Information Technology

Table Of Contents

Computer and Network Usage and Security

Type of Policy: Administrative
Effective Date: 2005-07-00T00:00:00
Last Revised: 2013-10-00T00:00:00
Review Date: 2017-02-00T00:00:00
Policy Owner: Info Tech- Information Security
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@oit.gatech.edu
Reason for Policy:
Georgia Tech's Computer and Network Usage and Security Policy (CNUSP) provides the guiding principles for use of Information Technology (IT) Resources at Georgia Tech. It is the policy of the Institute that its IT resources be used ethically and legally, in accord with applicable licenses and contracts, and according to their intended use in support of the Institute's mission. Faculty, staff, and students are expected to behave in an ethical[1] and professional manner when using IT Resources.

The CNUSP establishes the necessary balance between Georgia Tech's culture of openness, trust, and integrity and the appropriate level of security to protect resources. The principles established are:

1. The Institute is committed to protecting Georgia Tech users of IT resources and data.
2. The Institute is committed to protecting the Confidentiality, Integrity, and Availability of Georgia Tech IT resources and data.
3. Users of Georgia Tech IT resources and data will be good stewards of the resources to which they have access and will act in a responsible manner.
4. The Institute is bound by federal, state, and local laws as well as contractual and regulatory obligations to protect access to Georgia Tech IT resources and data.

[1]The University System of Georgia and Georgia Tech Ethics Policies may be found at:
www.usg.edu/audit/compliance/ethics/
www.president.gatech.edu/about-office/institute-ethics

Policy Statement:

The policy statements below apply to all Georgia Tech account holders and users of Georgia Tech IT (Information Technology) resources including but not limited to students, applicants, faculty, affiliates, staff and contractors

Copyright and Intellectual Property	
Copyrighted Material **Users of Georgia Tech IT resources must respect copyrights and trademarks.**	Copyrighted or Trademarked works including but not limited to computer programs, movies, television programs, music, photographs, and published material (e.g. books, journals) must not be copied, distributed, or shared without prior permission from the copyright or trademark holders. More information on copyright and Fair Use may be found at: www.library.gatech.edu/services/reserves/copyright.php
Intellectual Property **Users creating intellectual property using Georgia Tech IT resources should consult the appropriate resources for guidance.**	The following resources should be consulted regarding creation, ownership, and use of intellectual property: • Determination of Rights and Equities in Intellectual Property, Board of Regents Policy Manual, section 603.03, 2/2/94 and subsequent revisions at www.usg.edu/policymanual/section6/ • Related Georgia Tech intellectual property policies at: Georgia Tech Faculty Handbook

Copyright and Intellectual Property	
Export Control **Users traveling abroad or working with foreign nationals must be aware of export control rules and regulations.**	Consideration should be given to the export of ideas, technology, and documentation. The appropriate management should be consulted prior to export of any material that is in question. More information about export control may be found on Georgia Tech's Office of Research Integrity Assurance site at: www.export.gatech.edu/ .
Software Licensing **User must respect licenses to install and use software.**	The number of copies of software must be handled in such a way that the number of simultaneous users in a unit does not exceed the number of copies purchased by the unit. Users must also be aware that in some cases licenses for sofware does not allow for the software to be installed on home machines or on machines at other campuses or locations.

Integrity of Resources and Protection of Data	
Respect for Users **Members of the Georgia Tech community have the responsibility to respect the privacy of others.**	Users of Georgia Tech resources must not attempt to access data or systems they are not authorized to access and are expected to respect the integrity of Georgia Tech IT resources.
Data Confidentiality and Integrity **Users of Georgia Tech IT resources are responsible for upholding the confidentiality and integrity of data to which they have access.**	Users of Georgia Tech IT resources are responsible for upholding the confidentiality and integrity of data to which they have access. Users are prohibited from inspecting, copying, altering, distributing or destroying anyone else's files or network traffic, including but not limited to those related to Institute business, research, and teaching, without proper authorization. Proper authorization may be required not only from the person from whom the data originated, but also from Institute management or Institute data stewards. If there is a question, users are encouraged to check with their management before attempting to access the data without permission. Users who are authorized to access sensitive data (e.g. student data) are not authorized to distribute this data to other uses or grant other users access to the same data without permission from the Data Steward. Permission to access sensitive data may be obtained through Data Stewards per the Data Access Procedures.
Protection of IT Resources **Georgia Tech users are expected to respect the integrity of Georgia Tech IT resources to which they have access.**	This includes but is not limited to modifying sftware, systems, or networks that are not owned or managed by the user; accessing systems that you are not authorized to access; knowingly installing or running malicious or disruptive sftware. Authorized users have a responsibility to ensure the security and integrity of personally owned or managed systems, as well as *Institute Data* accessed through

