



University Policy

University Policy No.: UP-01-04

BOT Policy Name: Institutional Data Governance Policy

Initial Adoption Date:

Revision Date(s):

Responsible Unit: SPAIE

Responsible Executive: VP SPAIE

Authority

Florida Statute § [119.071](#); [1004.055](#); [1004.0962](#); BOG Regulation [3.007](#); [3.0075](#); University Regulations [5.003](#); [1.019](#); [10.129](#); BOT Policy [2008-01a](#)

Applicability

Faculty, Students, Staff, Affiliates and Third-Party Vendors

I. Policy Statement and Purpose

A. Objective.

1. Protecting information is critical to administrating, planning, and decision-making and is a strategic asset of Florida Agricultural and Mechanical University (“FAMU” or “the University”).
2. This Policy establishes a data governance framework for managing FAMU’s data assets, recognizing that data varies in relevance to the University’s strategic goals.
3. The Policy defines governance structures, roles, and the Data Quality Assurance Committee (DQAC) to oversee the program. The DQAC includes leadership, ex officio members, and divisional representatives.

B. Scope.

1. This Policy outlines data governance and management data which support the administrative, educational, competitive, or institutional research functions of the University, regardless of where the data is used or maintained. While this data exists in different source systems and/or may reside in different physical locations, this data in aggregate is considered part of a single, logical database known as the Institutional Database (IDB). As part of the IDB, the procedures for data governance and management will be applied uniformly and as part of a coordinated effort.

II. Definitions.

- A. **Data Governance:** Management of data availability, usability, integrity, and security based on internal data standards and policies.
- B. **Compliance:** Adherence to laws, regulations, guidelines, and specifications relevant to FAMU’s data.

- C. **Institutional Data:** Data that is generated, collected, stored, or maintained by FAMU during its operations.
- D. **Data Custodian:** An individual or team charged by the data owner to provide information asset services to data owners and data users (i.e., Chief Information Officer or designee).
- E. **Data Steward:** An individual responsible for planning, prescribing, and managing the sourcing, use, documentation, and maintenance of data assets. Functional data stewards are required to be knowledgeable regarding data assets in relation to business processes. Technical data stewards are expected to be knowledgeable about the underlying structure and administration of data assets. It is possible that a data steward could have both functional and technical knowledge.
- F. **Data Stewardship:** The governance, management, and protection of an organization's data assets that results in high-quality data that is easily accessible and reportable.
- G. **Data Administrator:** An individual responsible for certifying and managing the University's responses and institutional data for official requests to the Florida Board of Governors (BOG), in accordance with BOG Regulation 3.007. The Data Administrator acts as a liaison between the University and the BOG offices of Academic & Student Affairs, Finance & Administration, and the General Counsel's Office, as well as University departments, colleges, and schools.
- H. **Data Owner:** An individual responsible for overseeing information resources or data assets.
- I. **Subject Matter Expert (SME):** Any employee with extensive knowledge of specific functional, technical, reporting, or security-related data issues.

III. Roles and Responsibilities.

- A. **Division of Strategic Planning, Analysis, and Institutional Effectiveness (SPAIE):** Leads the development, implementation, training and oversight of data governance and compliance policies.
 - 1. **Data Quality Assurance Committee (DQAC):** A cross-functional team providing strategic direction and prioritizing data initiatives, serving as a central advisory committee for data. The DQAC is comprised of the advisory chair, co-chair, a lead technical data steward, and a lead functional data steward and selected divisional representatives.
 - a. The committee chair is the Vice President of SPAIE or the discretionary delegate who shares the managerial functions with the executive sponsors and other members of the DQAC.
 - b. The committee co-chair is the chief information security officer from the Division of Informational Technology Services or divisional designee who shares the managerial function with the executive sponsors and other members of the DQAC.
 - c. All divisions, except Academic Affairs (due to the default representation of multiple units), are to appoint one divisional representative to the DQAC. Divisional

representatives will serve for a one-year term running from September 1 to August 31 and may be re-appointed for consecutive terms. Divisional representatives will function as the lead data steward for their area.

- d. The DQAC coordinates activities and recommends practices to enhance the quality, accuracy, consistency, security, and accessibility of University data and reports, making recommendations to the future Institutional Technology Services Governance Committee.
2. **Data Stewards:** Ensure data quality, define data standards, and enforce data policies within their domains.
3. **Data Custodians:** Implement technical measures to protect data, manage access controls, and ensure data integrity including, but not limited to, storing, archiving and disposal of data.
4. **All Employees, Students, Third-Party Vendors, and Affiliates holding University data:** Adhere to data governance policies and report any data breaches or compliance issues.

IV. Data Governance Framework.

The DQAC is responsible for:

A. Data Quality

1. Establishing and enforcing data standards to ensure accuracy, completeness, and consistency.
2. Conducting regular data audits and quality assessments.
3. Implementing data cleansing processes to rectify any quality issues.

B. Data Security

1. Implementing robust security measures, including encryption, access controls, and regular security audits.
2. Developing and maintaining an incident response plan to address data breaches promptly.
3. Ensuring compliance with federal and state regulations such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley-Act (GLBA), Cybersecurity Maturity Model Certification (CMMC), International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), General Education Provisions Act (GEPA) and General Data Protection Regulation (GDPR).

C. Data Access and Usage

1. Defining and documenting data access policies, ensuring that access is granted based on role and necessity.
2. Monitoring and logging data access to detect and prevent unauthorized use.
3. Providing training and resources to promote responsible data usage.

D. Data Lifecycle Management

1. Establishing protocols for data creation, storage, archiving, and disposal.
2. Ensuring that data retention policies comply with legal and institutional requirements.
3. Regularly reviewing and updating data lifecycle policies.

