Information Technology

The Computer Network Usage and Security Policy (CNUSP) has been replaced by the Georgia Tech Cyber Security policies - the Acceptable Use Policy, the Cyber Security Policy, and the Data Privacy Policy.

Table Of Contents

Information Technology 1
Acceptable Use Policy 3
Controlled Unclassified Information 5
Credit Card Processing 6
Cyber Security Policy 8
Data Access 11
Data Privacy Policy 16
Email Forwarding for Life 18
GLBA Information Security Program 20
Identity Theft Prevention Policy 24
Information Technology Accessibility Policy 27
Password Policy 31
Policy Exceptions 34
Responsible Disclosure Policy 37
Telecommunications 39
Broadband Connections for Faculty and Staff 39
Long Distance Telephone Usage 41
Wireless Communication Devices/Cellular Telephone Service 42

Acceptable Use Policy

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jan 2017
Last Revised: Jan 2017
Review Date: Jan 2020
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
The Georgia Institute of Technology (Georgia Tech) Acceptable Use Policy (AUP) provides the guiding principles for use of Information Technology (IT) Resources at Georgia Tech. Users of Georgia Tech IT Resources are expected to be good stewards of these resources and to act in a responsible manner. Appropriate use of IT Resources allows the Institute to achieve its academic and research missions while maintaining a culture of openness, trust, and integrity within our digital spaces.

Policy Statement:
Institute IT Resources must be used in accordance with applicable licenses and contracts, and according to their intended use in support of the Institute's mission.

All users must comply with federal, state, and local laws, as well as Georgia Tech policies, when using Georgia Tech IT Resources.

The following sections define the acceptable uses of Georgia Tech IT Resources. Any conflict between these policies and the legitimate business of the institute can be resolved through the policy exception request process as defined with the Policy Exception Policy.

Acceptable Use
Employees and student employees -
With the exception of incidental personal use, as defined below, Georgia Tech IT Resources must be used only to conduct the legitimate business of the Institute (e.g., scholarly activity, academic instruction, research, learning, business operations).

Incidental personal use of Georgia Tech IT Resources by Georgia Tech employees is permitted if the personal use does not interfere with the execution of job duties, does not incur cost on behalf of the Institute, and is not unacceptable as defined in the Unacceptable Use section below.

Students -
Georgia Tech students may use the ResNet, EastNet, and LAWN networks for recreational and personal purposes to the extent that such use is not unacceptable as defined in the Unacceptable Use section below, and does not adversely affect network service performance for other users engaged in academic, research, or official business activities.

Unacceptable Use
Georgia Tech employees, including students acting as employees, are prohibited from the following actions when using Georgia Tech IT Resources:

- Unauthorized use of IT Resources for commercial purposes or personal gain
- Transmitting commercial or personal advertisements, solicitations, or promotions

All users are prohibited from using Georgia Tech IT resources in a manner which results in a violation of law or policy or potentially adversely affects network service performance. Examples of Unacceptable Use include, but are not limited to, the following:

- Activity that violates federal, state, or local law
- Activity that violates any Institute or Board of Regents policy
- Activities that lead to the destruction or damage of equipment, software, or data belonging to others or the Institute
- Circumventing information security controls of Institute IT Resources
- Releasing malware
- Intentionally installing malicious software
- Impeding or disrupting the legitimate computing activities of others
- Unauthorized use of accounts, access codes, passwords, or identification numbers
- Unauthorized use of systems and networks
- Unauthorized monitoring of communications

This list is not complete or exhaustive. It provides examples of prohibited actions. Any user in doubt about the acceptable use of Georgia Tech IT Resources should contact Cyber Security for further clarification and assistance.

Scope:
All Georgia Tech IT resource users are covered by this policy.

Policy Terms:
Georgia Tech IT Resources – Georgia Tech owned computers, networks, devices, storage, applications, or other IT equipment. “Georgia Tech owned” is defined as equipment purchased with either Institute funding (including sources such as Foundation funds etc.) or Sponsored Research funding (unless otherwise specified in the research agreement).

Enforcement:
Violations of this policy may result in loss of Georgia Tech system and network usage privileges, and/or disciplinary action (up to and including termination or expulsion) as outlined in applicable Georgia Tech policies.

If user suspects that they are a victim of a violation of this policy, then the violation may be reported directly to the Georgia Tech Cyber Security team by sending an email to cyber@security.gatech.edu per the Incident Reporting procedures found in the Cyber Security Policy.

Users should report any other violations through Georgia Tech’s EthicsPoint, a secure and confidential reporting system, at https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=7508.

Related Information:
Cyber Security Policy
Data Access Policy
Data Privacy Policy
Policy Exceptions
Responsible Disclosure Policy
Ethics Point

Policy History:

Revision Date	Author	Description
TBD	OIT	New Policy

Controlled Unclassified Information

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Dec 2017
Last Revised: Dec 2017
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
NIST Special Publication 800-171 (NIST 800-171), is a Federal standard that standardizes security controls applied to Controlled Unclassified Information (CUI) and systems and processes involved with this data within federally funded environments. Georgia Tech is obligated to ensure that all systems and processes involved with CUI are compliant with NIST 800-171 to continue receiving Federal funds associated with the use of this data (either directly received from the government or indirectly through associated covered contracts and contractors).

Policy Statement:
This approval process applies to all activities involving the use of CUI: All environments (see definitions section) involved with CUI must comply fully with the NIST 800-171 standards (either directly or through compensating controls) and follow the guidance provided by the Georgia Tech System Security Plan (GT SSP). Any deviations from the GT SSP must be approved by the Chief Information Security Officer (CISO). The CISO will route such request to either the Executive Vice President of Research (for research-related activities) or the Executive Vice President for Administration and Finance (for administrative activities), as appropriate, for additional approval. All environments that are involved with CUI must undergo an annual NIST 800-171 compliance assessment by Cyber Security before interacting with CUI. These assessments will result in an attestation report signed by the CISO, or designee. The assessment results will be reported to the Georgia Tech Research Corporation and the Executive Vice President of Research (for research-related activities) or the Executive Vice President for Administration and Finance (for administrative activities). Any items of non-compliance found during the assessment must be remediated before any interaction with CUI is allowed. All environments that are involved with CUI must also operate in a manner which allows incident reporting of cyber incidents involving CUI within 72 hours. This policy provides requirements and guidance for all use of CUI for the Georgia Institute of Technology. These are the minimum requirements for securing CUI - all Institute and other applicable requirements still apply as well.

Scope:
Anyone who handles CUI on behalf of the Institute must abide by this policy.

Definitions:

Compensating Controls	A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time. Compensating controls for a NIST 800-171 requirement need to mitigate the underlying risk that the requirement is designed to address. Cyber Security will work with the labs and units to design and approve compensating controls.
Controlled Unclassified Information (CUI)	Controlled Unclassified Information is any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526,

	Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.
Environment	Environment is defined as the systems upon which CUI resides and the physical infrastructure that houses these systems. Examples might be an individual research lab consisting of a room with desktop computers housing CUI or a student records system residing on multiple servers within a cabinet in a datacenter. The room(s) or area(s) housing the computer systems along with the computer systems themselves define the environments to which this policy applies.

Related Information:
DFARS 252.204-7012
Georgia Tech System Security Plan
Georgia Tech System Security Plan Procedures Document
NIST Special Publication 800-171

Policy History:

Revision Date	Author	Description
December 2017	Cyber Security	New Policy

Credit Card Processing

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jul 2003
Last Revised: Oct 2018
Review Date: Sep 2022
Policy Owner: Info Tech- Information Security
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
This policy provides requirements and guidance for all credit card processing activities for the Georgia Institute of Technology (Georgia Tech). This policy preempts all other campus policies and procedures for all elements within the scope of this policy.

Policy Statement:
This approval process applies to all merchant credit card processing activities at Georgia Tech:

The Associate Vice President of Financial Services (or delegate) must approve all credit card processing activities at Georgia Tech prior to entering into any such contracts or purchasing equipment.

This requirement applies regardless of the transaction method used (e.g. online processing at Georgia Tech, outsourced to a third party, swipe terminals).

All technology implementation associated with the credit card processing must be approved by the Vice President of

Information Technology (or delegate) prior to entering into any contracts or purchasing equipment.

Storage of cardholder data on Georgia Tech systems is not allowed."
All environments that process or transmit cardholder data are contractually obligated to and must comply fully with the Payment Card Industry Data Security Standards (PCI DSS). All units that process or transmit cardholder data must undergo an initial and annual PCI DSS compliance assessment by Georgia Tech Cyber Security. Any items of non-compliance found during the assessment must be remediated before processing of credit cards is allowed to resume.

The use of non-traditional credit card-type merchant services (such as Square, PayPal, etc.) and supporting technology for Georgia Tech business are not allowed without prior approval by the Associate Vice President of Financial Services and the Vice President of Information Technology (or their delegates).

Violations of this policy should be reported through the Ethics Point process.

Scope:
The scope of this policy includes all credit card merchant activity at Georgia Tech. All environments, units, technologies, and people associated with Georgia Tech merchant IDs and/or that support credit card merchant activity at Georgia Tech must abide by this policy.

This policy does not apply to non-credit card financial tools (such as Buzzcards).

This policy does not apply to end-user use of credit cards, including procurement cards (PCards), or any other such instance where Georgia Tech is not acting in a merchant capacity and/or supporting merchant activity.

