APPROVED BY COMPUTER ADVISORY COMMITTEE
07-06-00

NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

COMPUTING AND NETWORKING USAGE POLICIES

Table of Contents

I. Nature and Purpose of the University's Computing and Networking Environment
   A. Computing
   B. Networking
   C. Purpose and Scope of these Policies

II. Ethical Responsibilities
   A. User Responsibilities
   B. System Custodian/ Security/System Administrator Responsibilities
   C. Data Owner Responsibilities

III. Policies
   A. Computer User Accounts
   B. Security
   C. Networking
   D. Software
   E. Hardware
   F. World Wide Web
   G. Academic Computing Facilities
   H. Privacy
   I. General

IV. Sanctions for Policy Violations (*Univ. Comp. Committee*)

References

Appendix

APPROVED BY COMPUTER ADVISORY COMMITTEE
07-06-00

NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

COMPUTING AND NETWORKING USAGE POLICIES

I. Nature and Purpose of the University's Computing and Networking Environment

A. Computing

Our campus computing environment has evolved from the three main types of computer processing models: centralized computing, distributed computing and client server computing.

Centralized Computing Model

During our earliest stage of computing development, the university used the *centralized computing model* which consisted of a mainframe or minicomputer and terminals. All the processing took place on the central computer, which is commonly referred to as the host computer. Multiple terminals accessed the host and it ran multiple programs at the same time. The terminals were considered "dumb terminals" because they did not do any processing in this model. This system was strictly character based. All the applications, data and backups resided at the host computer which was also responsible for system security.

Distributed Computing Model

The next stage of university computing development brought about Distributed computing which was facilitated with the development of the personal computer (PC). Users worked on PCs with each PC having its own CPU and being able to process individual user requests . Later on in the development of this computing model, the PCs became interconnected, which allow them to share information and peripherals. These interconnected systems also acquired specialized PCs, which became file servers. This network system became know as a file-server-based network. The file server on this type of computing model cannot directly access applications or data.

Client Server Computing Model

The university is now in a cooperative computing environment also known as client/server computing. In this model, the server runs one part of an application and the client PC runs another part. The client application is commonly known as the front-end to the back-end server application. Both machines work together to produce an end result. An example of this type of computing model would be Microsoft SQL Server. SQL Server is the back-end server database application. Client machines use applications such as Microsoft Query or

Access to work with the data that is stored in the SQL Server database. When a query is executed, the processing usually takes place on the server and the results are sent to the client computer. This type of system is less bandwidth intensive because only the requests for specific data and the resultant data set are transmitted across the network. The University's computing resources are available to faculty, administrators, staff and students, for administrative, academic and research work. These resources include, but are not limited to, administrative systems, email and web services, academic computing services and public access facilities.

University computing resources include diverse hardware and software such as IBM-compatible PCs running all versions of Microsoft Windows, Apple McIntosh computers running various versions of MacOS, Sun Solaris and Digital Alpha machines running many flavors of UNIX and VMS operating systems. As a higher education and research institution, North Carolina Agriculture and Technical State University's computing environment is diverse. While staff and administrators may support the university's operation using standard hardware and software, faculty and students may choose to select alternative tools necessary to conduct their research and academic work thus allowing a rich learning environment for both faculty and students.

B. Networking

North Carolina Agricultural and Technical State University operates through its central administrative offices, a wide-area (inter-building) digital transport network. All networks have three basic elements: pathway, rules and sharing. Pathway is the way to get information from one computer to another. This is the level where the transmission media is used. The transmission media is the physical cable or wireless device that carries the data signal from one location to the next. Rules use protocols and conventions to ensure error free communication between computers. The protocols that computers use to establish communication are similar to language that we use to speak to each other. The main purpose of our network is to share information. Sharing resources such as file and printers are usually done by servers and used by clients. In peer-to-peer networks, computers can act as both clients and servers. Some networks include both client/server and peer-to-peer resource sharing. File and print resources are not the only service that can be shared on a network. Many networks share resources such as fax modems and applications.

