GEORGIA INSTITUTE OF TECHNOLOGY

DATA SECURITY CLASSIFICATION HANDBOOK

Protecting the Confidentiality, Integrity, and Availability of the Institute's Data

www.itpolicies.gatech.edu

TABLE OF CONTENTS

INTRODUCTION

To accomplish the education, research, and business objectives of Georgia Tech, employees require access to computer systems and services where protected university administrative data is stored. This activity carries an implicit trust that the user will be vigilant in the appropriate use and disposal of that information.

The improper maintenance, disposal, or release of administrative data exposes any organization to significant risk. A security breach violates individual privacy, compromises the Institute's reputation, and brings the potential for lawsuits and other recriminations. Faculty, staff, and student workers who possess or have access to university administrative data are custodians of this data, and bear responsibility for its use or misuse.

To mitigate security breaches and risk to the Institute, this guide is intended to help:

- Clearly define the Institute's four data categories;
- Assist employees with categorizing a variety of institute data;
- Document the steps needed to request and grant access to sensitive data;
- Reference applicable state and federal laws associated with the data; and
- Offer notes and tips to consider when accessing, handling, or transporting Institute data.

Every employee is encouraged to review and follow the guidelines outlined in this guide and the Georgia Tech Data Access Policy (DAP), located under "IT Policies" at **www.oit.gatech.edu**. The DAP provides a structured and consistent process for employees to obtain necessary data access, outlines the relevant mechanisms for delegating authority at the unit level, and defines data classification and related safeguards.

All employees of the George Institute of Technology and all data—electronic, paper, or otherwise—used to conduct operations of the Institute are covered by the Data Access Policy. The policy does not address public access to data as specified in the Georgia Open Records Act. For information on how to handle an Open Records Act request, see the Georgia Open Records Request section on page 5 of this guide.

HOW TO USE THIS GUIDE

Employees should use this guide as a reference for understanding the appropriate categorization of the most popular Institute data used to conduct Georgia Tech operations. Since it is impossible to list all data used at the Institute, the guide can be used to look up the categorization of a similar data type. This guide should be used in conjunction with the Georgia Tech Data Protection Safeguards document, located under "IT Policies" at **www.oit.gatech.edu**, to ensure that the data is being stored, accessed, and handled according to Institute guidelines.

Everyone who works at Georgia Tech has a role to play in helping to protect Institute data, systems, networks, and other IT resources. To ensure that any data used by your department, but not listed in this guide, is classified appropriately, use the contact information listed under GT Point of Contact of the overarching data type listed in the Common Data Sets section of this guide. For questions about the information contained within this guide, e-mail **dapquestion@gatech.edu**.

When used appropriately, this handbook along with the supporting resources mentioned in the guide will assist employees with mitigating the risk of data exposure. Protecting the *confidentiality*, *integrity*, and *availability* of the Institute's data and computer systems is imperative to ensure the success of the Institute's mission.

- **Confidentiality—**Assurance that information is not disclosed to unauthorized entities or processes.
- **Integrity—**Protection against unauthorized modification or destruction of information.
- **Availability—**Timely, reliable access to data and information services for authorized users.

DATA CATEGORIES FOR THE INSTITUTE

The term data classification used in this guide 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.

- **Category I—Public Use:** This information is for general public use such as the Institute's Web site contents, press releases, and annual reports.
- **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 Web sites. Public disclosure of the information would cause minimal trouble or embarrassment to the Institute.
- **Category III—Sensitive:** This information is considered private and should be guarded from disclosure; disclosure of the information may contribute to financial fraud. Disclosure may also violate state and/or federal law.
- **Category IV—Highly Sensitive:** Data which must be protected with the highest levels of security, as prescribed in contractual and/or legal specifications.

DEFAULT DATA CLASSIFICATION FOR THE INSTITUTE

The default data classification for Institute data is Category II—"Internal Use." If there are local, state, or federal regulatory requirements for a data element, then the data must meet the minimum required guidelines for protection. In the absence of any explicit data classification labels, any and all Institute data shall be presumed to be Category II—"Internal Use," and should be protected as such.

MANAGING, CATEGORIZING, AND GRANTING ACCESS TO GEORGIA TECH DATA

Chief Data Stewards: Senior administrative officers of the Institute are responsible for managing information resources while conducting Georgia Tech business. The provost and vice president for Academic Affairs and the senior vice president for Administration and Finance are the chief data stewards.

Data Stewards: Deans, vice presidents, associate vice presidents, or others identified by the chief data stewards to manage a subset of data, as well as categorizing their subset of data. They are responsible for the accuracy, integrity, and implementation of policy and procedures. 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.

