Title: Data Stewardship and Access

1. Overview
For all USG organizations, information is a strategic asset critical to administration, planning, and decision-making. Effective and responsible use of information requires that data are secure, well documented, and accessible for use by authorized, trained personnel. The Business Procedures Manual provides the data governance infrastructure and management practices required for USG organizations.

As directed by University System of Georgia (USG) Business Procedures Manual (BPM) sections 12.4.2, 12.4.3 and 12.4.4 respectively, USG institutions must develop standards and procedures to classify and control access to data; and establish an adequate system of separation of duties.

2. Purpose
To establish procedures and processes that support compliance with Board of Regents (BOR) and USG policies and procedures; federal and state legislation and regulation and standards concerning data classification. To establish a standard for the classification of data to be used in establishing proper handling procedures and safeguards.

3. Scope
This policy applies to All MGA units, employees, students, and third parties employed by or doing business with, Middle Georgia State University.

4. Standard
The Middle Georgia State University data governance and management structure is responsible for implementing policies, standards and procedures to effectively manage and provide necessary access to institutional data, while ensuring the confidentiality, integrity and availability of the information. This policy defines a structured and consistent process to obtain necessary data access for conducting Middle Georgia State University operations (including administration, clinical, instructional and research), identifying the relevant mechanisms for delegating authority to accommodate this process at the unit level while adhering to segregation of duties and other best practices, as well as defining data classification and safeguards in compliance with existing laws, rules, and regulations.

Data Classification Categories
This standard requires that all institutional data be classified into one of three categories as defined by USG BPM Section 12.4.2.

Unrestricted/Public Information -"Unrestricted/Public Information is information maintained by a USG organization that is not exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws. Some level of control is required to prevent unauthorized modification or destruction of public information." This is the default classification.

Sensitive information - "Sensitive Information is information maintained by a USG organization that requires special precautions to protect from unauthorized use, access and disclosure guarding against improper information modification, loss or destruction. Sensitive information is not exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws but is not necessarily intended for public consumption."

MGA designates the following as examples of sensitive data elements:

- Non-directory information identifiable to an individual (including students, staff, faculty, trustees, donors, and alumni), including but not limited to, dates of birth, employee and student id numbers, license plate numbers and compensation information.
- The institution's proprietary information, including but not limited, to intellectual research findings, intellectual property, financial data, and donor and funding sources.
- MGA financial transactions and regulatory actions.

Confidential information -"Confidential Information is information maintained by a USG organization that is subject to authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (44 USC Sec 3542) Confidential classified documents are exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws."

Access to confidential information must be for legitimate use only.

MGA designates the following as examples of confidential data elements:

- Data exempt from disclosure under the Georgia Open Records Act or the Georgia Open Meetings Act
- All regulated data protected under the following, but is not limited to:
    - Family Educational Rights and Privacy Act of 1974 (FERPA)
    - Gramm-Leach-Bliley Act (GLBA)
    - Georgia Personal Identity Protection Act (GPIPA)
    - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - Payment Card Industry (PCI)
    - Federal Tax Information ("FTI")
    - Export Controlled Materials
    - Controlled Unclassified Information (CUI)

Roles and Responsibilities

Drawing from Business Procedures Manual (BPM) section 12.2 and the USG IT Handbook, this standard defines six roles, Data Owner, Data Trustee and Data Steward, Chief Information Officer (CIO), Chief Information Security Officer (CISO), Data User, Information System Owner and Data Custodian. Individuals in each role have a responsibility to ensure data security, privacy, quality and authorized access. The roles and responsibilities are as follows.

Data Owner

The data owner ensures that an appropriate data governance structure is in place, operating effectively, and supported by other institutional leaders. The President of MGA is identified as the data owner.

Responsibilities:

- Identify, appoint, and be accountable for data trustees for each data domain
- Inform the institution's global data governance committee of data trustee appointments including office, name, and contact information
- Have ultimate responsibility for submission of organizational data to the USG
- Discuss solutions for unresolved data issues brought by the data trustee
- Communicate responsibility of data governance solutions to other institutional leaders

Data Trustees

Data trustees are appointed by the data owner and have overall responsibility for the data read, created, collected, reported, updated or deleted in their data area(s) and timely submission of accurate data to the USO. Institutional data trustees consist of the Provost and Vice-Presidents.

