Georgia State University Policy

7.20.04 Data Classification, Access and Information Protection

Policy Summary

All university information will be used with appropriate and relevant levels of access and with sufficient assurance of its integrity in compliance with existing university’s policies, laws, rules and regulations.

Full Policy Text

Information systems storing, processing, or serving confidential data will be secured. Appropriate and relevant levels of access to university data will be provisioned and revoked in accordance with existing federal or state law laws, university policies, rules, and regulations.

Responsibility

All University data that has been classified as "confidential" must have an identified Data Steward. Data Stewards have the primary responsibility for the privacy and security of the university data under his/her responsibility. Furthermore, all data users, not just Data Stewards, administrators, or processors, are responsible for the security and privacy of the data they access, transmit, and store as prescribed in university policy.

Standards

Data Categories All university information data elements exist in one of three categories: Confidential, Sensitive, or Unrestricted (derived from Board of Regents definitions).

Confidential Data. Data for which the highest levels of restriction should apply due to the risk or harm that may result from disclosure or inappropriate use.

Examples of Confidential Data: Social Security Numbers, Credit Card Information, Electronic Protected Health Information.

Sensitive Data. Data for which users must obtain specific authorization to access since the data’s unauthorized disclosure, alteration, or destruction may cause perceivable damage to the institution.

Examples of Sensitive Data: Date of Birth, University Email, Purchasing Data, Student Grades.

Unrestricted Data. No access restrictions. Available to the general public.

Data Stewardship and Access Procedures Data Stewards are responsible for ensuring that a security review has been successfully completed prior to granting access to confidential data elements and for ensuring that access privileges are revoked for terminated employees in a timely manner. Data Stewards are also responsible for annually submitting a signed Protected Data Elements Report which includes details about their confidential data elements so that users are aware of the definitions, restrictions, or interpretations, and other issues which ensure the correct use of data. Moreover, the Protected Data Elements Report must be updated and resubmitted by the Data Steward whenever there are changes to their confidential data elements. Examples of documented changes include reclassification, additional confidential data, and/or major system modifications. This Protected Data Elements Report includes information such as:
Social Security Numbers  The University is required to collect SSNs from students, staff and faculty for legitimate business and reporting purposes. SSNs are classified as "confidential" and the university does not request, collect, store or otherwise utilize social security numbers except when required by "business necessity." Moreover, a social security number shall not be used as the primary identifier for a students, staff or faculty member in any university database system. 

Please contact the Responsible Office for information on Standards & Procedures.

Additional Resources

Data Access Request Form (For requests other than SSNs):

http://solutions.technology.gsu.edu/files/2013/06/data_access_request_form.doc

Data Steward Security Review Procedure:

http://solutions.technology.gsu.edu/files/2013/06/data_steward_review_procedure.doc

Data Access Request Form:

http://solutions.technology.gsu.edu/files/2013/06/ssn_access_request_form.doc

Data Steward Protected Data Elements Report:

http://solutions.technology.gsu.edu/files/2013/06/data_steward_protected_data_elements_report.doc

Instructions on How to Secure Campus Systems:

http://solutions.technology.gsu.edu/policies-and-procedures/information-protection-and-access-procedures/
Administration of Policy

Mandating Authority:
Administrative Council

Responsible Office(s):
Information Systems and Technology, 13th floor, Commerce Building, 3-4357

Responsible Executive(s):

Policy History

Approving Body: Administrative Council

Rationale or Purpose

The rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the university. Statistics indicate that a very large percentage of potentially damaging incidents can be avoided by the use of existing anti-virus detection and elimination procedures. Establishing policy centrally and issuing standards and utilities from a central authority allows for rapid incident response and continuous of protection methods.

Additional Information

Originally approved and made effective by Administrative Council November 7, 2007

Additional Helpful Resources