This network connects local-area networks operated by academic and administrative departments that have agreed to adhere to the University's Campus Standard Wiring Guidelines available at http://nts.ncat.edu/wiring-guidelines.html and to the network management policies coordinated by Computing and Information Technology. The resulting connection of networks is the "University's network." It is one of the institutionally operated networks that make up the global Internet and that adhere to the open standards and protocols adopted by the Internet Engineering Task Force. In addition to an Internet gateway, the University's network also includes a gateway to the North Carolina Information Highway. Through its gateways to the Internet and the North Carolina Information Highway, the University's network becomes an extended global network that provides access to

information and information processing technologies, only a fraction of which is under the stewardship of the University.

This extended network and the resources accessible through it serve the following two primary purposes in the framework of the University's mission:

A. To Enhance Institutional Effectiveness and Efficiency

By having access to the University's network and its resources, including its gateways to the Internet and the North Carolina Information Highway, the faculty, the staff, and the student body can communicate and collaborate among themselves and with their counterparts elsewhere, who can connect to the Internet or the North Carolina Information Highway. Network connections are a starting point for internal collaboration and efficiencies, for extending the reach of the University, and for expanding the resources available to the faculty, the staff, and the student body. The University's network is a powerful lever for institutional effectiveness and efficiency only to the extent that network connections are:

1. easily established and broadly available;
2. accompanied by easy-to-use services, accessible;
3. are based on the standards that guide the development of the Internet and the North Carolina Information Highway.

B. To Publish Institutional Information about the University

The network's gateways to the Internet and the North Carolina Information Highway are the primary means by which the University meets its responsibility to the public to publish much of its institutional information in useful digital formats. By publishing this information via the University's network, often in the form of institutional databases, the University not only meets a public obligation, but serves its own goal of continuous quality improvement in a distributed management model that depends on the free flow of information and that is essential to academic effectiveness. Institutional information, whether for the public or for internal purposes, therefore is published on-line in an open, democratic framework designed to encourage**:**

1. consistent and readily affordable access to digital information;
2. stability and reliability from the inquirer's perspective;
3. integration among disparate databases with minimal duplication in capturing, storing, and maintaining these databases;
4. useful, unifying perspectives on the University's programs and resources; and
5. information literacy and the use of institutional data in decision making.

C. Purpose and Scope of Policy

APPROVED BY COMPUTER ADVISORY COMMITTEE
07-06-00

The rapid development of the Internet and of information technology requires North Carolina Agricultural and State University to establish a specific policy applicable to the technology arena.

Appropriate use of computing and networking resources and insuring the integrity of data and privacy is everybody's responsibilities. Technological and information resources and the access provided by the University to campus resources are to be governed by this policy. Just as there are policies that apply to property and privacy of physical items, this policy applies when we involve computers.

The Computing and Networking Usage Policy applies to technology administered by individual departments, to student owned hardware connected to the campus network, to the resources administered by central administrative departments such as University Libraries or Computing and Information Technology, and to actions originating from computer systems maintained by members of the campus community off-campus connecting remotely to the University's network services.

The Computing and Networking Usage Policy applies to all systems owned, managed or administered by the University and any use of those systems. Many specific areas and or systems may have service-specific policies that apply in addition to this umbrella Computing and Networking Usage Policy. Please refer to postings available with each system to identify all applicable policies.

The policies described herein are those that the University intends to use in normal operation of its facilities. This document does not waive any claim that North Carolina Agricultural and State University may have to ownership or control of any hardware, software, or data created on, stored on, or transmitted through it's systems.

As technology changes and users find new ways to use technology for administrative, academic and research endeavors, the Computing and Networking Usage Policy must evolve. The campus Computer Advisory Committee would be entrusted with the responsibilities to propose any necessary changes.

Updated Computing and Networking Usage Policy and other related policies and procedures shall be posted at http://www.ncat.edu/~cit/policies/ .