Procedures:
The following are procedures to be followed prior to accepting credit cards in a merchant capacity at Georgia Tech:

- Document the business need for accepting credit card transactions in that particular unit, method, or location.
- Meet with Financial Services for justification and approval of the business case.
- Meet with Cyber Security to evaluate options and costs for implementation (using existing facilities, implementing separate facilities, or outsourcing transaction processing).
- Meet with the Vice President of Information Technology or designee for technical approval of implementation.
- Meet with Georgia Tech Legal Affairs to ensure that all contracts meet federal, state, and contractual requirements.
- Meet with Cyber Security on an annual basis to re-affirm PCI DSS compliance

Related Information:
Ethics Point
Georgia Tech Buzzcard Center
Payment Card Industry Data Security Standards (PCI DSS)

Policy History:

Revision Date	Author	Description
10-02-2018	Cyber Security	Simplified and aligned policy with current regulatory environment.

Cyber Security Policy

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jan 2017
Last Revised: Mar 2020
Review Date: Jan 2023
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
The Georgia Institute of Technology (Georgia Tech) Cyber Security Policy (CSP) provides the guiding principles for securing information technology (IT) resources at Georgia Tech.

Policy Statement:
Georgia Tech IT Resource users (IT Resource users include both students and employees) are responsible for protecting the security of all data and IT Resources to which they have access. This includes implementing appropriate security measures on personally owned devices which access Georgia Tech IT Resources. All users must follow the Security Procedures and Standards published by Georgia Tech Cyber Security including the Georgia Tech Protected Data Practices. In addition, users must to keep their accounts and passwords secure in compliance with the Institute Password Policy.

Georgia Tech employees may grant IT Resource guest access to third parties (e.g., visiting scholars). Any Georgia Tech employee who grants guest access to IT Resources is responsible for the actions of their guest users.

Research
Georgia Tech recognizes the value of research in the areas of computer and network security. During the course of their endeavors, researchers may have a need to work with malicious software and with systems that do not adhere to the security standards as prescribed by the Chief Information Security Officer. Researchers are responsible for their actions and must take all necessary precautions to ensure that their research will not affect other Georgia Tech IT Resources or users. In addition, researchers are responsible for making all appropriate notifications to those that may be affected by their research (see Responsible Disclosure Policy).

Network Management
The Office of Information Technology (OIT) is responsible for planning, implementing, and managing the Georgia Tech network, including wireless connections.

The following network appliances cannot be implemented at Georgia Tech without prior written approval by OIT or a Unit's IT lead:

- Routers
- Switches
- Hubs
- Wireless access points
- Voice over IP (VOIP) infrastructure devices
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Virtual Private Networking (VPN)
- Consumer grade network technologies
- Other networking appliances that may not be included in this list

Units or individuals who install any of the technologies listed above are responsible for capturing network traffic logs and storing them for a minimum of 365 days or an appropriate amount as negotiated with the OIT network team. Network traffic logs should include the following information:

- Source MAC address
- Source and destination IP address
- Physical interface (where applicable)
- Date and time
- User account where available (e.g. VPN logs)

System Administration
Every Institute owned IT Resource (including virtual resources such as virtual machines and cloud based services) must have a designated system administrator. The Institute expectation is that every Institute owned IT Resource will be professionally managed by the unit technical support team unless prevailing regulations dictate otherwise.

The system administrator is responsible for proper maintenance of the machine, even if the system administrator is not a member of the unit technical support team. This responsibility must be acknowledged and documented. In addition, the machine must be accessible to the unit technical support team for incident management purposes unless legal restrictions will not allow such access.

Negligent management of an Institute owned IT Resource resulting in unauthorized user access or a data breach may result in the loss of system administration privileges.

System administration responsibilities for all Institute owned IT Resources, including those that are self-administered include the following found here: System Administration Responsibilities.

Scope:
All Georgia Tech IT resource users and all Georgia Tech IT resources are covered by this policy.

Policy Terms:
Endpoint - Laptop computers, desktop computers, workstations, group access workstations, USB drives, personal network attached storage.

Georgia Tech IT Resources – Georgia Tech owned Computers, Networks, Devices, Storage, Applications, or other IT equipment. “Georgia Tech owned” is defined as equipment purchased with either Institute funding (including sources such as Foundation funds etc.) or Sponsored Research funding (unless otherwise specified in the research agreement).

Procedures:
Reporting an Incident
If a Georgia Tech IT Resource user suspects that a security incident has occurred or will occur, they should report the suspicion immediately to the system administrator or unit technical lead. Users may also report the suspected security incident directly to the Georgia Tech Cyber Security team at https://security.gatech.edu/report-incident.

System administrators and unit technical leads who have identified any of the following security events should report the suspected security event to the Georgia Tech Cyber Security team:

- Any occurrence of a compromised user account
- Any breach or exposure of Category 3 sensitive data (see Data Access Policy)
- Any occurrence of a server infected with malware
- Three or more simultaneous occurrences of endpoints infected with malware

- Any other instance of malware or suspected intrusion that seems abnormal

Responsibilities:
Chief Information Security Officer
The Chief Information Security Officer is responsible for creating and maintaining a cyber security program and leading the Georgia Tech Cyber Security team. The purpose of the cybersecurity program is to maintain the confidentiality, integrity, and availability of Institute IT Resources and Institute data. In addition, the Chief Information Security Officer, or a designee, is responsible for leading the investigation of and response to cyber security incidents. The response to any incident will be developed in collaboration with the data steward, Institute Communications, Legal Affairs, and other campus offices as appropriate.

Enforcement:
Violations of this policy may result in loss of Georgia Tech system and network usage privileges, and/or disciplinary action, up to and including termination or expulsion as outlined in applicable Georgia Tech policies.

To report suspected instances of ethical violations, please visit Georgia Tech's Ethics Hotline a secure and confidential reporting system, at: https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=7508

Related Information:
Georgia Tech Acceptable Use Policy
Georgia Tech Data Privacy Policy
Georgia Tech Password Policy
Georgia Tech Policy Exceptions
Georgia Tech Responsible Disclosure Policy
Georgia Tech Security Procedures and Standards
Georgia Tech Approved Endpoint Software
Georgia Tech System Administration Responsibilities
Georgia Tech Protected Data Practices

Policy History:

Revision Date	Author	Description
January 27, 2017	OIT	New Policy
January 23, 2018	OIT	Minor clarifications about end point agents
March 6, 2020	OIT	Updated to include Secure Data Practices
April 22, 2020	OIT	Minor edit regarding hyperlink and terminology

Data Access

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Nov 2005
Last Revised: Jul 2015
Review Date: Mar 2020
Policy Owner: OIT-Information Security
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
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 to obtain necessary data access for conducting Georgia Tech operations (including administration, research, and instruction), 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 the Data Categories section of this document. Insofar as this policy deals with access to Georgia Tech computing and network resources, all relevant provisions in the Acceptable Use Policy, the Cyber Security Policy, and the Data Privacy Policy. and Unit-Level Network Usage Policies 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.

Policy Statement:
The Chief Data Stewards have defined the following guiding principles governing access to Institute Data by any individual 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.

  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.* 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).

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 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.

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.

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.

Scope:
All employees, students, affiliates, contractors, consultants, vendors, or other consumers or users of Georgia Institute of Technology data, 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.

Policy Terms:
Cloud Computing/Cloud Services
A network of remote servers or services, hosted by third parties, used to store, manage, and process data. Examples of cloud computing services include Gmail, Hotmail, Yahoo Mail, DropBox, Rackspace, etc.

Data
All information generated or owned by Georgia Tech. Also, information not generated by Georgia Tech, but which Georgia Tech has the duty to manage. This information can exist in any form including, but not limited to, print and electronic.

Data Steward

Faculty or staff member who has been assigned as the person directly responsible for the care and management of a certain type of data at Georgia Tech. Data Stewards are ultimately responsible for access to the data they manage. For example, the Registrar is responsible for approving access to student data.

Endpoint
Desktop computers, laptop computers, workstations, group access workstations, USB drives, small servers, cloud hosted virtual machines, and personal Network Attached Storage (NAS)

Mobile Device

Mobile devices at Georgia Tech include, but are not limited to:

- Cellular telephones
- Smart phones (e.g. iPhones, Android Phones, BlackBerrys)
- Tablet computers (e.g. iPad, Kindle, Kindle Fire, Android Tablets)
- Wearable Devices (e.g. Google Glass, watch devices)
- Personal Digital Assistants
- Any other mobile device containing Georgia Tech data (e.g handheld scanning devices)

Laptops and USB drives are considered Endpoints for the purpose of this policy (see definition above).

Server
Any computer system that hosts a campus unit or institute wide service, or acts as an authoritative source of data for the institute or campus unit.

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.

Requesting Data Access
Detailed procedures and guidelines for requesting data access under this policy are contained in the Georgia Tech Data Access Procedures. These documents shall be updated on an “as needed” basis, reflecting any changes to the process and/or roles involved.

Protecting Sensitive Data
The internal computers, mobile devices, 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 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 the Data Categories section 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.

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: Refer to Data Protection Safeguards
- 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.

Sensitive Data as it pertains to Endpoints and Mobile Devices
When storing Georgia Tech data on Georgia Tech owned or personally owned endpoints (e.g. desktops, laptops, or workstations), mobile devices, and devices that are not used or configured to operate as servers, the device must be configured as described in the Data Protection Safeguards document. **Any deviation from mandatory requirements within the Data Protection Safeguards must be documented and covered by adequate compensating control(s).** The department of Internal Auditing is available to assist in reviewing compensating controls.

