Auburn University Network Policy

Chapter 1: Introduction

The **Information Technology (IT)** network is an inter-network of local area networks (LANs) located in various buildings on the Auburn University campus. These LANs, sometimes referred to as subnets, are connected together with other departmental LANs to form the **Auburn University network (AUNET)**. **AUNET** is connected to the Alabama Research and Education Network (AREN) which is connected to the worldwide Internet.

Computing resources maintained by OIT and connected to the OIT network include the OIT **Sun Network**, the central **AU Web server** (www.auburn.edu), Windows web servers (fp.auburn.edu and oitapps.auburn.edu), a streaming media server (rm.auburn.edu), the Blackboard servers, database servers, the machines in the OIT **Labs**, the **AU Office** servers and **GroupWise** servers.

The purpose of this manual is to explain the policies and guidelines that have been developed to insure effective and appropriate use of OIT computing resources and network services. More information about specific services is available from the OIT Web site.

Chapter 2: User Accounts

User accounts are required to access the OIT host computers, OIT Lab machines, AU Access and administrative computing resources. Accounts are provided free of charge to AU faculty, staff, and currently enrolled students. Each user's account name is the same as his or her unique **username**, which is composed of seven characters. Once activated, accounts remain active as long as the user is enrolled or employed by Auburn University, and may not be changed. Retirees retain Auburn University usernames.

Requests for **faculty and staff account services** should be made through the appropriate departmental Administrative Computing Coordinator (ACC). ACCs work with the OIT **Accounts Administrator** to establish and customize each faculty and staff computing profile, including e-mail addressing, access to administrative records, and other computing resources.

Student accounts on the OIT Sun Network are generated automatically when a student is enrolled. Student accounts expire after the second term for which the student is not enrolled.

On the OIT Sun Network, each account belongs to the default access group called "other". Additional group membership may be obtained for work groups, projects, etc. and should be requested by e-mail to helpdesk@auburn.edu.

Section 2.1 Eligible Users

All AU faculty, staff, and students (enrolled for the current term) are eligible for **usernames**.

The OIT **Sun Network** is available to all faculty, staff and students. Use of the IBM mainframe is restricted to employees. Student employees are granted access to the IBM mainframe by appropriate departmental request.

Group accounts are intended for use by small, well-defined units, and requests are granted only in exceptional cases and for organizations supported by the general fund. Student groups desiring **organizational e-mail** capabilities should contact the OIT Accounts Administrator to establish a mail list or submit an **Account Update Form** to create an **e-mail alias** for the group.

Guest accounts are provided given that certain requirements are met. Please read Section 2.2 Sponsored Guest Accounts for more information.

Retired AU employees may request a computing account by providing a copy of the **retired username** and submitting a **Computing Access Request Form** to the OIT **Accounts Administrator**. The retiree keeps his or her current username and e-mail address.

Section 2.2 Sponsored Guest Accounts

Sponsored guest accounts are available for individuals not otherwise eligible as an employees or contracted agents. They must be sponsored by a University department and there must be a direct relationship to Auburn University's academic mission or business function. Alumni, employee spouses and their dependents who are not directly involved in the University mission are not eligible.

Sponsored guest accounts are billable and may be paid by the sponsoring department or by the individual. These accounts are valid for the length of time they are needed and are billed on a monthly basis.

Requirements for a sponsored guest account:

- Sponsorship letter from the department head indicating the mission/business function relationship.
- Billing information, departmental account or individual billing information.

Section 2.3 Appropriate Use

Usernames are provided for academic research and instruction, electronic mail, Internet access, and for activities related to the mission of Auburn University. Each account represents an allocation of computing resources and as such is monitored by OIT administrators for appropriate use. Each username is assigned for the sole use of a single user. Sharing of usernames is prohibited. The user for whom the account was created is responsible for the security of the account and all actions associated with its use. An account may be revoked if it is found to have been used for activities that violate any portion of this policy, the owner of the username has been found violating any portion of this policy, or the owner of the username is no longer enrolled or employed by Auburn University. Activation of an account on an OIT host computer constitutes an agreement stating that the user understands and will abide by all policies regarding the use of the OIT network.