Responsibilities:

- Ensuring that data accessed and used by units reporting to them is done so in ways consistent with the mission of the institution;
    - Trustees have functional responsibility/ownership for information systems, some of which store confidential/sensitive information
    - Trustees have responsibility for approving policies and procedures to ensure appropriate data access and use
- Appointing data stewards within each functional area for which they are responsible. The data trustees will inform the Middle Georgia State University Data Governance Committee of their data stewards' appointments, including office, name and contact information of the incumbent;
- Participating as a member of the Global Data Governance Committee; and,
- Communicating unresolved concerns about data to the data owner
    - Unaddressed data security or privacy risks
    - Lack of collaboration across units to effectively manage data assets
- Overall accountability for protection of cardholder data and maintaining PCI DSS compliance in their domain

Data Access Responsibilities:

- Data trustees, data stewards, and data users share the responsibility of preventing unauthorized access to information systems
- Data trustees, data stewards, HR and data custodians should collaborate to define both administrative and technical access controls
- Ensure information systems access controls include:
    - Documented procedures to grant, review, deactivate, update or terminate account access
    - Resources to authenticate and verify authorized access
    - Resources to prevent and detect unauthorized use

Data Stewards

Data stewards are concerned with the meaning of data and the correct usage of data and are expected to have domain content knowledge.

Responsibilities:

- Be responsible for the data read, used, created, collected, reported, updated or deleted, and the technology used to do so (if applicable)
    - Depending on the size/complexity of a functional department/division, it may be necessary to identify associate data stewards
- Be responsible for accuracy and timeliness of submission of data to the USG system office
- Recommend policies to data trustees and establish procedures and guidelines concerning the access to, completeness, accuracy, privacy, and integrity of the data
- Act as an advisor to the data trustees and have management responsibilities for data administration issues
- Participate as a member of the Functional Data Governance Committee(s) for your data area as appointed by the data trustee
- Communicate concerns about data (such as data quality, security, access, etc.) to the data trustees
- Domain implementation of data governance policies, standards, practices
- Socialization of data governance in domain

Data Quality Responsibilities:

- Develop standard definitions for data elements created/used within the functional unit
    - Definitions will also include metadata such as data format, source, security, and privacy classifications
- Ensure data quality standards in place and met
- Work with the Data Governance Committee to identify and resolve issues related to data elements 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.

Data Security and Privacy Responsibilities

- Identify the privacy level of data elements as unrestricted, sensitive or confidential, for data within their area(s) and communicate it to personnel responsible for ensuring data is handled according to its appropriate classification

Data Access Responsibilities

- Establish data access authorization procedures with Data Governance Committee and ensure procedures are in place and implemented for data security
- Analyze user roles and determine the level of access required to perform a job function based on Principle of Least Privilege
  - The principle of least privilege requires that any user, program, or process should have only the bare minimum privileges necessary to perform its function
- Work with data custodians to adjust data access based on notifications from HR of personnel status changes in job function, status, transfers, referral privileges, or affiliation
- Review user access to information systems every six months and document findings
- Maintain authorization and access review documentation

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.

Data Users

Data users are Middle Georgia State University employees who have been granted authorization to access institutional data. Authorization is granted for a specific level of access, as defined by the data management policies, solely for the conduct of institutional business.

Responsibilities:

- Follow cybersecurity policies and procedures and report violations
- Use data as intended and in compliance with applicable regulations
- Report issues with data quality, availability, or misuse
- Ensures the privacy of data by viewing and storing data, and the information derived from data, under secure conditions
- Ensures accuracy and timeliness of the data they enter or update
- Collects, prepares, enters or maintains data for the appropriate unit(s), as authorized

Information System Owner

At the highest level, every IT application and service should have an identified information system owner. This individual should be the senior person in the organization responsible for the application or service and ensures that the application or services renders value to the organization. For most infrastructure services such as the local area network and email, the CIO is that information system owner. For most business and educational support systems, the Vice President or Provost to whom the function reports is normally the information system owner.

In his or her capacity, the information system owner serves as both an owner and as the central point of contact between the system authorization process and subsystem owners. Examples of subsystems are application, networking, servers or workstations, owners or stewards of information stored, processed or transmitted by the system, and owners of the mission and business functions supported by the system.

Responsibilities:

The information system owner is responsible for addressing the operational interests from the framework of people, process and technology. For example:

- People
    - The information system owner determines and communicates the access rights and privileges to the information system for the purpose of ensuring compliance with regulatory and security requirements.
    - The information system owner ensures system users and support personnel receive requisite cybersecurity training.
- Process
    - In coordination with the Information Security Officer, the information system owner provides information and support for creating and maintaining the system security plan addressing the people, process and technology elements, and ensuring the system is deployed and operated in accordance with the agreed-upon security controls.
    - In coordination with the data owner or data steward, the information system owner is also responsible for maintaining a documented process describing access entitlements for the purpose of ensuring compliance with regulatory and security requirements.
    - Conveys through documentation, authorization of information system operation and explicit acceptance of the residual risk.
- Technology
    - Establish through contract, statement of work, memorandum of understanding, or service level agreement the responsibilities in support of the information system or services.
    - Provide liaison between the customers served by the information system and the information system or services provided.