Sensitive Data as it pertains to Cloud Computing Services
When using cloud computing services or storage with Georgia Tech data, Data Users must follow procedures described in the Data Protection Safeguards. Regulatory requirements, such as International Traffic in Arms Regulations (ITAR) and U.S. Export Controls, must be considered when utilizing cloud computing services. Category IV data (credit card data) is not covered by this policy statement, refer to the institute Credit Card Processing Policy.

Sensitive Data as it pertains to Email Services
Data Users must use official Georgia Tech email services when emailing Institute data. Using third party email services (e.g. Gmail, Hotmail, Yahoo Mail) to send or store Institute data is prohibited.

Communication

Upon approval, this policy shall be published on the Georgia Tech Policy Library. 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

In addition, the Georgia Tech Office of Information Technology shall provide training and awareness. Avenues for training and awareness will include:

- New employee orientation
- New faculty orientation
- FASET
- Campus unit faculty/staff training and awareness sessions

Form Links:
Acceptable Use Policy
Data Privacy Policy
Cyber Security Policy
Data Protection Safeguards
Data Categorization
Enforcement:
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 for legitimate Institute business or authorized academic use 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 person affiliated with the Institute will be responsible for being familiar with the policy as it relates to him or her. Violations of the policy may result in loss of data access privileges, administrative sanctions (including termination or expulsion) as outlined in applicable Georgia Tech disciplinary procedures, as well as personal civil and/or criminal liability.

Policy History:

Revision Number	Author	Description
3.0	Jimmy Lummis	Major review and revision
2.9.1	Jimmy Lummis	Modified section 4.2.1 to include updated sensitive server reporting process
2.9	Richard Biever	Changed Data Classification references to Data Categorization and added section 3.3.

Data Privacy Policy

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jan 2017
Last Revised: Jan 2017
Review Date: Jan 2020
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
The Georgia Institute of Technology Data Privacy Policy provides the standards the Institute follows when accessing the files and communications of its students and employees. In the interest of promoting academic freedom and the mission of the Institute, the Georgia Institute of Technology (Georgia Tech) recognizes its obligation not to infringe upon the reasonable privacy expectations of its employees and students in their electronic communications and data.

Policy Statement:
Georgia Tech provides information technology resources to faculty members, staff and students for the purpose of furthering Georgia Tech's mission and conducting Georgia Tech business. While personal use of such systems is permitted, as per the Georgia Tech Acceptable Use policy, personal communications and files transmitted over or stored on Georgia Tech systems are subject to the same regulations as business communications.

Georgia Tech is committed to respecting the privacy expectations of its employees and students; however, consistent with this policy, electronic information that is transmitted over or stored in Georgia Tech systems and networks is subject to being audited, inspected and disclosed to fulfill administrative or legal obligations which may include, but are not limited to, the following:

- is necessary to comply with legal requirements or process (e.g., Georgia Open Records Act or subpoena);
- may yield information necessary for the investigation of a suspected violation of law or regulations, or of a suspected infraction of Georgia Tech or Board of Regents policy;
- is needed to maintain the security of Georgia Tech computing systems and networks;
- is needed for system administrators to diagnose and correct problems with system software or hardware;
- may yield information needed to deal with an emergency;
- is needed for the ordinary business of the Institute to proceed, (e.g., access to data associated with an employee who has been terminated/separated or is pending termination/separation, is deceased, is on extended sick leave, or is otherwise unavailable);
- is necessary to comply with a written request from the Vice President for Student Life on behalf of the parents, guardian, or personal representative of the estate of a deceased student; or
- is for research authorized by Georgia Tech under a data use agreement that precludes the disclosure of personally identifiable information.

Scope:
This policy governs access to the files and communications transmitted on or stored in Georgia Tech's IT Resources.

Any individual whose personal files and communications exist on a Georgia Tech IT Resource by virtue of unauthorized access will have no expectation of privacy.

Definitions
Information Technology Resources (IT Resources) – Computers, Networks, Devices, Storage, or other IT equipment

Procedures:

Application, System, and Network Login Banner

Where possible, all Georgia Tech applications and systems (excluding endpoints and mobile devices) must display the following login banner to all users prior to authentication of user credentials:

TERMS OF USE
This information technology resource is the property of the Georgia Institute of Technology and is available for authorized use only, in accordance with Institute IT policies (http://policylibrary.gatech.edu/information-technology). Any and all files on this system are subject to being audited, inspected and disclosed to authorized system administrators and/or law enforcement personnel to fulfill administrative and/or legal obligations. By using this system, I acknowledge these terms.

Requests for Access

All requests for access to information that is transmitted over or stored on Georgia Tech systems and networks should be directed to the Chief Information Officer or designee. The determination of whether access to information is necessary to fulfill administrative or legal obligations is made by the Chief Information Officer or designee, and may not be made at the departmental or unit level.

Business Continuity

Refer to Security Standards and Procedures for detailed procedures.

Deceased Students

Refer to Security Standards and Procedures for detailed procedures.

Emergency

Refer to Security Standards and Procedures for detailed procedures.

Legal Requirements

Refer to Security Standards and Procedures for detailed procedures.

Research

Refer to Security Standards and Procedures for detailed procedures.

System Integrity

Refer to Security Standards and Procedures for detailed procedures.

Violation of Law or Policy

Refer to Security Standards and Procedures for detailed procedures.

Enforcement:

Violations of the policy may result in loss of system, network, and data access privileges, administrative sanctions (up to and including termination or expulsion) as outlined in applicable Georgia Tech disciplinary procedures, as well as personal civil and/or criminal liability.

Related Information:

Acceptable Use
Cyber Security
Data Access Policy
Policy Exceptions Policy
Security Standards and Procedures

Policy History:

Revision Date	Author	Description
TBD	OIT	New Policy

Email Forwarding for Life

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jun 2006
Last Revised: Nov 2007
Review Date: Sep 2022
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Alana DeAngelis
Contact Title: IT Support Professional Manager Senior
Contact Email: alana.deangelis@oit.gatech.edu
Reason for Policy:
The Georgia Institute of Technology offers and encourages the use of electronic mail services in support of the academic, research, and public service mission of the Institute, and the administrative functions that support this mission. An extension of these services includes Email- for-Life (EMFL) for eligible members of the GT community once they separate from Georgia Tech (e.g., alumni and retirees). The service allows users to keep a single, OIT provided, Georgia Tech email alias in the “gatech.edu” domain, and the ability to forward email messages to a user-selected address. This policy addresses eligibility criteria and proper use of Email-for- Life services provided by Georgia Tech, while recognizing that the Terms of Use for the service may change periodically. As email aliases are an integral part of the EMFL service, the Email Alias Guidelines (See Related Documents) are applicable and included by reference in this document.

Policy Statement:
Email-for-Life service is intended for the private use of authorized, Institute-affiliated individuals.

Appropriate Use

EMFL users are encouraged to use these services in a manner consistent with all applicable laws and policies. Users are prohibited from using the service for commercial use, such as selling products. Any use, which disparages the image and reputation of Georgia Tech, is prohibited and will result in termination of user privileges.

Eligibility

The following groups are eligible for EMFL services:

Alumni – for purposes of this policy, an alumnus/a is defined as any student who successfully completed at least one Georgia Tech credit course, and who leaves Georgia Tech in good academic and disciplinary standing..

Retirees – faculty and staff who retire from Georgia Tech.

Ex Faculty / Staff Member – faculty and staff who leave Georgia Tech prior to retirement are eligible for EMFL privileges.

Affiliates – individuals not categorized above whom the affiliated Unit Head has approved for business reasons.

Non-Eligibility for Georgia Tech Employees

EMFL is a privilege offered to employees. As such, Georgia Tech reserves the right to deny or terminate EMFL to any employee in its sole discretion. This includes, but is not limited to, employees that are terminated with cause.

Review Process

Should an employee feel that they were denied EMFL wrongly, they may appeal the decision in writing to the Associate Vice President of the Office of Human Resources or his/her designee, who is the final authority in determining EMFL eligibility for former Georgia Tech employees.

Privacy

EMFL Users understand that they may periodically receive email communications from Georgia Tech and/or affiliated organizations. Georgia Tech will take reasonable steps to protect the privacy of EMFL users, including but not limited to, not making forwarding addresses available to any non-affiliated organization.

SPAM and Virus Filtering

To protect Institute computing assets, Georgia Tech may drop messages deemed to contain viruses, SPAM, or other messages that may cause damage to Institute systems. While every effort is made to protect all e-mail users from damaging messages, Georgia Tech is not responsible for damage caused by malicious content contained in messages forwarded through the EMFL program.

Administration & Termination of Service

EMFL users are expected to set up and manage their own email alias, their forwarding email address, and any necessary administrative procedures to manage their user profiles. In an effort to streamline the service, Georgia Tech will send annual renewal messages to all EMFL users. Users who do not respond to the second renewal requests will have their email alias and forwarding service inactivated. Georgia Tech reserves the right to cancel or modify the EMFL service with notice, should the need arise including, but not limited to changes in technology, service availability, or campus resource issues.

Scope:
This policy applies to all email services provided, owned, or funded in part by the Georgia Institute of Technology under the Email-for-Life program; and to all users of such services regardless of intended use. The EMFL program provides only an e-mail alias to be used for forwarding purposes. EMFL does not include a functioning mailbox or mail storage.

