

**Georgia Institute of Technology  
School of Civil & Environmental Engineering**

**CEE Computing and Network Policy**

**February 2001**

## Quick Reference Guide

(<http://www.ce.gatech.edu/isg/quickreferenceguide.html>)

<b>CEE Computing/Network Policy:</b>	<a href="http://www.ce.gatech.edu/isg/policy.html">http://www.ce.gatech.edu/isg/policy.html</a>
<b>CEE Official Web Page:</b>	<a href="http://www.ce.gatech.edu/">http://www.ce.gatech.edu/</a>
<b>CEE Faculty/Staff Webmail Site:</b>	<a href="http://webmail.ce.gatech.edu/">http://webmail.ce.gatech.edu/</a>
<b>CEE Graduate Student Webmail Site:</b>	<a href="http://gradmail.ce.gatech.edu/">http://gradmail.ce.gatech.edu/</a>
<b>Georgia Tech Official Web Page:</b>	<a href="http://www.gatech.edu/">http://www.gatech.edu/</a>
<b>Information Systems Group (ISG):</b>	Provides CEE service for all computing and networking repairs, installations, web creation, and questions
<b>ISG Contact Information:</b>	
Web Page:	<a href="http://www.ce.gatech.edu/isg/">http://www.ce.gatech.edu/isg/</a>
Phone:	404-894-2210
Location:	SEB 317
E-mail Problems:	<a href="mailto:helpdesk@ce.gatech.edu">helpdesk@ce.gatech.edu</a>
E-mail Questions:	<a href="mailto:isg.questions@ce.gatech.edu">isg.questions@ce.gatech.edu</a>
<b>CEE Internal Documents/Assistance:</b>	<a href="http://www.ce.gatech.edu/internal/">http://www.ce.gatech.edu/internal/</a>
<b>Reservation System for CEE:</b>	<a href="http://www.ce.gatech.edu/reservations/">http://www.ce.gatech.edu/reservations/</a> Used to reserve CEE rooms and computers
<b>Office of Information Technology (OIT):</b>	Provides computing service to the Georgia Tech community. All faculty, staff, and students have a computer account here, referred to as your prism account.
<b>OIT Contact Information:</b>	
Web Page:	<a href="http://www.oit.gatech.edu">http://www.oit.gatech.edu</a>
Telephone:	404-894-7173
Location:	Rich Building
<b>OIT Computer/Network Policy:</b>	<a href="http://www.oit.gatech.edu/oithome/policy.html">http://www.oit.gatech.edu/oithome/policy.html</a>
<b>OIT's What Faculty/Staff Need to Know:</b>	<a href="http://www.oit.gatech.edu/oithome/staff.html">http://www.oit.gatech.edu/oithome/staff.html</a>
<b>OIT's What Students Need to Know:</b>	<a href="http://www.oit.gatech.edu/oithome/students.html">http://www.oit.gatech.edu/oithome/students.html</a>
<b>Student Computer Ownership:</b>	<a href="http://www.sco.gatech.edu">http://www.sco.gatech.edu</a>
<b>Virus Software for Georgia Tech:</b>	<a href="http://software.oit.gatech.edu">http://software.oit.gatech.edu</a> This software is licensed for faculty/staff/student home computers also.
<b>Virus Alert/Hoax Information:</b>	<a href="http://www.nai.com">http://www.nai.com</a>

## **Georgia Tech School of Civil & Environmental Engineering Computing and Network Policy**

Security concerns are paramount in a networked computing environment like that of the Georgia Tech School of Civil and Environmental Engineering (CEE). Networked computers are the targets of daily attempts to compromise security and gain unauthorized access to the campus network and data. Once hackers infiltrate the GT system, they can access and distribute confidential data, damage and destroy critical files, send harmful messages that appear to come from Georgia Tech, and link to systems outside of Georgia Tech (making any damage to these systems look as if it were perpetrated by Georgia Tech students or employees). Compromises to network security open the Institute and individual faculty, staff, and students to potential legal and financial liabilities that arise from resulting damage.

Most successful security attacks occur on computers running network-related services. In most cases, CEE faculty, staff, and students do not have sufficient knowledge or time to properly configure and maintain systems to minimize the risk of a security breach. Because hackers develop new security exploits every day, it is difficult for users to make necessary security-related configuration changes for networked computers. CEE's Information Systems Group (ISG) staff have the expertise and responsibility to configure and maintain computer configurations to avoid common attacks and to minimize the consequences that result when hackers compromise the network. To perform these tasks, the ISG staff must have administrative access to all CEE computers. Faculty and staff also typically require administrative access to install software and perform routine administrative tasks. The key is to ensure: 1) that routine maintenance and changes made by faculty and staff do not compromise network security; 2) that such changes do not damage existing hardware and software setups; and 3) that open communication is maintained between faculty/staff and ISG.

To provide a secure academic computing environment, CEE has adopted the following Computing and Network Policy. This policy is designed to ensure that CEE faculty, staff, and students have access to all CEE systems while ensuring that the integrity and privacy of CEE systems and data are maintained. The CEE policy extends existing Institute policies and clarifies these policies as they relate to computer usage in CEE. This CEE policy document is available at <http://www.ce.gatech.edu/isg/policy.html>.

All CEE computer facility users agree to abide by the CEE Computing and Network Policy, as well as the Georgia Institute of Technology Computer and Network Usage Policy (<http://www.itis.gatech.edu/security/security>). The Georgia Tech Office of Information Technology (OIT) oversees the implementation of campus-wide computing policy. Georgia Tech deals with violations of School and Institute computing and network policies seriously. Violations can result in loss of computer access privileges and imposition of Georgia Tech disciplinary proceedings implemented under policies of the Georgia Tech Office of Human Resources and/or Office of Student Services.