NOTE: Any usage of an OIT computer for an activity that violates any local, state or federal regulation is considered a serious violation of OIT network policy even though that activity may not be explicitly referred to in this document.

Section 2.4 Inactive Accounts

Active accounts are changed to the inactive state prior to deletion. The inactive state is an intermediate step between an active account and a deleted account. In the inactive state, all host access is denied and electronic mail addressed to the account is returned to the sender. Some files may be archived and deleted. An account may be re-activated from the inactive state as long as it has not actually been deleted. When an account is deleted, the username is considered unused, and all files in the user's home directory are deleted, and electronic mail sent to the user is rejected.

Section 2.5 Restricted Accounts

On occasion an account may be temporarily restricted. There are many reasons why this may occur, ranging from misuse of network resources, to important information that needs to be given to the user before they attempt to log in again. Upon attempting to log in, the user sees a short message to the effect of "Please see the System Administrator", and the user is immediately logged out. In most cases, once a meeting with the System Administrator is completed, the account is reinstated.

Section 2.6 Sharing Accounts

Any abusive activities initiated from a username are traced back to the person assigned that username, and the owner of the username is held accountable. The behavior of someone with whom you have shared your account becomes your responsibility. If the abuse is such that network privileges are terminated, it is the username owner (you) who suffers. Therefore, it is the policy of OIT that usernames are not to be shared. Each username has only one authorized user. If users wish to share information or otherwise collaborate in a group, then the users shall use appropriate file permissions combined with appropriate group membership to share data.

In the case of group accounts, the sponsoring department head is responsible for the activity conducted under the username. A group username is subject to inactivation or deletion in cases of account misuse.

Section 2.7 Determining Account Misuse

Often users are the first persons to detect unauthorized use of their accounts. If this occurs, please immediately contact the OIT HelpDesk (334-844-4944 or helpdesk@auburn.edu).

- Stolen passwords and account misuse

Chapter 3: Security

Section 3.1 Selecting a Password

Perhaps one of the most vulnerable parts of any computer system is the username password. Any computer system, no matter how secure it is from network or dial-up attack, Trojan horse programs, and so on, can be fully exploited by intruders who can gain access via a poorly chosen password. It is important to select a password that is not easily guessed and to not share the password with ANYONE.

- Selecting a strong password

Section 3.2 Changing Your Password

It is your responsibility to change your password. You should change your password periodically, usually every three months. Selecting strong passwords and changing your password on a regular basis will frustrate even the most patient intruder.

Students who forget their password should bring a picture ID to the OIT HelpDesk office in the RBD Library (1st Floor).

Faculty and **staff** who forget their password may contact the OIT HelpDesk by phone at 844-4944.

- Reset password screen
- Forgotten passwords

Section 3.3 Sharing and Protecting Data

Users are responsible for assigning the permissions for files and directories.

By default, OIT **Sun Network** accounts are created such that all files and directories created by the user are readable, writable, and executable only by the user. For informational uses, the user's home directory is executable by others but not readable or writable by others. The change mode (chmod) command may be used to change permissions on files and directories so that data may be shared or protected. Users may request access groups containing specified user names be set up to control access to data on the Sun Network.

- Understanding unix file permissions

(NOTE: Changing the permissions of your home directory on the OIT Sun Network so that it is world writeable (chmod 777) is considered a breach of security.

Security of central administrative systems is controlled by the Administrative Computing Coordinators and the OIT Accounts Administrator. Administrative data should be safeguarded in accordance with the Data Security Policy.

Section 3.4 Use of .rhosts Files

The use of **.rhosts** files is prohibited on the OIT Sun Network. The purpose of .rhosts files is to allow unauthenticated execution of commands remotely from accounts on remote hosts specified in the file. Since it is possible to set up a computer so that it appears to be a remote host with a particular account, .rhosts files are a threat to the security of the entire system, even when used properly. When used improperly, as they often are, they are even more dangerous. All they offer is the convenience of not having to enter a password when you execute commands from the remote system. The man hours that would have to be devoted by OIT system administrators to safeguarding the Sun systems from improper .rhosts files are better utilized improving the services that we offer.