Data Coordinators: Individuals designated by the data stewards to coordinate data access for subsets of data, maintain records of authorized data users, and serve as contact points for the data administrator(s). Examples of "subsets of data" include employee data, student data, Auxiliary Services data, financial data, and Sponsored Programs data.

Data Administrators: Individuals responsible for documenting and enabling users access to a domain of Institute data.

AGGREGATE DATA AND DATA VIEWS

Aggregate data repositories or data views shall be classified with the highest (most restrictive) categorization applicable to any individual data element contained therein. For example, on a repository, form, or screen displaying both "Internal Use" (Category II) and "Sensitive" (Category III) information, the data shall be entirely classified as "Sensitive" (Category III).

OPENS RECORDS REQUEST

As a state university, Georgia Tech is subject to the provisions of the Georgia Open Records Act (ORA) (www.legalaffairs.gatech.edu/rec_dev.html). The ORA provides that all citizens are entitled to view the records of state agencies on request and to make copies for a fee. The ORA requires that Georgia Tech produce public documents within three business days. If you receive a request for information under the Act, call the Office of Legal Affairs immediately at 404-894-4812; if the request is in writing, fax the request to 404-894-3120. The Georgia Institute of Technology data classification and protection requirements are independent of any obligations and responsibilities under the Georgia Open Records Act.

Note: There is no legal requirement that ORA requests be made in writing.

REQUESTING AND GRANTING ACCESS TO SENSITIVE DATA

The Georgia Tech Data Access Procedures document outlines the steps an employee must take to request access to Institute-wide systems such as PeopleSoft and Banner; departments should apply the same philosophy with servers and systems that contain sensitive information. If a department has a server or system with sensitive information, the following steps should be taken:

- Develop and document an access request process.
- Develop and document the approval process for granting users access to the server or system (this process may include multiple signatures).
- Develop and document the process for terminating user access.
- Maintain a list of users that have been approved to access the server or system and what data views each user is approved to access.

Continued on next page

REQUESTING & GRANTING ACCESS TO SENSITIVE DATA (Continued)

Access requests should include the following information:

- Department or unit that has been granted access to the data
- User name
- gtID#
- Job title
- Phone number
- Which data view and why
- Access end date (if applicable)
- All expected user groups for the data requested, including third parties

DAILY BUSINESS INFORMATION

DAILY BUSINESS INFORMATION

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
Organizational Charts	Any	Public Use Data Category I			Contact the specific department.
Web Pages Internal to the Institute and Department	Any	Internal Use Data Category II		**CAUTION** This may be elevated to "sensitive" (Category III) depending on the type of information stored on the pages, or in a database.	Contact the specific department.
E-mail (un-secured e-mail in general)	Any	Public Use Data Category I		ⓘ Do not include social security number or any other personal information in e-mail when requesting information from payroll and other GT departments. Use the gtID# instead.	pay.ask@ohr.gatech.edu 404.894.4614
Faculty and Staff GT E-mail Addresses	Any	Public Use Data Category I		ⓘ All faculty and staff e-mail addresses provided by Georgia Tech are considered public information.	pay.ask@ohr.gatech.edu 404.894.4614
Faculty and Staff GT Phone Numbers	Any	Public Use Data Category I		ⓘ All faculty and staff office phone numbers are considered public information.	pay.ask@ohr.gatech.edu 404.894.4614
Customers' Personal Checks	Any	Internal Use Data Category II		ⓘ In transit checks should be protected as "internal use" information.	bursar.ask@ business.gatech.edu
Purchasing Receipts	Any	Internal Use Data Category II		**STOP** All digits of the credit card receipt must be blocked out, except for the last four prior to submitting for payment.	ap.ask@ business.gatech.edu
Login Passwords	Any	Internal Use Data Category II (when in digital format) Sensitive Data Category III (when in readable format)		**CAUTION** Do not share your password with anyone for any reason.	security@gatech.edu