II. Ethical Responsibilities

All members of the University community who use the University's computing and information resources must act responsibly. Every user is responsible for the integrity of these resources. All users of University-owned or University-leased computing systems must respect the rights of other computing users, respect the integrity of the physical facilities and controls and respect all pertinent license and contractual agreements. It is the policy of NC A&T that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations and the highest standard of ethics.

Access to the University's computing facilities is a privilege granted to University students, faculty and staff. Access to University information resources may be granted by the owners of that information based on the owner's judgment of the following factors: relevant laws and contractual obligations, the requester's need to know, the information's sensitivity and the risk of damage to or loss by the University.

The University reserves the right to limit, restrict or extend computing privileges and access to its information resources. Data owners-whether departments, units, faculty, students or staff-may allow individuals other than University faculty, staff and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement, University policy or any federal, state, county or local law or ordinance.

University computing facilities and accounts are to be used for the University-related activities for which they are assigned. University computing resources are not to be used for commercial purposes or non-University-related activities without written authorization from the University. In these cases, the University will require payment of appropriate fees. This policy applies equally to all University-owned or University-leased computers.

Users, Data Owners and System Custodians must all guard against abuses that disrupt or threaten the viability of all systems, including those at the University and those on networks to which the University's systems are connected. Access to information resources without proper authorization from the data owner, unauthorized use of University computing facilities and intentional corruption or misuse of information resources are direct violations of this Computing and Networking Usage Policy. They may also be considered civil or criminal offenses.

A. User Responsibilities

If you use the University's computing resources or facilities, you have the following responsibilities:

- Use the University's computing facilities and information resources, including hardware, software, networks and computer accounts, responsibly and appropriately, respecting the rights of other computing users and respecting all contractual and license agreements.

- Use only those computers and computer accounts for which you have authorization.
- Use server accounts only for the purpose(s) for which they have been issued. Use University-owned workstations for University-related projects only.
- Be responsible for all use of your accounts and for protecting each account's password. In other words, do not share computer accounts. If someone else learns your password, you must change it.
- Report unauthorized use of your accounts to your project director, instructor, supervisor, system custodian, security administrator or other appropriate University authority.
- Cooperate with system custodian and security administrator requests for information about computing activities. Under certain unusual circumstances, a system custodian and security administrator is authorized to access your computer files.
- Take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on any system, network or server that you operate.

Each user is ultimately responsible for his or her own computing and his or her own work using a computer. Take this responsibility seriously. Do not leave the workstation unattended. Also, remember to make backup copies of the data, files, programs, diskettes and tapes, particularly those created on microcomputers and those used on individual or departmental systems. Furthermore, users with desktop computers or other computers that they operate themselves must remember they may be acting as the system custodian for those computers and need to take that responsibility very seriously.

If you are a project director for a group of server computing users, a supervisor whose staffs use computers or a faculty member whose students use computers, you must help your project members, staff or students learn more about ethical computing practices. You should also help your project members, staff or students learn about good computing practices and data management.

B. System Custodian/ Security/System Administrator Responsibilities

System Custodians and Security Administrators use of the University's computing resources is governed by the same guidelines as any other user's computing activity. However, there are additional responsibilities to the users of the network, site, system, or systems he or she administers:

- Manage systems, networks, and servers to provide available software and hardware to users for their University computing.
- Take responsibility for the security of a system, network, or server.
- Take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on all systems, networks, and servers for which he or she has responsibility.
- Take reasonable precautions to guard against corruption of data or software or damage to hardware of facilities.
- Treat information about and information stored by the users as confidential.

C. Data Owner Responsibilities

It is the responsibility of the Data Owner to:

- Disclose to the users relevant legal requirements and ethical obligations for the release of information
- Publish any departmental policy on the release of information
- Implement a data classification system whereby data is rated according to sensitivity, confidentiality. Proprietary value, and/or other criteria
- Maintain a list of authorized users
- Develop procedures related to the granting of, modification of, and denial of access for new, existing and terminated/transferred employees
- Review methods for safeguarding information from unauthorized use, improper disclosure, accidental alteration and accidental or intentional destruction
- Develop an electronic records retention and disposition policy
- Provide users with sufficient training in the use and protection of information

The Associate Vice Chancellor for Academic Affairs/Chief Information Officer shall, from time to time, issue recommended guidelines to assist Data Owners with this effort.