Integrity of Resources and Protection of Data	
	such systems. Unit Technical Leads have the responsibility to authorize connections to the unit or departmental networks, excluding LAWN connections. Users may consult with their *Technical Leads* on security and system administration issues and responsibilities, although Technical Leads bear no responsibility for maintaining personally owned systems. Systems connecting to Georgia Tech resources must adhere to an appropriate set of security requirements, as documented in the Computer and Network Security Procedures. Georgia Tech recognizes the value of the research being done in the areas of computer and network security. During the course of their endeavors, researches may have a need to work with malicious sftware and with systems that do not adhere to the security standards described above. Researchers are responsible for their actions and research and must take all necessary precautions to ensure that their research will not affect other Georgia Tech systems, networks, or users.
Protection of Sensitive Data **In receiving access to privileged or sensitive data, authorized users accept responsibility to protect the information accessed and used on their computer.**	Authorized users may have access to privileged information that must be protected. Employees must take all necessary steps to prevent unauthorized access to this information. Users may obtain help in protecting their systems and data from their unit's IT staff or from OIT.
Protection of Research Data **Researchers are responsible for the safeguarding of data that is created during the course of research projects.**	Researchers should review contracts that are in effect for a research project and make sure that all IT security requirements are being met. In addition, researchers should make sure that research data is stored in a safe, secure manner so that it may be recovered in the event of a loss.
Remote Access to GT Protected Resources **Georgia Tech users should use a secure method to access protected Georgia Tech resources remotely.**	In the event that a user needs to connect to protected Georgia Tech resources (e.g. servers with sensitive or research data) using a remote access solution, several safe and secure options are available from Georgia Tech OIT and Unit IT departments. Additional information is available in the Georgia Tech Remote Access Policy and Standard. Administrators of Georgia Tech's enterprise systems should use the campus VPN service as a secure method to connect to these resources.

Unauthorized Access and Circumventing Security	
Protection of Accounts & Passwords **Authorized users are individually responsible for the security of their Georgia Tech accounts and passwords.**	Users are required to keep their accounts and passwords secure and must not share their Institute provided account or password information with anyone without the express written permission of his or her supervisor. Users that choose to do so accept the risk that the user account and password may be used to access resources other than the mail account.

Unauthorized Access and Circumventing Security	
	Shared accounts and passwords are typically not permitted, but in cases where they are needed (e.g. machine accounts or lab accounts); an exception may be documented using the Policy Exception Process outlined below. Georgia Tech employees will never ask users to provide their password information. Additional information on passwords may be found in the Georgia Tech Password Policy and Standard.
Permitting Unauthorized Access **Users may not access Georgia Tech IT resources, run software or hardware, or configure Georgia Tech hardware or software without appropriate authorization or permission.**	Georgia Tech users may not intentionally allow access to Georgia Tech resources by unauthorized users. Unauthorized access to GT resources is explicitly denied.
Circumventing Security **Users are required to respect security measures implemented on Georgia Tech systems, networks, and applications.**	Users are prohibited from attempting to circumvent or subvert these measures. This does not preclude the use of security tools by appropriately authorized personnel. Under no circumstances is a user of Georgia Tech IT resources and data authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Georgia Tech-owned resources.
Incident Reporting **Suspected security incidents should be reported to system administrators or unit technical leads immediately.**	If a Georgia Tech user suspects that a security incident has occurred on a system they have access to, they should report the suspicion immediately to the system administrator or unit technical lead.

Usage of IT Resources Users of Georgia Tech IT resources must respect the rights of other users. Resources use has the following responsibilities:	
Responsible Use of IT Resources **Users must ensure that Georgia Tech IT resources, including electronic communication, are used for scholarly or Georgia Tech business purposes only.**	Incidental personal use is permissible if the use meets the requirements set forth in the USG Ethics guidelines (http:// www.usg.edu/compliance/ethics/): “USG property shall not be used for personal gain or purposes except for incidental personal use of email, a telephone to make a local telephone call or incidental Internet use that is not inconsistent with applicable laws and policies. However, members of the USG community should note that such use must not interfere with the performance of official functions or that individual’s own job performance. Additionally, members of the USG community should understand that there is no expectation of privacy once any personal material is

Usage of IT Resources Users of Georgia Tech IT resources must respect the rights of other users. Resources use has the following responsibilities:	
	placed on a government system." ResNet and EastNet residents may use their assigned wired-network port connections for recreational purposes to the extent that such use does not violate other provisions of this policy or adversely affect network service performance for other users engaged in academic activities.
Limitations on Use of IT Resources	Such resources include electronic communication technologies like email and instant messaging and web browsers. Prohibited materials include fraudulent, harassing, obscene, threatening, or other messages or material that are in violation of applicable law or Institute policy. In general, Georgia Tech IT resources should not be used to transmit commercial or personal advertisements, solicitations, or promotions. Some mail lists or web sites have been set up for use of the Georgia Tech community to sell items and may be used for this purpose.

Management of IT Resources	
Network Management **The Office of Information Technology is responsible for planning, implementing, and managing the Georgia Tech network, including wireless connections.**	The following technologies 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 protection systems (IPS), and other networking technologies that may not be included here. The procedure for requesting implementation of new (wired or wireless) networking service to an area, or the expansion in coverage, is described in Section 2.2.4 of the Computer and Network Security Procedures. Network planning and administration responsibilities may be delegated to specific units through officially approved unit-level procedures, in keeping with administrative, research, or instructional requirements.
Network Devices **Units or individuals who install network devices that perform Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), or Virtual Private Networking (VPN) are responsible for tracking and identifying network traffic generated by the individuals using these services.**	Units or Individuals deploying such devices should consult with OIT before proceeding. Unless otherwise exempted, units or individuals who install such a device must retain logs, for a minimum of thirty (30) days, documenting whose use is represented by the traffic. For computers using NAT or DHCP, this information will include the MAC and IP information so that the IP can be traced back to a specific computer. For computers that

