



12.0 Protection and Security of Records

Introduction

Information, in all forms, is a strategic asset to an institution and to the University System of Georgia (USG). The purpose of this section is to provide guidelines for the management and access to data, which is critical to the administration of each institution and the USG.

Topics in this section include:

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



12.1 Purpose

While USG and institutional information may reside in paper format, in different database management systems, or on different machines, these data, in the aggregate, may be thought of as forming a single, logical database. These data will be called **institutional data**. This section will describe the roles and responsibilities of stewardship for, and procedures for establishing access to, institutional data.

It is the desire of the University System of Georgia that all institutional data be used with appropriate and relevant levels of access and with sufficient assurance of its security and integrity in compliance with existing laws, rules, and regulations. The goal of this section is to provide reasonable guidance to USG institutions to increase the value and security of data by use of appropriate guidelines, procedures and methods.

Note: For more detail, please refer to the Guidelines for the Use of the University System of Georgia Data Warehouse document, which is available at: <http://www.usg.edu/>.

Material in this section has been taken from the following sources:

1. Georgia State University, Data Stewardship and Access Policy for University Information.
2. University of Maryland, Baltimore County. UMBC Data Management Structure 6/18/2003. Draft version.

12.1.1 Scope and Restrictions

This section applies to institutional data only, as defined below, and is intended to improve access to these data by employees for conducting institution business. In all cases, applicable statutes, rules, and regulations that guarantee either protection or accessibility of institutional records will take precedence over this section. While this section is especially pertinent to information stored electronically, it is applicable to all information, such as paper, microform, and video, as well as the content of confidential meetings and conversations.

This section does not apply to notes and records that are the personal property of individuals in the institution community and is not directed to data whose primary purpose is scholarly; e.g., instructional material, research notes, etc.

The scope of this section is to have broad application, particularly with respect to data and information resources, which have impact on institutional operation. Data that may be managed locally may also have significant impact if it is used in a manner that can impact institution operations. It is expected that the intent of this section be extended in analogous manner to all data and information used at all operational levels of the institution.



12.1.2 Institutional Data Definition

A data element is considered institutional data if it 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 an organizational unit to conduct institution business.
3. Data included in an official institution administrative report.
4. Data used to derive an element that meets the any of the criteria above.

12.1.3 System Data Definition

A data element is considered **system data** if it is created by the University System Office (USO) and used by the USO for official purposes. Examples of system data include, but are not limited to, institutional enrollment information, financial information, and data warehouse information.

Information may be considered system data if it satisfies one or more of the following criteria:

1. Data included in the University System Data Warehouse.
2. Data that serve the policy development of the Board of Regents.
3. Data that inform decisions for, or operating, planning, managing, or auditing a major administrative function of, the System.
4. Data used to produce USG reports for internal and external constituencies.



12.2 Data Management Structure

A data management structure is required at each institution to ensure proper handling of institutional data. This data management structure should consist of the following positions.

12.2.1 Data Owner

The individual institution is the data owner of all institutional data. The USO is the data owner for information that has been submitted to the USO for use in aggregate reports, in the data warehouse, or other purposes.

No single person or unit within the institution or the USO “owns” institutional data. However, units within an institution or the USO have policy and operational responsibility for managing subsets of institutional data.

12.2.2 Data Trustees

Data trustees are institute executives who have overall responsibility for all the data sets maintained by the units reporting to them. Institutional data trustees consist of the Provost, other Vice-Presidents, General Counsel and the Chief Information Officer (CIO). Individually the data trustees are accountable for all the data sets within their division. The CIO has the additional responsibility for ensuring an adequate and appropriate technical infrastructure is in place to support the data needs of the institution across all divisions. USO data trustees are the counterparts of the institutional trustees.

The data trustees are responsible for ensuring that campus institutional data resources are used in ways consistent with the mission of the institution. The data trustees have the responsibility for the appointment and accountability of data stewards.

