Computer & Network Usage and Security Policy

Policy No. 05.GIT.160 Rev. 3.7

Effective Date: July 1, 2005
Last Revised: September 7, 2005

Status
☐ Draft
☐ Under Review
☑ Approved
☐ Obsolete

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

Responsible University Officer
Associate Vice President / Associate Vice Provost for Information Technology (CIO)

Responsible Coordinating Office
Office of Information Technology (OIT)

1. Executive Summary

The purpose of this policy is to outline *employee* and *student* behavior requirements for the protection of the GIT *information technology resources.* Specific policy requirements for information protection are detailed in the GIT Data Access Policy and its associated documents. Access to networks and computer systems owned or operated by Georgia Institute of Technology (GIT) is a privilege, not a right, and implies user responsibilities. Such access is subject to Institute policies, standards, and procedures; and federal, state, and local laws.

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

2. Scope

This Institute-wide policy addresses proper use of all GIT computing and network resources, including proper management of those resources. All business agreements and contracts must comply with this policy and the GIT Data Access Policy.

While this policy is written with careful consideration of other GIT, unit, and organization information technology policies, this policy is the governing information technology policy for GIT whenever a policy conflict occurs. 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. It is the intention of this policy to reduce policy complexity at GIT by eliminating the need for unit-level information security policies.

3. Statement of Policy

3.1. Student and Employee Responsibilities

The responsibilities below extend to every student and employee.

3.1.1. Privacy

In accordance with BOR policies regarding the use of State resources and notwithstanding the procedures implemented to protect the privacy of individuals, users should have no expectation of privacy when using GIT's computing resources.

3.1.2. Intellectual works and copyrights

Users creating intellectual works using GIT computers or networks, including but not limited to software, should consult Determination of Rights and Equities in Intellectual Property (refer to Board of Regents Policy Manual, section 603.03, 2/2/94 and any subsequent revisions at http://www.usg.edu/regents/policymanual/600.phtml and related GIT policies).

Users are prohibited from unlawfully installing, using, inspecting, copying, storing, or distributing copyright-protected material (e.g. computer programs, movies, television programs, music) on GIT owned systems or on the GIT network.

3.1.3. Data confidentiality and integrity

Users are responsible for upholding the confidentiality and integrity of data. Users are prohibited from inspecting, copying, altering, or destroying anyone else's files without proper authorization.

3.1.4. Responsible use of resources

Users must ensure that GIT computer systems and network resources are used for scholarly or business purposes only. Incidental personal use is permissible if the use meets the following standards:

- Does not create a security or legal risk for Georgia Tech
- Does not interfere with worker productivity
- Does not consume more than a trivial amount of resources that could otherwise be used for scholarly or business purposes
- Does not require the installation of any software or hardware unrelated to business or scholarly use.
- Does not constitute inappropriate behavior for a professional work environment.

ResNet and EastNet residents may use their assigned wired-network port connections for recreational purposes to the extent that such usage does not violate other provisions of this policy or adversely affect network service performance for other users engaged in academic activities.

Messaging and publication technologies (e.g. e-mail, *instant messaging*, *newsgroups*, daily journals, *blogs*) carry a common set of responsibilities, including appropriate content, distribution, and security. Messages should only be distributed to those requiring the information.

3.1.5. Networking implementation and management

The Office of Information Technology is responsible for planning, implementing, and managing the GIT network, including wireless connections. The following technologies cannot be implemented at GIT without prior written approval by OIT: routers, switches, hubs, wireless access points, and other networking technologies. 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.

3.1.6. Use of personally-owned systems

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. Any connection to the GT network, excluding LAWN connections, requires approval by the unit Technical Lead. 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.

3.1.7. Security responsibilities

3.1.7.1. Sharing of access

Authorized users are individually responsible and accountable for any use of their account and password. These passwords should not be shared under any circumstances.

3.1.7.2. Permitting unauthorized access

Authorized users may not run or otherwise configure software or hardware to intentionally allow access to any GIT information resources by unauthorized users.

3.1.7.3. Protection of information

Authorized users may have access to privileged information that must be protected. In receiving access to this information, authorized users accept responsibility to protect the information accessed and used on their computer.

3.1.7.4. Management of services

With the permission of the appropriate unit head, units and individuals may configure computing systems to provide information retrieval services to the GIT community and/or public at large. All such services must be in strict compliance with all applicable provisions in this policy as well as the Data Access Policy.

Users must be familiar with the risks associated with remote access to their computers.

Requests to establish new domain names within the GIT network domain will be forwarded to the Office of Information Technology. Requests for names not ending in “gatech.edu” will typically not be given favorable consideration. All such requests

require the approval of the Associate Vice President and Associate Vice Provost for Information Technology.