Chapter 4: Rights and Responsibilities of Users

An username provides access to the Internet and a multitude of resources, including web hosting, web-based instructional and collaborative tools, e-mail, Directory Services, list-servers, OIT computing labs, and network printing services.

Section 4.1 Use of Licensed Software

OIT provides access to a suite of supported software applications on its host computers and on the OIT Lab machines. Various licensing arrangements have been negotiated to provide this software. In some cases, OIT has purchased a copy of the software for each machine. In other cases, software packages have "floating node" licenses that limit the number of concurrent users.

Copyrighted and licensed software and documentation may not be duplicated unless the license explicitly states that it may be copied. Copying software to diskette or to an unauthorized machine is not only a violation of OIT policy, but it also violates various state and federal laws.

Section 4.2 Use of CPU Cycles on Host Computers

The combined processing power available to users by the various hosts and servers on the OIT network is substantial. However, a large computational task on a machine can make the machine so slow as to be nearly unusable for other users.

OIT reserves the right to kill any process or break any network connection that it determines is adversely affecting the system or the rights of other users.

Section 4.3 Use of Sun Storage Resources

All OIT Sun Network accounts are created with a disk quota that limits the amount of disk space a user can access. This space is called the user's "home directory". Personal web space is also available within the same space in a directory named **"public_html"**. A user has access to this space when he or she logs into the OIT Sun network remotely. The home directory is also available to the user as **drive H:** (and the web space as drive P:) whenever the user is logged into an OIT lab machine.

There is an assigned disk quota for students, faculty, and staff. Whenever the total amount of disk space used by a user's files exceeds this amount, a warning is printed to the display (the warning is displayed on the terminal screen in a secure shell session - no warning is displayed when the user is storing files to "drive H: or P: " in the OIT labs). The user then has 24 hours to erase or compress files to reduce the total to less than the assigned disk quota. After this time period, or any time the "hard limit" is reached, the user is not allowed to create any files (this includes compressing files, extracting news files, FTP'ing from another location, etc.) until the quota is no longer exceeded.

- How to check your disk quota

OIT provides additional disk space for temporary use by staff or faculty as needed.

By default new user accounts are set up with a **coredumpsize limit** of 0. This is to prevent programs from creating core images of themselves when they crash. Programmers interested in allowing core files to be created for debugging purposes may change the default by adding the appropriate commands to the .cshrc after the .master_cshrc file has been executed.

The following file types are not permitted to be transported, stored, printed, or otherwise exist on any of the OIT hosts, file servers, or OIT lab machines.

- files not used for the purposes of academic research, education or extension
- .rhost files (see section 3.4)
- copyrighted material (without the permission of the copyright holder)
- games

Section 4.4 Use of Printing Resources

OIT provides access to networked laser printers in each of the OIT Labs for a fee.

Section 4.5 Use of Archiving Resources

OIT does not allow storage of user data on the **OIT Lab machines**. Instead, access to the user's OIT Sun Network pace is provided on drives H: and P: for that purpose (see section 4.3) Consequently, OIT does not provide backup on the OIT Lab machines, and these machines are reformatted regularly.

User directories on the OIT **Sun Network** are backed up nightly. In addition, users may wish to make their own archives.

Department directories on the AU Web server are backed up nightly. Data on the OIT-managed Windows web servers is backed up nightly as well. Backups are generally available for one week.

OIT regularly backs up disk data sets on the **IBM mainframe** but keeps these backups for a limited time only. No backup is maintained for tape data sets. Users are responsible for maintaining backup copies of their data sets. For more information on disk data set maintenance procedures on the IBM mainframe, contact the OIT HelpDesk at 844-4944 or helpdesk@auburn.edu .

OIT provides the **TSM** (Tivoli Storage Manager, formerly named ADSM) client as a means for AU faculty, staff, and students to back up PC and workstation hard drives to the IBM mainframe. A TSM account is automatically assigned to all AU employees when the username is assigned. The TSM password is assigned and maintained separately from other OIT passwords. Students may request a TSM account contacting the OIT HelpDesk at 944-4944 or helpdesk@auburn.edu.