## **1. Overview**

- a. This document is the "School of Civil and Environmental Engineering (CEE) Computing and Network Policy."
- b. All users of CEE computer facilities agree to read this policy and understand that they are bound by the policies outlined in this document.
- c. CEE faculty, staff, and students should direct questions about this policy to the CEE Information Systems Group (ISG) at [isg.questions@ce.gatech.edu](mailto:isg.questions@ce.gatech.edu) or 404-894-2210.

## **2. Applicability**

- a. This policy applies to all faculty, staff, and students in the School of Civil and Environmental Engineering (CEE) and other individuals using CEE facilities.
- b. This policy applies to all computers and networking services in CEE located in the Mason Building, Sustainable Education Building, Daniel Lab, and Structures Lab.

## **3. Computer and Network Access**

- a. ISG assigns each computer account and unique password to one, and only one, individual. Use of accounts by more than one individual is strictly prohibited. Users will login to a CEE computer system and/or attached network using a user id and password assigned only to them.
- b. ISG staff will create a user id and password for new or returning employees when notified by the CEE business office. ISG staff will need to know when the person will start work, where they will be located, and with which group they will be affiliated. This policy also applies to temporary staff.
- c. The CEE business office will notify ISG when an employee leaves CEE so that login accounts and network access can be disabled. As a courtesy, CEE will maintain an e-mail forwarding alias for six months.
- d. ISG will create accounts for short course attendees to provide access to appropriate computer facilities needed for the course. Course instructors need to contact ISG to arrange these accounts more than one week before the scheduled course.

## **4. Passwords**

- a. All CEE computer passwords expire after 90 days. Users must create new passwords every 90 days and may not re-use a previously assigned password again in the same year.
- b. Passwords must consist of a minimum 6 characters, one of which is not a letter. Passwords may not be based upon any common name or dictionary word (even if the word is spelled in a language other than English).
- c. ISG staff will reset CEE faculty and staff passwords for their account upon request.
- d. CEE students can obtain passwords from either ISG staff or the user assistants working in the computer labs (Mason 297).

## 5. E-mail accounts

- a. The official method of Institute and CEE communication to all faculty, staff, and students is by e-mail to the e-mail address of record.
- b. The faculty and staff e-mail address of record for CEE, the Georgia Tech Office of Information Technology, and Georgia Tech Human Resources is the e-mail computer account administered by CEE. The format of the e-mail address is [firstname.lastname@ce.gatech.edu](mailto:firstname.lastname@ce.gatech.edu). This address shall serve as the official e-mail address on all written and electronic communications, from e-mail to business cards.
- c. The CEE graduate student address of record is the Acme/Prism account issued by Georgia Tech Office of Information Technology. CEE students also receive a CEE e-mail address ([firstname.lastname@ce.gatech.edu](mailto:firstname.lastname@ce.gatech.edu)) while enrolled at Georgia Tech (ISG obtains the `firstname.lastname` format from registrar's office information). The CEE e-mail alias automatically forwards messages to the student's address of record.
- d. ISG supports a web-based e-mail server for remote access to e-mail. Faculty and staff can read e-mail in a secure manner from any computer connected to the Internet. This service is available to all CEE faculty and staff at <http://webmail.ce.gatech.edu>. The web server requires the e-mail user id and password to login.
- e. ISG also supports a web-based e-mail facility for CEE graduate students at <http://gradmail.ce.gatech.edu>. The web server requires the e-mail user id and password to login.
- f. To ensure that Georgia Tech faculty, staff, and students do not inadvertently release intellectual property rights without written permission, only Georgia Tech e-mail services shall be used to conduct Georgia Tech business. Many outside companies and organizations that host e-mail services claim intellectual property rights on all content of e-mail sent to/from their servers. Hence, faculty, staff, and students will not use accounts on Hotmail, Yahoo, or other non-approved services for Georgia Tech business.
- g. Attachments to CEE e-mail have an aggregate size limitation of 10MB (OIT Prism accounts have a 2MB size limitation). If a file larger than 10MB must be exchanged, ISG can provide other means to send/receive the file.
- h. CEE blocks the most common types of e-mail attachments that carry automatically launched network viruses. Currently, the following types of attachments are blocked by CEE: \*.bat, \*.com, \*.cpl, \*.dll, \*.exe, \*.ocx, \*.pif, \*.scr, \*.shs, and \*.vbs files. ISG will add any new file types to the list that it deems necessary. ISG will notify users by e-mail as they add new file types to the list. Senders of these file types receive an automatic reply from the CEE mail server that the intended recipient cannot receive these files. For CEE faculty and staff to receive files of this type, the sender must convert them into a \*.zip format before sending.

## 6. E-mail Software Support

- a. ISG supports Eudora and other approved web-based clients for e-mail access. ISG may support other software packages on a case-by-case basis.

## **7. Use of CEE Computing Facilities**

- a. Faculty, staff, and graduate students may reserve the CEE general computing labs for CEE courses by requesting the use through the CEE reservation system (CEE web page).
- b. Food, drink, and tobacco products are not permitted in the computing labs at any time for any reason.
- c. Graduate students may keep the lab open beyond its closing time with permission of the User Assistant in charge, only after completing a lab procedures course offered by ISG. Any student exercising these privileges will be responsible for the security of the equipment in the lab and for closing and locking the facility upon leaving. Students seeking these privileges must take the class every year.
- d. Computers in the CEE computing labs require a user id and password.
- e. Each student's user id is the same as his or her Prism user id. However, ISG will issue a CEE password for logging in to the CEE system. All students registered in CEE classes receive such access. Once a student has graduated, or is no longer enrolled as a CEE student, his/her account will be disabled.
- f. Each faculty and staff member's user id and password are the same as his/her regular CEE user id. However, faculty and staff should log in to the Mason domain, rather than the Lab domain, on these computers.
- g. Network drives on the Lab domain provide temporary storage, and ISG does not back up these files. ISG staff may remove files on the Lab domain network drives at any time without notice.
- h. Users will not encrypt files on any CEE system unless approved by ISG and the user provides ISG with the encryption key.
- i. CEE charges a fee of \$25/computer/day for computer facility use by short courses. The School will use such fees to maintain and upgrade CEE computing facilities.

