Computer and Network Usage and Security

Type of Policy: Administrative
Effective Date: July 2005
Last Revised: October 2013
Review Date: February 2017
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
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 contidentiality 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 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**	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

method to access protected Georgia Tech resources remotely.	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. 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 prohibited from attempting to circumvent or subvert these measures. This does not preclude the use of security tools by appropriately authorized personnel.

Users are required to respect security measures implemented on Georgia Tech systems, networks, and applications.	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 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 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 justifications 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/intellectual.shtml.

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

Employee Account Terminations	
Employee Account Terminations **Each Unit must establish a procedure to revoke or revise access rights to Unit IT resources.**	Employee access rights (informational and physical should be reviewed following any significant shift in job responsibilities (e.g. transfer between operational areas within the unit, transfers outside the unit within GT, retirement, termination, or reclassification). Accounts should be disabled and/or deleted when employees leave the Unit.

System & Network Administration

Specific computer system and network implementation by unit technical leads. management processes are noted in this section for The technical lead and the technical support team hold system administration authority for their unit and the associated responsibilities.

	By default, a member of the unit technical support team is considered to be the designated system administrator. However, if the administrator is not a member of the unit technical support team, he or she must sign a document (physical or electronic) accepting the administrative privileges and responsibilities (see sample). All exception cases must be filed with the unit technical lead. System administration privileges include all of the following: • Physical access to the system at all times • Ownership of the controlling account for the computer (e.g. "root" or "Administrator")

Administrators **Every GT-owned networked device (e.g. server, workstation, laptop) must have a designated system administrator.**	Ownership of the controlling account for the computer (e.g., "root" or "Administrator") • Control over the assignment of access rights on the administered system and providing access to systems as noted by the data coordinator or data steward. • Authority to change the system configuration, reboot the system, and/or disconnect/connect the system to the GT network as needed • Authority to manage the system logs, security logs, user access logs, etc. • Installation or modification of system software or hardware System administration responsibilities include the following: • Full compliance with all applicable policies and procedures as well as the Data Protection Safeguards. • Updating the system and applications regularly with security patches • Running anti-malware software (e.g. antivirus) • Running a host-based firewall
System and Network Monitoring **OIT provides monitoring for malicious content on GT IT resources.**	As part of its enterprise services and network management responsibilities, OIT is responsible for providing scanning for malicious content (e.g. viruses, trojan horses, web pages crafted to compromise computers), scanning wasteful content (e.g. spam), and monitoring network performance in a manner appropriate to GT as a whole. OIT also provides centralized as well as on demand scanning for units.
Inspection of Files During System and Network Monitoring	In the event of unintentional discovery of unlawful content, federal and state laws compel system administrators and technical support to report situations that are against the law (e.g. child pornography). The Institute may specifically monitor the activity and accounts of individual users of the Institute's computing resources, including individual login sessions and communications, without notice. This monitoring includes all network-based traffic, wireless traffic, and GT systems' use (e.g. e-mail, voice over IP communications (VoIP), content on computers owned by GT, sponsors, and contracted entities). This monitoring may occur in the following instances: 1. The user has voluntarily made the files accessible to the public. 2. It reasonably appears necessary to do so to protect the integrity, security, or

A system administrator may access others' ï¬les for the maintenance of networks and computer and storage systems, such as to create backup copies of media.	2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Institute or to protect the Institute from liability. 3. There is reasonable cause to believe that the user has violated, or is violating, GIT information technology policies. 4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns. 5. Upon receipt of a legally served directive by appropriate law enforcement agencies. Any such individual monitoring other than that specified in point (1) above, required by law, or necessary to respond to bona fide emergency situations, must be authorized in advance by the Chief Legal Advisor and the Associate Vice President and Associate Vice Provost for Information Technology or their designee(s). In all such cases, the appropriate unit head will be informed as time and the situation allows. In all cases, all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.
Process for requesting new or extended network services **The Remedy "Request for Service" web form should be used whenever possible to log any request for new networking service, or to request extensions to existing service.**	The following information must be included in the request in order to route the request to the appropriate support group and expedite the request: • In the "Summary" field, enter "Networking – New Service Request" • In the "Detail of the Problem" field, enter the following information in free text: ◦ "On behalf of" (if logging the request on behalf of someone else), ◦ "School/Business Unit", ◦ "Building/Room/Area to be covered" (wired or wireless coverage), ◦ "Peak number of users anticipated", ◦ "Justification" (Research Applications, Other – please elaborate), and ◦ "Requested Start Date for Service."
Process for requesting network policy exceptions **The Remedy "Request for Service" web form should be used whenever possible as**	The following information must be included in the request: • In the "Summary" field, enter "Networking – Policy Exemption Request" • In the "Detail of the Problem" field, enter the following information in free text: ◦ On behalf of" (if logging the request on behalf of someone else), ◦ "School/Business Unit, Building/Area affected" (wired or wireless)