- File Backup (TSM) at Auburn University

Section 4.6 Use of Remote Computing Resources

The OIT network is directly connected to the Auburn University network (AUNET), and OIT computing resources may be utilized to communicate with hosts on departmental LANs. OIT cooperates fully with departmental system administrators in investigating violations of departmental computing policies. Under certain circumstances, the loss of departmental computing privileges could result in the loss of OIT computing privileges as well. For example, attempting to breach the security of a departmental host computer will be treated the same as if the attempt was made against an OIT host.

4.7 Use of Electronic Mail

University-Wide E-mail policies issued by the Office of the Provost:

- Employee E-mail Policy
- Faculty E-mail Policy
- Student E-mail Policy

OIT provides Novell GroupWise as the e-mail solution for students and employees.

- GroupWise (client software for e-mail)
- TigerMail (web access to e-mail)

OIT operates a mail forwarder for members of the Auburn University community who use electronic mail (e-mail). The mail forwarder allows users to publish an e-mail address which never changes but allows users to change the server or account where they actually read e-mail. The mail forwarder address for each user is ***username*@auburn.edu**

E-mail addresses are published to Internet users through the LDAP directory on the AU Web.

Employees and retirees may change the address where the mail forwarder sends mail by submitting an **Username Update Form**. Some AU departments require approval of mail forwarding requests. Check with your departmental Administrative Computing Coordinator for more information.

Student e-mail is not forwarded to external systems.

Mail addressed to a specific system (some system other than @auburn.edu) must be forwarded from that system. E-mail cannot be forwarded when the person leaves Auburn, except in the case of retirees. A person must be an employee, a guest under written contract, or retiree of Auburn in order to have a username registered with the mail forwarder (see section 2.2).

- Username Update Form
- E-mail at Auburn University

Users or campus organizations may create e-mail aliases to forward mail to a specific username by submitting an **Account Update Form** online. A username may have up to three e-mail aliases. OIT reserves the right to deny offensive or otherwise inappropriate e-mail aliases.

Users are encouraged to read their e-mail regularly and file mail items they wish to keep. Other items should be deleted.

There is a **10MB limit on the size of an e-mail message (including attachments) for students; 50MB for employees**. The total Inbox size limit is 100MB for students; 100MB for employees. Persons who need to send large files to other users are encouraged to consider FTP or a web-based service.

- Using File Transfer Protocol (FTP) at Auburn University

Users should be aware that e-mail is not private or secure although OIT does make every effort to ensure confidentiality. E-mail should not be used to transfer secure or confidential information.

4.8 Use of the World-Wide Web

The **World Wide Web** is a global information system that incorporates the use of hypertext links and makes extensive use of text integrated with imagery, video and audio data. OIT operates the official Auburn University World Wide Web server which is referred to as the AU Web Page (http://www.auburn.edu). A web browser is available on all OIT Lab machines.

Every user on the OIT Sun Network is allowed to create a **personal home page** using their username. The URL for a personal home page is **http://www.auburn.edu/~*username*** where *username* is the username of that account.

OIT and Auburn University are not responsible for the content of personal web pages. Personal web pages on the AU web server must abide by the OIT Network Policy and copyright laws of the United States.

- Web Page Topic Home

University departments and **organizations** may request web space by contacting the OIT HelpDesk (844-4944 or helpdesk@auburn.edu). **Student organizations** must be chartered by the Student Government Association (SGA) or in the probationary period prior to charter in order to qualify for web space on the AU web server.

There is currently no disk space quota on departmental or organizational web space. However, since space on the server is limited, only files linked to the department's or organization's web page should be stored in the web directory.

Personal, departmental, and student Web pages must abide by the copyright laws of the United States. Penalties for copyright infringement at Auburn include but are not limited to temporary restriction of network privileges, permanent restriction of network privileges, and criminal prosecution.

- Additional Copyright Regulations Information
  includes information on the Digital Millennium Copyright Act and AU's designated agent
- Student Organization Web Space Policy
- Student Government Association - Chartered Organizations

4.9 Use of Directory Services

OIT provides LDAP Directory Services to Internet users. Information about faculty, staff and students at Auburn University is provided through this online service.

The online directory is updated nightly from the administrative records. Changes appear the following business day.

