Georgia Tech Information Security

[Informational update for fall semester 2009]
Executive Overview

While Georgia Tech has made tremendous strides over the last 6 years in the area of Information Security, it is important that we continue to meet the security challenges facing higher education. New threats to the environment continue to emerge, and the campus must be prepared to address these threats as they pertain to Institute resources, people, and data.

Georgia Tech has been successful in building a strong Information Security Program through collaboration between the Office of Information Technology (OIT) and the various campus academic, administrative, and research units. Input from campus units is an integral part of information security projects and efforts designed to proactively protect campus. Additionally, as issues or incidents are identified, OIT works closely with the affected areas of campus to resolve them. Programs are implemented to address critical strategic and operational issues specific to the Institute’s mission keeping in mind the requirements of our educational, research, and business constituencies.

Contents:

Strategic goals for Georgia Tech Information Security ..........................................................1
Georgia Tech Data Security & Incident Response Fact Sheet .............................................2
Georgia Tech Information Security Impact Chart ...............................................................3
Georgia Tech Information Security Architecture ..............................................................4
Georgia Tech Information Security Guidelines .................................................................5 & 6
Georgia Tech Collaborative Incident Response Model ....................................................7
Information Security Programs Successes/Goals...............................................................8
Appendix : Computer Network Usage & Security Policy (cheat sheet & policy)

Data Access Policy (cheat sheet & policy)
Strategic Goals for Information Security at Georgia Tech

The goals for Information Security on campus are as follows:

1. Support the Institute’s academic and research goals of attracting top professors and students, obtaining NSF and other research funding and by providing a trusted computing environment that not only protects Tech’s intellectual property but purveys a certain level of confidence to funding agencies that we can be trusted. This goal will also include efforts to enhance secure collaboration efforts between Tech faculty and their colleagues and vendors located around the world in an open yet trusted environment.

2. Protect Institute users, IT resources, and data. Every decision we make and every project we initiate must keep in mind what is necessary to protect the Confidentiality, Integrity, and Availability of Institute IT resources and data as well as the reputation of the Institute.

3. Work closely with our campus leadership located in other countries to ensure that seamless and secure access to teaching and administrative resources housed on the Atlanta campus is achieved and periodically reviewed for effectiveness.

4. Enhance the Education and Awareness Program to include a component focused on the technical support personnel within the units. The desired outcome is to have a well trained technical staff that understands and consistently implements appropriate security controls in their respective units. The Education and Awareness Program is also flexible in content, message, and design to accommodate multiple targeted audiences: Institute administration officials, deans, chairs, department heads, business managers, system administrators, faculty, and students.

5. Ensure compliance with various regulatory and legal bodies. Georgia Tech is bound by regulatory and legal requirements that must be addressed in order to stay compliant. In particular, Georgia Tech must adhere to the provisions of the following:
   - Family Educational Rights and Privacy Act (FERPA)
   - Gramm-Leach-Bliley Act (GLBA)
   - Health Insurance Portability and Accountability Act (HIPAA)
   - Payment Card Industry Data Security Standards (PCI DSS)
   - Fair and Accurate Credit Transactions Act (FACTA)

The core philosophy used by Georgia Tech to meet these goals is one of risk management – that is, identifying areas of risk to campus, documenting and prioritizing the risks found, and making a decision on accepting or mitigating the risk.
Georgia Tech Data Security & Incident Response Fact Sheet

Data Security
- Georgia Tech and our users are targets due to the type of data (student, research, financial, and medical) and infrastructure we have and work with.
- It is very important that faculty/staff read and understand the campus CNUSP and DAP for their role in protecting the data. ([http://www.oit.gatech.edu/georgia-tech-institute-level-policies](http://www.oit.gatech.edu/georgia-tech-institute-level-policies))
- While Georgia Tech has been very successful in repelling attacks on the GT network and exposure of data, it only takes one exposed or lost computer for us to have a major security breach.
- OIT regularly works with campus to help mitigate the risk of data exposure through:
  - Policies & Standards
  - Regular risk discussions with GT data owners
  - Updates to campus leadership
  - Education and awareness activities with Faculty, Students and Staff
  - Communicating risk and providing mitigation solutions to college, school, research center and administrative unit IT Directors and IT staff
  - Unit-level IT risk assessments as requested by Deans, AVPs or Chairs
  - Network Intrusion Detection Systems
  - Network firewalls and monitoring
  - System vulnerability scanning
  - Antivirus scanning and monitoring

General Incident Response Process
- Incidents are typically classified as Level 1 (malware) or Level 2 (affecting desktops/servers). If the incident is something beyond a normal malware infection, OIT is engaged to perform a deeper analysis. ([http://www.oit.gatech.edu/sites/default/files/CSR Incident Response 2008.png](http://www.oit.gatech.edu/sites/default/files/CSR Incident Response 2008.png))
- When routine incidents are reported, OIT notifies the IT Director and IT staff (system owner students/some faculty) of the issue and assists in the clean up as part of our general incident response process.

