MGA Data Governance Charter

Purpose

The University System of Georgia Business Procedures Manual Section 12.2.1 requires each USG organization to establish a data governance structure. The data governance structure will demonstrate accountabilities for the data assets of the organization to ensure proper use and handling of data being read, created, collected, reported, updated or deleted.

This Data Governance Charter will **identify the offices/positions responsible for fulfilling the roles defined in Business Procedures Manual Section 12.2.1.**

This charter was last updated on October 1, 2025. This charter was approved by the President on October 6, 2025.

Roles

The Data Governance Structure shall consist of three required roles, Data Owner, Data Trustee, and Data Steward.

Data Owner

Each USG organization is responsible for all data read, created, collected, reported, updated, or deleted by offices of the organization. As the chief executive officer, the president of Middle Georgia State University is identified as the **Data Owner**. The data owner has ultimate responsibility for submission of organizational data to the USO. The data owner has responsibility for the identification, appointment and accountability of **Data Trustees**, and providing guidance on institutional data strategy.

Data Trustees

Data trustees are designated by the President and this charter and constitute a board of the whole. These **data trustees are executives of the USG organizations who have overall responsibility for the data read, created, collected, reported, updated or deleted in their data area(s)**. USG organization data trustees have overall responsibility for accuracy and timeliness of submission of data to the USO. These positions/offices would normally be cabinet-level positions reporting directly to the entity data owner.

The President designates the following executives as data trustees:

- Provost
- All Vice Presidents

Data Stewards

- **Data Stewards**, designated by the data trustees as a whole, are personnel responsible for the data read, used, created, collected, reported, updated or deleted, and the technology used to do so if applicable, in their data area(s). Data stewards recommend policies to the data trustees and establish procedures and guidelines concerning the access to, completeness, accuracy, privacy, and integrity of the data for which they are responsible. Data stewards act as advisors to the data trustees and have management responsibilities for data administration issues in their functional areas. Data stewards have responsibility for accuracy and timeliness of submission of data to the USG system office in their area. Selected data stewards shall participate as members of the Functional Data Governance Committee (FDGC) as appointed by the Global Data Governance Committee (GDGC).

Responsibilities of the data stewards include, but are not necessarily limited to:

- Developing standard definitions for data elements created and/or used within the functional unit. The data definition will extend to include metadata definitions as well as the root data element definition.
- Ensuring data quality standards are in place and met within the functional unit.
- Identifying the privacy level as unrestricted, sensitive or confidential, for functional data within their area(s) of supervision/direction and communicate it to those responsible for ensuring data is handled according to its appropriate classification. (See 12.4.2 Classification)
- Establishing authorization procedures with the organization's FDGC and/or chief information officer (CIO) to facilitate appropriate data access as defined by institutional/office data policy and ensuring security for that data. Authorization documentation must be maintained.
- Working with the organization's FDGC or GDGC, identifying and resolving issues related to stewardship of data elements, when used individually or collectively, that cross multiple units or divisions. For example, the individual data element "Social Security Number" may have more than one data steward since it is collected or used in multiple systems.

- Communicating concerns and petitions about data (such as data quality, security, access, etc.) to the FDGC and to the Special Assistant to the President.

Data trustees must appoint data stewards for all necessary data domains. These data stewards are appointed because their position reports directly to an identified data trustee/Vice President (VP) on the MGA organization chart. It is the intent of the data trustees that this Charter will be updated automatically upon any re-organizations that alter the organization chart in a way that adds to or subtracts from data trustees' direct reports. The chair of the FDGC shall have the authority to update this Charter in accordance with the above without the need of approval from the data trustees or the FDGC, unless the change affects designation as a member of the FDGC.

The following position appointees are approved and designated as Data Stewards by the Data Trustees as a whole. Ten (10) designated FDGC representatives for each division are underlined.

- Academic Affairs Division
    - Academic Deans
    - Advising representative
    - Faculty Development representative
    - Institutional Effectiveness representative
    - Student Success representative
    - Dean of Library Services
    - Dean of Graduate School
- Advancement Division
    - Advancement representative
    - Marketing and Communications representative
- Finance and Operations Division
    - Budget representative
    - Facilities representative
    - Financial Services representative
    - Human Resources representative
    - Public Safety representative
- Enrollment Management Division
    - Admissions representative
    - Financial Aid representative
    - Registrar representative

- Planning and Institutional Strategy
    - Chief Information Officer
    - Enterprise Systems Management representative
    - Technology Resource representative
    - University Counsel
    - Title IX representative
- Student Affairs Division
    - Student Affairs representative
    - Athletic representative
    - Career & Leadership representative
    - Housing & Residence Life representative
    - Student Engagement representative

Chief Information Officer (CIO)/Chief Information Security Officer (CISO)

Responsibilities of the CIO and CISO are to ensure that technical infrastructure is in place to support the data needs and assets, including availability, delivery, access, and security across their operational scope.

Committees

An important part of the Data Governance Structure is group decision making. Three committees have been established to achieve this goal.

Global Data Governance Committee

The Global Data Governance Committee (GDGC) consists of all data trustees. The GDGC is responsible for defining, implementing, and managing policies and procedures for data governance and data management functions, under the guidance of the data owner. The chair and convener of the GDGC, as appointed by the MGA Data Owner, is the Vice President for Institutional Strategy.

Specific responsibilities include, but are not necessarily limited to the following:

- Ensuring that data accessed and used by units reporting to individual areas is done so in ways consistent with the mission of the office and the USG organization;
- Appointing data stewards within each functional area. The chair of the GDGC will inform the USG organization's Data Governance Committee of data stewards' appointments, including office, name, and contact information of the incumbent;

- Identifying the Functional Data Governance Committee structure and membership;
- Defining data management roles and responsibilities contained in this section and other policy and procedure documentation;
- Maintaining documentation pertaining to data governance and management policy and procedure in a centralized and accessible location for the participant organization staff;
- Ensuring that cybersecurity control processes detailed in the Cybersecurity section are developed and operational; and,
- Assisting the chairs of the functional and technical committees to ensure effectiveness.