Management of IT Resources	
	access the network via a VPN, this information will include the source and the user. Should an incident (e.g. an event that is a violation of the CNUSP) arise, the Unit or Individual managing such a device will be responsible for providing information about the traffic and/or users behind the device involved in the incident. Failure to comply with the policies and procedures regarding use of such devices may result in loss of usage privileges or other administrative sanctions as referenced in this policy.
Information Retrieval Systems **With the permission of the appropriate unit head, units and individuals may configure computing systems to provide information retrieval services to the Georgia Tech community and/or public at large.**	All such services, including but not limited to, web servers, ftp servers, and other servers that present material to the community or the public must be in strict compliance with all applicable provisions in this policy as well as the Data Access Policy. In addition, users must be familiar with the risks associated with remote access to their computers.
Domain Names **Requests to establish new domain names must be forwarded to the Office of Information Technology for review and evaluation.**	Requests for names not ending in “gatech.edu” will undergo more scrutiny and must have the appropriate justifi•cations and level of appropriateness for approval. All such requests require the approval of the Vice President for Information Technology and Chief Information Officer.

Policy Exceptions	
Exception Requests **Users or Units may apply for policy exceptions when a legitimate scholarly or business need exists.**	Georgia Tech recognizes that there will be instances where a user or Unit may have a legitimate business or scholarly reason to not follow a policy or portion of a policy. In these cases, the user or Unit may apply for a Policy Exception for their particular need. The purpose of the process is to document those exceptions so that the Institute is aware of any potential areas of risk. The Exception Policy may be found at: Information Security Exception Policy Units may request exceptions via remedy tickets: http://www.remedy.gatech.edu/ (Select OIT IS: Policy Exception Records)

Scope:
This Institute-wide policy addresses proper use of all Georgia Tech IT resources and applies to all users of Georgia Tech resources. All business agreements and contracts must comply with this policy and the Georgia Tech Data Access Policy.

The CNUSP is the governing information technology policy for Georgia Tech. Other policies, standards, procedures, and safeguards documents may augment restrictions for the sake of security, but may not reduce the minimum requirements established in this policy.

Expectation of Privacy

Georgia Tech provides Users computing and network resources (together, "Computing Resources") for the purpose of conducting authorized Georgia Tech business. Computing Resources are to be used in a safe and efficient manner. Users have no expectation of privacy to any information created or stored on any Georgia Tech Computing Resource. Authorized Georgia Tech Officials have the right, at any time and in their sole discretion, to monitor, access, search and read any information stored on any Computing Resource. Any examination of a User's usage of Georgia Tech's Computing Resources will be conducted in accordance with Federal and state laws, as well as approved University System of Georgia and Georgia Tech policies and procedures. Users should use discretion and good judgment before using Georgia Tech Computing Resources for personal use, and should remember that any personal content will not be confidential.

Policy Terms:
Account Holders
Individual accounts are given to all authorized Georgia Tech users. These accounts identify users by a username or screen name. The accounts are used in conjunction with a password to authenticate users to various Georgia Tech services.

Authorized Georgia Tech Officials
Georgia Tech officials in management positions who are authorized by the Institute to make decisions regarding IT issues such as monitoring users and initiating an incident investigation that may involve Institute employees.

Bulk Email (spam)
Bulk email involves the sending of identical or nearly identical messages to numerous recipients.

Computing Resources
Computer and network devices that are provided to users for the conduct of Institute Business. This can include computers, laptops, desktops, network access, smart phones, PDA’s, printers, USB devices, and other machines purchased by the Institute.

Data Steward
Data Stewards are ultimately responsible for access to the data they manage. For example, the Registrar is responsible for approving access to student data.

DOS/DDOS
Stands for Denial of Service. This is a type of computer attack in which a computer system is made inaccessible to its intended user. Typically, a DOS attack involves one user and/or one computer. DDOS stands for Distributed Denial of Service. This is a DOS attack from many computers against one or a few computers.

Employee
An employee is any individual who works for Georgia Tech.

Electronic Communications
Electronics communication services at Georgia Tech include, but are not limited to:

- Telephone services
- Network services
- Email
- Instant Messaging and other “chat” programs

Information Technology Resources

Information Technology resources at Georgia Tech include, but are not limited to:

- Network services
- Lab computers
- Servers containing Georgia Tech data
- Application services (e.g. web, email, and database access)
- Computers, including laptops/desktops owned by Georgia Tech

Intellectual Property
Intellectual Property, or IP, are the legal rights over creations of mind, both artistic and commercial. Under IP law, owners are granted rights over intangible assets such as ideas, discoveries, inventions, etc. More information on IP protection at Georgia Tech may be found at: www.osp.gatech.edu/policies.

Keyboard Logging
The practice of covertly recording what keys are struck on a computer keyboard to ascertain information such as usernames and passwords.

Network Packet Capture
The act of capturing data packets crossing the network. This is often done with tools called network sniffers that record the data on a network, and store it for analysis.

Security Incident
An event that occurs due to a malicious act or intent to do harm to a computer system or network.

Sensitive Data
As defined by the Data Access Policy, sensitive data is information that is considered private and should be guarded from disclosure; disclosure of the information may contribute to financial fraud or violate state and/or federal law.

Student
Students are individuals enrolled in classes at Georgia Tech.