Specific Incident Response Process
- OIT does NOT monitor email & files, or inspect faculty/staff computers unless there is an incident, complaint, or subpoena that would trigger OIT to perform a review.
- Before investigating faculty/staff computers, email, or files, senior leadership will review the request, and if warranted, approve a specific set of review actions. ([http://www.audit.gatech.edu/IACollabratrive2.pdf](http://www.audit.gatech.edu/IACollabratrive2.pdf))
- Results of the review dictate what actions, if any, the Institute will take.
Threats Over the Years:
- 2001: Nimda, Klez
- 2002: Blaster
- 2003: Mydoom, Bagel, Sasser, Botnets
- 2004: Mydoom.ax, Worms
- 2005: Mydoom
- 2006: Phishing, BotNets
- 2007: Conficker
- 2008: Fake AV

Incidents per Year:
- 2001: 5500
- 2002: 2875
- 2003: 2463
- 2004: 1662
- 2005: 556
- 2006: 81
- 2007: 172
- 2008: 118

Average attacks per week:
- 2001: 5500
- 2002: 2875
- 2003: 2463
- 2004: 1662
- 2005: 556
- 2006: 81
- 2007: 172
- 2008: 118

Office of Information Technology
http://www.oit.gatech.edu
GT Information Security Architecture

A Road Map - Assuring information confidentiality, data integrity and systems availability.

**Deterrent Mechanisms**
- Secured Services
- Campus Border Filters
- Unit Level Firewalls
- Virtual Private Networks
- Host Based Security
- Intrusion Prevention

**Detective Methods**
- Self Assessment
- Vulnerability Scans
- Process Review
- Intrusion Detection Systems
- Network Monitoring
- System Audit

**Prevention**
- Computer and Network Usage Policy
- Unit Level Information Security Policy
- Incurred Residual Risk
- Education and Awareness Programs
- Sharing Incident Information
- Systems Administrator Skill Sets
- Process Improvement

**Reactive Measures**
- Incident Response Procedures
- Computer Forensics
- Service Restoration
- Legal Action
- System Modification

**Threat**
- Natural
- Manmade
- Internal
- External
- Ease of Use tools
- Knowledge Base

**Catalyst**

**Attack**

**Exploits**

**Vulnerability**
- Business Process
- Information Systems

**Results in**

**Impact to Our Mission**
- Business Continuity
- Financial
- Regulatory
- Legal
- Reputation

**Prompts**

**Reduce chance of**

**Disclose & generate statistics of**

**Reduces**
# Information Security Guidelines for Georgia Tech

## Deans & AVPs Responsibilities
- Implement OIT’s defense-in-depth approach to information security where possible. Also known as a layered security approach that includes security guidelines, best practices, policies, and procedures. Exceptions to this approach should be documented and sent to OIT Information Security and Internal Auditing.
- Assign an Information Security Lead with the responsibility to coordinate all major technical and information security issues for the College or Unit.
- Monitor for compliance with the Data Access Policy.
- Approve standards for software & hardware and promote centrally supported and funded applications when applicable.
- Approve a vulnerability management and risk aversion approach for information systems.
- Every system must have an assigned administrator (with the appropriate skill set) that is coordinated with the Technical Lead.
- Review each unit’s annual security self assessment and ensure a plan is in place to remediate issues in a timely manner.

## Chairs, Directors & Managers Responsibilities
- Clearly assign technology roles within the unit.
- Verify that every system has a qualified system administrator with the appropriate skills to maintain the system.
- Develop unit-level security guidelines and procedures that support unit-level policy.
- Ensure the implementation of the data access policy within the unit to include training of authorized users.
- Approve a list of mission critical services and servers containing sensitive information and provide the list to OIT Information Security.
- Coordinate software & hardware standards for approval by the Dean or AVP.
- Coordinate all major technology and information security issues with the Security and/or Technical Lead.
- Review monthly vulnerability scans and report outstanding issues to OIT-Information Security for assistance with resolution.
- Conduct an annual security self assessment and develop a plan to remediate issues.