In support of the information system owner, Information Security Officers are responsible for managing the repository of inventoried information systems, the information systems security plans associated with each information system identified, and any additional documentation collected in support of the information system security plans.

Data Custodians

Data Custodians manage the actual data, servers, backups, or networks and possess application / system knowledge and technical skills. The data custodian is the employee responsible for day-to-day maintenance of an Information System and is responsible for implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of institutional data. In some cases, some or all of these system administration responsibilities are assigned to a third-party vendor. For example, cloud services generally handle these responsibilities, while an MGA employee handle the additional responsibilities below.

Additional responsibilities:

- Provisioning and de-provisioning access to institutional data under their care as authorized by the Data Steward
- Maintenance of data and metadata according to data governance policies, standards, practices
- Adherence to data governance procedures provided by data stewards
- Support for data governance program and data stewards in application activities
- Data and metadata quality control
- Understanding and reporting on how institutional data is stored, processed and transmitted
- Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of institutional data
- Maintenance of data system documentation
- Acts as liaison between users and the service provider or information system owner

There may be more than one custodian. For example, there may be a custodian responsible for the operating system and a separate custodian responsible for the database.

Data Access

Data access is the process of being granted authorization to interact with data at a level that includes, but is not limited to, read, write and modify.

Data Access Request Procedures

1. Requests for access must be made in writing to the appropriate Data Steward. Such requests must include approval by the requestor's supervisor or management.
2. Data stewards will analyze user roles and determine level of access required to perform a job function. The level of authorized access must be based on principle of least privilege (POLP).
3. Upon approval by the Data Steward, the request is forwarded to the Data Custodian for technical implementation via provisioning of accounts, login ids, or view access. The request should be for minimal access to perform the role.
4. The Data Custodian will receive the request, fulfill the requested access and provide information back to the Data Steward on its completion status.
5. The Data Steward will notify the requestor of their access, and will provide a copy of the Privacy Standard, the relevant functional guidelines for use, and any restrictions on the data, such as the Family Educational Rights and Privacy Act regulations.
6. If they are no longer necessary Data access privileges can be revoked by the Data Steward by placing a request to the Data Custodian.
7. Upon employee termination, the Data Steward for the functional unit is responsible for placing a request to Data Custodians to remove all privileges to information systems and ensuring a Personnel Action Request Form (PARF) is submitted to Human Resources.
8. The Chief Information Security Officer, in collaboration with the Chief Privacy Officer and the Department of Human Resources, reserves the right to remove data access at any point.

5. Laws and Regulations

Family Educational Rights and Privacy Act of 1974 (FERPA) protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

Gramm-Leach-Bliley Act (GLBA) provides limited privacy protections for private financial information. Additionally, the GLBA codifies protections against pretexting, the practice of obtaining personal information through false pretenses and implements rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information.

Georgia Personal Identity Protection Act (GPIPA) is an effort to protect individuals from the growing threat of identity theft caused by data breaches, the Georgia General Assembly passed the Georgia Personal Identity Protection Act. A GPIPA Event is the combination of a person's first name (or initial) and last name, plus one or more of the following: (i) social security number; (ii) driver's license number; (iii) state identification card number; (iv) account number; (v) credit card number; (vi) debit card number; (vii) account passwords;(viii) PINs; or (ix) other access codes. Items (iv), (v), and (vi) only apply if the account number could be used without additional access codes.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US law designed to provide privacy and security standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.
Protected health information means individually identifiable health information that is:

i. Transmitted by electronic media;
ii. Maintained in electronic media; or
iii. Transmitted or maintained in any other form or medium.

Protected health information excludes individually identifiable health information in:

i. Education records covered by the Family Educational Rights and Privacy Act, as
ii. amended, 20 U.S.C. 1232g;

iii. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
iv. Employment records held by a covered entity in its role as employer."

The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information.

Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

Federal Tax Information (FTI) includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS),or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

Export-controlled information or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulations (EAR).

Controlled Unclassified Information (CUI) is any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under [EO 13526] or any predecessor or successor order, or [ATOM54], as amended.

6. Definitions

Institutional Data is data that provides support to, and meets the needs of, units of the institution. Examples of institutional data include, but are not limited to, many of the elements supporting financial management, student curricula, payroll, personnel management, and capital equipment inventory.

Information may be considered institutional data if it satisfies one or more of the following criteria:
1. Data used for planning, managing, reporting, or auditing a major administrative function;
2. Data referenced or used by a participant organization to conduct organization business;
3. Data included in an official participant organization administrative report; or,
4. Data used to derive an element that meets any of the criteria above.