Procedures:

User Education	
Security Education Methods **User education is an important part of Georgia Tech's information security strategy. Responsibilities, policies and best practice topics must be communicated to all new employees.**	This may be accomplished through the following: • Unit training (e.g. orientation for new employees) • OIT Information Security training for new employees (at the request of Units) • Security classes through OOD: http://www.training.gatech.edu
Security Education Topics **Current security topics that should be covered include:**	• Computer and Network Usage and Security Policy (CNUSP) • Password policy and how to choose good passwords • Social engineering attacks, including phishing and web browser attacks • Insecurity of email • Information security resources on campus (e.g. OIT-IS website and policy website) • Physical security recommendations • Incident reporting

Responsibilities:
Unit Heads

Unit heads are responsible for technology planning, implementation, and maintenance. While speciï¬•c responsibilities and authorities noted below may be delegated, this overall responsibility cannot be delegated. Specific responsibilities include:

	Unit Head	OIT
Policy Communication and Education	Communicate new policies and/or standards to Unit faculty/staff. Facilitate regular awareness sessions (for example, during semi-annual staff meetings) or promote the OIT-IS provided training on new or revised policies and standards.	Provide training on security policies and standards. Communicate new policies and/or standards to the Units.
Information Technology and Security Support	Maintain an adequate technical support team including at least one non-student permanent employee as technical lead. Ensure that sufficient funding is provided to support the unit's IT infrastructure.	Provide centralized IT services to campus.
Policy Enforcement	Ensure information systems planning, implementations, and operations are in keeping with this policy and the Data Access Policy	Provide support in the way of education and awareness efforts and risk assessments to units.
Incident Response	Immediately report suspected instances of security or policy violations to OIT Information Security.	Manage IT incidents per http://www.oit.gatech.edu/service/incident-response/incident-response
Unit Self Assessments	Perform and approve an annual self-assessment conducted by the unit, with a semi-annual follow-up on identified risks using the supplied Georgia Tech tools	Provide self-assessment templates and training to units.

Enforcement:
Compliance

Any person who uses the Institute's information technology resources consents to all of the provisions of this policy and agrees to comply with all of its terms and conditions, and with all applicable state and federal laws and regulations. Users have a responsibility to use these resources in an effcient, effective, ethical, and lawful manner. Violations of the 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.

Policy History:

Revision Number	Author	Description
4.01	Richard Biever	Major revision draft.

Revision Date	Author	Description
10-2013	Policy Library	Policy update per Legal Affairs recommendations
09-2013	Policy Library	Corrected title for the Vice President for Information Technology and Chief Information Officer

Credit Card Processing

Type of Policy: Administrative
Effective Date: 2003-07-00T00:00:00
Last Revised: 2003-07-00T00:00:00
Review Date: 2016-09-00T00:00:00
Policy Owner: Info Tech- Information Security
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@oit.gatech.edu
Reason for Policy:
This policy provides requirements and guidance for all credit card processing activities for the Georgia Institute of Technology.

At this inital publication of this policy the following sources were consulted and provided the basis for this program: ISO 17799, Visa CISP, MasterCard SDP.

This policy deals with access to Georgia Tech computing and network resources. All relevant provisions in the Computing & Network Usage and Security Policy (CNUSP) are applicable and included by reference in this document. This policy pre-empts all other campus policies and procedures for ALL issues within the scope of this policy.

REVIEW Comment: This policy will be considered effective July 31 st , 2003 based on the provisional approval of the Associate Vice President of Financial Services and the Associate Vice President of the Office of Information Technology. Final approval of this policy will be by the President of the Georgia Institute of Technology based on a review by the Information Security Policy Committee.

Policy Statement:
The approval process for all credit card processing activities:

The Associate Vice President of Financial Services or delegate must approve all credit card processing activities at the Georgia Institute of Technology prior to entering into any 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, or swipe terminals).

All technology implementation associated with the credit card processing must be in accordance with the *Credit Card Processing Procedures* and approved by the Associate Vice President of Information Technology prior to entering into any contracts or purchasing equipment .

All credit card numbers must be handled in accordance with the *Data Access Policy* requirements for category 4 data. Please contact OIT Information Security for assistance with interpretation and implementation. However, instances of P-card numbers or corporate cards where 4 or fewer numbers are functionally present may be handled as category 3 data. Any conflicts between the requirements of the *Data Access Policy* and the *Credit Card Processing Procedures* will be resolved in favor of the *Credit Card Processing Procedures* .

Units approved for credit card processing activities must maintain the following standards:

Provide appropriate training to all employees handling systems with credit card numbers including both personnel within the unit handling the credit card transactions and appropriate personnel in the Office of Information Technology

Create, maintain and test annually business continuity/disaster recovery plans and system compromise response plans.

All outsourcing agreements must meet the standards set forth in the Credit Card Processing Procedures.

All servers storing or processing credit card numbers will be housed with the Office of Information Technology. All servers and POS Terminals will be administered in accordance with the requirements of the *Credit Card Processing Procedures*.

Credit card numbers will be retained for a maximum of 90 days. The only exception is transactions for future events, which may be retained up to 180 days from the transaction date. All media used for credit card numbers must be destroyed when retired from this use. All hardcopy must be shredded by at least a cross-cut shredder prior to disposal.

Access to credit card numbers must be restricted to the minimum number of people possible. No employee may have access to credit card numbers until he or she has attended the Credit Card Processing Policy Training and has tendered written acknowledgement of receipt of a copy of this policy, the *Credit Card Processing Procedures* and other appropriate policies (e.g., CNUP, Data Access Policy, Service Certification Process and Procedure, and unit level security policy). After completion of these requirements, the unit head may issue, in writing, authorization for the employee's access. No employee will have access to credit card numbers without such written authorization.