III. Policies

A. **Computer User Accounts**

Computer user accounts are required to access many computing resources such as the administrative systems, email and web servers, and open computing facilities' machines. Computer user accounts are available to faculty, staff, registered students and guests for the duration of their University affiliation. An identification and/or proof of current status may be required. Use of accounts by anyone other than the owner is strictly prohibited. Computing and Information Technology account management policies are designed to protect resources, accounts, and data from anyone who would misuse or abuse them.

There are three major types of accounts available for the university community:

1. User Account:

Users who expect to use diverse computing resources available on campus need to have a valid user account. User account is the account that gives access to most common electronic services on campus. These services include email account, web service, shared disk spaces, academic computing resources, dial-up connection, and access to open academic computing facilities, etc. Types of affiliation determines the procedure for receiving such an account:

A. Students

Accounts for new students are automatically generated at the start of each semester. Other students can obtain a user account by contacting the Aggie Help Desk in the lower level of Fort IRC Building (subject to procedure in place).

Graduate students may obtain access to restricted computer resources, if needed, by contacting the Aggie Help Desk; this access does not include disk space in addition to that allocated under the user account.

B. Courses

Faculty members who want to obtain an account specifically for a class for a semester should contact the Aggie Help Desk for assistance.

C. Faculty, Staff and Retirees

Current and retired NC A&T SU faculty and staff are eligible for user accounts. To obtain an account, current faculty and staff must submit a request (subject to procedure in place to the Aggie Help Desk.

Retired faculty and staff may request an account, or may request that their existing account be retained when they retire. To do so, they should submit to the Aggie Help Desk a completed account application along with a letter from

their department head stating their retired status. Accounts for retired staff and faculty must be renewed annually.

D. Departments and Organizations

Different campus departments and organizations affiliated with the university may request a user account that will allow them to have a email and web identity associated with the university. To obtain an account, departments and organizations must submit a request (subject to procedure in place), to the Aggie Help Desk.

E. Alumni

Alumni of North Carolina Agricultural and Technical University may request via Alumni Affairs at the time of graduation to have their mail forwarded to a new email address. If such a request has been made, all email will be forwarded for a period of one year and than the service will cease. Additionally, active account of a graduating student will automatically be kept active for a period of six months with all privileges of that account.

F. Others

Accounts for special guests, special programs, affiliated agencies, and state or federal government agencies may be created for applicants who are not associated or are only loosely associated with the University. Sponsors of these accounts will apply for guest accounts through the Aggie Help Desk.

2. Administrative Account

Administrative account is an account that allows a user to university's main databases containing student information (SIS), financial information (FRS), human resources information (HRS), etc. Accesses to these accounts are controlled by the data owner and are provided in need to know basis.

Administrative Accounts for faculty and staff may be obtained by completing the **Request for Administrative Account Form** and by obtaining his/her department head's signature. Access to administrative sub-systems will be granted by completing the application for access to that particular sub-system and completing required training on that sub-system.

3. Local Area Network (LAN) Account

Many departments on campus operate and maintain separate local area network. These LANs allow the departmental users access to data and applications relevant to a specific area of operation. One needing to have an account in such a system must see their LAN administrator of the system and follow the departmental procedure in place to obtain an account.

Other policies that apply to User and Administrative Accounts are:

A. *Changing A User ID*
If an account owner's name has officially changed in the University records (because of marriage, divorce, or some other reason), Computing and Information Technology will update the name associated with the account. The account ID will not normally be modified.

B. *Changing Password*
All computer accounts are secured by passwords. User Account password is changed at the users discretion. Users who forget their passwords must bring their ID to the Aggie Help Desk to have their passwords reset. Administrative passwords are set to expire periodically. Faculty and staff who are administrative users and forget their password must contact the AIS administrative security officer in the Fort IRC Building.