## **8. System Administration**

- a. ISG is the primary Administrator of all computers connected to the network in CEE facilities. As such, ISG must have administrator or root access on all network-connected computers.
- b. Faculty and staff will be granted Administrative privileges on individual machines upon request, provided the individual attends an ISG 1-hour network security training session every year.
- c. Both the faculty/staff administrator and ISG will have authority to perform any routine support for these machines.
- d. Faculty/staff administrators will not use the Administrator account for regular day-to-day use of the computer. The Administrator account shall be used only when necessary (i.e., to upgrade and maintain the machine or when proprietary software requires the user to be logged in with administrative privileges).

- e. Faculty/staff administrators may not start any network-related services or change any network settings on any machines without the explicit approval of ISG. ISG will respond to such requests in two working days. Network-related services include FTP, Telnet, Web Servers, Mail Servers, DHCP, DNS, WINS, and other services defined by ISG.
- f. On all systems, the faculty/staff administrator shall comply with OIT policy, assigning each user a unique user id and password. Faculty/staff administrators shall ensure that shared accounts do not exist on the system.
- g. The faculty/staff administrators will provide ISG with the Administrator password and any changes to that password. The faculty/staff administrators shall deliver the account and password information to ISG staff in person (users must not send confidential information through the network via e-mail).
- h. The faculty/staff administrators will not share the administrative password with other individuals nor allow administrative access to any users other than ISG.
- i. Faculty/staff administrators will provide the user ids, names, and contact information for any accounts established on a machine. The faculty/staff administrator shall ensure that ISG always has a current copy of this user account list. These records shall be delivered in person to ISG staff (do not send via e-mail).
- j. Only ISG staff or the faculty/staff administrator shall perform routine equipment maintenance or support on the computer. Only ISG-approved contractors may provide supplemental support for CEE computers. The faculty/staff administrator will coordinate the scheduling of any maintenance or support work so that ISG can observe the work and ensure that contractors do not compromise security from inside the network.
- k. The faculty/staff administrator will maintain a record of all major software and hardware upgrades and installations so that ISG staff can trace any security holes back to the problem software. Critical software upgrades include those made to the operating system, any Microsoft products, Eudora, and other software packages that interface with the network.
- l. Should the faculty/staff administrator find any evidence of suspicious activity on the machine, the administrator will leave the evidence intact and contact ISG immediately.
- m. In the event that ISG finds that the faculty/staff administrator is not meeting the above conditions, ISG will request via e-mail that the faculty/staff administrator make necessary changes. If the faculty/staff administrator does not make necessary changes within two working days, ISG may remove the system from the network until the problem is resolved.
- n. If ISG determines that any system constitutes an immediate security threat to CEE or Georgia Tech systems or data, ISG will immediately remove the system from the network until the problem is resolved. ISG will attempt to notify the faculty/staff administrator of this action.

- o. For non-networked computers, the faculty/staff administrator shall ensure that a third party has the administrator password. The faculty/staff administrator shall provide the name, address, and telephone number of this individual to ISG staff so that institute data can be recovered in case of an emergency.
- p. If a dispute arises between a faculty/staff administrator and ISG staff, the CEE Computer Committee will hear any appeals of ISG decisions within two working days. CEE Computer Committee decisions may be appealed to the School Chair.

## **9. Connecting to the Network**

- a. Because connecting to the network, even for brief periods, can cause access violations and open security holes, only ISG shall approve and connect computers to the GT/CEE computer network. This applies to any computer connected to any data port in a CEE-operated building. Violations of network connection provisions can result in OIT removing the entire CEE network from the Georgia Tech system.
- b. Because network services introduce security risks, computers connected to the CEE network shall not run network services such as FTP, Telnet, Web Servers, Mail Servers, DHCP, DNS, WINS, etc., without the approval of, and configuration by, ISG staff. This applies to any computer connected to any data port in a CEE-operated building.
- c. Only ISG staff may create Windows domains on network-connected machines.
- d. Georgia Tech and CEE IP addresses shall not be used on off-campus computers connected to the Internet.

## **10. New Equipment**

- a. CEE administrative staff will route all new machines directly to ISG upon arrival at the School so that ISG can open the boxes, inventory the new equipment, and apply appropriate GT property stickers. Within one day, ISG staff will notify the faculty or staff member that their new equipment has arrived in CEE.
- b. When notified by ISG that the equipment has arrived, the faculty or staff member will provide ISG with a list of software that they intent to install on the machine. This will allow ISG to develop a software installation order that will minimize installation conflicts.
- c. ISG will deliver the equipment and software installation order to the faculty or staff member within two working days of receiving the software installation list. The faculty or staff member may begin installing standard office productivity and research-oriented software packages (for which they have valid licenses) once they receive the machine and the software installation instructions from ISG.
- d. The faculty or staff member shall install the software into the default installation directory or into an alternate directory, as directed by ISG staff.
- e. Only ISG staff shall install network-related software and set up the computer for network access.
- f. Only ISG staff shall plug the new computer into the network port.