The Georgia Tech Email alias service does not guarantee access to other services that may or may not be provided by Georgia Tech.

Procedures:

The following guidelines apply to the usage of EMFL services as they do to the usage of Institute email services in general:

Email Alias Guidelines

Communication

Upon approval, this policy shall be published on the Georgia Tech IT Policy 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:

- Office of Human Resources (OHR)
- Alumni Office

Enforcement:
Any person who uses the Institute's Email-for-Life service consents to all of the provisions of this policy as well as the Acceptable Use Policy, Cyber Security Policy, and Data Privacy Policy and agrees to comply with all of its terms and conditions, and with all applicable state and federal laws and regulations. Violations of these policies or applicable state and federal laws and regulations may result in loss of usage privileges.

Georgia Tech reserves the right to make modifications to the EMFL policy as it deems necessary. Georgia Tech will use reasonable efforts to communicate changes to the EMFL policy to EMFL users in a timely manner. Changes to the EMFL policy apply to all EMFL users and EMFL users agree to comply with these changes.

Related Information:
Acceptable Use Policy
Cyber Security Policy
Data Privacy Policy
Related Documents: Email_Alias_Guidelines.pdf
Policy History:

Revision Number	Author	Description
1.2.1	Richard Biever	Review and Update of the EMFL policy.
1.2.2	Jimmy Lummis	Updated reference links

GLBA Information Security Program

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jun 2004
Last Revised: Nov 2009
Review Date: Sep 2020
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
This Information Security Plan ("Plan") describes safeguards implemented by Georgia Tech to protect covered data and information in compliance with the FTC's Safeguards Rule promulgated under the Gramm Leach Bliley Act (GLBA). These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information;

- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

This Information Security Program also identifies mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by Georgia Tech;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the program; and
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Policy Statement:
GLBA mandates that the Institute appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

Information Security Program Coordinator(s)

The Associate Vice President of Financial Services and the Associate Vice President / Associate Vice Provost for Information Technology (CIO) have been appointed as the coordinators of this Program at Georgia Tech. They are responsible for assessing the risks associated with unauthorized transfers of covered data and information, and implementing procedures to minimize those risks to the Institute. Internal Audit personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that all departments comply with the requirements of the security polices and practices delineated in this program.

Identification and Assessment of Risks to Customer Information

Georgia Tech recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, Georgia Tech Cyber Security will actively participate and monitor appropriate cybersecurity advisory groups for identification of risks.

Current safeguards implemented, monitored and maintained by Georgia Tech Cyber Security are reasonable, and in light of current risk assessments are sufficient to provide security and confidentiality to covered data and information

maintained by the Institute. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

Employee Management and Training

References and/or background checks (as appropriate, depending on position) of new employees working in areas that regularly work with covered data and information (e.g. Cashier,Äôs Office, Financial Aid) are checked/performed. During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student records, student financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts should help minimize risk and safeguard covered data and information.

Physical Security

Georgia Tech has addressed the physical security of covered data and information by limiting access to only those employees who have a legitimate business reason to handle such information. For example, financial aid applications, income and credit histories, accounts, balances and transactional information are available only to Georgia Tech employees with an appropriate business need for such information. Furthermore, each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

Information Systems

Access to covered data and information via Georgia Tech,Äôs computer information system is limited to those employees and faculty who have a legitimate business reason to access such information. The Institute has policies and procedures in place to complement the physical and technical (IT) safeguards in order to provide security to Georgia Tech,Äôs information systems. These policies and procedures, listed in Section 3 below, are available upon request from the Chief Information Security Officer.

Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). As such, Georgia Tech has discontinued the use of social security numbers as student identifiers in favor of the gtID# as a matter of policy. By necessity, student social security numbers will remain in the student information system; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

Management of System Failures

Georgia Tech Cyber Security has developed written plans and procedures to detect any actual or attempted attacks on Georgia Tech systems and has an Incident Response Plan which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This document is available upon request from the Chief Information Security Officer.

Oversight of Service Providers

GLBA requires the Institute to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program will ensure that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. The Security Program Coordinator(s) will identify service providers who have or will have access to covered data, and will work with the Office of Legal Affairs and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to

protect the security of covered data.

Continuing Evaluation and Adjustment

This Information Security Program will be subject to periodic review and adjustment, at least annually. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Information Security Program Coordinator(s), who will assign specific responsibility for technical (IT), logical, physical, and administrative safeguards implementation and administration as appropriate. The Information Security Program Coordinator(s), in consultation with the Office of Legal Affairs, will review the standards set forth in this program and recommend updates and revisions as necessary; it may be necessary to adjust the program to reflect changes in technology, the sensitivity of student/customer data, and/or internal or external threats to information security.

Policy Terms:
Covered data and information
for the purpose of this program includes student financial information (defined below) that is protected under the GLBA. In addition to this coverage, which is required under federal law, Georgia Tech chooses as a matter of policy to include in this definition any and all sensitive data, including credit card information and checking/banking account information received in the course of business by the Institute, whether or not such information is covered by GLBA. Covered data and information includes both paper and electronic records.

Pretext calling
occurs when an individual attempts to improperly obtain personal information of Georgia Tech customers so as to be able to commit identity theft. It is accomplished by contacting the Institute, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit (sometimes referred to as ‚Äúsocial engineering‚Äù), convincing an employee of the Institute to release customer-identifying information.

Student financial information
is that information that Georgia Tech has obtained from a student or customer in the process of offering a financial product or service, or such information provided to the Institute by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student‚Äôs parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

Procedures:

Related Policies, Standards and Guidelines

Georgia Tech has adopted comprehensive policies, standards, and guidelines relating to information security, which are incorporated by reference into this Information Security Program. They include:

Policies

Cyber Security Policy

Unit-Level Network Usage Policies

Data Access Policy (including Sensitive Data & Server Registration)

Credit Card Processing Policy

Standards

Data Protection Safeguards

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 program and upon any subsequent revisions or amendments made to the original document:

- Associate Vice Provosts
- Deans
- Associate Vice Presidents
- Chairs
- Department Heads
- Unit-level business officers
- Internal Auditing

Related Information:
Gramm-Leach-Bliley Act
FTC: Final Rule--Standards for Safeguarding Customer Information (16 CFR Part 314)
FTC: Final Rule--Privacy of Consumer Financial Information (16 CFR Part 313)
FTC Guidance: Financial Institutions and Customer Data--Complying with the Safeguards Rule
NACUA Cyber Security Resources Page
NACUBO GLB Act Resources Page

Identity Theft Prevention Policy

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Oct 2009
Last Revised: Apr 2013
Review Date: Apr 2020
Policy Owner: OIT-Information Security
Contact Name: Blake Penn
Contact Title: Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
The Georgia Institute of Technology (Georgia Tech• or the Institute•) developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's (FTC•) Red Flags Rule. The Red Flags Rule implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of the Institute's operations and account systems, and the nature and scope of the Institute's activities, the Institute determined that this Program was appropriate.

Policy Statement:
Requirements of the Red Flags Rule
Under the Red Flags Rule, the Institute is required to establish an Identity Theft Prevention Program.• The program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts. and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected in order to help prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the Institute from Identity Theft.

Oversight
Responsibility for developing, implementing, and updating this Program lies with an Identity Theft Committee (Committee•) for the Institute. The Committee is headed by the Chief Information Security Officer who is the Program Administrator. The Institute's Chief Information Officer, the Vice President for Legal Affairs and Risk Management, and such other individuals as may be appointed by the President of the Institute comprise the remainder of the committee membership. The Program Administrator is responsible for ensuring appropriate training of Institute staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program.

Staff Training and Reports
Institute staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the steps to be taken when a Red Flag is detected. Institute employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the Institute's failure to comply with this Program.

At least annually, or sooner if requested by the Program Administrator, Institute staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

Service Provider Arrangements
In the event the Institute engages a service provider to perform an activity in connection with one or more Covered Accounts, the Institute will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the Institute's Program and report any Red Flags to the Program Administrator or the Institute employee with primary oversight of the service provider relationship.

Non-disclosure of Specific Practices
For the effectiveness of the Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation, and prevention practices may need to be limited to the Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered confidential• and should not be shared with other Institute employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

Program Updates
The Committee will periodically review and update the Program to reflect changes in risks to students and the soundness of the Institute from Identity Theft. In doing so, the Committee will consider the Institute's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the Institute's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

Scope:
All employees, students, affiliates, contractors, consultants, vendors, or other consumers of Covered Accounts data, and all Institute data (electronic, paper or otherwise) that could be leveraged to conduct identity theft from Covered Accounts are covered by this policy.

Policy Terms:
Covered Accounts
All student accounts or loans that are administered by the Institute, including tuition payment plans, federal and school loans involving multiple payments, and campus payment cards.

Identifying Information
Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,• including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

Identity Theft
A fraud committed or attempted using the identifying information of another person without authority.

Program Administrator
The individual designated with primary responsibility for oversight of the Identity Theft Prevention Program.

Red Flag
A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.•

Responsibilities:

5.1. Program Administrator
This policy confirms the need for an Information Security organization, which is responsible for ensuring Institute compliance with this policy, and maintaining this policy as business processes, technology, and methods of identity protection improve. The Program Administrator monitors the activities of and works with the Data Stewards on the development and implementation of campus unit level Identity Theft Prevention Programs.

