Policy 01:009 – Data Governance

Purpose

This policy sets forth the framework for data governance at The University of Montevallo. The University recognizes that institutional data are assets that must be properly maintained to support the mission and vision of the institution and is committed to data governance management that ensures data quality, data accessibility, data maintenance, and assigns appropriate responsibility for data.

Scope

Institutional data are the property of the University and shall be managed and protected as a vital asset. Institutional data are defined as collections of data elements relevant to the operations, planning, compliance, or management of any unit at the University, or data that are reported or used in official administrative University reports. The University retains rights to all data, content, and information the university collects, produces, transmits, and stores regarding its constituents, services, programs, and operations, including administrative data and information and content supporting the operation of the university, primarily in the domains of student records, human resources, and finance. The University complies will all applicable federal and state laws and regulations governing the collection, storage, retention, access, and usage of institutional data.

This policy is not binding for content produced for or by teaching and learning activities, or academic research data that may be generated or maintained through activities, outputs and findings of university faculty, staff, students, and affiliates except when data or activities are protected by Federal or State laws, including but not limited to PII, PIHI, FERPA, PCI, GLB, or University Policy.

RESPONSIBLE PARTIES

No one division or individual "owns" data. The governance of the University's data is multi-layered, with different individuals, departments, and divisions assuming specific tasks and responsibilities for data; including governing the management of appropriate use; access and risk mitigation for institutional data; and assuring that data and information are collected and managed in accordance with this and other applicable policies, procedures, and practices. It is the responsibility of all University employees to practice responsible uses of data. The stakeholder types directly responsible for the management and security of University data are listed below.

Technology Advisory Council (TAC)

TAC reports to the Chief Information Officer (CIO) and facilitates and supports data governance and data stewardship activities. TAC will review ad recommend all policy and procedures related to data quality, compliance, privacy, security, architecture and IT governance; collect and align policies, standards, and guidelines from stakeholder groups; articulate the value of data governance and stewardship activities; provide centralized communications for governance-led and data-related matters; and maintain governance records.

Data Governance Officer

The Data Governance Officer (DGO) will be the University CIO or his/her designee. The DGO works in collaboration with TAC to keep track of data stakeholders and stewards; facilitate and coordinate meetings of data stewards; arrange for the providing of information and analysis to projects as requested; facilitate and coordinate data analysis and issue analysis projects; collect metrics and success measures and report on them to data stakeholders; and provide ongoing stakeholder care in the form of communication, access to information, record keeping and education/support.

Data Agents

Data Agents are defined as institutional officers (e.g., vice presidents, vice provosts, deans, etc.) who have authority over policies and procedures regarding definitions of, access to and usage of data. Each data trustee appoints data stewards for their division or college.

Data Usage Committee **(DUC)**

DUC is an auxiliary committee of TAC and is comprised of functional data stewards from across all functions and departments of the university. DUC will have representation on all relevant subcommittees of TAC.

Data Stewards

Data Stewards are university employees who have direct operational-level responsibility for the management and accuracy of one or more types of institutional data and have the authority to make decisions.

Data Custodians

Data Custodians are system administrators responsible for the operation and management of systems and servers that collect, manage and provide access to institutional data.

Data Users

Data Users are university units or individual university community members 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; this access is granted solely for the conduct of university business.

Principles

The following principles are set forth to govern data quality, data accessibility, data usage, and data maintenance:

Data Quality

Data quality is crucial to operational and transactional processes and the reliability of analytics and reporting. Data quality is affected by the way data are entered, stored, and managed. Data quality dimensions include accuracy, completeness, consistency, and currency. Quality standards for institutional data shall be defined and monitored by Data Stewards and Custodians.

Data Access

Institutional data shall be accessible according to defined needs and roles with appropriate access to units as needed without unnecessary restrictions such that the procedures established to protect data should not interfere unduly with the efficient conduct of University business. Institutional data will be protected through security measures related to data classification that ensure proper use of the data when accessed and stored. Data access will be conducted in accordance with policies established by TAC. This policy applies to all entities employed or contracted by UM and covers all uses of institutional data, regardless of the office(s) or data format(s) involved.

Data Systems Integration and Accuracy

To provide the highest levels of accuracy and consistency across data systems, specific rules or constraints should be implemented to validate data integrity over its lifecycle. Data validation is an immediate and ongoing commitment that requires far-reaching management protocols and verification tools to identify data corruption. Data corruption is the failure to maintain data integrity and includes but is not limited to any unintended modifications to data that affect stability, performance, and predictability.

Data Usage and Maintenance

Access to and the use of University data are dependent upon security levels assigned by data stewards. Data should be utilized ethically and in accordance with applicable laws and regulations, and should not be abused or misused. Individual privacy must be duly considered in regard to all data usage. Employees or certified contractors must only access and use data according to their job duties or obligations; their access should be limited to the security levels assigned. Data should not be used for personal gain or for other inappropriate activities.

Review of Policy

TAC will review this policy and make any recommendations for changes to the President at least every 3 years and more frequently if necessary.

Approved 11/18