12.2.3 Data Stewards

Data stewards, designated by the data trustees, are senior level institution officials who have planning and policy responsibilities for data in their functional areas. Data stewards, or their designees, are responsible for recommending policies, and establishing procedures and guidelines concerning the accuracy, privacy and integrity of the data subsets for which they are responsible. Individually, data stewards act as advisors to the data trustees and have management responsibilities for data administration issues in their functional areas.

They have overall responsibility for the data in the subsets overseen by all their designated data managers. These responsibilities include:

- Interpreting and implementing Federal, State and USG policies and guidelines.
- Ensuring data quality and data definition standards are met.
- Identifying the privacy level, such as unrestricted, sensitive, or confidential, for the data subsets.



- Establishing authorization procedures to facilitate appropriate data access as defined by campus data policy and ensuring security for that data.
- Resolving issues related to stewardship of data elements that cross multiple units or divisions. For example, Social Security number may have more than one data steward since it is collected or used in multiple systems, such as financial, human resources, and student systems.
- Developing standard definitions for data elements, including those that cross multiple units or divisions. For example, there should either be a single definition of “full-time employee” or new data elements should be created for each unique definition.

12.2.4 Data Managers

Data managers, designated by the data stewards, are generally operational managers within a functional area overseeing the data for a particular subject area. Data managers have day-to-day responsibility for managing administrative processes and establishing business rules for the transactional systems. They have operational responsibility for the data management activities related to the collection, maintenance, protection, and dissemination of data in their functional areas.

The data manager may authorize operational tasks to be performed by data users outside the units that report to the data manager. The data managers are accountable for the data subsets they manage, whether the data is collected or maintained directly by the data manager (or their staff), by data users in other units or by external sources.

Responsibilities include:

- Reviewing and approving requests for access by other USG users, as defined by campus data policy.
- Determining the type of access given to USG users.
- Assuring compliance with federal, state and campus regulations regarding the release of, responsible use of, and access to, data.
- Training USG users in relevant regulations and proper understanding of data.
- Providing data definitions for each data element within the domain of their operational unit(s).
- Communicating any data definition or database changes to the appropriate data administrator.
- Ensuring the accuracy, privacy and integrity of the data they manage.
- Assisting in the design of data warehouse structures that contain data from their subject areas.

12.2.5 Data Users

Data users are institution employees who have been granted authorization by the data managers 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 institution business.

Responsibilities include:

- Following the policies and procedures established by the data stewards for responsible use of the USG data.
- Using institution data only as required to conduct institution business.
- Ensuring the privacy of data by viewing and storing data, and the information derived from data, under secure conditions.
- Ensuring accuracy and timeliness of any data entered or updated.
- Collecting, preparing, entering or maintaining data for the authorized unit(s), if authorized by the data manager.



12.3 Data Classification

By default, all institutional data will be designated as internal data for use within an institution or to satisfy institution external reporting requirements to the USG Board of Regents (BOR), and to State, Federal, or other external agencies. Institution employees will have access to these data for use in the conduct of institution business. These data, while available within the institution, are not designated as open to the general public unless otherwise required by law. The permission to view or query institutional data should be granted to all data users for all legitimate institution purposes.

As part of the data definition process, data stewards will assign each data element and each data view in institutional data to one of three categories: unrestricted, sensitive, and confidential.

Note: In some circumstances, as long as specific identifying data elements are removed, a data view may include elements of institutional data that would otherwise be sensitive or confidential.

12.3.1 Unrestricted Data

Where appropriate, data stewards may identify institutional data elements that have no access restrictions as available to the general public. These data will be designated as **unrestricted** or public data.

12.3.2 Sensitive Data

Where necessary, data stewards may specify institutional data elements as **sensitive** data for which users must obtain specific authorization to access since the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the institution.

The specification of data as sensitive should include reference to the legal or externally imposed constraint that requires this restriction, the categories of users typically given access to the data, and under what conditions or limitations access is typically given.

Note: It is assumed that all administrative output from the central administrative systems is classified as sensitive unless otherwise indicated.