5.2. Identity Theft Committee
The Identity Theft Committee is responsible for confirming incidents of identity theft and determining the appropriate course of action when incidents occur. Additionally the committee is responsible for supporting the Program Administrator in ensuring the ongoing success of the Identity Theft Prevention Program.

5.3. Data Stewards
Data Stewards are responsible for developing and implementing Identity Theft Prevention within their purview. Data Stewards report to the Program Administrator on their activities in implementing unit level Identity Theft Programs.

Enforcement:
Individuals covered by the scope of this policy are expected to: a) respect the confidentiality and privacy of individuals whose records they access; b) observe any restrictions that apply to sensitive data; and c) abide by applicable laws, policies, procedures, and guidelines with respect to access, use, or disclosure of information.

Individuals who become aware of potential Identity Theft are expected to report such an incident per the procedures defined by the Identity Theft Prevention Program Administrator. The Program Administrator will report violations to the appropriate Faculty and/or Employment body. Violations of this policy may result in loss of usage privileges, administrative sanctions (including termination or expulsion) as outlined in applicable Georgia Tech disciplinary procedures, as well as personal civil and/or criminal liability.

Related Information:
Red Flags Rule
Data Access Policy
Acceptable Use Policy
Cyber Security Policy
Data Privacy Policy
Policy History:

Revision Date	Author	Description
XX-XX-XXXX	OIT-Information Security	New policy
04-2013	OIT-Information Security	Update to policy

Information Technology Accessibility Policy

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jan 2016
Last Revised: Jan 2016
Review Date: Jan 2019
Policy Owners:
Office of Compliance
Office of Information Technology
Contact Names:
J. Denise Johnson-Marshall, ADA Coordinator, dmarshall@gatech.edu
Lori Sundal, Deputy Chief Information Officer-Service Delivery, lori.sundal@oit.gatech.edu
Reason for Policy:
The Georgia Institute of Technology (“Institute”) is committed to providing equality of opportunity to persons with disabilities, including equal access to Institute programs, services and activities provided through Information Technology (IT). This policy establishes minimum standards and expectations regarding the design, acquisition or use of Information Technology.

Policy Statement:
The Institute commits to ensuring equal access to all Institute programs, services and activities provided through

Information Technology, whether provided directly by the Institute or by a vendor. As provided in Part VII, below, all Institute offices using vendor-provided Information Technology shall ensure that such IT complies with the Accessibility Standards contained in this policy. Unless an exemption applies, all schools, colleges, departments, offices and entities of the Institute shall adhere to the Institute's Accessibility Standards, as defined below.

Scope:
Incorporating principles of universal design in the development, acquisition, and implementation of IT and related resources helps the Institute ensure that these resources (documents, web pages, information, and services) are accessible to the broadest possible audience.

Individual web pages published by students, employees or non-Institute organizations that are hosted by the Institute and which do not conduct Institute-related business are encouraged to adopt the accessibility standards contained in this policy, but fall outside the jurisdiction of this policy.

Definitions:

Information Technology	"Information Technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources, including, but not limited to computers and ancillary equipment, instructional materials, software, videos, multimedia, telecommunications, or web-based content or products developed, procured, maintained, or used in carrying out Institute activities.
Institute Accessibility Standards	"Institute Accessibility Standards" means, at a minimum, the standards of the Web Content Accessibility Guidelines 2.0, Level AA, as created and published by the Web Accessibility Initiative of the World Wide Web Consortium, as well as the requirements of Sections 504 and 508 of the Rehabilitation Act of 1973 and their implementing regulations. "Institute Accessibility Standards" also means, more generally, those generally accepted principles of universal design which helps individuals with disabilities access the services, programs, and academic, extracurricular and research offerings of the Institute.
Legacy Web Pages **Legacy Documents** **Legacy Multimedia**	"Legacy Web Pages," "Legacy Documents," and "Legacy Multimedia", mean web pages, electronic documents, and multimedia created before January 1, 2013.

Revised Web Page	"Revised Web Page" means any web page where a significant alteration or update is made to the visual design of the page or a major revision of the content of the page is made.
Universal Design	"Universal Design" means a concept or philosophy for designing and delivering products and services that are usable by people with the widest possible range of functional capabilities, which include products and services that are directly accessible (without requiring assistive technologies) and products and services that are interoperable with assistive technologies.

Applicability:

This policy applies to all IT resources that are acquired, developed, distributed, used, purchased or implemented by or for any Institute unit and used to provide Institute programs, services, or activities, including but not limited to:

1. Web Pages

a. All new web pages and Revised Web Pages, website templates, and website themes must comply with the Institute's Accessibility Standards.
b. All new and Revised Web Pages must indicate in plain text a method for users having trouble accessing the page to report that inaccessibility.
c. Legacy Pages determined by the publishing department or unit to be of the highest priority in providing Institute services online (core institutional information) shall comply with the Institute's Accessibility Standards.
d. Unless an exception applies and is appropriately documented, for any Legacy Web Page or any other web page that for any reason does not comply with the Institute's Accessibility Standards, the Institute will, upon request, convert or render the non-compliant web page so as to meet the Institute's Accessibility Standards or will provide to the requestor access to the web page's information in manner that is equally effective as the original page.

2. Electronic Documents

This policy and the Institute Accessibility Standards apply to all electronic documents.

3. Multimedia

This policy and the Institute Accessibility Standards apply to all multimedia.

Exemptions:

1. Legacy Web Pages, Legacy Documents, and Legacy Multimedia are not required to comply with Institute's Accessibility Standards unless

- specifically requested by an individual with a disability (though units are encouraged to identify and improve the accessibility of Legacy Pages even in the absence of specific requests),
- significant and substantial revisions to the web pages, documents, or multimedia are undertaken after the creation of the original, or
- the nature or function of the web page, document, or multimedia is determined by the creating department to be essential to the purpose of the department or program.

2. Undue burden and non-availability may qualify as an exemption from this policy when compliance is not technically possible, or is unreasonably burdensome in that it would require extraordinary measures due to the nature of the IT or would alter the purpose of a web page. The conclusion of undue burden or non-availability is an institutional decision to be made by the Institute's Office of Compliance Programs in consultation with the affected unit(s) and others with relevant perspective or expertise. Notwithstanding the foregoing, an individual in need of an accommodation to access the program, service or activity shall request the same of the Institute's ADA Coordinator or IT Accessibility Coordinator.

3. IT resources specific to a research or development process in which no member of the research or development team requires accessibility accommodations may be exempt. In such cases, the lead investigator must document that, upon inquiry, no member of the research or development team identified as requiring an accommodation.

Purchasing:

In order to ensure accessibility of IT products, Institute officials responsible for making decisions about which products to procure must consider accessibility as one of the criteria for acquisition. This is especially critical for enterprise-level systems or technologies that affect a large number of students, faculty, and/or staff. Considering accessibility in procurement involves the following steps:

1. Vendors must be asked to provide information about the accessibility of their products as required by the Institute's Computer Technology Request (CTR) process.
2. The information provided by vendors must be valid and measured using a method that is reliable and objective.
3. Those making procurement decisions must be able to objectively evaluate the accessibility of products and to scrutinize the information provided by vendors.

Assistance with ensuring that appropriate contractual language is included in all IT purchasing documents may be obtained through the Institute's Purchasing Office.

Compliance:

The Institute's ADA Coordinator is responsible for overseeing compliance with regard to state and federal laws and regulations that prohibit discrimination on the basis of disability and require reasonable accommodation. Questions or concerns regarding compliance with this policy, or complaints of discrimination, should be directed to the ADA Coordinator, who contact information is contained below.

Questions regarding the Institute's Accessibility Standards, resources, and other technical matters may be addressed to the Institute's IT Accessibility Coordinator, who contact information is below.

To report an accessibility issue or non-compliance with this policy, please email gtaccessibility@gatech.edu.

Enforcement:
To report suspected instances of noncompliance with this policy, please visit Georgia Tech's *EthicsPoint*, a secure and confidential reporting system, and read more about the EthicsPoint Portal.

Contacts

Institute ADA Coordinator:

Denise Johnson-Marshall

ADA Coordinator
dmarshall@gatech.edu
(404) 385-5151

IT Accessibility Coordinator:

Lori Sundal
Deputy CIO – IT Service Delivery
lori.sundal@oit.gatech.edu
(404) 894-5348

Assistance with IT Purchasing:

Purchasing Office
purchasing.ask@business.gatech.edu
(404) 894-5000

Related Information:
Accessibility Information
USG Accessibility Policy
Policy History:

Revision Date	Author	Description
1/15/2016	Compliance Programs and OIT	New Policy

Password Policy

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jul 2016
Last Revised: Jul 2016
Review Date: Jul 2022
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
This policy establishes the minimum requirements for generating and managing Georgia Tech user passwords, or other authentication factors, used by operating systems, applications, databases, and network devices owned by or managed by Georgia Tech. The intent of this policy is to protect access to Sensitive Data, and Georgia Tech systems and networks.

Policy Statement:
Single factor authentication (i.e. password authentication) or multifactor authentication (i.e. password and token) must be used to authenticate to any system or application which requires unique logon as defined by the Data Access Policy and Data Protection Safeguards Standard. The standards for single factor password authentication and multifactor

authentication are defined in the standards section below.

Georgia Tech account users must take all reasonable measures to protect their passwords and accounts. Georgia Tech users must never share their account passwords with anyone, including third party service providers (e.g. Google). Each user is accountable and responsible for any action taken with that user's account and password. If there is a business need to share access to an account, such sharing should be accomplished through system permission delegation.