## **11. Equipment Inventories and Equipment Moves**

- a. The occupant of each office and lab space must maintain an inventory of all computer equipment and installed software on CEE inventory sheets posted on the back of office and lab doors. Forms can be found online at <<http://www.ce.gatech.edu/forms>>.
- b. The occupant of each office and lab space is responsible for completing an inventory move form and submitting the form to ISG whenever relocating equipment to another room. Forms can be found online at <<http://www.ce.gatech.edu/forms>>.

## **12. Disposition of Old Equipment**

- a. Institute inventory guidelines require ISG staff to document the removal of any components from an existing CEE machine. Faculty, staff, and students may not remove, exchange, or throw away components from existing machines without the written approval of ISG.
- b. The assigned user of the equipment, according to property inventory records, will be responsible for the equipment until it is officially surplus by the Institute. To surplus equipment, the user must complete the appropriate surplus property form, submit the form to ISG, and request that ISG remove the equipment. Surplus forms can be found online at <http://www.ce.gatech.edu/internal/forms.html> .
- c. Faculty and staff will report equipment theft, damage, or loss to the School Chair as soon as practicable and will file police reports as required.
- d. The distribution and redistribution of state purchased computer equipment is at the discretion of the Associate Chair for Information Technology. Computing equipment purchased with start-up funds are considered state-purchased equipment.
- e. Sponsored project principal investigators may distribute or redistribute computer equipment purchased with research funds.

## **13. Sources of Computing Support**

- a. ISG is responsible for providing support for all approved CEE computer systems.
- b. All support on Institute-owned or licensed equipment must come from (or be approved by) ISG staff. ISG must approve any service contracts.
- c. Faculty should consult ISG staff prior to purchasing new computing equipment to be sure that support for the equipment can be performed and that the computer configurations will be compatible with networking and other computer operations within CEE.
- d. Computers owned by faculty, staff, and students may not be connected to Georgia Tech's network without specific approval of ISG. ISG shall ensure that the computer meets any applicable hardware and software security-related specifications and ISG shall install such standard security provisions when purchased and provided by the user.
- e. ISG cannot service any personally owned computers.

#### **14. CEE Shared Equipment Checkout**

- a. CEE faculty and staff may check out portable computer equipment for use in the classroom and for seminars. ISG will inspect the portable computer before it is picked up and upon return to be sure that all equipment is returned and in operating condition. The portable computer must be reserved 48 hours in advance via the CEE web page. Reservations are on a first come, first served basis.
- b. CEE faculty and staff may check out a portable projection device for remote locations. These reservations are on a first come, first served basis. The projection equipment must be reserved one working day in advance via the CEE web page. Reservations are on a first come, first served basis.
- c. Individuals may pickup reserved equipment 15 minutes prior to the reserved time from either ISG (SEB 317) or Ms. Abram's office (SEB 323), assuming the equipment is not currently in use. If the user does not pick up the equipment by the time of the reservation, ISG may redirect the equipment to others who request the equipment.
- d. Users will return the equipment immediately after its use, even if the equipment is reserved multiple times in the day (unless approved by ISG).
- e. The Associate Chair for Information Technology has the right to limit or redirect the use of CEE equipment to provide for equitable access within the School.

#### **15. Taking CEE Computers Home**

- a. If approved by the School Chair and ISG, an employee may take CEE equipment home.
- b. To ensure that Institute insurance covers the equipment, a standard equipment loan agreement form (available in the CEE Business Office) must be completed by the employee, approved by the School Chair, and submitted through the CEE Business Office.
- c. Faculty and staff may only use a CEE computer at home if the user purchases, installs, and operates a current version of a virus scanning software approved by ISG staff and performs regular updates of the virus software. If the computer connects to the Internet via a service provider (e.g. AOL, Juno, Earthlink, etc.), the user must also purchase, install, and operate a network firewall software package (e.g., Black Ice) approved by ISG staff.
- d. ISG will not service CEE computers at employee's homes. It will be the responsibility of the individual to bring the computer to campus for service.

#### **16. Off-Campus Access to Computing Resources**

- a. Only OIT and/or ISG-approved methods may be used to access Georgia Tech and CEE computer resources from off campus. Users shall not access, nor allow others to access, CEE computers in any manner not specifically approved by ISG.
- b. Only the Board of Regent's Internet Service Provider, CampusCWIX, may provide dial-up access to CEE computer systems <<http://www.campuscwix.com>>.

- c. Computers linked to the CEE network shall not receive calls via modem, unless ISG staff approves and configures the modems and network software.

## **17. Copyright Issues**

- a. CEE recognizes the copyrights of individual software providers.
- b. CEE recognizes the copyrights of web pages and the information contained within those sources. CEE does not allow copying of material created by others onto the School's web servers without written permission from the copyright owner.
- c. CEE recognizes that some forms of multimedia files (e.g., MP3, AVI, etc.) are legal for download for personal enjoyment, but the transfer of these files to others is often illegal. Given the limited disk space and computational resources available for CEE faculty/staff/students, CEE does not allow the presence of multimedia files on its servers or lab computers.

## **18. Education Computing Resources and Software Requests**

- a. Faculty may request software purchase and installation in the computer labs for CEE courses. Faculty and staff should direct such software requests to the CEE Computer Committee for consideration. Software requests shall be made two months prior to the date which the software is needed in the computer labs. The number of licenses that CEE must purchase depends upon the requirements of the software license agreement.
- b. Faculty and staff must provide any software (and original license agreements) needed for a short course to ISG for installation at least three weeks before the short course is to be held.
- c. Faculty and Staff will notify ISG staff at least two weeks before the start of each quarter if one of their courses requires the use of a large amount of plotting paper or other items that require advance ordering.