C. *Mail Forwarding*
Account holders can have their e-mail forwarded to a different account by making the request via the Aggie Help Desk. E-mail forwarding will be purged of July 1 of each year.

D. *Account Inactivity, Deactivation, and Reactivation*
All student accounts are removed six month after leaving the University. Faculty, staff, and administrative users accounts will be removed when Computing and Information Technology receives the Human Resources Clearance Form.

E. *Resource Allocation*
Computing and network resources are to be used only for University-related research, instruction, learning and enhancement of scholarly information and for administrative activities. When appropriate technology is in place, Computing and Information Technology may grant students, faculty and staffs dedicated media space and printing quotas. A request may be made via Aggie HelpDesk to increase any quotas and it will be considered against the user’s need and currently available University resources.

B. Security

As the role of computer is changing, so is the role of the computer security. When computer systems were a room filled with hardware secured behind closed doors and no time-sharing was allowed, security of these systems, physical or otherwise, was not much of a problem. As information protected by the walls around the mainframe moves to local area network, it becomes susceptible to a lot of threats. Given herein are some general information and *recommendations* for various users on the campus.

1. General Security Threats & Vulnerabilities

- Foremost is the physical vulnerability of the computer system. If a system has been physically challenged, all other security measures become worthless.
- Natural vulnerabilities exist in terms of natural disasters such as earthquake and flood, power loss
- Computers connected to a network or one that can be accessed by telephone can allow one to get into a system and cause security problems for data and programs.
- Unintentional threats are brought about from ignorance of a user or a poorly trained system administrator. Not understanding or reading the documentation, not following the security procedure are just a few examples of unintentional threats.
- Programmed threats such as logic bombs, viruses, worms, etc. can be a threat to a system. .
- Although most security mechanism protect best against outside intruders, survey after survey indicates that 80% of all attacks are made by insiders.

2. Basic Computer Security Measures

- *Physical Security***:** Most security expert notes that physical security of the system is more often than not is overlooked. Computers are often one of the most expensive item in a premises and proper guard against theft and other damages must be assessed:

a. Environmental damages from fire, smoke, dust, earthquake, explosion, biological, bugs, electrical noise, lightening, vibration, humidity and water.
b. Accidental damages from food and drink.
c. Physical access to the computers through air ducts and glass walls.
d. Vandalism and terrorism.

- *Personnel Security***:** Since computer security breach are caused by the people and employees are a big part of the people category -- it is important to have proper measures so the computer system, its operation or data and programs inside it are not easily compromised by them:

a. Background check for all applicants before hiring.

b. Provide initial training on security procedures and policies.
c. Provide ongoing training on policy and changed procedures.
d. Audit access to the equipment and data.
e. Give minimum access to an employee to get the job done and separate duties appropriately.
f. When an employee leaves, make changes to the system to prevent any further access.
g. Have written policy and procedure for key employees.
h. Outsiders get only temporary access at the minimum privilege required to get the job done.

- *Programmed Threats*: Be aware of all known program threats and check to ensure that appropriate measures are in place. It is suggested that security tools be used to check for holes in the system. Close all back and trap doors, if possible. Use appropriate commercial software to protect the system from viruses, worms, and the likes.

- *Backups*: Having backups for the full system can provide security for all data and save time if the system has to be restored. However, physical security for the backup also must be assured. Proper policy and procedure for backups must be in place for all department that value their data from any type of loss.

C. Networking

1. Remote Access

Computing and Information Technology provides a limited number of free modem lines and remote access servers for use by the University. Access to the modem lines is limited to 3 hours daily, unless prior approval is obtained through employee's supervisor and CIT personnel.

- Recreational use of modem lines and remote access servers is prohibited. This includes the use of any games, IRCs (Internet Relay Chat), MUDs (Multi-User Dimension), or recreational Bulletin Boards.

- Users shall not leave computers permanently dialed into the remote access servers.

- Users shall not use multi-user software and hardware (i.e. WinGate) to provide access to more than one computer.

