

Ivan Allen College
Georgia Institute of Technology

Computer and Network Usage Policy

December, 2004

Ivan Allen College
Computer and Network Usage Policy

Contents

1. Overview.....	3
2. Applicability	3
3. User Accounts	4
4. Passwords.....	4
5. Email Accounts.....	4
6. Email Software Support.....	5
7. Use of IAC Computing Facilities	5
8. Connecting to the Network	5
9. Off-Campus Access to Resources.....	5
10. Acceptable Use/Traffic	5
11. New Equipment	6
12. Equipment Inventories and Equipment Moves.....	6
13. Disposition of Old Equipment	6
14. Shared Equipment Checkout.....	7
15. Taking Equipment Home	7
16. Sources of Computing Support.....	7
17. Software Licenses	8
18. Educational Computing Resources and Software Requests	8
19. Security Sweeps	8
20. Anti-Virus Software.....	8
21. Supported Software/Operating Systems	8
22. Disk Shares and Backups.....	9
23. Web Pages Published on IAC Computers	9
24. Printing Limitations	9
25. Support Staff Responsibilities.....	9
26. System Administration.....	10
27. Backups/Disaster Recovery	11
28. Patches/Updates	11
29. Log Monitoring.....	11
30. Virus/Worm control.....	11
31. Network Physical Security.....	11
32. Password Protection (encryption).....	11
33. Logon Banners	12
34. Security Incident Response.....	12
35. Accountability and Auditing.....	12
36. Copyright Issues.....	12
37. Enforcement of Policies.....	12
38. Policy Revisions.....	13
39. Summary Statement	13

**Ivan Allen College
Computer and Network Usage Policy (CNUP)
December 2004**

Purpose

The IAC Computer and Network Usage Policy (CNUP) is intended to provide IAC faculty, staff, and students with information regarding the use of IAC computers and networks. It is designed to provide an appropriate balance of access and security. The information security policy and procedures included in the IAC CNUP are designed to facilitate research and teaching within an environment which assures:

- safeguarding of Tech-owned hardware and software
- elimination of illegal use of software
- protection of the IAC and Georgia Tech network
- protection of IAC data

Sources of the Policy

The IAC CNUP conforms with Georgia Tech policy on computer use as expressed in the *Georgia Tech Computer and Network Usage Policy*, *Security Policy*, the *Georgia Tech Faculty Handbook*, and the *Georgia Tech Statutes*, and it applies these documents to the IAC environment.

General Policy

The IAC CNUP, with its provisions for the protection of information security, attempts to insure that members of the IAC community can protect physical assets, safeguard the integrity of the network, protect the integrity of data, and assure privacy and freedom from harassment for all in the community. It does this by assigning specific responsibilities to each member of the community.

1. Overview

- a. This document is the “Ivan Allen College (IAC) Computing and Network Policy” (CNUP).
- b. All users of IAC computer facilities are bound by the policies described in this document.
- c. IAC faculty, staff, and students should direct questions about implementation of this policy to IAC Computer Support. Suggestions or queries about the overall intent of the policy should be sent to their School’s representative on the IAC Information Technology Council.

2. Applicability

This policy applies to all faculty, staff, and students employed by or enrolled in the Ivan Allen College (IAC) and other individuals using IAC facilities. This policy applies to all

computers and networking services owned by IAC and all computers and networking services located in Ivan Allen College (IAC) facilities.

3. User Accounts

- a. IAC Computer Support assigns each computer account, including a unique username and password, to one individual. Use of an account by more than one individual is strictly prohibited. Users will login to a IAC computer system and/or attached network using a user id and password assigned only to them.
- b. When possible, authentication through OIT's centralized authentication servers using GT Account username and passwords should be implemented in lieu of locally assigned and managed usernames and passwords.
- c. IAC Computer Support will create a user ID and password for new or returning employees when notified by the IAC staff. This policy also applies to temporary staff.
- d. IAC Computer Staff will create a user ID and password for students only when requested by faculty or administrative staff.
- e. IAC Administrative Staff will notify IAC Support promptly when an employee leaves IAC so that login accounts and network access can be disabled.