12.3.3 Confidential Data

Where required, data stewards may identify institutional data elements as **confidential**, for which the highest levels of restriction should apply due to the risk or harm that may result from disclosure or inappropriate use.

This includes information whose improper use or disclosure could adversely affect the ability of the Institution to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.



12.4 Data Access

Data stewards will work together to define a single set of procedures for requesting access to sensitive elements of institutional data, and to document these data access request procedures.

12.4.1 Data Access

Data stewards at the institution are responsible for developing and obtaining approval of data access procedures and approving all requests for data access via these procedures. It is recommended that such a process be developed that includes the following steps:

1. Requests for access must be made in writing to the appropriate functional data steward. Such requests must include approval by the requestor's supervisor or management, and should be specific as to the data needed and the purpose for accessing the data. All requests are maintained for use in case of a need to audit access permissions.
2. Upon approval by the functional data steward, the request is forwarded to the data administration unit of the institution's Information Technology (IT) department for technical implementation via provisioning of accounts, login ids, or view access.
3. The requestor will be notified of their access, and will be provided a copy of the institution's Data Stewardship & Access Policy, the relevant functional guidelines for use, and any restrictions on the data, such as the Family Educational Rights and Privacy Act regulations.
4. All data access will be reviewed and renewed on an annual basis by each functional data steward to ensure that the access remains appropriate.

Note: Permission to access data does not necessarily imply permission to change data. Data stewards will ensure that the proper access rights, such as read, write, modify, or delete, are given to users who request data access.

12.4.2 Data Documentation

Data stewards are responsible for documenting the data maintained within their functional area. This documentation should include, at a minimum:

- Data name;
- Data description;
- Data sensitivity;
- Data location;
- Data retention; and,
- Data backup plan.



Data stewards also have responsibility for documenting the meta-data about their data so that users are aware of the definitions, restrictions, or interpretations, and other issues that ensure the correct use of the data.



12.5 Privacy and Security

Institutions should focus on two critical areas as they consider protection of institutional data: Privacy and Security. **Privacy** deals with the classification and release of protected data, while **Security** deals with the protection or confidentiality, integrity, and availability of data.

The protection of institutional data is governed by a growing collection of federal and state laws relating to privacy and security. All institutions are morally, and now legally, responsible for the protection and integrity of the data they create and maintain on their campus. Through a number of legal statutes and regulations, institutions now have a legal responsibility for protection of student, employee, and faculty information.

An institution is responsible for complying with all current laws and regulations concerning data privacy and security. The institution should identify an individual or group that will have responsibility for compliance with new regulations.

The following sections describe the major current laws that effect educational institutions. Due to the rapid changes in information technology and privacy requirements, however, new laws are being introduced at a rapid pace. Each institution must be vigilant and stay aware of new legal requirements in the Privacy and Security areas.

Reference: IT Security for Higher Education: A Legal Perspective. White paper produced for Educause by Kenneth D. Salomon, Peter C. Cassat, Briana E. Thibeau Dow, Lohnes & Albertson, PLLC, March 20, 2003

12.5.1 Family Education Rights and Privacy Act (FERPA)

The primary law that governs the privacy of educational information is the Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g(b).

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing “personally identifiable education information,” such as grades or financial aid information, without the student’s written permission. FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers.

Generally, institutions must have written permission from the student in order to release any information from a student's education record. However, FERPA does allow institutions to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

- School officials with legitimate educational interest
- Other schools to which a student is transferring



- Specified officials for audit or evaluation purposes
- Appropriate parties in connection with financial aid to a student
- Organizations conducting certain studies for or on behalf of the school
- Accrediting organizations
- To comply with a judicial order or lawfully issued subpoena
- Appropriate officials in cases of health and safety emergencies
- State and local authorities, within a juvenile justice system, pursuant to specific State law

Institutions may disclose, without consent, "directory" information, such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, institutions must tell students about directory information and allow students a reasonable amount of time to request that the school not disclose directory information about them.