## **19. Software Licenses**

- a. CEE computers may only use software for which an original valid license agreement is in hand and when the license allows installation of the software on the computer.
- b. ISG staff will only install software when provided a copy of the valid software license agreement allowing the software placement on the computer.
- c. ISG will retain either the original license or a copy of the original license for all software installed on all CEE computers. Users shall supply copies of any original licenses to ISG staff upon request.
- d. ISG staff will store the original software license agreement (or the copy of the license agreement) in a folder dedicated to specific computer. ISG staff will also retain the original purchase order and other technical specification sheets in this folder. ISG will store the original software media in the same folder, unless otherwise requested.

- e. When original software agreements are not retained in the ISG filing system, faculty and staff must be able to provide the original license agreements to any Georgia Tech OIT representative or a law enforcement official for inspection and verification. When ISG does not maintain original software in the ISG filing system, faculty, staff, and students must also ensure that the original software media available for inspection upon request.

## **20. Security Sweeps**

- a. OIT and/or ISG perform automated and targeted network security scans on all CEE machines to identify security holes that lead to unauthorized network access. Network security scans look for open ports and services operating on the ports that constitute a security threat. Security scans do not include scanning of hard drive content.
- b. When ISG identifies unapproved services or a security breach that threatens CEE systems or data, ISG will immediately disconnect the computer from the network. ISG will immediately notify the user of the problem and schedule a meeting with the Administrator to repair the problem.

## **21. Anti-Virus Software**

- a. ISG-approved anti-virus software shall be installed and operated on all CEE computers. The automatic update features of the anti-virus software must also be installed and operated on these machines.

## **22. Supported Software/Operating Systems**

- a. ISG staff strive to support as many hardware and software configurations as possible. However, ISG staff cannot support every operating system and software package. The CEE Computer Committee, in consultation with the Associate Chair for Information Technology, determines which computing environments and software packages CEE supports. Unless referenced otherwise, the latest version of each product is supported:
  - i. Hardware, PC Platforms - Compaq, Dell, and Gateway
  - ii. Hardware, Apple Platforms - PowerMac
  - iii. Hardware, Unix Platforms - SGI, Sun
  - iv. Operating Systems, PC Platforms - Windows NT4 and 2000 (Windows 95, 98, and ME are allowed in limited applications, such as data collection laptops, when approved by ISG).
  - v. Operating Systems, Unix Platforms - IRIX, Linux, Solaris
  - vi. Software Packages: AutoCAD, Eudora, MatLab, Microsoft Explorer, Netscape, Adobe Acrobat Reader, Office 97 and Office 2000 (Access, Word, Excel, and PowerPoint), Georgia Tech's virus package, and WinFax.
- b. ISG will consider supporting additional software packages upon request on a case-by-case basis.

## **23. Disk Shares and Backup**

- a. ISG staff maintains a disk share on the server for each affinity group. This disk share is available to all faculty/staff affiliated with the group.
- b. ISG provides backup service on approved disk shares. These common disk shares on the server are backed-up by ISG on a daily basis. ISG does not provide back up services on individual computers.
- c. Each faculty member has read/write access on the classes.ce.gatech.edu web server for provision of course-related educational materials. Faculty can log into this system on the Mason domain using their regular user id and password.
- d. ISG staff must approve all disk shares to ensure that the security setup precludes unauthorized network access.
- e. Each faculty member has read access to their research projects account ledgers maintained by the CEE Business Office.

#### **24. Disk Partitioning**

- a. All new faculty and staff computers shall have a standardized directory structure on the C:\ drive containing CEE-supported software. The partition shall employ a standardized format and content determined by ISG, so that upgrades, patches, and support software can be electronically distributed and updated automatically.
- b. All new software on all machines shall be installed into default installation directories, unless approved by ISG staff.

#### **25. Web Page Publishing on CEE computers**

- a. Faculty and staff will comply with all applicable Georgia Tech policies pertaining to web publishing (see <http://www.oit.gatech.edu/security/policy/www/>).
- b. All web pages must include a contact e-mail address for the content author and page administrator.
- c. Web pages must be free from copyrighted text (e.g., journal papers), tables, figures, graphics, etc., unless the copyright owner provides written permission.
- d. Faculty and staff may host CEE course home pages on non-CEE computers with approval of ISG staff. Faculty and staff shall ensure that the main CEE course Web page (<http://classes.ce.gatech.edu>) provides a direct link to their CEE course web pages.

#### **26. Acceptable Network Traffic**

- a. All CEE users will conduct themselves in a fashion that represents Georgia Tech and the School of Civil & Environmental Engineering in a professional manner in all forums of electronic information (e.g., e-mail, web pages, etc.).

#### **27. Printing Limitations**

- a. All printers in the CEE computer labs, and in research labs at the decision of the lab manager, are subject to printing limitations.

- b. All students enrolled in CEE are allotted a fixed number of pages (250 pages/semester) to print each term, regardless of the number of CEE classes they are taking. Unused pages do not roll over to subsequent semesters.
- c. Students may purchase additional pages for \$0.05/page by submitting forms available in the CEE Computer clusters or from the CEE web page to the CEE Business Office. Upon receipt of payment, the business office will notify ISG staff via the helpdesk. ISG will update the print allocation within one working day of being notified that payment was received.