Continued on next page

DAILY BUSINESS INFORMATION

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
BuzzCard Numbers of Individuals	Any	Internal Use Category II		ⓘ A card number will change based upon lost or stolen card replacement. The BuzzCard number is not the same as the gtID#, which will remain the same upon card replacement.	buzzcard.ask@buzzcard.gatech.edu 404.894.2899
Network Diagrams of the Institute's Network with IP addresses	Any	Internal Use Data Category II		**STOP** Network diagrams with IP addresses should not be distributed outside the Institute. ⓘ The Office of Information Technology will only provide a hard copy of this information when required and the recipent must sign for a copy of this information.	The Office of Information Technology, Chief Network Architect 404.894.4660
Network Diagrams of the Institute's Network without IP Address	Any	Public Use Data Category I			The Office of Information Technology, Network Services Department 404.894.4660
PeopleSoft ID	Any	Internal Use Data Category II			pay.ask@ohr.gatech.edu 404.894.4614
Financial Account Numbers of the Institution	Any	Internal Use Data Category II			gl.ask@business.gatech.edu
Purchasing and Receiving Reports	Any	Internal Use Data Category II	GLBA, SOX		purchasing.ask@business.gatech.edu
Travel Reimbursement Forms	Any	Internal Use Data Category II	GLBA, SOX	**STOP** It is strongly recommended that travelers block all but the last four digits of their personal credit card information prior to forwarding to their administrative office. The Georgia Tech Credit Card Processing Policy (http://www.oit.gatech.edu/inside_oit/policies_and_plans/overview.cfm) requires the removal of all personal credit card information from the paper form prior to it being submitted for reimbursement.	travel.ask@business.gatech.edu

Continued on next page

CREDIT CARD INFORMATION

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
Customer Credit Card	Any	Highly Sensitive Data Category IV	PCI, GLBA	**STOP** All credit cards containing customer information are considered highly sensitive/category IV and must be protected to the highest level of controls as defined in the DAP Safeguards document. Under no circumstances should the entire number be sent via e-mail or retained in a GT system. ⓘ When responding to a customer via e-mail to verify a credit card transaction, it is permissible to send only the last four digits of the credit card number.	bursar.ask@business.gatech.edu
P-card Number (GT Issued P-card)	Any	Internal Use Data Category II	GLBA, SOX	**CAUTION** End users should not download P-card numbers to the desktop or other departmental systems.	pcard.ask@business.gatech.edu

PUBLIC RELATIONS INFORMATION & MATERIALS

Public Relations Brochures Containing General Information about the Institute	Any	Public Use Data Category I			Contact the advertising department or the company that created the material.
Public Web Pages Containing General Information about the Institute	Any	Public Use Data Category I			Contact the specific department, unit, or web master for information regarding the web content.
Annual Reports	Any	Public Use Data Category I			Contact the specific department listed in the report. For information regarding specific Institute data, contact the Institute Research & Planning Department at requests@irp.gatech.edu.

EMPLOYEE INFORMATION

EMPLOYEE INFORMATION

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
Faculty and Staff—Personal & Emergency Contact Information	Any	Internal Use Data Category II		ⓘ This information is not considered sensitive, but should be stored in a safe location at all times and should not be shared with others without approval by the department head or HR representative.	pay.ask@ohr.gatech.edu 404.894.4614
Police Officer's Personal Contact Information	Any	Sensitive Data Category III		**STOP** This information is considered private and must be protected with appropriate controls.	pay.ask@ohr.gatech.edu 404.894.4614
Salary Information with an Individual's Name Associated (faculty, staff, or student workers)	Any	Internal Use Data Category II			pay.ask@ohr.gatech.edu 404.894.4614
Performance Evaluations	Any	Internal Use Data Category II			pay.ask@ohr.gatech.edu 404.894.4614
Compensated Absence Report Form (CARF)	Any	Internal Use Category II			pay.ask@ohr.gatech.edu 404.894.4614
Personal Address with Permission to Publish in the GT Directory	Any	Public Use Data Category I		ⓘ Personal information can be updated anytime via www.techworks.gatech.edu	pay.ask@ohr.gatech.edu 404.894.4614
Personal Address without Permission to Publish in the GT Directory	Any	Internal Use Data Category II	GLBA		pay.ask@ohr.gatech.edu 404.894.4614
Work Address of GT Employees	Any	Public Use Data Category I			pay.ask@ohr.gatech.edu 404.894.4614

Continued on next page

EMPLOYEE INFORMATION

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
gtID# Alone (faculty, staff, or student)	Any	Internal Use Data Category II	GLBA, SOX		pay.ask@ohr.gatech.edu 404.894.4614
Individual Benefits Elections	Any	Sensitive Data Category III	HIPAA	ⓘ Benefits information is protected from opens records.	pay.ask@ohr.gatech.edu 404.894.4614
Social Security Numbers (SSN) (faculty and staff)	Any	Sensitive Data Category III	GLBA	**STOP** All social security numbers are considered Category III/ "sensitive," and must be protected at all times. **NEVER SEND SOCIAL SECURITY NUMBERS VIA E-MAIL.** When conducting GT business, never use the person's social security number unless absolutely necessary. Instead use the gtID or employee ID numbers. When submitting travel documents always remove or retract social security and credit card numbers.	pay.ask@ohr.gatech.edu 404.894.4614
All Other Personal Data Not Included in the above List	Any	Internal Use Data Category II		ⓘ A few examples of personal data in the personnel file include, but are not limited to the following: 1. Personal Services Form (PSF) 2. Resume 3. Completed Application	