2. IP Address Allocation

NC A&T State University has adopted the use of DHCP (Dynamic Host Configuration Protocol) to assign IP addresses. DHCP allows for the computer to automatically obtain an IP address from a DHCP server. DHCP allows for network personnel to document and track IP address allocation on campus. DHCP also allows for a fast and convenient method to change IP addresses in the event of a network reconfiguration. All computers and network devices on the NC A&T network must be configured to use DHCP, unless otherwise stated by CIT personnel.

- Users shall not manually enter IP address onto computers or network devices, unless prior approval is granted.
- Only IP addresses (152.8.X.X) officially designated for NC A&T may be used on University computers.

When a new computer or network device is connected to the network the following information shall be provided to the CIT helpdesk in order to register the device: Ethernet address (MAC), Machine type, Location, and owner. Once this information is obtained and entered into the DHCP server, the machine is registered and will get an IP address.

NC A&T has a different methodology in the use of DHCP. Instead of using DHCP to provide a truly dynamic IP address, A&T provides the same address all of the time. This is basically the same as providing a static IP address, but it eliminates user error when entering the address. It also lets computer staff make changes to a machine's network configuration without having to visit the machine.

3. Network Connections

It is becoming increasingly possible for computer systems owned by students, staff, or faculty to be attached directly to the University network via on-campus attachment or dial-in services. The use of the University network and dial-in services is subject to all of the policies stated in this document.

- User must submit to any authentication process and policies in place for the use of computing and network resources in campus, including the network access itself.
- All computers connected to the University network shall be properly registered and have a correct IP address.
- The owner of a computer connected to the University network is responsible for the behavior of users of that computer and for all network traffic to and from the machine.
- A system connected to the University network may not be used to provide network access to individuals who would not have access through official University systems. The system may not be used as a router to other networks nor may it serve in any way as an electronic gateway to non-University affiliated systems.
- Private systems may not use the University network for commercial gain or profit. Private systems may be used to support anonymous ftp, http, or gopher services when these services fall within the definition of scholarly or administrative use. Provision of interactive login services to non-University affiliated users is forbidden.
- Should the University have reason to believe that a privately owned system is using the network inappropriately, network traffic to and from that system will be monitored and, if justified, the system will be disconnected and action taken with appropriate authorities.
- A system connected to the University network may not be used to participate in any activities that may seriously offend or hurt others within or outside of the University community. These activities may include, but not limited to, distribution or transmission of pornographic materials and any literature promoting extreme views or supporting crime against other race, religion, sex, nationality, etc.

4. Port Scanning/Network Monitoring

The use of port scanning or network monitoring software, by persons other than CIT network personnel is forbidden. CIT personnel will occasional use port scanning and network monitoring tools to help solve network problems.

D. Software

Software is a term used to describe computer-generated applications that are designed to produce desired output. Various applications are available at the University because software is an essential component of each academic curriculum and every administrative operation.

Software that belongs to the University is to be used for University related business by employees, students, and guests. Persons that have not been extended formal invitations to the University are prohibited from using University resources.

Illegal or unauthorized use of software purchased, with University funds, includes but is not limited to:

- Removing software from the University without receiving approval from authorized personnel
- Not complying with licensing agreements for software, such as installation of software without appropriate license or installation of software in multiple machines without adequate licenses.
- Installing software on non-University computers without obtaining approval from authorized personnel
- Using software to gain unauthorized access to computer systems that may or may not belong to the University
- Disposing of software improperly
- Purchasing software with University funds not intended for University related business
- Making illegal copies of software
- Receiving personal compensation for business conducted with University owned software

Users that purchase software with non-University funds must receive approval from their supervisors before installing the software on University owned computers. Additionally, software installed in University computers must meet the University's set standard in place at the time.

Illegal use of computer software can be considered a violation of federal law, a breach of the license agreement, and/or copyright infringement.

E. Hardware

Computer hardware that is considered the property of the University is to be utilized for University related business by employees, students, and guests. Persons that have not been extended formal invitations to the University are prohibited from using University resources.