## College/Unit Technical Lead/CSR Responsibilities
- Coordinate all technology and information security issues within the unit.
- Develop security guidelines and procedures.
- Develop software & hardware standards and use centrally supported and funded applications when applicable.
- Work with unit leadership to generate a list of mission critical services and sensitive information servers.
- Audit unit systems under the control of approved system administrators, report systems with poor controls and maintenance to the Security Lead or management.
- When possible use GT Active Directory or Kerberos for managing department passwords.
- Review system access logs and service offerings, report any issues to management.
- Perform monthly vulnerability scans on all systems, resolve issues and generate reports for leadership to review.
- Implement a patch management system for the unit.
- Participate in an annual security assessment.

*Last Revised: 3/19/2007*
Information Security Guidelines for Georgia Tech

Server/Desktop Administrators

Responsibilities

- Install host-based anti-virus, anti-spyware and firewalls on all desktops and servers when possible.
- Limit access to systems only to those who need access to your servers and desktop computers.
- Review system logs for unauthorized access/attempts.
- Create strong administrative passwords and change them at least every 90 days.
- Apply operating system and application patches in a timely fashion.
- Coordinate technology purchases, service offerings, security issues with the CSR.
- Back up systems and perform periodic restores.
- Scan your system(s) monthly for vulnerabilities, review the report and remediate high vulnerabilities as soon as possible.
- Before you discard, transfer or surplus a computer, use a proven drive wipe method to erase the drive contents. In cases of sensitive data, remove and destroy the drive.

Computers Users

Responsibilities

- Become familiar with applicable computing and security policies.
- Choose “strong” passwords, change them frequently and do not share them with others. A strong password has at least eight characters, a combination of numbers, upper and lowercase letters, and has at least one special character such as !@#$%^&*.
- Contact your CSR before installing new software on your system.
- Do not transmit sensitive information such as social security or credit card numbers via email.
- Log off or lock your keyboard when stepping away from your work area and use a password activated screensavers.
- Report security problems, issues, or misuse to your CSR as soon as possible for remediation.
- Shred documents with sensitive information before discarding.
- When traveling, do not carry a laptop or other mobile devices that contain sensitive information.
- Complete the online information security tutorial.

GT References & Resources

Computer and Network Usage & Security Policy
http://www.oit.gatech.edu/policies

Data Access Policy
http://www.oit.gatech.edu/policies

OIT Information Security
www.oit.gatech.edu/information_security

Export Control Guideline
www.export.gatech.edu

Internal Auditing
http://www.audit.gatech.edu/

On-line Security Tutorial
http://www.oit.gatech.edu/security_tutorial

Information Security Incident Hotline:
404-385-7506

Fraud/Waste/Abuse Hotline:
404-894-4606

security@gatech.edu

abuse@gatech.edu
## Event or Incident Requiring Collaboration

Critical incidents that require collaboration are incidents that extend beyond the borders of the local hardware or software system, and pose a threat of an adverse impact on the Institute’s reputation, financial position, information systems security posture, or health and safety of faculty, staff and students. Examples of Incidents Requiring Collaboration:

- Unauthorized access to sensitive information (e.g., SS#, credit card #’s)
- Suspected misuse of IS resources resulting in widespread compromise of information security
- Large scale intrusions

## Ad-Hoc Group Convenes

- Chief Information Officer
- Director of Internal Auditing
- Chief legal Advisor
- Associate VP – Office of Human Resources
- Director of Information Security
- Director of Institute Communications
- Director of Homeland Security/Police Chief

## Other resources to be considered on a situational basis:

- Associate VP – Financial Services
- Unit Head of Affected Area
- Dean of the College of Computing
- Director, Georgia Tech Information Security Center
- Chief Technology Officer
- Dean of Students Office

## This Ad-Hoc Group will determine the resources necessary to reach a resolution on the incident. The Group will also identify appropriate internal and external communication channels, and make the following assessments:

### 3a Is this incident likely to result in criminal or civil legal action?

If the answer is yes, the path below should be pursued. If no, 3b should be followed.

**Scope:**
A decision needs to be made to determine the point at which GIT will stop its internal investigation and hand over to law enforcement and then to which law enforcement agency (e.g., FBI, GBI, Secret Service, and/or local law enforcement).

**Review Method:**
The standards of evidence for an investigation which is likely to result in criminal prosecution are far higher than those for which administrative action only is expected. For example, prior to any internal investigation of the machines involved, it would likely be appropriate to have law enforcement mirror the drives of machines, then turn the mirrored drives back to GIT for its internal investigation.

**Investigation:**
After coordinating with law enforcement, and preserving the integrity of the data on the machines, GIT will proceed with an investigation of the mirrored drives.