ENVIRONMENTAL SAFETY AND PHYSICAL SECURITY SYSTEM DATA

ENVIRONMENTAL SAFETY & PHYSICAL SECURITY SYSTEM DATA

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
Chematix Chemical Tracking System	Any	Sensitive Data Category III		**STOP** All Georgia Tech labs are required to inventory and post lab chemicals in the Chematix Chemical Tracking System. Online training is mandatory prior to an employee accessing the Chematix Chemical Tracking System. Contact Environmental Health and Safety if accessing this system is a requirement for an employee's job function.	Chemical Information Specialist 404.894.4635
Blueprints of GT Buildings	Any	Internal Use Data Category II		ⓘ Registered GT students can access drawings via the GT Library archives. Students must sign a registry prior to access being granted. Employees needing access to building drawings must contact the Facilities Design & Contracting Office and demonstrate a valid need in order to obtain this information.	Facilities Design & Contracting Office 404.894.4800
Building HVAC Monitoring/ Control Data	Any	Sensitive Data Category III		**STOP** This information is restricted to Facilities operating personnel only.	Facilities Design & Contracting Office 404.894.4800
BuzzCard System	Any	Sensitive Data Category III		**STOP** Access to or a data feed from this system is restricted.	buzzcard.ask@buzzcard.gatech.edu 404.894.2899
Continuum System	Any	Sensitive Data Category III		**STOP** Access to or a data feed from this system is restricted.	cshelp@police.gatech.edu 404.385.1098
Building Safety Plans	Any	Sensitive Data Category III			Director of Emergency Preparedness, GT Security & Police Department

LIBRARY RECORDS

LIBRARY RECORDS

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
Active Circulation Records	Any	Sensitive Data Category III		**STOP** Student information regarding books checked out from the Georgia Tech Library is considered private and will not be disclosed to anyone.	Library/Circulation, Department Manager
Active Interlibrary Loan Records	Any	Internal Use Data Category II			Librarian in Charge of Active Interlibrary Loan Records
Library Databases (purchased, licensed, or owned)	Any	Internal Use Data Category II			Librarian in Charge of the Library's Databases
Library Catalogue Information	Any	Public Use Data Category I			Librarian in Charge of Catalogue Information
Security Camera Recordings	Any	Sensitive Data Category III		ⓘ Security camera recordings are available for two weeks.	Library, Security Supervisor

RESEARCH INFORMATION

RESEARCH INFORMATION

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
Research Data		Sensitive Data Category III		ⓘ Examples of this type of research data are human or animal subject, and biochemical information.	Office of Research Compliance
Sponsored Project Contracts, Grants, and Associated Protocols	Any	Internal Use Data Category II		ⓘ Sponsored Programs projects' information is usually classified as "internal use."	Office of Research Compliance
Non-Sponsored Research Information	Any	Internal Use Data Category II			For disclosure and patent questions, contact Office of Technology Licensing.
Technology Licensing and Invention Disclosure Information	Any	Sensitive Data Category III		ⓘ If the intellectual property does not have contractual restriction, the data can be reclassified as "public use."	Office of Technology Licensing
Proprietary Information Obtained by GT under a Nondisclosure Agreement (NDA)	Any	Sensitive Data Category III		**STOP** Close attention must be given to the contractual requirements of the Nondisclosure Agreement to determine if the protection of the data should be changed from the baseline data classification of "sensitive" to "highly sensitive." If the classification is required to change to "highly sensitive," then the appropriate safeguards must be applied to meet the contractual requirements. NDAs not linked with sponsored projects such as evaluating a product are not considered to be "sensitive data."	Office of Sponsored Programs (OSP) Data Coordinator
Intellectual Property Information Owned by the Institute	Any	Sensitive Data Category III		ⓘ Here are some examples: 1. Invention Disclosure 2. Patentable Invention 3. Copyrights 4. Trade Secrets 5. Proprietary Techniques	Office of Technology Licensing