## **28. ISG Responsibilities**

- a. ISG support staff will provide service to CEE computers and software, and will follow the policies outlined above.
- b. ISG support staff will protect the privacy of all users' data, unless requested otherwise by law enforcement officials.
- c. ISG staff will not browse user directories, files, or e-mails, unless required by the School Chair and approved in writing by the Georgia Tech legal department.
- d. ISG staff will only provide passwords to the account owner.
- e. ISG staff will not send passwords by e-mail.
- f. ISG staff will not forward e-mail to another user without the permission of the intended e-mail recipient.
- g. ISG staff will prioritize all requests for service, help, and computer repair, with the assistance of the Associate Chair for Information Technology. Prioritization is as follows: 1) school related servers and networking equipment, 2) CEE computer labs, 3) research related servers, 4) network access and hardware repair for existing faculty/staff computers, and then 5) hardware and software upgrades to individual faculty and staff computers.
- h. In the event that a computer is modified/upgraded by ISG when the user is not available, ISG will leave a note on the computer terminal summarizing the work performed.

## **29. Enforcement of Policies**

- a. The Chair of the School of CEE has the authority to enforce any provisions of the policy statement.
- b. Faculty, staff, and students requesting network access must follow the policies contained in both the CEE Computing and Network Policy and the Georgia Institute of Technology Computer and Network Usage Policy. Violations of computing and network policies are dealt with seriously and can result in loss of computer access privileges and imposition of applicable Georgia Tech disciplinary proceedings.
- c. The Associate Chair for Information Technology has the authority to invoke CEE usage restrictions on student accounts as needed.

- d. The CEE Computer Committee will hear any disputes between individuals and ISG staff.
- e. Faculty and staff shall cooperate fully with ISG and OIT staff and law enforcement officials in the investigation of any network security compromise.

### **30. Policy Revisions**

- a. The CEE Computer Committee will propose updates and changes to the CEE Computing and Network Guidelines and Policy.
- b. The CEE School Chair and OIT shall approve proposed changes to the existing policy before such changes take effect.
- c. The CEE Associate Chair for Information Technology has the authority to modify the CEE Computing and Network Guidelines and Policy immediately in case of an emergency. In such situations, the CEE Computer Committee will call a meeting to address the issue(s).

### **31. Summary Statement**

- a. All employees will comply with the CEE Computing and Network Policy and the Georgia Institute of Technology Computer and Network Usage Policy.
- b. The use of a CEE computer account signifies acceptance of all CEE and OIT computer and networking policies.
- c. The business office will provide a copy of the CEE Computing and Network Policy and the Georgia Institute of Technology Computer and Network Usage Policy to all new employees.

Rev. 02/01

***This portion of the document has been copied from the OIT web page for your information.  
For the latest information, see <http://www.oit.gatech.edu/oithome/policy.html>***

*Georgia Institute of Technology*  
**COMPUTER AND NETWORK USAGE POLICY**

*"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."*

*The EDUCOM Code.*

**1. BACKGROUND AND PURPOSE**

*This document constitutes an Institute-wide policy intended to allow for the proper use of all Georgia Tech computing and network resources, effective protection of individual users, equitable access, and proper management of those resources. This should be taken in the broadest possible sense. This policy applies to Georgia Tech network usage even in situations where it would not apply to the computer(s) in use. These guidelines are intended to supplement, not to replace, all existing laws, regulations, agreements, and contracts that currently apply to these services.*

*Campus units that operate their own computers or networks may add, with the approval of the unit head, individual guidelines which supplement, but do not relax, this policy. In such cases, the unit should inform their users and the Information Resources Security Coordinator in OIT prior to implementation.*

*Access to networks and computer systems owned or operated by Georgia Tech imposes certain responsibilities and obligations and is granted subject to Institute policies and local, state, and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty, reflect community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance. Appropriate use of computing and networking resources includes instruction; independent study; authorized research; independent research; communications; and official work of the offices, units, recognized student and campus organizations, and agencies of the Institute.*

## 2. DEFINITIONS

### 2.1. Authorized use

*Authorized use of Georgia Tech-owned or operated computing and network resources is use consistent with the education, research, and service mission of the Institute, and consistent with this policy.*

### 2.2. Authorized users

*Authorized users are: (1) current faculty, staff, and students of the Institute; (2) anyone connecting to a public information service (see section 6.5); (3) others whose access furthers the mission of the Institute and whose usage does not interfere with other users' access to resources. The policy Access by External Entities to Institute Information Technology Resources (OIT, 11/3/93, and any subsequent revisions) may apply. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.*

## 3. INDIVIDUAL PRIVILEGES

*It is the following individual privileges, all of which are currently existent at Georgia Tech, that empower each of us to be productive members of the campus community. It must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities.*

### 3.1. Privacy

*To the greatest extent possible in a public setting we want to preserve the individual's privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, users must recognize that Georgia Tech computer systems and networks are public and subject to the Georgia Open Records Act. Users, thus, utilize such systems at their own risk.*

### 3.2. Freedom of expression

*The constitutional right to freedom of speech applies to all members of the campus no matter the medium used.*

### 3.3. Ownership of intellectual works

*People creating intellectual works using Georgia Tech computers or networks, including but not limited to software, should consult Determination of Rights and Equities in Intellectual Property (Board of Regents Policy Manual, section 603.03, 2/2/94 and any subsequent revisions), and related Georgia Tech policies.*

### *3.4. Freedom from harassment and undesired information*

*All members of the campus have the right not to be harassed by computer or network usage by others. (See 4.1.3.)*

## *4. INDIVIDUAL RESPONSIBILITIES*

*Just as certain privileges are given to each member of the campus community, each of us is held accountable for our actions as a condition of continued membership in the community. The interplay of privileges and responsibilities within each individual situation and across campus engenders the trust and intellectual freedom that form the heart of our community. This trust and freedom are grounded on each person's developing the skills necessary to be an active and contributing member of the community. These skills include an awareness and knowledge about information and the technology used to process, store, and transmit it.*

### *4.1. Common courtesy and respect for rights of others*

*You are responsible to all other members of the campus community in many ways, including to respect and value the rights of privacy for all, to recognize and respect the diversity of the population and opinion in the community, to behave ethically, and to comply with all legal restrictions regarding the use of information that is the property of others.*