Each unit responsible for credit card processing must complete audits quarterly on all systems storing or processing credit card numbers to ensure compliance with this policy and the associated procedures. The Office of Information Technology will participate in these audits. Annual audits must be performed by Office of Information Technology Information Security to confirm the results of the quarterly audits.

All computers handling, processing, or storing credit card numbers must be registered in accordance with the revised Computer and Network Usage Policy.

Scope:
All academic units, administrative units, organizations, and employees of the Georgia Institute of Technology or that use systems or networks supported Georgia Institute of Technology must abide by this policy.

This policy specifically addresses all credit card processing by the Georgia Institute of Technology. All POS terminals handling credit card numbers (in full or truncated) and all servers receiving, storing, or transmitting credit card numbers (in full or truncated) are subject to this policy. An exemption is provided for P-card numbers provided the credit card number are functionally truncated to four digits or less.

Policy Terms:
Application Server
The computer hosting the application that the general end-user or the point-of-sale (POS) terminal connects

Category III Data ï¿½ Sensitive
This information is considered private and should be guarded from disclosure.However, public disclosure of this information due to a system compromise generally does not result in financial fraud or violation of State and/or Federal law. Examples include intellectual property information, private directory listings, and contract negotiations.

Category IV Data ï¿½ Highly Sensitive
Any disclosure of this information, intentional or otherwise, may contribute to financial fraud and/or violate State

and/or Federal law. Examples include Social Security numbers, credit card numbers, financial institution account numbers, and employee and student health records.

Cardholder Information Security Program (CISP)
The formal data protection program mandated by Visa

Card Verification Value 2 (CVV2)
An additional verification code used in transaction processing

Credit Card Number
Any part or all of the unique number identifying the account for a financial transaction

Database Servers
The computer storing the sales and/or credit card numbers>/p>

eCommerce Application
Any internet-enabled financial transaction application, whether a buying application or selling application

Employee
Any employee (as defined by the Employee Handbook) faculty, student employee, or contractor employed by a third party and providing services to the Georgia Institute of Technology

Encryption
Scrambling data in a recoverable format

Firewall
A network device or host-based software implementation designed to restrict network access to a computer

Hashing
Scrambling data in an unrecoverable but verifiable format

Intrusion Detection System (IDs)
A network monitoring device for recognition of attempts to compromise monitored systems

ISO 17799
The International Standards Organization document defining computer security standards. The credit card vendors may have based their policies on this standard.

POS Terminal
Point-of-Sale (POS) computer terminals either running as standalone systems or connecting to a server either at the Georgia Institute of Technology or remotely off site

Purchase Cards (P-Cards)
Credit cards obtained by Georgia Tech through a customer agreement with a bank for procurement purposes.

Site Data Protection Program (SDP)
The formal data protection program mandated by MasterCard

Swipe Terminal
POS credit card terminals

Two-factor Authentication
Authentication requiring two different methods confirming identity typically based on something the user has (e.g. a card, a key, a fingerprint) and something the user knows (e.g. a password)

Web Development
The design, development, implementation and management of the Ôø?front-endÔø? of the eCommerce application

Procedures:
Executive Summary

These procedures are required in direct support of the Georgia Institute of Technology Credit Card Processing Policy and were included in the original approval of the policy. This document sets forth the technical details and procedural requirements for implementing credit card processing at the Georgia Institute of Technology or outsourcing that processing to a third party. The procedures' scope, revisions, exceptions, and compliance are noted in the Credit Card Processing Policy.

Enforcement:
Failure to comply with this policy and the associated required procedures by employees will be deemed a violation of Institute policy and subject to personnel action up to and including termination as noted in the Employee Handbook and/or the Faculty Handbook. Technology that does not comply with this policy and the associated required procedures is subject to disconnection of network services or confiscation of equipment pending review and approval of processes, procedures, and/or equipment.

DRAFT: Acceptable Use Policy

Type of Policy: Administrative
Last Revised: 2016-03-00T00:00:00
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@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 legally, 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 both the acceptable and unacceptable 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
With the exception of incidental personal use, as defined below, Georgia Tech IT resources must be used 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 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 considered unacceptable as defined in the Unacceptable Use section below.

Students may use the ResNet, EastNet, and LAWN networks for recreational and personal purposes to the extent

that such use is not considered 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
The following actions are prohibited when using Georgia Tech IT resources:

- Activity that violates federal, state, or local law
- Activity that violates Institute policy
- Illegally harassing, defaming, or threatening others
- 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
- Copyright Infringement (per Title 17 of the United States Code)
- Violation of software license agreements
- Violation of patent protections and authorizations
- Violation of protections on proprietary information
- Violation of the privacy of other users
- Committing academic dishonesty
- Sending spoofed communications

In addition, Georgia Tech 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

This list should not be considered complete or exhaustive. It should serve as a set of examples of prohibited actions. If you are in doubt about the appropriateness of something you wish to do with Georgia Tech IT resources, contact the policy owner listed above 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).

Spoofed communications – Any form of electronic message (e.g. email) where the sender has forged their identity to make the message appear to come from a different user

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.

DRAFT: Cyber Security Policy

Type of Policy: Administrative
Last Revised: 2016-03-00T00:00:00
Review Date: 2019-03-00T00:00:00
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@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:
The Institute is committed to protecting Georgia Tech IT resources as well as the personal and Institute owned data residing on those IT resources; however the Institute cannot guarantee the security of data, networks, or systems.