4. Passwords

- a. All IAC computer passwords expire automatically 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 contain a minimum of 7 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. Passwords must not be written down anywhere that is readily available during a casual search of a person's work area.
- d. IAC Computer Support staff will reset IAC student, faculty and staff passwords for their account upon request. Requests for new or reset passwords should be sent to the appropriate IAC helpdesk email address (helpdesk@iac.gatech.edu or lcc-support@iac.gatech.edu). New passwords will not be sent to users via email.

5. Email Accounts

- a. The official method of Institute and IAC communications to all faculty, staff and students is by e-mail to the e-mail address of record. The faculty and staff e-mail address of record for IAC, the Georgia Tech Office of Information Technology, and Georgia Tech Human Resources is the e-mail computer account administered by OIT, formatted as `firstname.lastname@[unitname].gatech.edu`. This address shall serve as the official e-mail address on all written and electronic communications, from e-mail to business cards. It is the responsibility of all IAC faculty, staff, and students to check this official point of contact on a regular basis
- b. The use of email accounts outside of Georgia Tech for the conduct of Georgia Tech business is not recommended. Some organizations that host such email accounts also claim intellectual property rights on the content of email sent to/from their servers. Since Georgia Tech does not release intellectual property rights without written permissions, users of such accounts may be in violation of Georgia Tech intellectual property

regulations. Therefore, IAC personnel should always use OIT computer accounts rather than other email accounts such as Hotmail, Yahoo, etc. Note that use of Internet Service Providers (ISP's) such as Earthlink to connect to Georgia Tech email systems is fully permissible and does not compromise any intellectual property rights.

6. Email Software Support

IAC Computer Support supports only OIT-approved clients that are configured to access OIT email accounts. Third party email providers and clients will not be supported by IAC Computer Support.

7. Use of IAC Computing Facilities

- a. Food, drink, and tobacco products are not permitted in any IAC computing lab at any time for any reason.
- b. Computers in IAC computing labs require a user id and password.
- c. Computers in IAC labs may be erased and re-imaged during each semester. Prior notice of disk re-imaging will not be provided. Notice of this policy will be clearly posted in each lab as a reminder to not save important files on the local hard drive of any lab computer.
- d. Users will not encrypt files on any IAC system unless approved by IAC Computer Support and the user provides IAC Computer Support with the encryption key

8. Connecting to the Network

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

9. Off-Campus Access to Resources

- a. Only OIT-approved methods may be used to access Georgia Tech and IAC computer resources from off campus. Users shall not access, nor allow others to access, IAC computers in any manner not specifically approved by IAC.
- b. Computers linked to the IAC network shall not receive calls via modem

10. Acceptable Use/Traffic

All IAC users will conduct themselves in a fashion that represents Georgia Tech and IAC in a professional manner in all forums of electronic information (e.g. e-mail, web pages, etc.).

11. New Equipment

- a. All new computer-related equipment will be configured by or approved by IAC Computer Support staff and purchased from preferred vendors in order to minimize the number of different brands, models, sizes and versions of equipment.
- b. IAC Administrative staff will route all new machines directly to IAC Computer Support upon arrival at the School so that IAC Computer Support can open the boxes, inventory the new equipment, and apply appropriate GT property stickers. IAC staff will notify the faculty or staff member that their new equipment has arrived in IAC. When notified by IAC Computer Support that the equipment has arrived, the faculty or staff member will provide IAC Computer Support with a list of software that they need installed on the machine. This will allow IAC to develop a software installation order that will minimize installation conflicts. IAC Computer Support will deliver the equipment and software installation order to the faculty or staff member within three to five 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 IAC.
- c. Only IAC Computer Support staff shall install network-related software and set up the computer for network access.
- d. Only IAC Computer Support staff shall plug the new computer into an IAC network port.

12. Equipment Inventories and Equipment Moves

- a. IAC Computer Support staff will maintain an inventory of all computer equipment.
- b. IAC Computer Support staff must approve all equipment moves (excepting laptop computers).

13. Disposition of Old Equipment

- a. Institute inventory guidelines require IAC staff to document the removal of any components from an existing IAC machine. Faculty, staff and students may not remove, exchange or discard components from existing machines without the written approval of IAC Computer Support.
- 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 IAC Computer Support, and request that IAC Computer Support remove the equipment. Hard disks will be removed and destroyed before equipment is surplus or discarded.
- 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 School Chair or designee.
- e. Sponsored project principal investigators may distribute or redistribute computer equipment purchased with research funds.