E. Compliance and Regulatory Requirements

SPAIE will ensure that all data governance complies applicable state and federal law, including but not limited to:

1. **FERPA**: Protects the privacy of student education records. See BOT Policy 2017-02.
2. **HIPAA**: Safeguards medical information from unauthorized disclosure.
3. **GLBA**: Regulates how financial institutions share and protect their customers' private information.
4. **STATE REGULATIONS**: Florida state laws regarding data protection and privacy, such as the Florida Information Protection Act (FIPA), (F.S. §501.171).
5. **CMMC**: Legal framework to ensure appropriate protection of controlled unclassified information by federal contractors.
6. **GDPR**: Legal framework that sets guidelines for the collection and processing of personal information.
7. **ITAR**: A set of U.S. government regulations that control the export, import, and manufacture of defense-related items and services.
8. **EAR**: Broadly governs and imposes controls on the export and re-export of most commercial goods, software, and technology.
9. **GEPA**: Specifically, section 427, applies to all applications for federal funds, such as the Elementary and Secondary Education Act Consolidated Application, and requires a description of the steps the applicant proposes to take in order to ensure equitable access to, and participation in, its federally-assisted program for students, teachers, and other programs.

F. Monitoring and Reporting

In accordance with best practices, SPAIE will:

1. Establish a system for continuous monitoring of data governance policies.
2. Develop and implement metrics to assess the effectiveness of data governance policies.
3. Require regular reporting to senior management and the DQAC.

G. Training and Awareness

1. SPAIE in collaboration with the Offices of Information Technology and Chief Privacy Officer will conduct annual training sessions on data governance policies, security protocols and compliance requirements.
2. SPAIE will provide resources and support to ensure understanding and adherence to data policies.

H. Reviews and Updates

1. SPAIE will regularly review and update this Policy to reflect changes in regulations, technology, and institutional priorities.

2. SPAIE will solicit feedback from stakeholders to improve and refine data governance practices.

I. Enforcement

1. SPAIE shall refer all data-related incidents to the appropriate offices for investigation.
2. SPAIE shall report any non-compliance with data governance policies to the appropriate vice president to take corrective action including, but not limited to, disciplinary measures.

J. Data Classification Chart

1. All data at the University shall be assigned one of the following classifications. Collections of diverse information should be classified as to the most secure classification level of an individual information component with the aggregated information.
2. **Restricted:** Data in any format collected, developed, maintained, or managed by or on behalf of the University, or within the scope of University activities, which are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to, medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records and export controlled technical data.
3. **Sensitive/ Confidential:** Data whose loss or unauthorized disclosure would impair the functions of the University, cause significant financial or reputational loss, or lead to legal liability. Examples include, but are not limited to, limited access records as defined in University Regulation 10.129, research work in progress, animal research protocols, financial information, strategy documents and information used to secure the University's physical or information environment.
4. **Open:** Data that does not fall into any of the other information classifications. This data may be available without specific information from the owner's designee or delegate approval. Examples include, but are not limited to, advertisements, job opening announcements, University catalogs, regulations and policies, faculty publication titles and press releases.

DATA TYPE	CLASSIFICATION	JUSTIFICATION	DEPARTMENT
Student Records (non-directory)	Restricted	FERPA , 34 CFR Part 99; F.S. §1002.225 ;	Registrar/Colleges
Patient Health or dental records (identifiable)	Restricted	HIPAA , 110 Stat. 1936; F.S. §119.071 ; F.S. §110.123 ; F.S. Chapters 384 , 385 , 395 ; F.S. §440.125	Student Health
Campus Emergency Response Plans	Restricted	F.S. §1004.0962 ; F.S. §119.071	Emergency Management
Investigation Related Information	Sensitive/ Confidential	F.S. §1004.055 ; F.S. §119.071 ; F.S. §1012.796 ; F.S. §1012.91 ; F.S. §119.0713 ; University Reg. 10.129	Varies
Export Controlled Data	Restricted (with exclusions)	ITAR , 22 C.F.R. Part 120; EAR , 15 C.F.R. Part 730	SPAIE

Credit Card Holder Data	Restricted	FIPA , F.S. §501.171	Varies
Social Security Numbers	Restricted	FIPA , F.S. §501.171; F.S. §119.071	Varies
Personally Identifiable Information (PII defined by FIPA)	Restricted	FIPA , F.S. § 501.171	Varies
Animal Research Protocols	Sensitive/ Confidential	Competitive and Commercial Potential	Research Sponsored Programs, Research Compliance
De-identified Patient Information	Sensitive/ Confidential	HIPAA/Patient Privacy	Student Health
System Security Information	Restricted	F.S. §119.071; F.S. §1004.055	Information Technology
Unpublished Research Results	Sensitive/ Confidential	Competitive and Commercial Potential	Varies
Exams (Question banks and Answer keys)	Sensitive/ Confidential	Exam Integrity	Academic Affairs
Employee Data (excluding SSNs)	Sensitive/ Confidential	Employee Privacy	Human Resources
FAMU Directory (students and staff)	Open	FERPA ; F.S. §1002.225; F.S. §1002.221; BOT Policy 2008-01a; F.S. Chapter 119	Registrar
University Regulations	Open	Intended for Public Use	Office of University Policy
Course Catalog	Open	Intended for Public Use	Registrar
Public Websites	Open	Intended for Public Use	Information Technology

V. Administration

The Division of Division of Strategic Planning, Analysis, and Institutional Effectiveness (SPAIE) is responsible for administering this Policy.


 Timothy L. Beard, Ph.D.
 Interim President

1/15/2025
 Date


 Roddrick D. Jones, Ph.D.
 Vice President SPAIE

1/15/2025
 Date

Attachment(s)

Related Resource(s) [Information Access Control/ Handling Procedure](#)