4.10 Use of List Servers

OIT operates list servers which handle e-mail for special interest groups. Lists covering various topics are available for subscription. Each user must request a subscription in order to be added to a mailing list. A new mailing list can be created by a member of the Auburn University community if the purpose of the list is directly related to the University's mission of research, education and extension. Requests for creating mailing lists should be submitted to the OIT Accounts Administrator along with all necessary information and justification.

- Electronic Mailing Lists (list servers) at Auburn University

4.11 Use of FTP

OIT operates an **Anonymous FTP** Server at ftp.auburn.edu that is available to departments needing to transfer large amounts of data. To request directory space on the anonymous FTP server, please contact the OIT HelpDesk. OIT does not support anonymous upload to any OIT server. The rules and regulations pertaining to software licensing and copyrighted material apply to files stored on the OIT Anonymous FTP server.

FTP client software is available on all OIT hosts and OIT Lab machines and via download from AU Install. Some servers require a secure connection.

4.12 Appropriate Use of Copyrighted Material

Auburn University expects all departments and students to be aware of how intellectual property laws, regulations, and policies apply to the electronic environment and to respect the property of others.

The **Digital Millennium Copyright Act** is a provision establishing limitation of liability for infringement of copyright laws by users of computing resources at institutions of higher education. In compliance with the rules of this act, Auburn has designated an agent to receive statutory notices from copyright owners about infringements and to send statutory notices to affected subscribers. Penalties for copyright infringement at Auburn include but are not limited to temporary restriction of network privileges, permanent restriction of network privileges, and criminal prosecution.

- AU's Designated Agent for Receiving Copyright Infringement Notices
- The United States Copyright Office
  The Digital Millennium Copyright Act is can be found on this site.
- American Library Association Intellectual Resources about Copyright
- How to Request Copyright Permission from Publishers

4.13 Use of Streamed Media

A streaming media server is provided for use by students, faculty, and staff. Departments and chartered organizations can request additional space for streaming media files. Live broadcast capability is available by request for departments.

- Streaming Media Support

Chapter 5: Abuse of Computing Resources

OIT computing resources are shared by all network users on a fair and equitable basis. It is the responsibility of OIT not only to provide these computing resources, but to ensure that the rights of users are not infringed upon by the abuse of another. Therefore, OIT utilizes every means available to detect, restrict and/or prosecute individuals responsible for the abuse of computing resources. This section serves to provide specific examples of the types of abuse not tolerated. This list is by no means complete and is subject to change without notice as new ways of abusing resources are discovered. Penalties for abuse of network resources include but are not limited to temporary restriction of network privileges, permanent restriction of network privileges, and criminal prosecution.

Section 5.1 Theft and Vandalism

Theft and vandalism of OIT Computing resources is handled by the appropriate authorities (Auburn City Police). OIT pursues and supports criminal prosecution of individuals suspected of theft and/or vandalism.

Section 5.2 Worms and Viruses

Anyone attempting to write, transfer, or knowingly proliferate worms or viruses of any size, shape, or form will be remanded for criminal prosecution (and will lose their computing privileges).

Section 5.3 Use of .rhosts Files

Through the use of .rhosts files users can allow others access to their account without the knowledge of a password. This is not only a breach of security but violates the policy on account sharing as well. Use of .rhosts files is prohibited. When found, they will be deleted. Repeat offenders will lose their computing privileges (see also Section 3.4).

Section 5.4 Transferring Files

Using FTP to transfer files to or from remote sites which violate the policies of the remote site is prohibited. In particular, transferring files which are large, contain material offensive to either site, contain information to be used for the financial gain of any party, or contain monetary or sexual solicitations is prohibited. Restrictions pertaining to the duplication of copyrighted materials also apply (see also Section 4.13).

Section 5.5 Games

Games are prohibited on all OIT computers. Games waste CPU cycles and network bandwidth and in some cases have detrimental effects on computer systems. Repeat offenders will lose their network privileges.

Section 5.6 Disruptive Behavior

The OIT Labs are designed to provide computing and network resources to University students and employees who need them to fulfill their role in the University's mission. Since OIT provides these resources for use in academic research, education, and extension, the OIT Labs are in effect no different from other classrooms and labs on campus, and lab patrons should behave accordingly. Loud talking, profanity, boisterous or otherwise disruptive behavior is prohibited. Children are not allowed in the OIT Labs. Eating, drinking, and the use of tobacco or controlled substances is also prohibited in the OIT Labs.