#### *4.1.1. Privacy of information*

*Files of personal information, including programs, no matter on what medium they are stored or transmitted, may be subject to the Georgia Open Records Act if stored on Georgia Tech's computers. That fact notwithstanding, no one should look at, copy, alter, or destroy anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulation). Simply being able to access a file or other information does not imply permission to do so.*

*Similarly, no one should connect to a host on the network without advance permission in some form. People and organizations link computers to the network for numerous different reasons, and many consider unwelcome connects to be attempts to invade their privacy or compromise their security.*

#### *4.1.2. Intellectual property*

*You are responsible for recognizing (attributing) and honoring the intellectual property rights of others.*

#### *4.1.3. Harassment*

*No member of the community may, under any circumstances, use Georgia Tech's computers or networks to libel, slander, or harass any other person.*

*The following shall constitute Computer Harassment: (1) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (4) Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; (5) Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.*

#### *4.2. Responsible use of resources*

*You are responsible for knowing what information resources (including networks) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources or from using them in whatever ways have been proscribed by the Institute and the laws of the State and Federal governments. Details regarding available resources are available in many ways, including consulting your Computing Support Representative (CSR) (see section 6.4), conferring with other users, examining on-line and printed references maintained by OIT and others, visiting the OIT Information Center, and contacting the OIT Helpdesk.*

#### *4.3. Game playing*

*Limited recreational game playing, that is not part of an authorized and assigned research or instructional activity, is tolerated (within the parameters of each department's rules). Institute computing and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a public computing facility must give up that seat when others who need to use the facility for academic or research purposes are waiting.*

#### *4.4. Information integrity*

*It is your responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information that you compile or use. Do not depend on information or communications to be correct when they appear contrary to your expectations; verify it with the person who you believe originated the message or data.*

#### 4.5. *Use of desktop systems*

*You are responsible in coordination with your CSR for the security and integrity of Institute information stored on your personal desktop system. This responsibility includes making regular disk backups, controlling physical and network access to the machine, and installing and using virus protection software. Avoid storing passwords or other information that can be used to gain access to other campus computing resources.*

#### 4.6. *Access to facilities and information*

##### 4.6.1. *Sharing of access*

*Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are responsible for any use of your account.*

##### 4.6.2. *Permitting unauthorized access*

*You may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. (See section 2.2.)*

##### 4.6.3. *Use of privileged access*

*Special access to information or other special computing privileges are to be used in performance of official duties only. Information that you obtain through special privileges is to be treated as private.*

##### 4.6.4. *Termination of access*

*When you cease being a member of the campus community (graduate or terminate employment), or if you are assigned a new position and/or responsibilities within the Institute, your access authorization must be reviewed. You must not use facilities, accounts, access codes, privileges, or information for which you are not authorized in your new circumstances.*

#### 4.7. *Attempts to circumvent security*

*Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by system administration personnel.*

##### 4.7.1. *Decoding access control information*

*You are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.*

#### 4.7.2. Denial of service

*Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Institute computer system or network are prohibited.*

#### 4.7.3. Harmful activities

*The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software, or data belonging to Georgia Tech or other users; and the like.*

#### 4.7.4. Unauthorized access

*You may not:*

- \* damage computer systems*
- \* obtain extra resources not authorized to you*
- \* deprive another user of authorized resources*
- \* gain unauthorized access to systems*

*by using knowledge of:*

- \* a special password*
- \* loopholes in computer security systems*
- \* another user's password*
- \* access abilities you used during a previous position at the Institute*

#### 4.7.5. Unauthorized monitoring

*You may not use computing resources for unauthorized monitoring of electronic communications.*

#### 4.8. Academic dishonesty

*You should always use computing resources in accordance with the high ethical standards of the Institute community. Academic dishonesty (plagiarism, cheating) is a violation of those standards.*

#### 4.9. Use of copyrighted information and materials

*You are prohibited from using, inspecting, copying, and storing copyrighted computer programs and other material, in violation of copyright.*

#### 4.10. Use of licensed software

*No software may be installed, copied, or used on Institute resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.*

#### *4.11. Political campaigning; commercial advertising*

*Board of Regents policy (section 914.01) states "The use of System materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden." The Georgia Tech Faculty Handbook (section 6.15.3.8(b)) states "Political campaign and commercial advertisement shall not be displayed on the campus." The use of Institute computers and networks shall conform to these policies.*

#### *4.12. Personal business*

*Computing facilities, services, and networks may not be used in connection with compensated outside work nor for the benefit of organizations not related to Georgia Tech, except: in connection with scholarly pursuits (such as faculty publishing activities); in accordance with the Institute Consulting Policy or the policy Access by External Entities to Institute Information Technology Resources (OIT, 11/3/93, and any subsequent revisions); or in a purely incidental way. This and any other incidental use (such as electronic communications or storing data on single-user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive. State law restricts the use of State facilities for personal gain or benefit.*

### *5. GEORGIA TECH PRIVILEGES*

*Our society depends on institutions like Georgia Tech to educate our citizens and advance the development of knowledge. However, in order to survive, Georgia Tech must attract and responsibly manage financial and human resources. Therefore, Tech has been granted by the State, and the various other institutions with which it deals, certain privileges regarding the information necessary to accomplish its goals and to the equipment and physical assets used in its mission.*

#### *5.1. Allocation of resources*

*Georgia Tech may allocate resources in differential ways in order to achieve its overall mission.*

#### *5.2. Control of access to information*

*Georgia Tech may control access to its information and the devices on which it is stored, manipulated, and transmitted, in accordance with the laws of Georgia and the United States and the policies of the Institute and the Board of Regents.*