Illegal or unauthorized use of University computer hardware includes but is not limited to:

- Moving computer hardware within the University's jurisdiction from its original placement without seeking approval from authorized personnel
- Taking University computer hardware outside of the University's boundaries without seeking approval from authorized personnel
- Installing or attaching computer hardware peripherals without obtaining permission from authorized personnel
- Receiving personal compensation for business conducted with University owned hardware
- Inflecting intentional damage to University computer hardware
- Using hardware to gain unauthorized access to computer systems that may or may not belong to the University
- Disposing of computer hardware improperly

Computer hardware purchased with non-University funds must adhere to the Computing and Networking Usage Policy while being utilized to conduct University related business. . Additionally, all computer hardware to be installed must meet the University's set standard in place at the time.

Each department is responsible for keeping accurate inventory records for all of the computer hardware it purchases either for itself or another department or approved party. Property Management should be contacted for any questions a department has pertaining to inventory management.

The University reserves the right to declare any action involving conduct that isn't deemed in the best interest of the University illegal or unauthorized.

APPROVED BY COMPUTER ADVISORY COMMITTEE
07-06-00

F. World Wide Web

University Web Guidelines

The World Wide Web (WWW) is a diverse and complex resource with a great potential to educate. North Carolina Agricultural and Technical State University's WWW Servers are one channel for distributing information about the University, its programs, and its activities to the world.

General oversight of the University's WWW home page is the responsibility of the Office of Development and University Relations.

1. **General Policy**
   Official North Carolina Agricultural and Technical State University WWW pages may be created by any administrative or academic unit of the University or any student organizations properly registered with the Student Development Office. Units have discretion in creating and organizing pages provided they:
   - place an officially recognized emblem of the University and/or alternate text reading "North Carolina Agricultural and Technical State University" on their homepage for people who access the homepage via a text-only browser**;**
   - identify their relationship with North Carolina Agricultural and Technical State University on homepages as well as other pages**;**
   - are accurate, current, and appropriate for on-line use;
   - maintain their page(s) on the WWW in a timely manner;
   - are overseen by a contact person who gathers, organizes, formats, updates, deletes, and manages the pages; [If this position is unfilled for any length of time, the unit's access privileges may be revoked, and the unit's pages may be removed from network access.] and
   - comply with the style and technical guidelines established by the University Web Master and IT staffs.

   While the responsibility of preparing materials resides with each University unit, the Computing and Information Technology will provide workshops, documentation, and other resources to aid in the creation and maintenance of high quality WWW pages. Individuals publishing homepages are strongly encouraged to attend the workshops.

2. **Prohibited Use**
   North Carolina Agricultural and Technical State University's WWW Servers may not be used in any manner prohibited by law or disallowed by licenses, contracts, or University regulations. Units creating web pages are accountable for the information they "publish" and should be aware of University policies regarding confidential information, harassment, use of University

computers/resources, and intellectual property. Areas of concern include but are not limited to use of:

- copyrighted images, text, or software without permission or in violation of the copyright laws of the United States**;**
- pages to provide obscene, offensive, or threatening materials**;**
- pages for private financial gain or compensation not relevant to the mission of the University or otherwise in violation of the University's ethics policy;
- pages to intimidate or single out individuals or groups for degradation or harassment in violation of federal or state law, the University of North Carolina System's Model Computer and E-mail Policies, and other University policies;
- pages to provide materials whose nature or volume compromise the ability of the server to serve other users' documents; and
- pages to engage in any illegal activity.

In cases where there is a violation of these guidelines or related regulations or laws, a page may be removed from network access while the matter is referred to the appropriate University authority. Violators will be subject to University rules and regulations. Anyone who is uncertain whether a particular use is proper should consult with University Web Master.

3. Linking to Commercial Websites

It is not within the purview of the Web Advisory Committee to pick and choose among the many web sites outside the University for the purpose of creating links from University pages to those sites, thereby making implicit endorsements. Therefore, it is the University's policy not to link to non-University personal pages, businesses and institutions on team-maintained, top-level University menus. However, individual research groups, departments and other organizations within the University are not prohibited from linking to non-University pages that offer information relevant to their area of expertise and reflect the same high standards expected of publications at North Carolina Agricultural and Technical State University.

