GEORGIA SOUTHERN UNIVERSITY

OFFICE OF THE VICE PRESIDENT FOR INFORMATION TECHNOLOGY
POST OFFICE BOX 8122
STATESBORO, GEORGIA 30460-8122
TELEPHONE (912) 478-1294
FAX (912) 478-7720

DATA STEWARDSHIP AND CLASSIFICATION STANDARD

Area:	University	Number:	
Subject:	Data Management	Issued:	10/15/2009
Applies To:	University	Revised:	n/a
Sources:	Information Technology Services	Page(s):	7

1. 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

2. Scope

These standards pertain to all employees, student staff, and contractors 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, information that is either stored or shared via any means, for example, electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

3. STANDARD: RESPONSIBILITY FOR DATA MANAGEMENT

Board of Regents procedures establishes that The Chief Information Officer (CIO) as a Data Trustee and is charged with ensuring an adequate and appropriate technical 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 Security Officer (CSO).

As stated in the Board of Regents procedures, "no single person or unit within the institution "owns" institutional data" and identifies four levels of data management responsibility. Each level designates the person(s) in the next level.

a. Data Trustees
   Data Trustees include the Vice Presidents and General Counsel. They have overall responsibility for all the data sets maintained by the units reporting to them.

b. Data Stewards
   Data stewards are senior level officials with planning and policy implementation responsibilities in their functional areas. This policy establishes the following positions as Data Stewards:

   i. Director of Technology for Academic Affairs
   ii. Director of Technology for Business Affairs
   iii. Director of Technology for Student Affairs and Enrollment Management
   iv. Director of Technology for University Advancement
   v. Director of Computer Center Operations, Division of Information Technology Services.

c. Data Managers
   Data mangers are operational managers within a functional area overseeing data for a particular subject area. By example, this policy establishes the following positions as typical Data Managers.
   i. University Registrar
   ii. University Bursar
   iii. Director of Human Resources
   iv. Etc…

d. Data Users
   Data users are institutional employees, contractors who have been granted authorization by the data managers to access data.

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

Departments' data managers will carefully evaluate the appropriate data classification for their respective information.

Nothing in this policy is intended to identify a restriction on the right of departments to require policies and/or procedures in addition to the ones identified in this document.

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, and will receive and maintain records of actions taken or policies and procedures developed in response to such reports.

Refer to Board of Regents Policy Section 12, Protection and Security of Records for more detailed information.

4. STANDARD: DATA CLASSIFICATIONS

The Data Classification Standards are intended to:

a) To augment Georgia Board of Regents Data Access Policy (12.4);
b) Provide functional guidelines for use of data including an understanding what information can be disclosed, and the relative sensitivity of information;
c) Provide a basis for categorizing and appropriately labeling the sensitivity of reports;
d) To educate the University community about the importance of protecting data generated, accessed, transmitted and stored by the University;
e) To identify procedures that should be in place to protect the confidentiality, integrity and availability of University data;
f) Establish procedures that comply with State and Federal regulations regarding privacy and confidentiality of information.

Sensitivity levels are guidelines for labeling data 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
Class II - Sensitive
Class III – Unrestricted

Questions about the proper classification of a specific piece of information should be addressed to your data manager.

a. Class I – Confidential

i. Class I is confidential information protected by statutes, regulations, University System policies, institutional policies or contracts. (e.g., HIPAA, FERPA, Gramm-Leach-Bliley, specific donor and employee data).
ii. Class I may be disclosed to individuals on a need-to-know basis only.
iii. Disclosure to parties outside the University must be authorized by the Data Trustees.
iv. When Class I data are disclosed to vendors or contractors pursuant to service agreements, such agreements must contain confidentiality clauses requiring the vendors or contractors to protect the confidentiality of the data.

v. Examples of Class I data include but are not limited to:
    1. Medical records
    2. Student records and other non-public student data
    3. Social Security Numbers