Exceptions to the requirements of this policy may be requested per the Policy Exceptions policy.

Standards:
General Standards

- Georgia Tech user account passwords must never be transmitted over the network in a clear text format
- Passwords must be protected at all times, and measures must be taken to prevent disclosure to any unauthorized person or entity
- Passwords must be protected during distribution to the end user
- Temporary passwords must be changed within 24 hours of creation
- Default passwords for new servers, endpoints, and applications must be changed

Single Factor Password Configuration Standards
Single factor passwords must:

- Contain at least 11 characters
- Contain characters from at least three of the following four character classes:
    - Upper case alphabetic (e.g. A-Z)
    - Lower case alphabetic (e.g. a-z)
    - Numeric (e.g. 0-9)
    - Special characters (e.g. .,!@#$%~)
- Expire every 120 days (service accounts that are not used to login interactively do not expire)
- Be different from the last three passwords selected

Multifactor Password Configuration Standards
When logging into systems or applications that require multifactor authentication, the associated password must:

- Contain at least 8 characters
- Contain characters from at least three of the following four character classes:
    - Upper case alphabetic (e.g. A-Z)
    - Lower case alphabetic (e.g. a-z)
    - Numeric (e.g. 0-9)
    - Special characters (e.g. .,!@#$%~)
- Expire every 365 days
- Be different from the last three passwords selected

Mobile Device Pin/Password Configuration Standards
When using a mobile device, such as a smart phone or tablet, that requires authentication, the associated password/pin must:

- Contain at least 6 characters, or
- Leverage some other form of authentication such as
    - Biometrics (e.g. facial recognition or thumbprint)

- Pattern code
- Swipe code

Scope:
This Institute-wide policy applies to any endpoint, mobile device, or application which requires unique logon as defined by the Data Access Policy and Data Protection Safeguards Standard, as well as all users of those systems.

Policy Terms:
Endpoint - Desktop computers, laptop computers, workstations, group access workstations, USB drives, small servers, cloud hosted virtual machines, and personal Network Attached Storage (NAS)

Mobile Device - Mobile devices at Georgia Tech include, but are not limited to:

- Cellular telephones
- Smart phones (e.g. iPhones, Android Phones, BlackBerrys)
- Tablet computers (e.g. iPad, Kindle, Kindle Fire, Android Tablets)
- Wearable Devices (e.g. Google Glass, watch devices)
- Personal Digital Assistants
- Any other mobile device containing Georgia Tech data (e.g handheld scanning devices)

Multifactor Authentication – A process for securing access to a given system, such as a network or website, that identifies the party requesting access through several categories of credentials (e.g. password and soft token or password and thumbprint).

Server - Any computer system that hosts a campus unit or institute wide service, or acts as an authoritative source of data for the institute or campus unit.

Single Factor Authentication - A process for securing access to a given system, such as a network or website, that identifies the party requesting access through only one category of credentials (e.g. password).

Enforcement:
Violations of this policy may result in loss of Georgia Tech system and network usage privileges, disciplinary action, up to and including termination or expulsion as outlined in applicable Georgia Tech Employment policies and the Georgia Tech Student Code of Conduct, as well as personal civil and/or criminal liability.

Related Information:
Acceptable Use Policy
Data Access Policy
Cyber Security Policy
Data Privacy Policy
Responsible Disclosure Policy
Policy Exceptions Policy

Policy Exceptions

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Jul 2010
Last Revised: Jul 2010
Review Date: Sep 2020
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
Situations or scenarios will arise that cannot be effectively addressed within the constraints Georgia Tech's security policies and standards. There will be times when business processes can and should take precedence over these policies. However, we must still consider the security of Georgia Tech's infrastructure and data. The process allows unit heads and Institute leadership to make an informed decision on whether or not to request an exception to a particular IT policy by understanding the risk and alternatives involved.

(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)

Policy Statement:
Exception Process

- Any deviation from security policies and standards must be reviewed via the Information Security Exception Review process.
- The exception review process must involve qualified information security professionals.
- The exception review process must log all findings and results in a central repository that is accessible to all Georgia Tech staff involved in the assessment of the exception request.
- Approved exceptions must be periodically reviewed by OIT-IS, Internal Audit, and the Unit requesting the exception.
- Exemption requests involving potentially significant risk to the Unit may require approval of the Unit Head, CIO, EVP, or Provost.

Exception Criteria

- Exception requests must be evaluated in the context of potential risk to the Unit and Georgia Tech as a whole.
- Exception request evaluations must take into account what value the exception will bring to the Unit requesting the exception.
- Exception requests that create significant risks without compensating controls will not be approved.
- Exception requests must be consistently evaluated in accordance with Georgia Tech's risk acceptance practice.

Scope:
This Institute-wide process applies to all units and individuals requesting an exemption to Georgia Tech's security policies and standards.

Procedures:

If a Unit determines they cannot follow an Institute-level policy or standard, then the Unit should request an exception. Before doing so, the Unit should consider what risks they may face by not adhering to the policy as well as the benefit

gained by requesting the exception.

The Unit should fill out the Policy Exception Request form and submit it to OIT-Information Security (OIT-IS).

Once OIT-IS has the request, they will review the submission for completeness (ensure no information is missing) and follow up with the Unit as necessary.

OIT-IS will perform a risk assessment of the request, the proposed mitigation, and the benefit of allowing the exception.

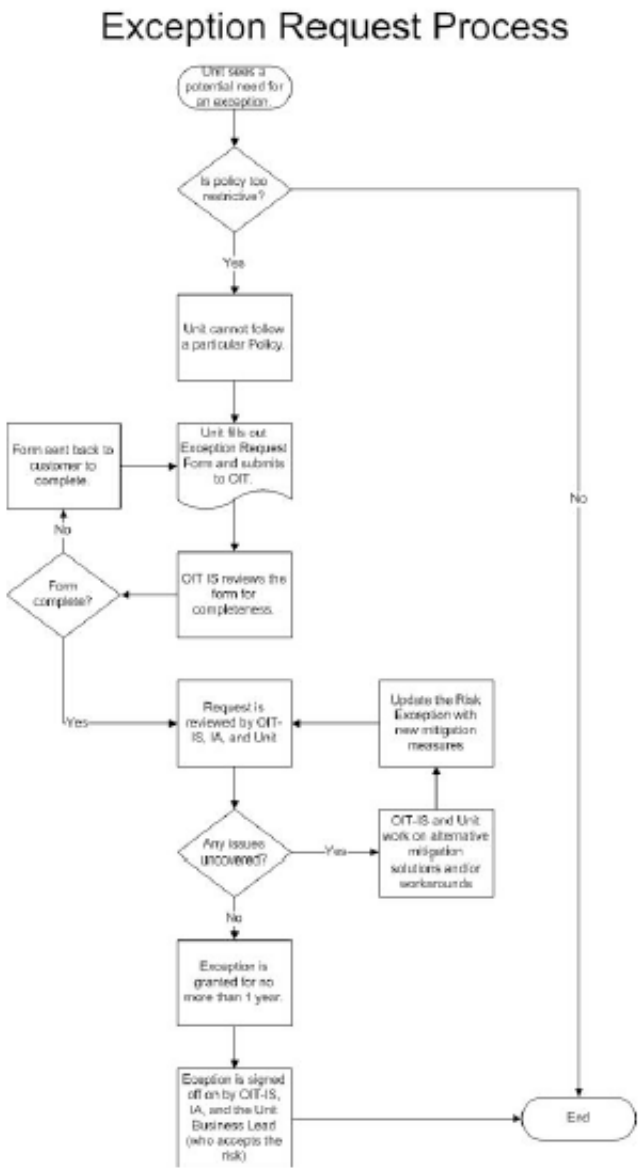
OIT-IS, Internal Audit, and the Unit will meet and review the risk assessment and the proposed mitigation measures. The purpose of the review is to examine the exception request, and discuss the potential risk and proposed mitigation by the Unit. If the exception poses a significant risk, OIT-IS will work with the Unit to understand the reason for the exception and propose reasonable alternatives to both mitigate the risk as well as provide the necessary functionality needed by the Unit.

If the review team finds the exemption could lead to significant risk to the Unit or the Institute, then they will inform the Unit Head (Dean, AVP), Director of Internal Audit, and the CIO.

Exemption requests involving potentially significant risk to the Unit may require approval of the Unit Head, CIO, EVP, or Provost.

Once the review of the exception has been completed and the exception approved, the exception will be signed off on by OIT-IS, IA, and the Unit Lead. In doing so, the Unit is accepting the potential risk caused by allowing the exception. An electronic copy of the exception will be maintained.

The exception will be granted for a period of no more than 1 year from the time the exception is granted. At the end of the year, the exception will be reviewed and either terminated or renewed for another period.



Communication

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

- Office Information Technology (OIT)
- Campus Deans and Chairs
- Unit Business/Administrative Leads
- Georgia Tech IT Directors
- ITAC
- Campus CSR’s
- Internal Audit

Form Links: Policy Exception Request
Frequently Asked Questions: LastPass FAQ
Responsibilities:
GT security policies and standards specify the minimum requirements that must be met throughout Georgia Tech's IT environment.

OIT-IS
Georgia Tech Cyber Security group is responsible for developing and maintaining this procedure.

Units
Georgia Tech Academic and Administrative Units, including OIT, are responsible for communicating this procedure to their users and submitting risk exception requests via the approved process.