Protecting the confidentiality, integrity, and availability of Institute IT resources requires the attention and participation of all users as well as the Georgia Tech CyberSecurity team.

Chief Information Security Officer

The Chief Information Security Officer is responsible for creating and maintaining a cyber security program and leading the Georgia Tech CyberSecurity team. The purpose of the cyber security 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 cyber incident response investigations. The Chief Information Security Officer, or a designee, is also responsible for providing digital forensic analysis capabilities in support of internal investigations being led by Georgia Tech Internal Audit or Georgia Tech Legal Affairs, and criminal investigations being led by the Georgia Tech Police Department.

Users

Georgia Tech IT resource users are responsible for protecting the security of all data and IT resources to which they have access. In addition, users are required to keep their accounts and passwords secure and must not share their Institute provided account or password information with anyone.

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.

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. By default, a member of a unit's technical support team is considered to be the designated system administrator. Unless prevailing regulations or circumstances dictate otherwise, a unit's technical support team must be the primary administrators for Georgia Tech IT resources.

If the administrator is not a member of the unit technical support team (i.e. self-administration or co-administration), he or she must sign a document (physical or electronic) accepting administrative privileges and responsibilities (see sample). All exception cases must be filed with the unit's technical lead.

Systems that are self-administered must still be accessible by unit technical support for incident management purposes unless legal restrictions will not allow such access.

Negligent management of an Institute IT resource resulting in unauthorized user access or a data breach may result in the loss of self-administration or co-administration privileges.

System administration responsibilities include the following:

- Full compliance with all applicable Institute IT policies and procedures
- Regularly updating the operating system and other applications installed on the system
- Perform an annual cyber security self-assessment for the set of IT resources administered
- Where possible, use central Georgia Tech IT services for system login and account management (e.g. Active Directory)

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:
Incident Reporting

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 CyberSecurity team by sending an email to cyber@security.gatech.edu.

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 CyberSecurity 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

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 may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site(s) and/or law enforcement personnel in order to meet administrative and/or legal obligations.

By using this system, I acknowledge and consent to these terms.

Georgia Institute Of Technology Domain Names

Official business use of domain names not ending in “gatech.edu” must be forwarded to the Vice President for Information Technology and Chief Information Officer, as well as the Vice President for Communications and Marketing, for approval.

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.

DRAFT: Data Privacy Policy

Type of Policy: Administrative
Last Revised: 2016-07-00T00:00:00
Review Date: 2019-07-00T00:00:00
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@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, Georgia Tech may at times need to access, review and release electronic information that is transmitted over or stored in Georgia Tech systems and networks.

Georgia Tech may access, without consent, information that is transmitted over or stored on its systems and networks when there is a reasonable basis to believe that such action:

- 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 serious infraction of Georgia Tech policy (e.g. alleged misconduct, plagiarism, financial fraud, or harassment);
- 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, which can include access to data associated with an employee that 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.

Any necessary access shall be minimized to the greatest extent possible in scope, quantity, duration, and frequency.

Georgia Tech will not attempt to access any individual's personally owned information technology resources without prior consent.

Scope:
This policy governs Georgia Tech's 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 information technology resource by virtue of unauthorized access will have no expectation of privacy.

Policy Terms:
Information Technology Resources (IT Resources) – Computers, Networks, Devices, Storage, or other IT equipment

Procedures:
Approval

Prior to Georgia Tech accessing, without consent, the content of electronic communications or other electronic records generated, stored, or maintained by Georgia Tech system users, procedures for access must be approved by the Vice President for Information Technology and Chief Information Officer or their designee and also approved by:

- the Executive Vice President who oversees the employee's home department, for all employees (including academic faculty, research faculty, and classified employees); or
- the Associate Vice President for Human Resources, or their designee, for non-faculty employees; or
- the Dean of Students, or their designee, for students; or
- the Office of Legal Affairs for purposes of complying with legal process and requirements.

Where an individual may have multiple affiliations to Georgia Tech (e.g. Student employees), access to data must be authorized based on the affiliation of the data being requested. If the appropriate approval path cannot be determined, authorization should be based on the primary affiliation.

Notification

When reasonable and legally authorized, notice of access will be provided via email from an appropriate campus official to the person whose data was accessed. The notification should document the specific user data that was accessed as well as the date and time the data was accessed.

Separation of Personal and Business Files and Communications

Whereas Georgia Tech cannot provide an absolute guarantee as to the privacy of personal records, employees should take reasonable measures to safeguard against inadvertent access to these records.

Employees should mark as "private" or "personal" all personal records. Employees should maintain this information in an identifiable separate location (e.g. folder or file) from their business records.

Where appropriate, files and data marked as personal will not be accessed. If personal and business information are not clearly marked and separated, all files and data may be treated as information related to Institute business.

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.

Data Access

Type of Policy: Administrative
Effective Date: 2005-11-00T00:00:00
Last Revised: 2015-07-00T00:00:00
Review Date: 2018-03-00T00:00:00
Policy Owner: OIT-Information Security
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@oit.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 Computer & Network Usage and Security Policy (CNUSP) 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. Online forms for requesting data access can be found at: http://www.oit.gatech.edu/content/data-access-request-forms

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.

Email for Life

Type of Policy: Administrative
Effective Date: 2006-06-00T00:00:00
Last Revised: 2007-11-00T00:00:00
Review Date: 2016-09-00T00:00:00
Policy Owner: Info Tech- Information Security
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@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

Mass Email Distribution Guidelines

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 Georgia Tech Computer and Network Usage and Security Policy[4] 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.