14. Shared Equipment Checkout

- a. IAC faculty and staff may check out portable equipment for use in the classroom and for seminars. The portable equipment must be reserved in advance; IAC Computer Support will publicize the lead time required for equipment reservations. Reservations are on a first come, first serve basis.
- b. Individuals must schedule a time with the School or IAC Computer Support to pick up the reserved equipment. If the user does not pick up the equipment by the time of the reservation, the equipment may be redirected to others who request the equipment.
- c. Users will return the equipment immediately after its use, even if the equipment is reserved multiple times in the day (unless approved by IAC Computer Support).

15. Taking Equipment Home

- a. An employee may take IAC equipment home for a limited period of time only with the explicit permission of the School Chair and in strict compliance with the following procedures.
- b. To ensure that Institute insurance covers the equipment, a standard equipment loan agreement form must be completed by the employee, approved by the School Chair, and submitted to the appropriate IAC Computer Support Office. This requirement does not apply to removable storage devices such as flash memory drives.
- c. Faculty and staff may only use an IAC computer at home if the user purchases, installs and operates a current version of a virus scanning software approved by IAC staff and performs regular updates of the virus software. If the computer connects to the Internet via a service provider (e.g. AOL, Earthlink, etc), the user must also utilize a host-based firewall software package (i.e. ZoneAlarm) approved by IAC staff.
- d. IAC Computer Support staff will not service IAC computers at an employee's home. It is the responsibility of the individual to bring the computer to campus for service.

16. Sources of Computing Support

- a. IAC Computer Support is responsible for providing support for all approved IAC computer systems. All support of Institute-owned or licensed equipment must come from (or be approved by) IAC Computer Support staff. IAC Computer Support must approve any service contracts.
- b. Faculty should consult IAC Computer Support staff prior to purchasing new computer 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 IAC.
- c. Computers owned by faculty, staff and students may not be connected to IAC's network without specific approval of IAC Computer Support. IAC shall ensure that the computer meets any applicable hardware and software security-related specifications and IAC Computer Support shall install such standard security provisions when purchased and provided by user.
- d. IAC Computer Support cannot support any personally owned computers.

17. Software Licenses

- a. IAC 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. IAC Computer Support staff will only install software when provided a copy of the valid software license agreement allowing the software placement on the computer.
- c. IAC will retain either the original license or a copy of the original license for all software installed on all IAC computers. Users shall supply copies of any original licenses to IAC staff upon request.
- d. IAC Computer Support will store the original software license agreement (or the copy of the license agreement) in a folder dedicated to license information. IAC will also retain the original purchase order and other technical specification sheets.
- e. When original software agreements are not retained in the IAC Computer Support filing system, faculty and staff must be able to provide the original license agreements to any GT OIT representative or a law enforcement official for inspection and verification. When IAC does not maintain original software in the IAC filing system, faculty, staff and students must also ensure that the original software media is available for inspection upon request.
- f. IAC Computer Support staff will not install IAC-owned software on personally owned computers.

18. Educational Computing Resources and Software Requests

Faculty may request software purchase and installation in IAC computer labs for IAC courses. Faculty and staff should direct such software requests to the IAC Information Technology Council for consideration. Software requests should be made two months prior to the date which the software is needed in the computer labs. The number of licenses that IAC must purchase depends upon the requirements of the software license agreement.

19. Security Sweeps

- a. OIT and/or IAC CS perform automated and targeted network security scans on all IAC 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 IAC CS identifies unapproved services or a security breach that threatens IAC systems or data, IAC CS will immediately disconnect the computer from the network. IAC will immediately notify the user of the problem and schedule a meeting with the Administrator to repair the problem.

20. Anti-Virus Software

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

21. Supported Software/Operating Systems

- a. IAC CS staff strives to support as many hardware and software configurations as possible. However, IAC staff cannot support every operating system and software

package. When appropriate, IAC CS will be assigned to assist with operating systems and software packages based on special proficiency. The IAC Information Technology Council determines which computing environments and software packages IAC supports. Unless referenced otherwise, the latest version of each product is supported:

- Hardware, PC Platforms – Dell
 - Hardware, Apple Platforms - Apple
 - Hardware, Unix Platforms – Dell
 - Operating Systems, PC Platforms – Windows 2000, XP
 - Operating Systems, Apple Platforms –OSX
 - Operating Systems, Unix Platforms – RedHat Linux
- b. IAC CS will consider supporting additional software packages upon request on a case-by-case basis.