Related Information:
Georgia Tech IT Policy Website
Acceptable Use Policy
Cyber Security Policy
Data Privacy Policy
Related Documents: Exception Request Process Flowchart.pdf
Policy History:

Revision Number	Author	Description
1.0	Richard Biever	Initial Draft
1.1	Richard Biever	Review/Changes from ITAC

Hidden Policy Images: Exception Request Process.png

Responsible Disclosure Policy

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Oct 2015
Last Revised: Oct 2018
Review Date: Oct 2022
Policy Owner: OIT-Information Security
Contact Name: Blake Penn
Contact Title: Information Security Policy and Compliance Manager
Contact Email: blake.penn@security.gatech.edu
Reason for Policy:
The Georgia Institute of Technology (Georgia Tech or the Institute) recognizes that security vulnerability research takes place on campus both through sponsored research, internally initiated research, and informal research. In addition, system users often find security vulnerabilities incidentally during the course of some other activity. Georgia Tech is fully committed to the identification and remediation of security vulnerabilities within Institute systems and networks. For these reasons the Institute developed this Responsible Disclosure policy to address the need for an ethical way to

identify and report security vulnerabilities within Georgia Tech systems and networks.

Policy Statement:
Any individual that is attempting to identify a security vulnerability within a Georgia Tech system or network must first obtain permission from the appropriate system owner prior to engaging in any testing or investigation. The reason system owners must be made aware in advance is to give the system owner an opportunity to prepare for any negative consequences of the security testing or investigation. The system owner may choose not to grant permission or may revoke permission at any time if such use interferes with owners use. The Georgia Tech CyberSecurity team is granted the right to perform vulnerability testing and investigation on Institute systems, networks, and users without obtaining explicit permission. Any system owner is granted the right perform vulnerability testing and investigation on their own systems without any outside permission. Once a security vulnerability has been identified within a Georgia Tech system or network, either through an approved investigation or incidentally, the person identifying the security vulnerability must disclose the security vulnerability to the Georgia Tech Cyber Security team as soon as possible, but no later than 48 hours from the time the investigator is aware of the vulnerability. System owners are not required to disclose vulnerabilities identified in their own systems to Georgia Tech Cyber Security. The identified security vulnerability may not be publicly disclosed before 180 days have elapsed from the time that the vulnerability was reported to Georgia Tech Cyber Security or until permission is received from Georgia Tech Cyber Security.

Scope:
All employees, students, affiliates, contractors, consultants, vendors, or other Georgia Tech system and network users are covered by this policy. Georgia Tech systems and networks specifically provisioned for information security research are exempt from this policy.

Policy Terms:
PGP
Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting e-mails.

Publicly Disclosed
Posting vulnerability information to a public website or forum, publishing the vulnerability information in a paper or article, or any other form of communication to individuals other than the appropriate Georgia Tech system owner, Georgia Tech Cyber Security, or the software vendor.

Security Vulnerability
A security vulnerability is a weakness in a system or network that could allow an attacker to compromise the integrity, availability, or confidentiality of that system or network.

Procedures:
Prior to attempting to identify security vulnerabilities within an Institute system:

- To identify the appropriate system owner, please first contact the Georgia Tech CyberSecurity team via email at ask@security.gatech.edu
- Obtain permission from the system owner. This step is not necessary if the system owner is attempting to identify security vulnerabilities in his or her own systems

If a vulnerability is identified inadvertently or incidentally:

- Proceed to the next section and follow the procedures on reporting the vulnerability to Georgia Tech CyberSecurity

When reporting a security vulnerability:

- Within 48 hours of discovering the security vulnerability, contact the Georgia Tech CyberSecurity team via encrypted email at vulnerability.reporting@gatech.edu using our PGP key (available on the public PGP servers and at https://security.gatech.edu/report-vulnerability).
- Include as much information as possible in your report, including a way for the system owner to reproduce the security vulnerability
- If you are unfamiliar with PGP and encrypting email, then please email us at vulnerability.reporting@gatech.edu and DO NOT include details of the security vulnerability
- Provide your contact information

Enforcement:
Violations of this policy may result in loss of Georgia Tech system and network usage privileges, disciplinary action, up to and including termination or expulsion as outlined in applicable Georgia Tech Employment policies and the Georgia Tech Student Code of Conduct, as well as personal civil and/or criminal liability. In addition, intentionally circumventing the security of a Georgia Tech system without permission is in violation of Georgia Tech's Cyber Security policies.

Related Information:
Data Access Policy
Acceptable Use Policy
Cyber Security Policy
Data Privacy Policy

Telecommunications

Broadband Connections for Faculty and Staff

Policy Book: Information Technology
Type of Policy: Administrative
Last Revised: Jan 2005
Review Date: Sep 2020
Policy Owner: Info Tech- Information Security
Contact Name: Cas D'Angelo
Contact Title: OIT Telecommunications Director
Contact Email: cas.dangelo@oit.gatech.edu
Policy Statement:
It is the responsibility of Georgia Tech and each of its budgetary units to implement procedures to effectively use communication services and equipment at the lowest possible cost. With the rapid growth in requirements for high speed broadband network access (e.g. DSL, cable-modem) for some Georgia Tech faculty and staff, and with the Georgia Tech philosophy of unit-based management, heads of budgetary units (Vice Presidents, Deans, School Chairs, Department Heads) or their designee are authorized to acquire broadband services for faculty and staff when required for institutional purposes.

The purpose of this policy is to outline the eligibility criteria, acceptable usage, and administration of Georgia Tech-funded broadband service granted to faculty and staff members. Insofar as this policy deals with access to Georgia Tech computing and network resources, all relevant provisions in the Acceptable Use Policy, the Cyber Security Policy, and the Data Privacy Policy are applicable and included by reference in this document.

Eligibility and Acceptable Use

Granting Institute-funded broadband service to faculty and staff members by individual units on campus, with the

express intent of conducting Institute business when it is demonstrated an employee cannot perform his/her duties without high speed (broadband service) access to the Internet and/or to the Georgia Tech network, or that improved performance and productivity ensuing from broadband service will justify the investment, shall be authorized under this policy. **Each department is to maintain approved justification documentation for each approval of broadband service.**

Examples of conditions under which broadband service may be granted to employees include:

- Broadband service is required to achieve business objectives by an employee who routinely or predominantly telecommutes.
- An employee cannot adequately meet communications needs with other available alternatives such as dial-up modems.
- Broadband service is required for on-call personnel required to respond to critical system failures or service disruptions.
- Broadband service is determined to be the most appropriate means of responding to campus emergencies.
- Broadband service is needed to facilitate program and business access to campus and Internet resources to remotely conduct Institute business.

Georgia Tech will cover the cost of a competitive broadband service plan used primarily for job-related activities. Employees who wish to add personally-owned computers to any such plan must do so at their own expense. Furthermore, all broadband service users are reminded that such privileges are covered by the Acceptable Use Policy, the Cyber Security Policy, and the Data Privacy Policy as well as any relevant Unit-Level Network Usage Policy.

Ordering and Payment Administration

Managers of employees qualifying for Institute-funded broadband service are to initially determine the business needs and select an appropriate package which meets these requirements. Both the business need and broadband service package selection should be reviewed periodically, at least annually.

The following ordering and payment options are allowed under this policy:

1. Departmental P-Card Departments may acquire broadband service via departmental P-cards, but they should note that special obligations go along with the convenience. Specifically, only designated Georgia Tech Procurement Officials may enter into contracts on Georgia Tech's behalf. This means Broadband service contracts obtained via P-card and signed by an employee are, in fact, personal obligations of the employee. Should the employee terminate while an agreement signed by the employee is still in force, it is the responsibility of the employee to fulfill the terms of the agreement. The department is to maintain the approved justification documentation for each broadband service obtained in this manner.
2. Georgia Tech Purchasing Georgia Tech Purchasing will process requests for Broadband service upon receipt of an approved purchase requisition. Purchasing will procure these services via standing agreements available to Georgia Tech. In special circumstances, Purchasing may utilize other agreements obtained from any carrier who best meets the needs of the Institute. Broadband service will be billed directly to the ordering department, based upon the information on the purchase order (FPO). Object code 773500 Cellular Services, will be used to account for Broadband service costs. Departments will review and verify Broadband service bills on a monthly basis and forward the approved invoice to Accounts Payable for payment. Invoices are to be submitted at least 10 days before due date to allow for payment processing and mail delivery. Invoices may be paid by Pcard. Effective May 1, 2003 the default account must be changed to 773500 utilizing the Georgia Tech Pcard reallocation tool.
3. Personal Contracts Heads of budgetary units may authorize employee reimbursement for business use of their personal broadband service contracts. Additionally, it may make economic and business sense to pay a differential price to boost an employee's current service package on their personal phone or cable

arrangement by an amount sufficient to cover the addition of authorized broadband service. If the unit head determines that this approach is in the best interest of the Institute, they should document the rationale for this decision, keep on file and review periodically (at least annually) to ensure that this is still the appropriate option.

Right to Monitor Communications and Right to Privacy

Georgia Tech reserves the right to investigate, retrieve and read any communication or data composed, transmitted or received through voice services, online connections and/or stored on its servers and/or property, without further notice to faculty and staff, to the maximum extent permissible by law. Express notice to faculty and staff stating that there is no right to privacy for any use of Institute telecommunications equipment and services, or funded by Institute resources, should be included in the approval form granting funding for broadband services.