Section 5.7 Unauthorized Use of Computing Resources

You must have a username to use the OIT computing resources. Persons found using OIT computing resources without an active user name of their own will be referred to the appropriate authorities. For University staff, students and faculty, the individual's department head an d/or dean will be notified. Incidents involving individuals not directly associated with the University will be handled by the AU Police Department. If direct expenses are incurred during unauthorized use (i.e., paper, printer supplies, etc.), OIT reserves the right to pursue full reimbursement of those costs from the individual.

Use of restricted network services without authorization is considered an abuse of privilege and a violation of security and may result in restriction or denial of network access. Current restricted network resources include OIT Lab printers, printers reserved for use by an individual, department or research group, and workstations and servers which have restricted login access.

Section 5.8 Breaking Into Accounts

Any attempt to gain access or to use an account or user name other than by the owner is considered a severe violation of network policy. Such attempts include, but are not limited to,

- gaining access to a user's account while the user is away from a terminal or a workstation or;
- making efforts to determine another user's password by closely watching a login, or
- developing applications which request or capture user passwords.

The appropriate action if you find an OIT Lab machine or computing resource that is logged into but the user is not near the machine is to 1) determine who the user is, 2) try to locate the user, and 3) if the user is not found, log the user out immediately. Do not tamper with any programs or data files in the user's directory.

Section 5.9 Cracking Passwords

Any attempt to crack or otherwise obtain passwords is prohibited. Storing or transferring encrypted or unencrypted password information is prohibited. Writing, transferring, compiling, storing or running programs designed to guess passwords or otherwise gain unauthorized access to user or system accounts or passwords is prohibited. This includes programs or techniques designed to trick users into divulging their password.

Section 5.10 Misuse of Accounts

A username is assigned to an individual. Account sharing is prohibited. Using instructional accounts for funded research purposes is prohibited. Your account is your user identification when accessing computing resources. Any attempt to impersonate another user or conceal your identity when send ing e-mail or posting to news groups is prohibited.

Group accounts may be created for use by small, well-defined units within an on-campus department. Activity under the group account user name is the responsibility of the department head or computing coordinator requesting the account (See also section 2.1).

Section 5.11 Unauthorized Access of User Files

Unauthorized access to information contained in a user's OIT-maintained directory space is prohibited, even if the files are readable and/or writable. When in doubt, don't read, copy, or change other users' files.

Section 5.12 Unauthorized Modification of Files

Modifying files anywhere on the system without consent of the file's owner is prohibited. This includes writing or modifying files which have file permissions set to allow modification or writing. This also includes creating new files, renaming, or deleting existing files in directories which may have directory permissions set to allow creation or modification of files. When in doubt, don't write.

Section 5.13 Unauthorized Broadcast Messages

Sending unauthorized broadcast messages is prohibited. Sending profanity or messages abusing another user is considered a severe network violation and will result in the loss of network privileges.

Section 5.14 Use of Computing Resources For Monetary Gain

Use of OIT computing resources for monetary gain or pecuniary purposes is prohibited. However, resume preparation is allowed.

Section 5.15 Licensing and Copyright Infringement

Most software packages and applications are licensed and/or copyrighted. Most licenses and copyright agreements specifically prohibit copying or unauthorized use of the software or data. When in doubt, don't copy. (See also Section 4.14)

Section 5.16 Disrupting or Degrading Service

Disrupting or degrading a network service is prohibited. In a large integrated computer network that is shared by a large number of users, such as the Auburn University network, many services depend upon distributed computing resources and often upon other network services. These resources include servers,

printers, workstations, and the network infrastructure (hubs, routers, cabling system). These resources function in a cooperative manner to provide the variety of network services enjoyed by our many users. It is often difficult to ascertain what impact the disruption or degradation of a computing resource or a network service may have on other network users. Therefore, any disruption or degradation of service is prohibited.