Institutions must notify parents and eligible students annually of their rights under FERPA. The actual means of notification, such as a special letter, student handbook, or newspaper article, is left to the discretion of each institution.

While violations of FERPA do not give rise to private rights of action, the U.S. Secretary of Education has established the Family Policy Compliance Office, which has the power to investigate and adjudicate FERPA violations and to terminate federal funding to any institution that fails to substantially comply with the law.

12.5.2 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to protect the rights of patients and participants in certain health plans. In 2000, the federal Department of Health and Human Services adopted copious regulations granting consumers the right to receive written notice of the information practices of entities subject to HIPAA.

Colleges and universities that are affiliated with health care providers are considered covered entities, and institutions must provide written notice of their affiliated health care provider's electronic information practices. Most employer-sponsored health plans also are considered to be "entities" subject to HIPAA. As a result, various compliance obligations are imposed on colleges and universities that sponsor and administer such plans.



HIPAA generally requires covered entities to:

1. Adopt written privacy procedures that describe, among other things, who has access to protected information, how such information will be used, and when the information may be disclosed.
2. Require their business associates to protect the privacy of health information.
3. Train their employees in their privacy policies and procedures.
4. Take steps to protect against unauthorized disclosure of personal health records.
5. Designate an individual to be responsible for ensuring the procedures are followed.

12.5.3 Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act (ECPA) broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. Protection of the “contents” of such communications, however, extends only to information concerning the “substance, purport, or meaning” of the communications.

In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved. As a result, the monitoring by institutions of students’ network use or of network usage patterns, generally, would not be prohibited by the ECPA, as long as the substance of the communication was not made public.

The ECPA will come into play when an institution is forced to monitor or intercept student, faculty, or employee electronic communications such as e-mail. The effect of the law may depend on the type of person being monitored and the person’s association with the institution, as a student, faculty member, or employee, and whether the communication system is considered a public or private system.

The ECPA also contains specific exceptions allowing disclosures to law enforcement agencies under certain circumstances.

12.5.4 USA Patriot Act

The USA Patriot Act can effect educational institutions in many ways. Probably the most significant effect is that it potentially prohibits institutions from revealing the very existence of a law enforcement investigation. All institutions should ensure that they have worked with their legal staff to produce written procedures on how to deal with law



enforcement information requests. Any institution employee faced with a request from law enforcement should follow these procedures.

12.5.5 TEACH Act

The TEACH Act relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use technology materials in educational settings. Institutions that want to take advantage of the relaxed copyright restrictions must limit “to the extent technologically feasible” the transmission of such content to students who actually are enrolled in a particular course, and they must use appropriate technological means to prohibit the unauthorized retransmission of such information. In other words, the TEACH Act may require institutions to implement technical copy protection measures and to authenticate the identity of users of electronic course content.

12.5.6 Gramm – Leach – Bliley Act (GLBA)

The Gramm – Leach – Bliley Act (GLBA), enacted in 1999, was largely directed at financial institutions and creates obligations to protect customer financial information. However, it has been determined that colleges and universities are also covered by the act.

The GLBA has two major sections: privacy and security. The Federal Trade Commission’s (FTC) regulations implementing the GLBA specifically provide that colleges and universities will be deemed to be in compliance with the privacy provisions of the GLBA if they are in compliance with FERPA. Therefore, GLBA privacy requirements should not effect educational institutions. They should therefore focus mainly on the security sections of the GLBA.

The information security, or Safeguard, section has five major requirements that an institution must follow:

1. Designate one or more employees to coordinate the security safeguards.
2. Identify and assess the risks to customer information in each relevant area and evaluate the effectiveness of the current safeguards.
3. Design and implement a safeguards program and regularly monitor and test it.
4. Select appropriate service providers and contract with them to implement safeguards.
5. Evaluate and adjust the program in light of relevant circumstances or the results of testing.



12.5.7 Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) criminalizes unauthorized access to a “protected computer” with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer. A “protected computer” is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States. An institution may use this law when there has been a break-in of their computer systems.