Enforcement:
All approval and justification documents shall be kept by unit business officers, and shall be subject to periodic reviews by Georgia Tech Internal Audit and/or external audit agencies.

Long Distance Telephone Usage

Policy Book: Information Technology
Type of Policy: Administrative
Effective Date: Mar 2001
Last Revised: Jan 2005
Review Date: Sep 2020
Policy Owner: Info Tech- Information Security
Contact Name: Cas D'Angelo
Contact Title: OIT Telecommunications Director
Contact Email: cas.dangelo@oit.gatech.edu
Reason for Policy:
It is the policy of Georgia Tech that the use of Institute's long distance telephone services is limited to official Georgia Tech business. Further, State law precludes Georgia Tech employees from using State resources for personal gain or benefit. Personal use is prohibited.

Policy Statement:
The department head is responsible for the business and financial operations of the unit, including the development and implementation of appropriate operating procedures and internal controls. Long distance telephone charges are included in this area of responsibility. Unit personnel are responsible for the timely review of all long distance telephone charges appearing on monthly Department of Administrative Services (DOAS) bills. Inquiries related to questioned charges are to be directed to OIT Telecommunication Services. Charges identified as unofficial are to be reimbursed by the caller.

Violation of this policy may result in disciplinary action, up to and including termination.

Unofficial Calls

Long distance calls other than those on official Georgia Tech business are to be charged to home telephones or personal telephone calling cards. In rare instances where special circumstances are present and unofficial long distance calls, including GIST calls, are made on departmental telephones, the following steps are to be taken:

- The employee and the unit's business officer are to work together in identifying unofficial long distance calls;
- The unit's business officer will obtain reimbursement from the employee for the cost of all unofficial long distance calls;
- The unit's business officer will complete a Long Distance Call Reimbursement Deposit Form indicating the project to which an appropriate expense credit is to be applied, and make a timely deposit (check or cash) with the Bursar's Office in Lyman Hall;
- A copy of the annotated DOAS bill noting the unofficial long distance call(s) and cost, and any other supporting documentation is to be retained by the department.

If an employee has terminated employment with Georgia Tech, the department may have an invoice issued to the former employee through Accounting Services Accounts Receivable, or reimbursement may be withheld from the employee's final paycheck.

Right to Monitor Communications and Right to Privacy

Georgia Tech reserves the right to investigate, retrieve and read any communication or data composed, transmitted or received through voice services, online connections and/or stored on its servers and/or property, without further notice to faculty and staff, to the maximum extent permissible by law. Express notice to faculty and staff stating that there is no right to privacy for any use of Institute telecommunications equipment and services, or funded by Institute resources, should be included in the approval form granting funding for broadband services.

Forms: long_dist_reimburse_form.pdf
Form Links: Purchasing Form Bank-Long Distance Reimbursement Form

Wireless Communication Devices/Cellular Telephone Service

Policy No: 14.1
Policy Book: Information Technology
Type of Policy: Administrative
Last Revised: Jan 2005
Review Date: Sep 2020
Policy Owner: Info Tech- Information Security
Contact Name: Cas D'Angelo
Contact Title: OIT Telecommunications Director
Contact Email: cas.dangelo@oit.gatech.edu
Reason for Policy:
It is the responsibility of Georgia Tech and each of its budgetary units to implement procedures to effectively use communication services and equipment at the lowest possible cost. With the rapid growth in wireless communication devices (WCDs), and with the Georgia Tech philosophy of unit- based management, heads of budgetary units (Vice Presidents, Deans, School Chairs, Department Heads) or their designee are authorized to approve the acquisition of wireless communication devices and services. WCDs for purposes of this policy include, but are not limited to: cellular or PCS phones, blackberries, personal digital assistants with connectivity, two-way radios (traditional and trunked-technologies), and pagers. By contrast, cordless telephones, headsets and other devices not subject incremental usage charges are not included.

Policy Statement:
Guidelines for Acquisition and Use and Unit Responsibilities

An Institute assigned WCD/ cellular telephone and service may be an appropriate resource to conduct Institute business when it is demonstrated an employee cannot perform his or her duties without a WCD/cellular telephone or that improved performance ensuing from WCD/cellular telephone service will justify the investment. The individual units

or departments are responsible for:

- Specifying authorized and unauthorized uses of wireless or mobile devices
- Maintaining the approval justification for each WCD/Cellular phone device and service issued or approved.
- Documenting procedures for processing reimbursement for business use of personal WCD or cellular telephones.
- Maintaining an inventory of wireless devices in shared pools and individually-assigned, by type.

The inventory of WCDs maintained by each unit shall document, at the very least, each individual device type, the service provider for such device, and the assignee (individual user or most granular organizational unit in the case of shared/pool devices). Such inventory must be kept current by each unit or department, and made available for inspection by GIT Internal Audit or any authorized external agency upon request. Inventory reports shall be forwarded to Financial Services and/or the Office of Information Technology on a semi-annual basis, as directed.

Criteria for Determining Need

A department may acquire WCD/a cellular telephone service for an employee where communications needs cannot be met with other available alternatives such as a paging device, a radio, or standard telephone equipment. Examples of conditions under which a WCD/cellular telephone devices and service may be obtained if these criteria are met include the following:

- A WCD/cellular telephone is required to directly enhance an employee's job responsibility of protecting the physical safety of the general public.
- A WCD/ cellular telephone is required for an employee to respond better to environmental emergencies.
- A WCD/cellular telephone is required for additional protection for the employee in potentially hazardous working conditions.
- An employee cannot adequately meet communications needs with other available alternatives such as a paging device or a radio.
- A WCD/cellular telephone is required for on-call personnel required to respond to critical system failures or service disruptions
- A WCD/cellular telephone is determined to be the most appropriate means of responding to campus emergencies or to achieve business efficiencies.
- Cost savings realized when an employee combines or eliminates landline or services.

The unit head (or designee) of employees using Institute owned WCD/telephones is to initially determine the business needs and select an appropriate airtime package that meets these needs. Additionally, call activity is to be reviewed on a monthly basis to ensure that the appropriate airtime bundle (minutes per month) has been selected and that no additional charges were incurred due to personal calls. If a manager identifies any non-reimbursed personal calls, which have not been reported by the affected employee, the department will collect the cost of such call(s) from the employee and take any appropriate disciplinary action.

Personal Usage

WCD/Cellular phones assigned to Institute faculty or staff members are PRIMARILY for official business use. While incidental personal use is reasonable in order to prevent the employee from carrying two devices, this use should not result in additional charges to the Institute. If a personal emergency arises that requires the extended or extensive use of the WCD/cell phone to make personal calls, the faculty or staff member is to notify their department head or supervisor and reimburse the Institute for those calls that create additional charges. Reimbursement to Georgia Tech for any WCD/cellular call for personal use should be deposited with the Bursar's Office (Lyman Hall) by the department, along with a copy of the annotated bill noting the personal call and cost.

Ordering and Payment Administration

The following ordering and payment processing options shall be used for all WCDs/cellular phones issued for positions meeting the requisite criteria. The Central Purchasing Office will procure WCD/cellular telephone services via negotiated agreements available to Georgia Tech employees. In special circumstances, Purchasing may utilize other agreements obtained from any carrier who best meets the needs of the Institute.

a. Institute-Owned WCD/Cellular Telephones and Service For positions meeting the requisite criteria, departments should acquire WCD/cellular telephone services via departmental PCard, after completing any necessary forms provided by the service vendor representative to establish legitimate Georgia Tech service account(s). Only designated Georgia Tech Procurement officials may enter into contracts on behalf of Georgia Tech, and any actual contracts should be forwarded to Procurement for review and signature; any contracts signed by an unauthorized employee are in effect, personal obligations of the employee. When using the PCard for payment, the default expense code must be changed to 773500 utilizing the Georgia Tech PCard reallocation tool or cost transfer application. The Request for Wireless Communication Devices/Cellular Telephone Service form should be completed by the employee and approved by the Dean, Vice President, School Chair, Department Head or their designee and filed in the department.
b. Privately-Owned WCD/Cellular Telephones and Service
Heads of budgetary units may authorize employees to receive reimbursement for business-related calls made from privately-owned WCD/cellular telephones. Such reimbursements shall be for the cost of business-related calls only and shall not include any portion of the cost of WCD/cellular telephone equipment, installation or basic monthly service fees unless the WCD is used solely for official business. A completed Check Request Form (CRF) should be submitted to Accounts Payable including a copy of WCD/cellular telephone bill with the business related calls and charges highlighted. For calls over $10.00, the person or organization called and business purpose is to be noted.

   Additionally, it may make economic and business sense to pay a differential price to boost an employee's current airtime package on their personal phone by an amount sufficient to cover the addition of business calls. If the unit head determines that this approach is in the best interest of the Institute, they should document the rationale for this decision, keep on file, and review annually to ensure that this is still appropriate. The employee shall keep a copy of all monthly usage bills for the current review period, to assist with the annual review and service renewal process.

Right to Monitor Communications and Right to Privacy

Georgia Tech reserves the right to investigate, retrieve and read any communication or data composed, transmitted or received through voice services, online connections and/or stored on its servers and/or property, without further notice to employees, to the maximum extent permissible by law. Express notice to employees stating that there is no right to privacy for any use of Institute telecommunications equipment and services should be included in the assignment form granting access to Institute WCDs/cellular telephones and/or services.