I. Purpose

These standards reflect Georgia Southern University’s implementation of The Board of Regents Business Procedures Manual on Protection and Security of Records. The Board of Regents procedures establish that all faculty, staff, student employees, contractors and vendors must familiarize themselves with the data classification and management handling guidelines. The standards address the following areas:

- Data Management Structure
- Data Classification
- Data Access and Reporting
- Privacy and Security

II. Policy Statement

These standards pertain to all faculty, staff, students, contractors and vendors of the institution and provide functional guidelines for the use of data and information and any relevant restrictions on the use of data and information assets. The information covered in these standards includes, but is not limited to, University information that is stored or shared via any means.

III. Exclusions

These are exclusions and exceptions to the policy.

IV. Procedures

A. Standard: Data Management Responsibility

Board of Regents procedures establishes that the Chief Information Officer (CIO) is a Data Trustee and is charged with ensuring an adequate and appropriate security infrastructure to support the data needs of the institution across all divisions. For the purposes of providing day-to-day oversight of this responsibility, the CIO delegates responsibility to the Office of Information Security and the Chief Information Security Officer (CISO).
**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 the USG institution, the Chancellor of the USG, or the head of other USG organizations is identified as the data owner. The University data owner has ultimate responsibility for submission of organizational data to the USO.

Data owners have the responsibility for the identification, appointment and accountability of data trustees. Data owners will inform the University’s Data Governance Committee of their data trustee appointments including office, name and contact information of the incumbent.

**Data Trustees**

Data Trustees are executives of the University who have overall responsibility for the data read, created, collected, reported, updated or deleted in their data area(s). University data trustees have overall responsibility for accuracy and timeliness of submission of data.

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

- Ensuring that data accessed and used by units reporting to them is done in ways consistent with the mission of the office and USG organization;
- Appointing data stewards within each functional area for which they are responsible. The data trustees will inform the USG organization’s Data Governance Committee of their data stewards’ appointments, including office, name and contact information of the incumbent;
- Participating as a member of the Data Governance Committee; and,
- Communicating unresolved concerns about data to the data owner.

**Data Stewards**

Data Stewards 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.

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.
- 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.

**Data Managers**

Data managers are operational managers within a functional area that oversee data for a particular subject area. By example, this policy establishes the following positions as typical Data Managers, but this list is not exhaustive.

- University Registrar;
- University Bursar;
- Director of Human Resources.
**Data Users**

Data users are institutional employees, students, vendors and/or contractors who have been granted authorization by the data managers to access data.

Data Stewards and Data Managers are responsible for implementing the appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of University data in compliance with this policy.

The Departments’ Data Manager(s) will carefully evaluate the appropriate data classification for their respective information.

This policy is not intended to restrict the right of departments to require policies and/or procedures in addition to the ones identified in this document.

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. As such, the Office of Information Security will receive and maintain reports of incidents, threats, and malfunction that may have a security impact on the University's information systems while maintaining records of actions taken in response to such reports. Refer to USG Business Procedures Manual (BPM) Section 12, Data Governance & Management for more detailed information.

**B. Standard: Data Classifications**

The Data Classification Standards are intended to:

1) Augment USG Data Access Procedures (BPM 12.4.3);
2) Provide functional guidelines for use of data, including an understanding of what information can be disclosed and the relative sensitivity of information;
3) Provide a basis for categorizing and appropriately labeling the sensitivity of data and reports;
4) Educate the University community about the importance of protecting data generated, accessed, transmitted and stored by the University;
5) Identify procedures that should be in place to protect the confidentiality, integrity and availability of University data;
6) Establish procedures that comply with State and Federal regulations regarding privacy and confidentiality of information.

Sensitivity levels are guidelines for labeling data and reports in order to protect Georgia Southern confidential information. Data owned, used, created or maintained by the University is known as institutional data and are classified into three categories:

- Class I - Confidential Information
- Class II - Sensitive Information
- Class III - Unrestricted Information

Questions about the proper classification of a specific piece of information should be addressed to the Data Manager.