22. Disk Shares and Backups

- a. IAC CS staff will maintain a disk share on the server for each administrative staff member. Quotas for disk share size will be established by the IAC Information Technology Council, which will also consider requests for exceptions to those allocations.
- b. IAC will provide backup service on approved disk shares. These common disk shares on the server will be backed up by IAC CS on a daily basis.
- c. IAC will provide document backup services for each faculty and staff member. Backups will occur at least once a week.

23. Web Pages Published on IAC Computers

- a. Faculty and staff will comply with all applicable Georgia Tech policies pertaining to web publishing (see http://www.oit.gatech.edu/information_security/policy/www.html).
- b. Web pages must be free from copyrighted text (e.g., journal papers), tables, figures, graphics, etc., unless the copyright owner provides written permission.

24. Printing Limitations

- a. All printers in the IAC computer labs, and in research labs at the decision of the lab manager, are subject to printing limitations.
- b. Students enrolled in IAC courses may use printers in lab classrooms only for uses directly related to the IAC course.

25. Support Staff Responsibilities

- a. IAC Computer Support staff will provide service to IAC computers and software, and will follow the policies outlined in this document.
- b. IAC Computer Support staff will protect the privacy of all users' data in accordance with the Georgia Tech CNUP.
- c. IAC CS 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. IAC CS staff will provide passwords only to the account owner. IAC CS staff will not send passwords by e-mail.
- e. IAC CS staff will prioritize all requests for service, help, and computer repair, with the assistance of the IAC Information Technology Council. Prioritization is as follows:

1) school related servers and networking equipment, 2) IAC classrooms and 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.

f. In the event that a computer is modified/upgraded by IAC Computer Support when the user is not available, IAC CS will leave a note on the computer terminal summarizing the work performed.

26. System Administration

IAC Computer Support is the primary Administrator of all computers connected to the IAC network in IAC facilities. As such, IAC must have administrator or root access on all IAC network-connected computers.

a. Desktop Computers:

i. IAC Computer Support will verify that every system has a qualified system administrator that is coordinated with IAC Computer Support. IAC Computer Support will have access and authority to perform any routine support for all computers connected to the IAC network in IAC facilities.

ii. Faculty/staff administrators may not start any network-related services or change any network setting on any machine without the explicit approval of IAC Computer Support. Network-related services include Web Servers, Mail Servers, FTP, Remote Access, DHCP, DNS, WINS, and other services defined by IAC.

iii. The faculty/staff administrators will not share the administrative password with other individuals nor allow administrative access to any user other than IAC computer support.

iv. Only IAC Computer Support shall perform routine equipment maintenance or support on the computer. Only IAC-approved contractors may provide supplemental support for IAC computers. The scheduling of any maintenance or support work should be scheduled through IAC Computer Support.

v. Should an Administrator find any evidence of suspicious activity on a machine, the administrator will leave all evidence intact and contact OIT Information Security immediately.

vi. If IAC Computer Support determines that any system constitutes an immediate security threat to IAC or Georgia Tech systems or data, IAC Computer Support will immediately remove the system from the network until the problem is resolved. IAC CS will attempt to notify the faculty/staff administrator of this action.

b. Servers:

i. IAC faculty and staff will not be granted administrative access to any IAC servers. Administrator passwords for IAC Servers will be written to a file and encrypted so that each IAC Computer Support member will have access to them.

ii. IAC Computer Support will not use the Administrator account for regular day-to-day use of any server. 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).

iii. IAC Administrator will maintain a record (change log) of all major changes to a server, including but not limited to configuration changes, software and hardware

upgrades and installations. This record must be accessible to all IAC Computer Support members

27. Backups/Disaster Recovery

- a. IAC Computer Support must have a system implemented, maintained, managed and tested that duplicates and preserves critical data. Depending on the importance of the information, some duplicate copies of the data may be kept “off-site”, or preserved against physical damage from fire, water, theft, erasure, etc.
- b. IAC Computer Support will regularly test backup systems to ensure that data can be recovered, starting from the assumption that the original data and the hardware on which it was stored is not available. At least one test is required when the system is implemented, and again when major components of the system change