4. Certain personnel and/or payroll or records
5. Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.

vi. Protection of Class I data:
1. When stored in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures in order to protect against loss, theft, unauthorized access and unauthorized disclosure.
2. Must not be disclosed to parties without explicit written management authorization.
3. Must not be sent in e-mail.
4. 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.
5. 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.
6. Must not be posted on any public website.

b. **Class II - Sensitive**

i. Class II data must be guarded due to proprietary, ethical, or privacy considerations, and must be sensitive from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statute requiring this protection. Class II data are restricted to members of the University community who have a legitimate purpose or are authorized to access such data.

ii. Examples of Class II data include but are not limited to:
1. Employment data that are not Class I data.
2. University partner or sponsor information where no more restrictive confidentiality agreement exists
3. Research detail or results that are not Class I data
4. Financial transactions which do not include Class I data (e.g., telephone billing)
5. Physical plant/Facilities detail
6. Certain management information

iii. Protection of Class II data:
1. Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.

2. Must be stored in a closed container (i.e., file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
3. Must not be posted on any unrestricted website.
4. Must not be sent in e-mail without using acceptable encryption methods.

c. **Class III - Unrestricted**

i. Class III data may or must 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 to all individuals and entities external to the University community.

ii. By way of illustration only, some examples of Class III data include:
1. Publicly posted press releases
2. Publicly posted schedules of classes
3. Publicly posted interactive University maps, newsletters, newspapers and magazines

5. STANDARD: REPORTING

a. Classification of Reports
The classification of data drives the level of sensitivity of reports. Therefore, reports inherit the classification of the data used in the report and each page of a report shall be labeled accordingly:

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

The summarizing of sensitive or confidential data may constitute a less restrictive classification of the report.

b. Labeling of Reports
In addition to identifying the sensitivity classification, reports should also indicate the following:

- Source of the report
(e.g. the Institution, Department and office publishing the report)
- Date of the report

c. Production of Reports
Producers and publishers of reports should be mindful of the locations where reports are printed so as to avoid unintended disclosure or taking of reports by

unauthorized persons. For example do not print confidential or sensitive reports to printers located in areas where unauthorized persons might view the file.

d. Distribution of Reports
Reports should be distributed through authorized channels. These channels are approved by data trustees and enforced by data stewards.

6. STANDARD: DISPOSAL;

Class I and II data must be destroyed when no longer needed subject to the University's Disposal of Records Policy. Destruction may be accomplished by:

a. "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction.
b. Electronic (hard disk drive, USB flash drives) storage media shall be sanitized appropriately by degaussing or another process that destroys the data beyond the ability to reconstruct data prior to disposal.
c. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and magneto-optic (MO) disks must be destroyed by pulverizing or crosscut shredding.
d. Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.
e. Disposal of electronic equipment must be performed in accordance with the University's Property Control Policy and Procedures.

7. STANDARD: TRAINING AND AWARENESS OF PROCEDURES
Data Stewards and Data Managers are responsible for implementing appropriate training and awareness material to provide for managerial, operational, physical, and technical controls to access, use, transmit, and dispose of University data in compliance with this policy. This standard will be included in the New Employee Orientation.

8. STANDARD: NOTIFICATION OF LOSS OR THEFT OF DATA
The Office of Information Security must be notified in a timely manner if Data Class I or Class II are lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place or is suspected of taking place.

9. AUDIT AND REVIEW
The Office of Information Security will assist the Office of Audit and Advisory Services, 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 Board policy. Court Orders, Subpoenas,

litigation discovery requests, and requests for access to information made pursuant to the Georgia Open Records Act shall be referred immediately to the Office of Legal Affairs.

10. RELATED DOCUMENTS

BOR Protection and Security of Records:
http://www.usg.edu/fiscal_affairs/bpm_acct/
USG Data and Storage Handling Policy:
http://www.usg.edu/infosec/policy_management/policies/
Georgia Southern University Disposal of Records:
http://services.georgiasouthern.edu/archives/index.htm
Georgia Southern University Property Control Policies:
http://services.georgiasouthern.edu/procurement/webpg6.htm

11. REMEDIES

Violation of this standard can 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 Vice President for Information Technology or his/her designee.