Policy 01:009 – Data Governance

1. Purpose

The University of Montevallo ("University") recognizes that institutional data are assets that must be properly managed and maintained to support the mission of the University. Further, the University is committed to data governance that assigns appropriate responsibility and promotes data security, integrity, accessibility, and ongoing maintenance that complies with applicable federal and state laws governing the use and disclosure of information. This policy establishes the University's framework for such data governance.

2. Scope

This policy applies to all University faculty, staff, students, official University affiliates, or any other individual, group, or office with University-approved access to data owned, leased, or used by the University (hereafter, "User" or "Users").

3. Policy Statement

No one division or individual owns institutional data. The use and management of the University's data is multilayered, with different individuals, departments, and divisions assuming specific tasks and responsibilities for data, including the management of appropriate use, access, risk mitigation, and assurance that University data and information are collected and managed in accordance with state and federal requirements and this and other applicable University policies, procedures, and practices. It is the responsibility of all Users to practice responsible data access and use.

While units are responsible for the use and management of data under their purview, guidance on the governance of all institutional data, including role assignments, data classifications, and storage protocols, shall be provided by the University's Data Governance Committee (DGC). This committee will annually review current data governance procedures and practices and submit changes and updates to all relevant campus Units.

This policy outlines core requirements for the safe, secure, and appropriate use and access to all University data. However, the University recognizes that some Units manage sensitive data that require more stringent procedures and practices that surpass those addressed in this policy. In such cases, the default practice is for those Units to adhere to the more stringent requirements.

3.1. Roles and Responsibilities: The University has established four roles associated with the management of institutional data. The roles and general responsibilities of each are described below.

Data Trustee: Senior University, division-level official or designee who has authority over policies and procedures regarding data access and usage. Responsibilities:

- Establish data policies in their division or area.
- Assign and oversee Data Stewards.
- Maintain awareness of and follow legal and regulatory data requirements in their division or area.
- Promote appropriate data integrity and use.

Data Steward: University official or designee with direct operational responsibility for the management of University data within assigned functional areas. Responsibilities:

- Assist in developing and maintaining data classification procedures.
- Assist in developing, implementing, and managing data access procedures.
- Ensure that data quality and definitions are developed and implemented.
- Interpret and assure compliance with state and federal regulations and University policies and procedures on the responsible access to and use of data.
- Ensure that individuals with access to restricted data have completed required training and agreed to confidentiality requirements.
- Resolve stewardship issues and definitions of data that cross multiple functional areas.
- Develop, implement, and maintain a business continuity plan for data under their control. Business continuity is an ongoing process supported by senior officials to ensure that necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, and ensure continuity of operations.
- Implement and communicate record retention procedures.

Data Custodian: University Unit or administrator responsible for the operation and management of systems and servers that collect, manage, and provide access to University data. Responsibilities:

- Maintain physical and system security and safeguards appropriate to the classification of data in their custody.
- Comply with applicable information security standards.
- Maintain disaster recovery plans relevant to the University's needs.
- Manage user access to data appropriate to user needs and data classification.
- Comply with all state and federal regulations and University policies and procedures on the responsible access to and use of data.

Data User: University Unit or individual who has been granted access to University data in order to perform assigned duties or to fulfill assigned institutional role. This access is granted exclusively to conduct University business. Responsibilities:

- Follow all established data access and use policies
- Comply with state and federal regulations and University policies and procedures associated with data.

- Use data only as required to conduct University business within the scope of employment.
- Implement all prescribed safeguards for limited access and Protected and Sensitive data.
- Maintain accuracy and timeliness of institutional data under their purview.
- Promptly report any unauthorized access, misuse, or data integrity issues to immediate supervisor.

University data shall be accessible according to defined needs and roles with appropriate access to Units as needed without unnecessary restrictions that interfere with the efficient conduct of University business. University data will be protected through security measures relevant to the data classifications below that ensure proper use of the data when accessed and stored.

3.2. Data Classification: The University uses various data types. Data types of similar risk sensitivity are grouped together in one of the following three classifications.

Restricted Data: University's *highly sensitive* data protected by law, regulation, or critical to University operations including Personally Identifiable Information (PII). PII includes an individual's first name or first initial and last name in combination with one or more of the following data elements.

- Social Security Number
- Driver's license number, state identification card number, or tribal identification number.
- Passport or Visa numbers
- Bank account or credit or debit card number, with or without any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account.
- Medical records or health insurance information
- Federal Tax information or IRS documentation
- Academic records such as grades, test scores, or courses taken
- Student financial aid data subject to Gramm-Leach-Blilely Act
- E-mail address with any required security code, access code, security Q&A, or password that would permit access to an individual's personal, medical, insurance, or financial account.

Important: *A breach of confidentiality, integrity, or availability of Restricted Data could have a significant adverse impact on the University's mission, safety, finances, or reputation.*

Confidential Data: University data not meant for public distribution but not classified as Restricted but still warrants careful management and protections to safeguard its privacy and availability. Some examples of Confidential Data include:

- Date of birth
- Student records such as advising records or disciplinary actions
- Employee records
- Doner contact and non-public gift information

- Family Educational Rights and Protection Act (FERPA) information
- Survey or assessment data containing identifiers
- Driver license numbers
- Non-public contact information
- Internal policies or memos

Public Data: University data meant for public distribution. Examples include:

- External website content
- Advertising
- Press releases
- Job postings
- University information not designated by owner as private
- Campus maps

3.3. Data Security: While the current policy provides the institutional framework for data governance and oversight, data security procedures are specified in Policy 01:11: Information Technology Security Program.

4. Policy Approval, Review, and Administration

Responsible Office(s):	Information Services & Technology
Responsible Individual:	Chief Information Officer
Effective Date:	11/2018
Last Revision:	08/2024