The following is a short list of some methods of causing disruption or degradation of service:

- turning a machine off;
- unplugging the network connection for a machine;
- modifying or reconfiguring the software or hardware of a computer or network facility. Do not modify the hardware, operating system, or application software of an OIT computer unless you have been given permission to do so by the OIT department or administrative unit in charge of the machine. The other users with whom you share the machine, and the technicians on whom you rely for support, expect to find it set up exactly the way they left it;
- attempting to use more resources than the machine can handle (i.e., running a large number of I/O or computationally intensive applications);
- excessive printing, using excessive disk space, or otherwise degrading system performance by monopolizing shared resources;
- sending excessive e-mail, and
- running programs which lock or unlock the screen or keyboard (exceptions to this are system administrators or system administration employees working on systems related programs and machines located in offices with the approval of the office occupant).

Section 5.17 CPU Usage

The machines on the OIT network provide an enormous amount of processing power. It is tempting for users to attempt to run programs on as many machines as possible to decrease the total turnaround time of the job. However, running jobs on remote machines can have a serious impact on the interactive performance of the machine. This could render the machine virtually unusable to anyone else. This problem is even more acute if the offending program performs a large amount of I/O, bogging down the network and the file servers. In general, using multiple remote machines for running computational programs is prohibited. A user with a large computational problem should contact the systems administrator to work out a plan BEFORE running the program.

Section 5.18 Exceeding Disk Quotas

Disk quotas are in effect on the OIT Sun Network. Failure to reduce your file storage below your quota within a reasonable period of time may result in the deactivation of your OIT Sun Network access and the removal of your files (see also section 4.3).

Section 5.19 Misuse of Electronic Mail

Electronic mail (e-mail) is covered under the Electronic Communications Privacy Act of 1986. This act provides for prosecution of individuals found capturing, reading or altering another's e-mail without permission.

Mail deemed obscene, in violation of the University's harassment/discrimination policy, or otherwise abusive by the recipient is considered an abuse of network privileges. Do not e-mail any message you would not be willing to sign and put in the mail.

- Rules Section of the *Tiger Cub*

Any attempt to forge an e-mail message is considered an abuse of network privileges. If a user receives mail that could have been forged, it is in the best interests of all parties involved to confirm the e-mail with the supposed sender via personal contact. If it is determined that the e-mail is a forgery, contact the OIT systems administrator or postmaster or contact the OIT HelpDesk at 844-4944 (helpdesk@auburn.edu). Please save a complete copy of the message for further investigation.

Chain letters are a violation of U.S. Postal regulations and are considered a serious violation of OIT network policies. Visit www.snopes.com to view an urban myths and e-mail hoax database.

Unauthorized mass mailings are prohibited and will result in the immediate loss of computing privileges. An example of an unauthorized mass mailing is using a mail client's address book or a directory service to send SPAM e-mail to every user listed there.

In cases where the System Administrator observes a decline in server performance due to excessive incoming e-mail, the e-mail recipient will be requested to reduce the volume by un-subscribing from lists, etc. Extreme cases of faculty e-mail abuse will be referred to Internal Auditing.

- Electronic Mailing Lists (list servers) at Auburn University

Section 5.20 Misuse of Web Resources

Web pages deemed obscene, unduly inflammatory or in violation of the University's harassment/discrimination policy as stated in the Rules Section of the *Tiger Cub* are prohibited and will be removed by the system administrator.

Section 5.21 Violation of Remote Site Policies

Users of remote sites or remote site services are bound by the rules and policies of the remote site. If you do not know the remote site's rules and policies, adhere to those outlined in this document. OIT cooperates fully with remote site system administrators in the investigation of remote site policy violations.

Section 5.22 Installing Software on OIT Lab Machines

OIT provides general purpose software in the Labs and installs approved applications at the request of AU departments. Lab patrons should not install unapproved or personal copies of software. Faculty should contact the OIT Computing Lab support via the HelpDesk at 844-4944 to request installation of course specific software on Lab machines.

Chapter 6: System Administrators' Responsibilities

System administrators are held to a higher standard than the average user because they have the capability and responsibility to maintain system integrity. On host systems such as the IBM mainframe and the Sun Network, system administrators possess access rights which allows them to read, write, or execute any file on the system. Thus systems administrators must be entrusted with the security and privacy of all data on the network.

Section 6.1 Privacy

System administrators have access to users' private information. Systems administrators are required protect the confidentiality and integrity of this information.