28. Patches/Updates

- a. IAC Computer Support shall monitor published information from the appropriate Georgia Tech mailing lists and, where appropriate, various security sources and vendors related to security risks on the computer systems they support.
- b. IAC Computer Support shall download or purchase the appropriate vendor-recommended patches, updates, fixes, scripts, etc that will mitigate reported security risks on a regular basis or immediately as needed. OIT will test patches within 48 hours to ensure that enterprise-level applications are compatible with patches

29. Log Monitoring

The IAC Computer Support system administrator (currently the IAC IT Program Manager) shall read server logs on a regular basis for the purpose of becoming familiar with the day-to-day activity of our servers and network so that deviations from the activity can be detected and addressed as potential threats to security.

30. Virus/Worm control

IAC Computer Support shall ensure that every server and desktop connected to the IAC network is outfitted with an anti-virus commercial software package that is set up to receive regular automated virus definition updates.

31. Network Physical Security

- a. Major file and computing servers will be placed in limited access rooms. At least one full copy of a system backup should be stored away from the system or off-site.
- b. Individual computers (for one person’s use) should be in rooms that are locked during non-worked hours, and secured by cables and locks.
- c. Computers physically accessible to more than one user should have password-protected screen savers enabled.

32. Password Protection (encryption)

All passwords that travel over the network to IAC resources must be encrypted. Services that do not provide encrypted password transport over the network must not be offered outside the IAC sub domain.

33. Logon Banners

All computers and remote users communications facilities within IAC, if capable, must be configured to display a pre-logon banner, which explicitly states that unauthorized access is prohibited; the banner may optionally include a reference to the GT Computer and Network Usage Policy. GT Information Security shall determine the exact wording of the pre-logon banner, in consultation with GT Legal.

34. Security Incident Response

- a. All actual or suspected instances of information technology abuse or information asset theft, as well as potential threats, will be reported at once to the IAC CS and the School Chair.
- b. All serious or potentially serious incidents will be reported by departmental computer support to GT Information Security.
- c. IAC Computer Support will have a recovery plan prepared for the case of both server and desktop security incidents.

35. Accountability and Auditing

- a. On systems which can have effective access controls (e.g. Windows 2000, Linux), a login process should always be required which can potentially capture the userID of the person logging on and the time at which they logged on and off. On systems where the security need is higher, the capture of the information should be enabled, and the audit log scanned on a regular basis. For remote user communication facilities, the information should always be captured and saved, and backed up for a defined period of time, and if possible, regularly analyzed for evidence of attempted security breaches.
- b. System auditing on servers must be enabled, and a regular scan of the audit files must be performed by IAC Computer Support – manually or automatically – to detect unusual events.

36. Copyright Issues

- a. IAC recognizes the copyrights of individual software providers.
- b. IAC recognizes the copyrights of web pages and the information contained within those sources. IAC does not allow copying of material created by others onto the School's web servers without written permission from the copyright owner. C. Plagiarism and copyright infringement are in direct violation of the Georgia Tech CNUP and will not be tolerated.
- d. Given the limited disk space and computation resources available for IAC faculty/staff/students, IAC does not allow the presence of non-project related multimedia files on its servers, desktop systems, or lab computers.

37. Enforcement of Policies

- a. Faculty, staff, and students requesting network access must follow the policies contained in both the IAC 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.

b. Faculty and staff shall cooperate fully with IAC and OIT staff and law enforcement officials in the investigation of any network security compromise.

38. Policy Revisions

- a. A final draft of this Policy, when approved by OIT and the Georgia Tech Counsel, is binding on all members of IAC and cannot be modified without approval of the IAC Dean, OIT, and the Georgia Tech Counsel.
- b. Georgia Tech regulations allow the Dean of the Ivan Allen College to make temporary modifications to the IAC Security Policy when necessary. Such modifications must be done in writing, may not violate Georgia Tech policy, and can be in effect for no longer than six months. IAC School Chairs must make modifications requests to the IAC Associate Dean with responsibility for Information Technology. If necessary, the IAC Information Technology Council will propose updates and changes to the IAC Computing and Network Guidelines and Policy.

39. Summary Statement

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