described in the previous section when requesting a network policy exemption.	~~School/Business Unit, Building/Area affected (wired or wireless);~~ ○ "Technical Point of Contact", and ○ "Justification" (Research Applications, Other – please elaborate).
Process for requesting security policy exceptions **The Exception Request Form should be used when requesting a security policy exception.**	The Exception Request Form may be found at: Exception Request Form The following information must be included in the request: • Unit Requesting Exception • Technical Lead information • Administrative Lead information • Policy exception is for • Why the exception is needed • Systems/networks/accounts the exception is for • Mitigating factors • Time Period of exception

Computer Lab Management

Computer labs are run both as a centralized resource and within specific units. Each computer lab must be administered in compliance with the following requirements.

Acceptable Use **Georgia Tech computer labs have established rules for users of lab resources to abide by.**	• Users must obey all posted rules (e.g. Food and tobacco products are not permitted in any computing lab at any time for any reason). • All use must be authenticated by ID and password or other means. • All use must be in compliance with the Computer & Network and Security Policy (CNUSP) and the Data Access Policy (DAP).
Software Installation and System Imaging	When appropriate (based on lab size), each lab should maintain a standardized image for easy restoration of systems in the event of a failure. Systems will be reformatted and reinstalled or

	re-imaged at the end of each semester.
Lab workstations should be conï¬gured to allow software installation only by the lab director/ manager.	Computers in labs could be erased and re-imaged multiple times during each semester. Therefore, lab users should have no expectation of data retention on individual systems between uses. Notice of this practice is clearly posted in each lab as a reminder to not save important files on local hard drives of any lab computer.

Policy Modifications

This policy may be changed by directive from the responsible university officer. The Computer & Network Security Policy and Procedures may be changed by directive from the Georgia Tech Associate Vice President and Associate Vice-Provost for Information Technology. Any changes to the policy or procedures must be promptly communicated to the individuals and offices noted in the Communication section.

Communication

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

- Associate Vice Provosts
- Deans
- Associate Vice Presidents
- Unit Heads
- Internal Auditing
- Office of Legal Affairs
- OIT Information Security
- Technical Leads

Frequently Asked Questions: CNUSP FAQ-Students
Frequently Asked Questions: CNUSP FAQ-Employess
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.

System Administrators/Tech Leads

The unit technical lead is the person delegated responsibility for information technology planning, implementation, and maintenance by the unit head. While the unit head retains ï¬nal responsibilities for all functions within their unit, the technical lead must have the appropriate skill set to meet the information technology planning, information technology budget planning, and information technology management required for the unit.

	Technical Lead	OIT
IT Evaluation	The technical lead must maintain familiarity with emerging technologies and how they may help and/or impact the unit's mission. The state of the technology (e.g. commercial viability, security, production quantities, and	Provide consulting on new

and Planning	costs) must be considered when evaluating any technology and planning the purchase and implementation of the technology.	technologies and purchases.
IT Maintenance	The technical lead is responsible for ensuring that appropriate maintenance occurs for all workstations, servers, and other information technology used within the unit. The maintenance must be in keeping with the Computer & Network Security Procedures and the Data Access Policy.	Provide centralized IT services, where possible, to help facilitate management and maintenance of Unit workstations and servers.
Security Planning and Implementation	The technical lead is also responsible for maintaining a holistic view of information security for the unit, and ensuring that implementation of a product or service does not compromise the security of the unit's IT infrastructure.	Provide consulting on products and services as well as assist the technical lead in scanning for potential vulnerabilities.
Application Development and Security	The technical lead (and staff) are responsible for evaluating custom- developed web applications for risk before putting them on a public or Internet facing server.	OIT is responsible for providing the tools and consulting to help units assess the potential risk to custom--developed web applications.

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.

Related Information:
Georgia Tech IT Policy Website
Georgia Tech Data Access Policy
Georgia Tech Password Policy
Local, state, and federal laws
Incident Response Guidelines

Georgia Tech Copyright Infringement Complaint Response Procedures
Georgia Tech Consulting Policy
Access by External Enties to Institute Information Technology Resources
Georgia Tech Internal Audit Internal Control Guide
OHR Policies and Procedures
Georgia Tech Academic Honor Code
Board of Regents Policy Manual
Policy Exceptions

Related Documents:

CNUSP_Review.pdf

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