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

Type of Policy: Administrative
Effective Date: 2004-06-00T00:00:00
Last Revised: 2009-11-00T00:00:00
Review Date: 2016-09-00T00:00:00
Policy Owner: Info Tech- Information Security
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@oit.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, the Information Security Office within OIT will actively participate and monitor appropriate advisory groups such as the EDUCAUSE Security Institute, the Internet2 Security Working Group, the SANS Top Twenty risks list, and the National Institute of Standards and Technology (NIST) Computer Security Resource Center for identification of risks.

Current safeguards implemented, monitored and maintained by the OIT Information Security Office 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 Director, OIT Information Security.

Social security numbers are considered protected information under both GLB 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

The Information Security Office within OIT 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 Director, OIT Information Security.

Oversight of Service Providers

GLB 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 GLB. 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

Georgia Tech Computer and Network Usage and Security Policy (CNUSP)

Unit-Level Network Usage Policies

OIT Information Security Policy

Data Access Policy (including Sensitive Data & Server Registration)

Social Security Number Policy

Credit Card Processing Policy

Retention, Archiving, and Destruction of Records

External Access to Institute Resources

Standards

Data Protection Safeguards

Secure Data Deletion Standard

Information Security Self-Assessments

Guidelines Credit

Card Processing Guidelines & Procedures

World Wide Web Publishing Guidelines

Mass Email Distribution Guidelines

General Security Measures

Wireless Access Point Implementation Guidelines

Disposition of Hard Drive Data

Identity Theft Prevention Policy

Type of Policy: Administrative
Effective Date: 2009-10-00T00:00:00
Last Revised: 2013-04-00T00:00:00
Review Date: 2019-04-00T00:00:00
Policy Owner: OIT-Information Security
Contact Name: Jimmy Lummis
Contact Title: Policy and Compliance Manager
Contact Email: jimmy.lummis@oit.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.

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.

Policy History:

Revision Date	Author	Description
XX-XX-XXXX	OIT-Information	New policy

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

Information Technology Accessibility Policy

Type of Policy: Administrative
Effective Date: 2016-01-00T00:00:00
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

Policy History:

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

Password Policy

Type of Policy: Administrative
Policy Owner: Georgia Tech CyberSecurity
Contact Name: Jimmy Lummis
Contact Title: Associate Directory of Cyber Security
Contact Email: jimmy.lummis@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 (365 days for non-interactive service accounts)
- 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 4 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.

Passwords

Type of Policy: Administrative
Effective Date: 2011-02-00T00:00:00
Last Revised: 2013-01-00T00:00:00
Review Date: 2017-01-00T00:00:00
Policy Owner: Info Tech- Information Security
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@oit.gatech.edu
Reason for Policy:
This document is in direct support of the Georgia Institute of Technology Computer and Network Usage and Security Policy (CNUSP). This policy establishes the minimum requirements for generating and managing Georgia Tech user passwords used by operating systems, applications, databases, and network devices owned by or managed by Georgia Tech. The use of passwords is an important security practice, as passwords are used to authenticate users and are the first line of defense for user accounts. The intent of this policy is to protect access to Sensitive Data. This policy was developed and reviewed by members of the Georgia Tech technical community, including OIT, the campus IT Directors, department CSR's (Computer Support Representatives), and the campus CSS (Computer Service Specialists) group.

Policy Statement:

Password Policies	
Protection of Passwords **Georgia Tech users must take all reasonable measures to**	Per the CNUSP, each user is accountable and responsible for any action taken with that user's account and

Password Policies		
	protect their passwords and accounts.	password.
	Password Complexity **Georgia Tech Users are required to use strong, complex passwords for user accounts on Georgia Tech systems.**	The stronger and more complex the password, the less likely it is to be “cracked” by an attacker.
	Password Expiration **Georgia Tech user passwords must be set to expire according to the requirements set forth in the Georgia Tech Password Standard.**	Changing passwords regularly helps to reduce the potential for a password being “cracked” by an attacker.
	Reuse of Passwords **Users must not reuse their last three passwords when choosing a new password.**	Users must not reuse their last three passwords when choosing a new password. Additionally, password history checking on password systems should be enabled to prevent the reuse of the last three passwords of the user.

Scope:
This Institute-wide policy applies to all accounts created on operating systems, applications, databases, network devices, and any other device that may require an account and password. BIOS passwords are excluded from this policy. If the computer, server, or network device being implemented cannot support password complexity, expiration, or reuse, then a policy exception request may be filed per the Information Security Exception Policy.

However, users are responsible for adhering to the Password Standards for creating a strong password. Services covered by this policy include:

- OIT-managed Kerberos
- OIT-•managed Georgia Tech Active Directory (GTAD)
- OIT-managed Georgia Tech Enterprise Directory (GTED)
- OIT or centrally-managed systems
- Unit-•managed systems
- Network equipment
- Enterprise databases
- Any system containing sensitive data

The Institute recognizes that in some cases, research devices or equipment will not be able to adhere to the provisions of this policy. In these cases, the Unit may file a blanket Policy Exception request for groups or classes of devices. In some cases, these devices, equipment, or computers may require additional safeguards such as separation from the Unit's production network.

Policy Terms:

Password Complexity
Passwords with multiple types of characters including upper and lower case letters, numbers, and special characters (e.g. %$#@!).