Section 6.2 Liability

Every effort is made to safeguard data stored on OIT computers. However, OIT system administrators are not liable for any loss of data or loss of service on the OIT network. The ultimate responsibility for safeguarding data rests with the user, through proper security and archival procedures.

Section 6.3 Investigation of Policy Violations

OIT system administrators are charged with investigating policy violations and suspected abuse of computing resources. During such investigations, system administrators may inspect program and data files and may monitor network traffic.

Chapter 7: Enforcement

Section 7.1 Temporary Restriction

An individual's account on the OIT network may be temporarily restricted due to many reasons, including:

- maintenance or servicing of network resources
- dissemination of information before continued use of an account
- investigation of policy violations or suspected abuse of resources

Temporary access restrictions are intended to be short-lived and usually require the account's owner to contact the appropriate system administrator for reactivation. Note that investigations of network policy violations may require any number of potentially affected accounts to be temporarily restricted. The owner of the account may not be the object of the investigation if, for example, it may be suspected that the user's password has been cracked by a third party.

Section 7.2 Permanent Restriction

If it is determined that a user's policy violations are so serious that continued use of the OIT Network would infringe upon the rights or security of other users, the user's account will be permanently restricted. Permanent access restrictions must be approved by the Director of the Office of Information Technology or his designated representative. All accounts assigned to a user may be restricted and future network privileges denied.

Section 7.3 Severe Abuse

Individuals accused of severe abuse may be referred to the University Discipline Committee for further action or to the appropriate law enforcement agency.

- Rules Section of the *Tiger Cub*

Chapter 8: Reporting Problems

Section 8.1 Physical Security

Physical security is the most important part of system security. Electronic security means nothing if the whole machine is stolen. Users should keep an eye out for any suspicious activity. If an alarm sounds in an OIT Lab, use the lab phone to report the problem to the OIT HelpDesk at 844-4944 or contact the AU Police at 911. The calls to the OIT HelpDesk are forwarded to the OIT machine room operators after hours. If you accidentally trigger an alarm, wait for security to arrive after notifying the HelpDesk.

Section 8.2 Theft and Vandalism

Theft and vandalism should be reported immediately to the Auburn University Police as well as to OIT. Do not touch anything at the scene of the crime in order to prevent the destruction of potential evidence.

Section 8.3 Electronic Security

Users who suspect that the security of their account has been breached should notify the OIT HelpDesk as soon as possible (844-4944 or helpdesk@auburn.edu). The OIT HelpDesk will alert the system administrator.

Section 8.4 Notification of Remote System Administrators

Violation of policies on remote system may require notification of the remote system administrator. If a remote system administrator is contacted, please notify OIT Networking Services via the OIT HelpDesk (844-4944 or helpdesk@auburn.edu) to advise them of the situation.

Section 8.5 Inoperative and malfunctioning Equipment

Inoperative/malfunctioning machines and other hardware problems in the OIT Labs should be reported to OIT Lab Support Services via the OIT HelpDesk (844-4944 or helpdesk@auburn.edu). Problems associated with the dial-up facility, or accessing the OIT network from AUNET should also be reported to the OIT HelpDesk (these calls are forwarded to the OIT machine room operators after hours). Network support personnel are on call after hours and on weekends but rely on the users to report problems.

Section 8.6 Software Problems

All software problems on OIT computers should be reported to the OIT HelpDesk (helpdesk@auburn.edu or 844-4944).

Section 8.7 Recovery of Deleted Files

User home directories and web directories on the OIT Sun Network are backed up daily. To request restoration of deleted files, contact OIT Network Services via the OIT HelpDesk (helpdesk@auburn.edu or 844-4944) and provide the following information:

- exactly which file(s) need to be restored; include the directory in which the files were located (i.e. *my home directory*, file *test.data*);
- the date and time the file(s) were created;
- the date and time the file(s) were last modified, and
- the date and time the file(s) were deleted.

If located on tape, the files will be restored and placed in a directory named *RESTORED* in the user's home directory. It is the responsibility of the user to move these files to their appropriate place and delete the RESTORED directory.

NOTE: Files which are restricted under OIT network policies will not be restored.