STUDENT INFORMATION

STUDENT INFORMATION

Institute Data Type	Data Amount	Data Categorization	Applicable Laws—State or Federal	Important End User Information and Instructions	GT Point of Contact for Questions Regarding Data
Student Records Excluding Directory Information	Any	Sensitive Data Category III	FERPA	**STOP** Grades, along with any other student information, should never be posted in public or shared with others.	comments@registrar.gatech.edu
Financial Aid and Grant Application Information	Any	Sensitive Data Category III	FERPA, GLBA	ⓘ Financial aid and grant applications contain information (i.e. parents' social security numbers, beneficiary information, etc.) that must be protected under state and federal regulations.	comments@registrar.gatech.edu
Social Security Numbers (SSN) (Student)	Any	Sensitive Data Category III	FERPA, GLBA, SOX	**STOP** All social security numbers are considered Category III/ "sensitive" and must be protected at all times. Never send social security numbers via email or Instant Messenger. When conducting GT business, never use a student's social security number unless absolutely necessary. Instead use the student's name and the last three digits of the gtID number.	Contact the Registrar or send an e-mail to comments@registrar.gatech.edu
gtID# Alone (Student)	Any	Internal Use Data Category II			Contact the Registrar or send an e-mail to comments@registrar.gatech.edu

GT DATA STEWARDS AND COORDINATORS

Below is a list of the chief stewards, data stewards, and primary data coordinators for the data stored on Institute-wide systems. If you need access to data or a system not listed below and you do not know who to contact, please send your request to **dapquestion@gatech.edu**.

	FUNCTIONAL TITLE
Chief Data Stewards for the Institute	
Student Information System	Provost and Vice President for Academic Affairs
Administrative Systems	Vice President, Administration and Finance
Banner Student Information System	
Data Steward	Registrar
Data Coordinator	Associate Registrar
Data Warehouse (student data)	
Data Steward	Registrar
Data Coordinator	Associate Registrar
Data Warehouse (employee data)	
Data Steward	Associate Vice President, Human Resources
Data Coordinator	Director, Human Resources Information Services
Data Warehouse (financial services data)	
Data Steward	Associate Vice President, Financial Services
Data Coordinator (Chart of Accounts & Ledger Posting Detail)	Associate Controller, Director Financial Systems Management
Data Coordinator (Grants & Contracts Accounting; Salary, Planning & Distribution)	Director, Grants and Contracts Accounts
PeopleSoft HR/Payroll	
Data Steward	Associate Vice President, Human Resources
Data Coordinator	Director, Human Resources Information Services
PeopleSoft Financials	
Data Steward	Associate Vice President, Financial Services
Data Coordinator	Associate Controller
PeopleSoft SPD	
Data Steward	Associate Vice President, Financial Services
Data Coordinator	Director, Grants & Contracts Accounts
Office of Sponsored Programs System	
Data Steward	Associate Vice Provost, Sponsored Programs
Data Coordinator	Director, Sponsored Programs

Board of Regents Records Retention Guidelines
www.usg.edu/usgweb/busserv/

Additional Institute Policies and Guidelines can be found at
www.oit.gatech.edu/policies

Contact EthicsPoint to anonymously report potential misuse of data
www.ethicspoint.com or 1.866.294.5565

GLOSSARY OF TERMS

- **FERPA—Family Educational Rights and Privacy Act.** FERPA is a federal law that protects the privacy of student education records, Students have specific, protected rights regarding the release of such records and FERPA requires that institutions adhere strictly to these guidelines. Therefore, it is imperative that faculty and staff have a working knowledge of FERPA guidelines before releasing educational records.

  www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

- **GLBA—Gramm-Leach-Bliley Act.** GLBA, also known as the Financial Services Modernization Act, provides limited privacy protections against the sale of private financial information.

  www.ftc.gov/privacy/privacyinitiatives/glbact.html

- **HIPAA—Health Insurance Portability and Accountability Act.** HIPAA is a federal law that mandates that health care providers and health plans protect the privacy of patient records.

  www.hhs.gov/ocr/hipaa

- **PCI—Payment Card Industry.** The PCI Data Security Standard (DSS) was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking, and various other security issues. A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant or risk losing the ability to process credit card payments.

  https://www.pcisecuritystandards.org

- **SOX—Sarbanes-Oxley Act.** The act establishes new standards for corporate accountability and seeks to improve the accuracy of financial reporting for publicly traded companies. However, there are several examples of how universities are taking the initiative to adopt many of the same principles outlined in Sarbanes-Oxley, and applying them to their stewardship practices.

  www.sec.gov/spotlight/sarbanes-oxley.htm

GEORGIA INSTITUTE OF TECHNOLOGY

www.itpolicies.gatech.edu