### 5.3. *Imposition of sanctions*

*Georgia Tech may impose sanctions and punishments on anyone who violates the policies of the Institute regarding computer and network usage.*

### 5.4. *System administration access*

*A System Administrator (i.e., the person responsible for the technical operations of a particular machine) may access others files for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.*

### 5.5. *Monitoring of usage, inspection of files*

*Units of Georgia Tech operating computers and networks may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, etc. These units may review this data for evidence of violation of law or policy, and other purposes. When necessary, these units may monitor all the activities of and inspect the files of specific users on their computers and networks. Any person who believes such monitoring or inspecting is necessary must obtain the concurrence of the unit head and the campus Legal Division. In all cases all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.*

### 5.6. *Suspension of individual privileges*

*Units of Georgia Tech operating computers and networks may suspend computer and network privileges of an individual for reasons relating to his/her physical or emotional safety and well being, or for reasons relating to the safety and well-being of other members of the campus community, or Institute property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the Office of the Vice President for Student Services (for students) or the employee's department in consultation with the Office of Human Resources (for employees).*

## 6. *GEORGIA TECH RESPONSIBILITIES*

### 6.1. *Security procedures*

*Georgia Tech has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, however stored, and to impose appropriate penalties when privacy is purposefully abridged.*

### 6.2. *Anti-harassment procedures*

*Georgia Tech has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment by use of its computers or networks and to impose appropriate penalties when such harassment takes place.*

### *6.3. Upholding of copyrights and license provisions*

*Georgia Tech has the responsibility to uphold all copyrights, laws governing access and use of information, and rules of organizations supplying information resources to members of the community (e.g., acceptable use policies for use of Internet).*

### *6.4. Individual unit responsibilities*

*Each unit has the responsibility of:*

- \* enforcing this policy*
- \* providing for security in their areas*
- \* providing individuals equipped with Institute-owned desktop systems with resources for regular disk backups (software, hardware, media, and training) and for virus protection*

*If warranted by the importance and sensitivity of information stored and processed in their facility, a unit must also:*

- \* provide system administration personnel*
- \* perform and verify integrity of regular media backups*
- \* employ appropriate security-related software and procedures*
- \* guard confidentiality of private information, including user files and system access codes*
- \* control physical access to equipment*
- \* provide proper physical environment for equipment*
- \* provide safeguards against fire, flood, theft, etc.*
- \* provide proper access administration; e.g., prompt and appropriate adjustment of access permissions upon a user's termination or transfer*
- \* control and record system software and configuration changes*
- \* monitor system logs for access control violation attempts*

*Units are to designate a person employed by the unit as their Computing Support Representative (CSR); the Director of Client Services, Office of Information Technology is to be notified of CSR appointments. CSRs should be knowledgeable about their unit's computing environment and about central resources and services. The CSR serves:*

- \* as the first point of contact for unit personnel seeking problem resolution, information, and other assistance regarding computing and networking*
- \* to facilitate interaction between the unit and the Office of Information Technology*

## 6.5. *Public information services*

*Units and individuals may, with the permission of the appropriate unit head, configure computing systems to provide information retrieval services to the public at large. (Current examples include "anonymous ftp" and "gopher.") However, in so doing, particular attention must be paid to the following sections of this policy: 2.1 (authorized use [must be consistent with Institute mission]), 3.3 (ownership of intellectual works), 4.2 (responsible use of resources), 4.9 (use of copyrighted information and materials), 4.10 (use of licensed software), and 6.4 (individual unit responsibilities). Usage of public services must not cause computer or network loading that impairs other services.*

## 7. *PROCEDURES AND SANCTIONS*

### 7.1. *Investigative contact*

*If you are contacted by a representative from an external organization (District Attorney's Office, FBI, GBI, Southern Bell Security Services, etc.) who is conducting an investigation of an alleged violation involving Georgia Tech computing and networking resources, inform the office of the Executive Director for Information Technology (EDIT) and the Chief Legal Advisor immediately. Refer the requesting agency to the EDIT office; that office will provide guidance regarding the appropriate actions to be taken.*

### 7.2. *Responding to security and abuse incidents*

*All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of Georgia Tech computers, networks, or other information processing equipment. If you observe, or have reported to you (other than as in 7.1 above), a security or abuse problem with any Institute computer or network facilities, including violations of this policy:*

*\* Take immediate steps as necessary to ensure the safety and well-being of information resources. For example, if warranted, a system administrator should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 5.6).*

*\* Ensure that the following people are notified: (1) your Computing Support Representative, (2) your unit head, (3) the Information Resources Security Coordinator (IRSC), who is located within the Office of Information Technology.*

*The IRSC will coordinate the technical and administrative response to such incidents. Reports of all incidents will be forwarded to Student Services (for apparent policy violations by students) or the unit head (for employees), and to the Executive Director for Information Technology and the Chief Information Officer.*

### *7.3. First and minor incident*

*If a person appears to have violated this policy, and (1) the violation is deemed minor by OIT, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the OIT or unit level. The alleged offender will be furnished a copy of the Institute Computer and Network Usage Policy (this document), and will sign a form agreeing to conform to the policy.*

### *7.4. Subsequent and/or major violations*

*Reports of subsequent or major violations will be forwarded to Student Services (for students) or the unit head (for employees) for the determination of sanctions to be imposed. Units should consult the Office of Human Resources regarding appropriate action.*

### *7.5. Range of disciplinary sanctions*

*Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the Institute, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws; the Institute will carry out its responsibility to report such violations to the appropriate authorities.*

### *7.6. Appeals*

*Appeals should be directed through the already-existing procedures established for employees and students.*

*Rev. 8/94*