### 3b Is this incident likely to not result in legal action and likely to result in an administrative action that is localized within the Institute?

If yes, the following path should be pursued.

**Scope:**
A decision needs to be made at what level the investigation will take place and the standard of evidence that will be maintained. A decision will also need to be made regarding the point at which enough evidence has been obtained to satisfy the requirement to take appropriate administrative action.

**Review Method:**
The standards of evidence for an administrative investigation are less stringent than those which may result in legal actions but are important to maintain nonetheless. This ad hoc group much decide at what level evidence of the investigation should be documented.

**Investigation:**
As the internal investigation proceeds, the ad-hoc group must be cognizant of situations encountered which may change the examination from administrative to a potential legal investigation and take appropriate steps.

## Assigning Investigation Oversight:
The Ad-hoc group will determine which internal agency will take the lead for coordinating the investigation and communicating the results. This Designated lead group will:

- Coordinate all efforts related to the investigation
- Determine the custodians of data
- Have responsibility for reporting results and ensuring continuing lines of communication

## Conducting The Investigation:
The department or group with oversight of the investigation has the responsibility to communicate the results of the investigation, and ensure as soon as data on this incident relevant to the position of the Institute is uncovered, it reaches the executive decision makers.

## Follow-up and Reporting:
The department or group with oversight of the investigation reconvenes the Ad-Hoc group at the end of the investigation and reports on:

- The outcome of the investigation
- Lessons learned (how the process worked)
- Cost of incident (in hard costs and personnel time devoted to the incident response)
- Discuss methods to prevent future incidents
<table>
<thead>
<tr>
<th>Program</th>
<th>Successes</th>
<th>2009 Goal Highlights</th>
<th>Future Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy &amp; Compliance</strong></td>
<td>• Developed a mature set of policies, standards, and procedures</td>
<td>• Acceptable Use (CNUSP) re-write</td>
<td>• Data Access Policy (DAP) Re-write</td>
</tr>
<tr>
<td></td>
<td>• Implemented process for drafting and reviewing policies</td>
<td>• Publish Password &amp; Remote Access policies &amp; associated standards</td>
<td>• Annual PCI &amp; HIPAA reviews</td>
</tr>
<tr>
<td></td>
<td>• Implemented a policy exception process</td>
<td>• Self Assessment templates &amp; schedule development</td>
<td>• Implement Unit Self Assessment schedule</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Annual PCI Review</td>
<td>• Additional Standards development</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Annual HIPAA review</td>
<td></td>
</tr>
<tr>
<td><strong>Host Security</strong></td>
<td>Deployed Central Management solutions for:</td>
<td>• Promote deployment of antivirus &amp; desktop mgt. software,</td>
<td>• Establish workstation &amp; server guidelines</td>
</tr>
<tr>
<td></td>
<td>• (%) Desktop Management</td>
<td>• Deploy WDE solution to schools and Admin areas</td>
<td>• Establish web application scanning guidelines</td>
</tr>
<tr>
<td></td>
<td>• (%) Antivirus Management</td>
<td>• Establish workstation &amp; server standards</td>
<td>• Deploy thumb &amp; external hard drive encryption service</td>
</tr>
<tr>
<td></td>
<td>• Whole Disk Encryption (WDE) pilot within OIT</td>
<td>• Deploy a new Vulnerability Management service</td>
<td>• Establish Self-service vulnerability scan service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Evaluate thumb &amp; external hard drive encryption</td>
<td>• Establish credentialed scanning of sensitive servers</td>
</tr>
<tr>
<td></td>
<td>Deployed Central Management solutions for:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dual-layer deployment of Firewalls for campus and Units</td>
<td>• Deploy new IDS architecture to include signature and anomaly-based detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote Access (VPN) solution deployed</td>
<td>• Self Service for firewall rule requests</td>
<td></td>
</tr>
<tr>
<td><strong>Network Security</strong></td>
<td>• Updated IR process and tools to reflect changes in technology and challenges to campus</td>
<td>• Review and update of IR procedures, tools, and processes</td>
<td>• Integrate IDS sensors with SIM appliance</td>
</tr>
<tr>
<td><strong>Incident Response (IR)</strong></td>
<td>• Inaugural Data Cleanup event for campus</td>
<td>• Communicate changes to campus</td>
<td>• Pre-scan of systems for firewall rules</td>
</tr>
<tr>
<td></td>
<td>• Published Data Classification Handbook</td>
<td></td>
<td>• Establish firewall audit program</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Education Awareness and Outreach</strong></td>
<td>• Central deployment of GT Enterprise Directory with Unit integration</td>
<td>• Data Cleanup 2009</td>
<td>• Data Cleanup 2009</td>
</tr>
<tr>
<td></td>
<td>• Implemented guest services</td>
<td>• Collaborate with faculty on guidelines for handling student data</td>
<td>• Implement guidelines for faculty handling of student data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Host security awareness events</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security Awareness month activities</td>
<td></td>
</tr>
<tr>
<td><strong>Identity and Access Management (IAM)</strong></td>
<td>• Central deployment of GT Enterprise Directory with Unit integration</td>
<td>• Implement levels of assurance for password resets</td>
<td>• GT Roles System deployment</td>
</tr>
<tr>
<td></td>
<td>• Implemented guest services</td>
<td>• IAM infrastructure upgrades</td>
<td>• Federation with external partners</td>
</tr>
<tr>
<td><strong>Business Continuity and Disaster Recovery</strong></td>
<td>• Initial phase of Business Continuity Data Center (BCDC) build-out completed.</td>
<td>• 2009 DR testing</td>
<td>• Continue evaluation of critical services for business continuity</td>
</tr>
</tbody>
</table>
CNUSP Review

