Data Access Policy

Policy No. 03.GIT.110 Rev. 2.9

Effective Date: November 2, 2005
Last Review Date: November, 2005
Status
☐ Draft
☐ Under Review
☑ Approved
☐ Obsolete

The following are responsible for the accuracy of the information contained in this document

Responsible University Officers

Chief Data Stewards

Responsible Coordinating Office

Office of Information Technology

1. Executive Summary

It is the responsibility of Georgia Tech, through the *Chief Data Stewards*, to implement procedures to effectively manage and provide necessary access to *Institute Data*, while at the same time ensuring the confidentiality, integrity, availability, accountability, and auditability (CIAAA) of the information. Appropriate implementation of the policy will ensure Institute compliance with the FTC's Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA), as well as the Family Educational Rights & Privacy Act (FERPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The purpose of this policy is to provide a structured and consistent process for employees to obtain necessary data access for conducting Georgia Tech operations, defining 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 related safeguards. Please note that the term data classification should not be confused with the practice of handling or working with "Classified Data" (e.g. Government Classified Data). Georgia Tech classifies all data into one of four Data Categories described in section 3.2 of this document. Insofar as this policy deals with access to Georgia Tech computing and network resources, all relevant provisions in the Computer & Network Usage and Security Policy (CNUSP) [1] and Unit-Level Network Usage Policies [2] are applicable and included by reference in this document. In all cases, applicable federal and State statutes and regulations that guarantee either protection or accessibility of Institute records will take precedence over this policy.

(**NOTE**: Phrases shown in *italics* at their first occurrence in this document are defined in the associated IT Policy Definitions - Standards Document No. 05.GIT.170)

2. Scope

All employees of the Georgia Institute of Technology and all data (electronic, paper or otherwise) used to conduct operations of the Institute are covered by this policy. This policy does not address public access to data as specified in the Georgia Open Records Act. Furthermore, this policy does not apply to notes and records that are the personal property of individuals in the Georgia Tech community.

3. Statement of Policy

The Chief Data Stewards have defined the following guiding principles governing access to Institute Data by employees conducting Georgia Tech operations:

- Inquiry-type access to official Institute Data will be as open as possible to individuals who require access in the performance of Institute operations without violating legal, federal, or State restrictions. Compelling justification is required to limit inquiry access to any data element.
- *Data Users* granted “create” and/or “update” privileges are responsible for their actions while using these privileges. That is, all campus units are responsible for the Institute Data they create, update, and/or delete.
- Any individual granted access to Institute Data is responsible for the ethical usage of that data. It will be used only in accordance with the authority delegated to the individual to conduct Georgia Tech operations.

Chief Data Stewards hereby delegate authority to *Data Stewards* for implementing the policy at the unit level.

3.1. Access Coordination

Data Stewards will designate individuals to coordinate Institute Data access for each functional data grouping. The *Data Coordinator* will maintain records of authorized Data Users, and serve as contact point for the *Data Administrator(s)*. The Data Coordinator will inform the appropriate Data Administrator on a timely basis of any changes that affect data access. Employees may request access to data through a designated *Authorized Requester*. [4] Procedures for requesting data access will be provided by the Data Administrator(s).
Documentation of data elements and their appropriate use is the responsibility of the Data Stewards, Data Coordinators and Data Administrator(s).

3.2. Data Categories

Georgia Tech Institute Data shall be classified into four major categories that are defined as described in this section. ***The Data Stewards, in consultation with the Data Coordinators and Data Administrators, are responsible for defining which data elements and data views fall into each data category.***

- **Category I – Public Use:** This information is targeted for general public use. Examples include Internet website contents for general viewing and press releases.

- **Category II – Internal Use:** Information not generally available to parties outside the Georgia Tech community, such as directory listings, minutes from non-confidential meetings, and internal (Intranet) websites. Public disclosure of this information would cause minimal trouble or embarrassment to the Institute. This category is the default data classification category.

- **Category III - Sensitive:** This information is considered private and must be guarded from disclosure; unauthorized exposure of this information could contribute to ID theft, financial fraud and/or violate State and/or Federal laws.

- **Category IV – Highly Sensitive:** Data which must to be protected with the highest levels of security, as prescribed in contractual and/or legal specifications.

3.3. OIT Access to Data

Office of Information Technology positions with direct responsibility in maintaining and supporting Institute Information Systems that contain data used to conduct operations of the Institute are not required to individually obtain approval for data access. Direct responsibilities of the position in relation to the access of data in these systems should be covered in each individual's Workload Assignment, as defined by their department head. OIT employees will be responsible for being familiar with the policy as it relates to his or her position and job duties. OIT Directorates will be responsible for conducting policy awareness training for new department hires and that policy awareness reminders occur on an annual basis.

3.4. Request for Review

Data Users may request that the Data Stewards and Chief Data Stewards review the restrictions placed on a data element, *Data View*, and/or the classification of data. All such requests will be submitted through an Authorized Requester to a Data Coordinator. The appropriate Chief Data Steward has final governance authority regarding matters of data restrictions and requests for access rights to Institute Data.

4. Procedures

The following paragraphs and referenced documents are intended to assist Authorized Requesters, Data Stewards, Data Coordinators, and Data Administrators with the unit-level implementation of the Data Access Policy.