3.1.8. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures. This does not preclude the use of security tools by appropriately authorized personnel. While the following list provides examples of disallowed practices, it is not a comprehensive list and is intended to only provide examples:

- Password decrypting or cracking tools
- *Denial of service* (DoS) or *distributed denial of service* (DDoS)
- Harmful activities (e.g. *IP spoofing*, *port scanning*, disrupting services, damaging files, or intentional destruction of or damage to equipment, software, or data)
- Unauthorized access (e.g. using another's account, using a special purpose account, escalating their own privileges)
- Unauthorized monitoring (e.g. *keyboard logging*, *network packet capturing*)

3.1.9. Personal business

Computing facilities, services, and networks may not be used in connection with compensated outside work, or for the benefit of organizations not related to GIT, except in accordance with the Institute Consulting Policy and/or the Access by External Entities to Institute Information Technology Resources Policy:

- http://www.admin-fin.gatech.edu/human/discipline/050400.html
- http://www.oit.gatech.edu/information_security/policy/xaccess.html

3.2. Unit Head Responsibilities

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

3.2.1. Policy communications and education

Ensure policies, standards, procedures, and guidelines are provided to appropriate groups based on their function. To ensure that the information is properly disseminated, the unit head must sponsor an internal information technology awareness program which includes (at least):

- A training session for all appropriate employees for implementation of new or revised policies, standards, or procedures.
- Regular reminders to appropriate employees regarding their responsibilities associated with their use of GIT information technology resources.

3.2.2. Information technology and security support

Maintain an adequate technical support team including at least one non-student permanent employee as technical lead. This individual has the responsibility for information technology and security planning, implementation, and maintenance under the direction of the unit head.

Ensure that sufficient funding is provided to appropriately support their unit's information technology infrastructure with proper life-cycle management, technology planning, and personnel training.

3.2.3. Policy enforcement

Ensure information systems planning, implementations, and operations are in keeping with this policy and the Data Access Policy.

3.2.4. Incident response

Immediately report suspected instances of security or policy violations to OIT Information Security in the following situations:

- If the data involved is sensitive or highly sensitive
- If employee or student disciplinary action is anticipated
- If laws are suspected of being broken
- If incident involves multiple networked devices or campus units

Refer to GIT's Incident Reponses Procedures for detailed guidance (http://www.oit.gatech.edu/information_security/architecture/incident_response_procedures/).

3.2.5. Self assessment and risk management

Perform and approve an annual risk evaluation conducted by the unit, with a semi-annual follow-up on identified risks using the supplied GIT tools (http://www.risks.gatech.edu).

3.3. Unit Technical Lead Responsibilities

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 final 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.

Based on the unit's support needs, this position may also manage a group of support personnel for system maintenance.

3.3.1. Information technology evaluation and planning

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 costs) must be considered when evaluating any technology and planning the purchase and implementation of the technology.

3.3.2. Information technology 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 (or the officially approved unit-level information technology procedures) and the Data Access Policy.

3.3.3. Security planning and implementation

While security evaluation of specific products and technology is noted elsewhere, the technical lead is also responsible for maintaining a holistic view of information security for the unit, and ensuring that implementation of a secure product or infrastructure does not compromise the security of another portion of the unit's infrastructure.

3.3.4. Technical communications

Unit-level information technology selection and implementations can have Institute-level impacts. Further, economies of scale may be achieved through use of standards throughout GIT. For these reasons, the technical lead must communicate with peers throughout GIT and with OIT to ensure appropriate coordination of efforts.

4. Procedures

This policy includes the GIT Computer & Network Security Procedures by reference. These procedures provide a specific set of measures for unit-level compliance with this policy and the GIT Data Access Policy. The Computer & Network Security Procedures may be superseded by unit-level procedures which have been officially approved by the unit head, OIT, and GT Legal.

5. 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 efficient, effective, ethical, and lawful manner. Violations of the policy may result in loss of usage privileges, administrative sanctions (including termination) as outlined in applicable Georgia Tech disciplinary procedures, as well as personal civil and/or criminal liability.

6. Policy Modifications

This policy may be changed by directive from the responsible university officer. The Computer & Network Security Procedures may be changed by directive from the GIT 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 Section 7.

7. Communication

Upon approval, this policy shall be published on the GIT 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

8. References

- GIT Data Access Policy

http://www.oit.gatech.edu/policies/policies/DAP.pdf

- GIT Computer & Network Security Procedures
  http://www.oit.gatech.edu/policies/procedures/CNS_Procedures.pdf
- Local, state, and federal laws
  http://www.oit.gatech.edu/policies/reference/law_library/
- Incident Response Guidelines
  http://www.security.gatech.edu/architecture/incident_response_procedures
- GIT copyright infringement complaints procedure
  http://www.oit.gatech.edu/policies/reference/copyright/gtcep.cfm
- Institute Consulting Policy
  http://www.admin-fin.gatech.edu/human/discipline/050400.html
- Access by External Entities to Institute Information Technology Resources policy
  http://www.oit.gatech.edu/policies/procedures/xaccess.html
- General Prevention Measures
  http://www.security.gatech.edu/policy/general_measures.html
- GIT Internal Audit Internal Control Guide
  http://www.audit.gatech.edu/icg.htm
- OHR Policies and Procedures
  http://www.admin-fin.gatech.edu/human/
- GIT Academic Honor Code
  http://www.honor.gatech.edu
- Board of Regents Policy Manual
  http://www.usg.edu/regents/policymanual/