**Class I – Confidential Information**

Class I Information is confidential information that is protected and is subject to authorized restrictions on information access and disclosure, including means for protecting personal privacy
and proprietary information. Restrictions for Class I Information are defined by Statutes, regulations, University System policies, institutional policies, or contracts (e.g., HIPAA, FERPA, Gramm-Leach-Bliley, etc).

Examples of Class I data include but are not limited to:

- Medical records;
- Student records and other non-public student data;
- Social Security Numbers;
- Certain personnel and/or payroll records;
- Any data identified by government regulation to be treated as confidential;
- Any data sealed by order of a court of competent jurisdiction.

Protection of Class I data: Class I Information will be enforced based on NIST 800-171 requirements and required federal and state regulations. Examples of requirements include but are not limited to:

- Must not be disclosed to parties without explicit written authorization from the Data Trustee(s).
- Must not be sent via e-mail.
- Must be stored only in a locked drawer or room or an area where access is controlled by a cipher lock and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- When sent via fax, must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public website.

Class II – Sensitive Information
Class II Information is information that requires special precautions to protect it from unauthorized use, access and disclosure. Class II Information is restricted to members of the University community who have a legitimate purpose or are authorized to access such data.

Examples of Class II Information include certain intellectual property, trade secrets, or plans that could be harmful to the University or its employees if disclosed.

Protection of Class II Information: Class II Information will be enforced based on NIST 800-171 requirements and required federal and state regulations. Examples of requirements include but are not limited to:

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure;
- Must be stored in a locked container (i.e., file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use;
- Must not be posted on any unrestricted website;
- Based on the sensitivity of the information, acceptable encryption methods may be necessary.

Class III – Unrestricted Information
Class III Information may be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Class III data, while subject to University disclosure rules, are available to all members of the University community.
and may be available to all individuals and entities external to the University community.

Examples of Class III data include but are not limited to:
- Publicly posted press releases;
- Publicly posted schedules of classes;
- Publicly posted interactive University maps, newsletters, newspapers and magazines.

C. Standard: Reporting
Classification of Reports
Reports inherit the classification of the most restricted data used in the report and each page of a report shall be labeled accordingly. The summary of sensitive or confidential data may constitute a less restrictive classification of the report.

Class I - Confidential
Class II - Sensitive
Class III - Unrestricted

Labeling of Reports
In addition to identifying the sensitivity classification, reports should indicate the following:
- Source of the report (e.g. the Institution, Department and office publishing the report);
- Date of the report.

Production of Reports
Producers and publishers of reports should be mindful of the locations where reports are printed to avoid unintended disclosure.

Distribution of Reports
Reports should be distributed through authorized channels approved by Data Trustees and enforced by Data Stewards.

D. Standard: Disposal
Class I and II data shall be destroyed subject to the University’s Records Retention Policy based on the examples below. The stricter of the two standards apply.

- Destruction can be accomplished based on NIST 800-88 guidelines.
- Disposal of electronic equipment must be performed in accordance with the University’s Asset Management and Property Control Procedures.

E. Standard: Training and Awareness of Procedures
Data Stewards and Data Managers are responsible for implementing appropriate training and awareness in compliance with this policy.

F. Standard: Notification of Loss or Theft of Data
The Office of Information Security must be notified within 24 hours of discovery if Class I or Class II data is suspected to be lost or disclosed to unauthorized parties.

V. Audit and Review
The Office of Information Security will assist the Office of Internal Audit, Risk & Compliance in
conducting periodic audits to determine University compliance with this policy.

The Office of Legal Affairs will review procedures issued under authority of this policy for compliance with applicable regulations and policy.

VI. Related Documents
BOR Business Procedures Manual

VII. Remedies
Violation of this any standard in this policy may lead to disciplinary action up to and including dismissal and/or legal action. Any known violation of this policy is to be reported to the Chief Information Officer or his/her designee.