4.1. Requesting Data Access

Detailed procedures and guidelines for requesting data access under this policy are contained in the Georgia Tech Data Access Procedures [3]. These documents shall be updated on an "as needed" basis, reflecting any changes to the process and/or roles involved. Online forms [4] for requesting data access can be found at:
http://www.oit.gatech.edu/policies/forms/Data_Access_Request_Forms.cfm

4.2. Protecting Sensitive Data

The internal computers, networks, application software and data repositories of Georgia Tech are critical resources of the Institute and must be protected against inappropriate access and/or disruption of service. Active measures are necessary to ensure data integrity and reduce the risk of system compromise, especially when sensitive information may be at risk. The rising frequency of security incidents involving network-attached devices significantly increases the probability that sensitive data, if not properly identified and protected, may be exposed to unauthorized viewing or modification. Established procedures for protection and release of sensitive information must be followed regardless of the platform used to store that data. The Data Protection Safeguards [5] document is a comprehensive set of Technical (IT), Administrative (procedural), and Physical safeguards which need to be put in place in order to ensure adequate protection for each category of data, as described in Section 3.2 (Data Categories) above. **Any deviation from mandatory requirements must be documented and covered by adequate compensating control(s).** The department of Internal Auditing is available to assist in reviewing compensating controls.

Data Stewards, in consultation with the Data Coordinators and Data Administrators, are responsible for:

- ***Categorizing and/or re-classifying data elements and views***
- ***Granting selective access to Institute Data***
- ***Educating authorized users on responsibilities associated with data access***
- ***Informing technology specialists about data classifications to determine physical and/or logical controls required***

On the other hand, it is the express responsibility of authorized users and their respective business units to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

4.2.1. **Sensitive Data as it pertains to Unit-Level Servers**

Serving devices (servers) storing sensitive information shall be operated by professional system administrators, in compliance with all OIT security and administration policies, and shall remain under management oversight. Each such unit-level server storing sensitive or highly sensitive data shall be registered as outlined below, and shall have a Technical (IT) as well as an Administration point of contact.

Deans, Vice Presidents and Associate Vice Presidents, in their stewardship roles, are responsible for monitoring compliance with the Data Access Policy and associated guidelines by:

- Directing the reviews of, and responding to technical reports for, servers within units for which approval has been given to store sensitive information;
- Ensuring that all unit-level servers storing sensitive or highly sensitive data are registered with OIT Information Security: https://server-registration.gatech.edu;
- Coordinating with OIT Information Security to ensure that the server(s) providing this information to the campus network and Internet are secured through reasonable procedures; and
- Conducting periodic access control assessments of any sensitive information devices or services within their business units, in coordination with OIT Information Security.

4.2.2. **Sensitive Data as it pertains to Desktops/Laptops/Workstations**

Storage of sensitive information on laptops, mobile devices, and devices that are not used or configured to operate as servers (see Section 4.2.1 above) is prohibited, unless such information is encrypted in an OIT-approved encryption format and the user responsible for the device takes proper care to isolate and protect files containing that information from inadvertent or unauthorized access. Firewalls and anti-virus software must be installed on all desktops, laptops and workstations that access or store sensitive information, and a procedure must be implemented to ensure that critical operating system security patches are applied in a timely manner. Assistance with securing sensitive information may be obtained from unit-level technical authorities with input from OIT Information Security as necessary.

5. Compliance

Data Users are expected to respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to sensitive data; and to abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information. The unauthorized storage, disclosure or distribution of Institute Data in any medium, except as required by an employee's job responsibilities is expressly forbidden, as is the access or use of any Institute Data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.

Each employee at the Institute will be responsible for being familiar with the policy as it relates to his or her position and job duties. Violations of the policy may result in loss of data access privileges, administrative sanctions (including termination) as outlined in applicable Georgia Tech disciplinary procedures, as well as personal civil and/or criminal liability.

6. Communication

Upon approval, this policy shall be published on the Georgia Tech website. The following offices and individuals shall be notified via email and/or in writing upon approval of the policy and upon any subsequent revisions or amendments made to the original document:

- Chief Data Stewards, Data Stewards, Data Coordinators, Data Administrators
- Department Heads
- Unit-level business officers

7. References

[1] Georgia Tech Computer & Network Usage and Security Policy (CNUSP)
<http://www.oit.gatech.edu/policies/policies/CNUP.pdf>

[2] Georgia Tech Unit-Level Network Usage Policies

<http://www.oit.gatech.edu/policies/unit_level_policy/index.html>

[3] Data Access Procedures

<http://www.oit.gatech.edu/policies/procedures/DAP_Procedures.pdf>

[4] Online Data Access Request Forms

< http://www.oit.gatech.edu/policies/forms/Data_Access_Request_Forms.cfm>

[5] Data Protection Safeguards

<http://www.oit.gatech.edu/policies/standards/GIT_Data_Protection_Safeguards.pdf>

[6] Information Security General Preventative Measures

<http://www.oit.gatech.edu/information_security/policy/general_measures.html>

[7] IT Policy Common Definitions

http://www.oit.gatech.edu/policies/reference/IT_Policy_Definitions.pdf

8. Revision History

Revision Number	Author	Description
2.9	Richard Biever	Changed Data Classification references to Data

		Categorization and added section 3.3.