancellor**	**N/A**	**September 1, 2024**
Revised			
Responsible Office:	**Responsible Administrator:**	**Contact information:**	**Applies to:**
Office of Institutional Effectiveness	**Director of Institutional Effectiveness**	**oie@antioch.edu**	**All employees**

I. Introduction

Data governance involves making decisions and exercising authority over issues related to data. Data governance focuses on the institution's management of the quality, consistency, usability, security, and availability of institutional data. The University's information technology (IT) 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 important 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 IT systems. This policy authorizes a framework for ensuring that University data meet these criteria.

II. Purpose

The purpose of this policy is threefold:

1. Establish uniform data management standards for institutional data;
2. Identify the shared responsibilities for addressing data gaps, and assuring the quality (suitability and effectiveness of data for its intended purposes) and

integrity (focuses on the preservation and protection of data's original state) of institutional data; and

3. Establish processes and procedures to assure that institutional data efficiently and effectively serve the needs of the University.

III. Scope of this Policy

The scope of this policy is limited to Institutional Data. For the purpose of this policy, Institutional Data is defined as 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 maintain 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 is expressly identified as work for hire under the University's Intellectual Property Policy 5.503 and for which intellectual property rights are held by the University; and
5. It is used to derive any data element that meets the above criteria.

Institutional Data includes the data housed in the University's IT physical and cloud-based systems as well as complementary systems that are managed by central University offices and supported by University IT. In limited instances, institutional data may also be stored in paper records.

The following types of data may also be subject to other data management practices, regulations and policies. For example:

1. Data maintained by the psychological services and counseling centers;
2. 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;
3. 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; and
4. 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.

IV. Data Management Roles and Responsibilities

Each employee whose job includes access to data has a duty to handle the data responsibly. For example, employees with access to student data are trained to understand their duties under the Federal Educational Records Protection Act ("FERPA") Policy 5.629, whereas Employees with access to employee data are trained to understand their duties under Personnel Records and Record Retention Policy 4.225. Following is a list of the various groups and individuals across the University who have responsibility for institutional data:

1. Data Governance Steering Committee (DGSC). The Data Governance Steering Committee will oversee and guide the work of the Data Governance Committee, including development and implementation of a comprehensive data governance framework. The Data Governance Committee is responsible for the following tasks:

    a. Collaboratively developing the agenda for the DGC Meetings;
    b. Resolving issues escalated by Data Stewards & Data Coordinators;
    c. Escalating unresolved issues to Data Trustees; and
    d. Actively engaging with and supporting DGC Task Groups.

2. Data Governance Committee (DGC). This committee is co-chaired by the Director of Institutional Effectiveness and the Vice Chancellor for Academic Affairs or designee, and is composed of Data Stewards from across all functions of the University. The Data Governance Committee is responsible for the following tasks:

    a. Document Data Stewards for each data domain and confirm processes are in place to ensure data is being accurately recorded;
    b. Create and oversee processes and procedures by which all external reports are reviewed for completeness and accuracy before they are released;
    c. Work with stakeholders to assess the need for additional data elements and determine the best location for those elements to be stored;
    d. Establish and maintain procedures governing user access to institutional data that follow best practices and are compliant with federal and state regulations;
    e. 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; and
    f. Recommend and coordinate structures and subcommittees to work on specific data issues; invite other individuals to participate on the Committee as needed.

The Data Governance Committee also maintains a Data Governance webpage that contains data governance resources.

3. Data Trustees. Data Trustees are members of the Chancellor's Cabinet 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. Example of a Data Trustee: the Vice Chancellor for Academic Affairs.

4. 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; ensuring and monitoring data quality; handling inquiries about data; and resolving data quality issues within their domain. 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. Example of a Data Steward: the University Registrar.

5. 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 the accurate application of the policies and procedures governing the data within their domain. Custodians also participate in setting data governance priorities. Example of a Data Custodian: the Associate Registrars.

6. 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.

V. Guiding Principles

Below are universal Data Governance Guiding Principles from the Data Governance Institute (https://datagovernance.com/the-data-governance-basics/goals-and-principles-for-data-governance/).

1. Integrity. Data Governance participants will practice integrity with their dealings with each other; they will be truthful and forthcoming when discussing drivers, constraints, options, and impacts for data-related decisions.

2. Transparency. Data Governance and Stewardship processes will exhibit transparency; it should be clear to all participants and auditors how and when data-related decisions and controls were introduced into the processes.

3. Auditability. Data-related decisions, processes, and controls subject to Data Governance will be auditable; they will be accompanied by documentation to support compliance-based and operational auditing requirements.

4. Accountability. Data Governance will define accountabilities for cross-functional data-related decisions, processes, and controls.

5. Stewardship. Data Governance will define accountabilities for stewardship activities that are the responsibilities of individual contributors, as well as accountabilities for groups of Data Stewards.

6. Checks-and-Balances. Data Governance will define accountabilities in a manner that introduces checks-and-balances between business and technology teams as well as between those who create/collect information, those who manage it, those who use it, and those who introduce standards and compliance requirements.

7. Standardization. Data Governance will introduce and support standardization of enterprise data.

8. Change Management. Data Governance will support proactive and reactive Change Management activities for reference data values and the structure/use of master data and metadata.

VI. Data Administration

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. These procedures must encompass the following aspects of data management:

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 VII. 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.

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 Data Stewards and ratified by Data Trustees.

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 needs to be shared with others, the appropriate data steward needs to authorize access to that 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).

E. Training. It is necessary for all employees who deal with Institutional Data to be trained and informed about the data, including but not limited to: its ecosystem and security.

VII. Data Management Roles and Responsibilities

Institutional Area	Functional Business Area	Data Trustee	Data Steward
Academic Affairs	Institutional Research and Reporting	Vice Chancellor for Academic Affairs	Director of Office of Institutional Effectiveness
Academic Affairs	Accreditation	Vice Chancellor for Academic Affairs	Assistant Vice Chancellor for Accreditation and Academic Assessment
Academic Affairs	Assessment	Vice Chancellor for Academic Affairs	Assistant Vice Chancellor for Accreditation and Academic Assessment
Academic Affairs	Compliance	Vice Chancellor for Academic Affairs	University Director for Academic Compliance
Academic Affairs	Continuing Education	Vice Chancellor for Academic Affairs	Program Manager, AU Center for Continuing Education
Academic Affairs	Curriculum	Vice Chancellor for Academic Affairs	University Registrar
Academic Affairs	Library Services	Vice Chancellor for Academic Affairs	University Librarian
Academic Affairs	Student Academic Records	Vice Chancellor for Academic Affairs	University Registrar
Academic Affairs	Student Success	Vice Chancellor for Academic Affairs	Assistant Vice Chancellor for Student Success

Academic Affairs	Veteran and Military-connected Students	Vice Chancellor for Academic Affairs	University Director of Veteran and Military Connected Students
Academic Affairs	Academic Personnel	Vice Chancellor for Academic Affairs	Associate Vice Chancellor of Academic Affairs for Academic Personnel
Enrollment Management	Admissions	Vice Chancellor for Enrollment Management	Executive Director of University Admissions
Institutional Advancement	Institutional Advancement	Vice Chancellor for Institutional Advancement	Director of Institutional Advancement
Institutional Advancement	Alumni Relations	Vice Chancellor for Institutional Advancement	Director of Donor Relations

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