Password Expiration
The date/time at which a password is no longer valid. For example, Georgia Tech account passwords "expire" after 120 days, at which time a user must choose a new password.

Password Strength
The measurement of the effectiveness of a password. Password strength is based on the length, complexity, and randomness of the password.

Password Length
The password length parameter is a basic parameter the value of which affects password strength against brute force attack and so is a contributor to computer security.

Password Randomness
Random passwords consist of a string of symbols of specified length taken from some set of symbol using a random selection process where each symbol is equally likely to be selected.

Procedures:
The policy statements below apply to all Georgia Tech account holders and users of Georgia Tech IT (Information Technology) resources including but not limited to students, applicants, faculty, affiliates, staff and contractors.

Protection of Passwords
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.
Password repositories must assure protection and integrity of passwords.
Application passwords must be

Protection of Passwords
protected and changed regularly, in the same manner as user accounts or system passwords.
Passwords must be protected during distribution to the end user.
Temporary passwords must be changed immediately upon completion of the assigned task.
Default passwords for new network devices, printers, operating systems, applications, and databases must be changed.
Users must never share or divulge their password to anyone. Georgia Tech will never ask a user to disclose their password for any reason including, but not limited, to via email and telephone.
Users should be able to change their own passwords. Users should not use Georgia Tech passwords for personal logins to external sites.
Users should not use Georgia Tech passwords for personal logins to external sites.

Responsibilities:
GT security policies and standards specify the minimum requirements that must be met throughout Georgia Tech's IT environment.

Role	Responsibilities
OIT-IS	Georgia Tech's OIT Information Security (IS) group is responsible for developing and maintaining this policy as well as facilitating regular reviews of this policy.
OIT	Georgia Tech OIT has the authority to approve and recommend central password management solutions for campus. OIT is also responsible

Role	Responsibilities
	for setting the password mechanisms for the centrally managed campus services including but not limited to Kerberos, Prism, GTED, and GTAD.
Units	Georgia Tech Academic and Administrative Units are responsible for setting the password mechanisms on systems and devices that they maintain to conform to the Georgia Tech Password Policy and Standard. Where possible, Units should leverage the existing central password systems. Unit Heads are responsible for communicating the provisions of this policy to users of any system or application they administer.
Users	Are responsible for knowing and complying with this policy. Georgia Tech users (including students, faculty, staff, and student workers) are responsible for keeping their passwords safe

Role	Responsibilities
	and secure. This includes not sharing the password with other parties as well as not storing the password in an unsafe manner (e.g. writing it down on a piece of paper or storing it in an unencrypted computer file).

Enforcement:
Compliance

All Georgia Tech faculty and staff that manage systems or devices that have user accounts and passwords are expected to abide by the provisions in this policy. Likewise, all Georgia Tech users with an account of any type are expected to abide by the provisions. Failure to comply with the provisions of this policy may result in loss of usage privileges or other administrative sanctions as referenced by the CNUSP.

Policy History:

Revision Number	Author	Description
1.0	Richard Biever	Initial Draft
1.1	Richard Biever	Review/Changes from ITAC
1.2	Richard Biever	Initial Release
1.3	Jimmy Lummis	Updated Procedures

Policy Exceptions

Type of Policy: Administrative
Effective Date: 2010-07-00T00:00:00
Last Revised: 2010-07-00T00:00:00
Review Date: 2016-09-00T00:00:00
Policy Owner: Info Tech- Information Security
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@oit.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.

Therefore, a review process is provided to approve and document requests for exemptions to Georgia Tech's security policies, which may be found at www.oit.gatech.edu/service/information-security/security-policies-standards-and-procedures. 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.

Responsibilities:
GT security policies and standards specify the minimum requirements that must be met throughout Georgia Tech's IT environment.

OIT-IS
Georgia Tech's OIT Information Security (IS) 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.

Policy History:

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

Responsible Disclosure Policy

Type of Policy: Administrative
Effective Date: 2015-10-00T00:00:00
Review Date: 2018-10-00T00:00:00
Policy Owner: OIT-Information Security
Contact Name: Jimmy Lummis
Contact Title: Information Security Policy and Compliance Manager
Contact Email: jimmy.lummis@oit.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 anytime 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 CyberSecurity 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 CyberSecurity. The identified security vulnerability may not be publicly disclosed until the Institute has had the opportunity to remediate or mitigate the identified security vulnerability, or permission is received from Georgia Tech CyberSecurity.
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 cyber@oit.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 http://security.gatech.edu/vulnerability-reporting).
- 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 a violation of the following Computer and Network Usage and Security Policy, "Users are required to respect security measures implemented on Georgia Tech systems, networks, and applications".

Telecommunications

Broadband Connections for Faculty and Staff

Type of Policy: Administrative
Last Revised: 2005-01-00T00:00:00
Review Date: 2016-09-00T00:00:00
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 Computing and Network Usage Policy (CNUP) 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 Campus Computing and Network Usage Policy (CNUP) 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:

A. 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.
B. 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.
C. 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

Type of Policy: Administrative
Effective Date: 2001-03-00T00:00:00
Last Revised: 2005-01-00T00:00:00
Review Date: 2016-09-00T00:00:00
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.

Wireless Communication Devices/Cellular Telephone Service

Policy No: 14.1
Type of Policy: Administrative
Last Revised: 2005-01-00T00:00:00
Review Date: 2016-09-00T00:00:00
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.