The primary role of the GDGC is to ensure implementation of University System of Georgia Business Procedures Manual section 12.

The GDGC will meet at least biannually and more often as needed. A majority of the committee members shall constitute a quorum. The committee chair will keep a copy of the committee meeting minutes and forward a copy to all committee members. The committee chair may invite any director, officer, staff member, expert or other advisor who isn't a member of the committee to attend, but these individuals have no voting power.

The GDGC will review this charter at least annually and recommend any proposed changes to the President for review. The President may make changes to this charter as needed.

Functional Data Governance Committee

The Functional Data Governance Committee (FDGC) is responsible for collective decision making around substantive changes to organization data collection, maintenance, access, and use within their functional area. These changes will generally be reflected in policies, procedures and guidelines to be submitted to the GDGC. It is the role of the FDGC to identify what the threshold is for decisions to require GDGC consideration.

The following representatives will serve on the committee.

- Data stewards appointed by the data trustees
- Chief Information Security Officer (CISO)
- Institutional Research representative

The FDGC will meet at least quarterly, or as often as needed to fulfill directives issued by the GDGC. A majority of the committee members shall constitute a quorum. The co-chairs

of the FDGC will be the Chief Information Officer and University Counsel, as appointed by the MGA Data Owner.

The following outlines the operational procedures of the FDGC:

- Establish and approve data governance standard operating procedures (SOPs) in each division that addresses data elements, data definitions, data integrity, and quality control.
    - Coordinate with other departments (e.g., academic affairs, enrollment management, student affairs) to ensure consistent data practices and support cross-functional initiatives.
    - Monitor effectiveness of data governance SOPs and policies and formally audit annually. Update as needed to adapt to changes in technology, regulations, or institutional needs.
- Solicit feedback and make improvements to address emerging challenges and adapt to changes in the data environment.
- Solicit feedback from stakeholders to identify areas for improvement and enhance the effectiveness of data governance practices.
- Promote training and awareness of data governance issues institutionally to foster a culture of responsible data management.
    - Disseminate SOPs and policies via email (as record of notice) to operational areas to inform of revised procedures and/or drafting of new and distinct procedures.
- Define access levels and permissions for staff and faculty to ensure that student data is available to authorized personnel only.
- Implement role-based access controls and regularly review access permissions to ensure they remain appropriate.
- Ensure proper publishing and archiving of SOPs as reference for auditing and compliance purposes.
- Addressing any concerns or petitions that are brought forward from any Data Steward to the FDGC. In the event a concern or petition cannot be resolved within the FDGC, the Chair of the FDGC shall present the issue to the GDGC for resolution.

FDGC Meetings

As a matter of compliance with the USG Business Procedures Manual and review by the committee, the following topics shall be included in a quarterly standing agenda of the FDGC:

- Data Governance Structure and Function (advisory to GDGC)
- Data Systems Documentation
- Data Elements and Data Definitions
- Data Quality Control
- Data Availability
- Data Lifecycle (Data Destruction and Retention)
- Cybersecurity (Data Security)
- Auditing / Monitoring / Compliance
- Data Privacy

The FDGC shall review all new or amended procedures at the next scheduled meeting. The FDGC chair will distribute to the committee membership both new and amended procedures scheduled for review before the next meeting for review. The sponsoring data steward or data trustee will present procedures for consideration. All procedures are adopted by default, unless a vote to disapprove out of failure to comply with a standard or policy is identified.

Note, standards will be based on established policy and will establish how policies are implemented. For example, MGA's Privacy Policy (MGA Policy 10.6) establishes that MGA shall comply with all appropriate federal and state privacy regulations. The Privacy Standard provides specific standards relative to MGA's Privacy Policy 10.6. Lastly, procedures such as the General Data Protection Regulation (GDPR) procedure are developed in accordance with standards at the functional level that provide further detail on implementation. To clarify, the hierarchy is (1) Policy, (2) Standards, and (3) Procedures.

Technical Data Governance Committee

The Technical Data Governance Committee (TDGC) is responsible for technical guidance to support the work of the other Data Governance Committees and for decision making about the feasibility of and methods for carrying out decisions of the FDGC.

Members of the TDGC will join other committee meetings when requested and meet separately as needed.

The TDGC consists of:

- Chief Information Officer (CIO)
- Deputy Chief Information Officer – Chair
- Chief Information Security Officer (CISO)

- Director of Enterprise Information Systems
- Director of Enterprise Systems Management
- Director of Network Administration
- Director of IT Services

The following outlines the operational procedures of the TDGC:

- The TDGC will meet as needed to approve standards and procedures.
- Members of the TDGC consult with the governance committees or committee individuals as needed during the development of standards and procedures.
- TDGC reviews and verifies standards and procedures to ensure they adhere to technical and cybersecurity best practices.
- TDGC is responsible for conducting thorough evaluations of all new software applications and technology platforms or systems undergoing significant change prior to organizational procurement.

TDGC evaluates standards and procedures to ensure the appropriate technical resources are available to implement them. The software vetting process ensures that potential purchases align with institutional data governance standards, security requirements, and regulatory compliance obligations. All software and platform acquisitions must receive formal approval from the Technical Governance Data Committee before purchase authorization can proceed, ensuring that technology investments support strategic objectives while minimizing operational and security risks.

References

Business Procedures Manual Section 12

https://www.usg.edu/business_procedures_manual/section12/