CNUSP Guiding Principles

1. 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
2. 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
3. The Institute is committed to protecting Georgia Tech users of IT resources and data
4. The Institute is committed to protecting the Confidentiality, Integrity, and Availability of Georgia Tech IT resources and data

Copyright & IP

- Users will respect copyrights and trademarks
- Users creating Intellectual Property should be aware of potential issues surrounding the creation, ownership, and use of IP
- Users will respect licenses to install and use software

Integrity of Resources and Protection of Data

- Users will respect the privacy of others
- Users are responsible for upholding the confidentiality and integrity of data & IT resources to which they have access
- Authorized users accept the responsibility to protect the information accessed and used on their computer
- Researchers are responsible for protecting data created during the course of a project

Unauthorized Access & Circumventing Security

- Authorized users are responsible for the security of their passwords
- Users may not access GT IT resources without appropriate permission
- Users are required to respect the security measures implemented at Georgia Tech
- Suspected security incidents are to be reported to the appropriate personnel

Usage of IT Resources

- GT IT resources are to be used for scholarly or business purposes only.
- Use of IT resources to send, view, or download inappropriate material is prohibited
- IT resources may not be used in connection with compensated outside work (except in accordance with the Institute Consulting Policy)

Management of IT Resources

- OIT is responsible for managing the GT network
- Units are responsible for identifying users behind network devices that provide NAT, DHCP, and VPN services
- OIT will facilitate the review of non-gatech.edu domain names for appropriateness

Policy Exceptions

- Users and units may apply for policy exceptions when there is a legitimate business or scholarly need
DAP Review

Guiding Principles

Data Stewards are responsible for defining who may have access to the data they are responsible for. In general, Data Stewards have defined the following principles:

- Inquiry-type access to official Institute Data will be as open as possible to individuals who require access in the performance of Institute operations.
- *Data Users* granted “create” and/or “update” privileges are responsible for their actions while using these privileges.
- Any individual granted access to Institute Data is responsible for the ethical usage of that data.

Access Coordination

- *Data Stewards* designate individuals to coordinate Institute Data access for each functional data grouping.
- The *Data Coordinators* maintain records of authorized Data Users, and serve as contact point for the *Data Administrator(s)*.
- Employees may request access to data through a designated *Authorized Requester*.

Data Categories

<table>
<thead>
<tr>
<th>Data Categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category I</td>
<td><strong>Public Use:</strong> This information is targeted for general public use. Examples include Internet website contents for general viewing and press releases.</td>
</tr>
<tr>
<td>Category II</td>
<td><strong>Internal Use:</strong> Information not generally available to parties outside the Georgia Tech community. This category is the default data classification category. Examples include travel authority forms, purchasing receipts, and performance evaluations.</td>
</tr>
<tr>
<td>Category III</td>
<td><strong>Sensitive:</strong> 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. Examples include Social Security numbers, non-directory Student information, and Research data under an NDA.</td>
</tr>
<tr>
<td>Category IV</td>
<td><strong>Highly Sensitive:</strong> Data that must be protected with the highest levels of security, as prescribed in contractual and/or legal specifications. Any credit card data except the Georgia Tech P-Card is considered Category IV.</td>
</tr>
</tbody>
</table>

Request for Review

- Data Users may request that the Data Stewards and Chief Data Stewards review the restrictions placed on the classification of data.
- The appropriate Chief Data Steward has final governance authority regarding matters of data restrictions and requests for access rights to Institute Data.