4. Style Guidelines

- The document should be dated and updated with revision dates. The Web site should not be cluttered with obsolete information. In addition, links to outdated pages will be broken.
- **Files may not include confidential student data.**
- There should be a link to files already available on the Web, instead of recreating the data, particularly if the data is "owned" by another college/department. The Web coordinator has the right to disconnect the link to any contested data; the link will not be reestablished until ownership has been resolved in writing.

- 0There should be a link to the University home page at the end of each unit's homepage. This link should match the one shown on top level University menus.
- All first level pages must follow the style guidelines outlined by the Office of Development and University Relations.

5. **Personal Web pages of Students and Employees**

The University is not responsible for information, including photographic images, published on or accessible through personal Web pages, including personal home pages. Personal Web pages created and maintained by employees and students are the sole responsibility of the person identified by the account. The University does not monitor the contents of these personal Web pages.

The individual creating or maintaining personal Web pages may be held liable for the materials posted on the Web site.

Personal Web pages contain the personal expression of their creators. The contents, including link identifiers, of these pages include academic subjects, hobbies, religion, art, and politics, as well as materials that some viewers may find offensive. Neither the contents nor the link identifiers are reviewed or endorsed by the University.

The University will investigate all complaints involving personal Web pages and will remove or block material or links to material that violate federal or state law or University policy.

6. **Disclaimer**

North Carolina Agricultural and Technical State University disclaims all responsibility for servers that may emerge other than the North Carolina Agricultural and Technical State University's WWW Servers. No such server may use North Carolina Agricultural and Technical State University's name, logo, or other symbols identified with the University nor purport to speak for the University or any of its units nor imply an association with or sponsorship by the University.

G. Academic Computing Facilities

North Carolina Agricultural and Technical State University has provided academic computing facilities for students, faculty and staff to conduct academic work and research. There are many open computing facilities sponsored by CIT and a host of specialized labs available via Departments.

- Users are expected to take proper care of the equipment in University facilities and to report any malfunction to staff on duty or to the organization responsible for the facilities and to report any malfunction to staff on duty or to the person in charge for the facility immediately. Users shall not attempt to move, repair, reconfigure, modify, or attach external devices to the systems. No food or drink is permitted in public facilities, unless otherwise posted.
- Recreational use of workstations in open university facilities during periods of light usage is permitted; however, games may not be played or recreational activities engaged in when others are waiting to use the workstations for academic purposes.
- Individual computer center facilities and other Departmental facilities may post additional operational rules and restrictions. Users are responsible for reading and following these rules.
- Children are allowed in open university facilities but must be accompanied by an adult affiliated with this University. During the times children are using the computers and a University user needs a machine and no other machines is available; the child must forfeit their seat to a University user waiting to use the facilities.
- Media needed to store data can be purchased at A&T Bookstore located in Brown Hall on the campus.
- Users must refrain from noise, sound effects, violent motion, etc., which may disturb others in the facility.
- Software installation in Academic Computing facilities by users is prohibited.
- Foreign devices are not allowed unless specific authorization by manager in charge is granted (such as: external disk, printer or video system).

H. Privacy

It is the policy of NC A&T to treat all transmissions over the network as private; however, all material residing on, or sent or received over the University computing systems or networks is public record (according to NC General Statutes 121 and 132), and subject to University inspection, examination, and management.

The University may monitor certain computing systems or networks, if it

- Has reason to believe that an account or system has been breached and is being used by someone other than the authorized user;
- Has received a complaint that an account or system is being used to gain unauthorized access or to attempt to gain unauthorized access to another network site;
- Has reason to believe that an account or system is being used in violation of University Policy, Federal, State or Local law; or
- Is required to audit activities in accordance with EDP audit policies, Federal, State, or Local laws.

The University reserves the right to take whatever steps are necessary to investigate possible network security threats, to investigate suspected violations of regulations, or to assist appropriate authorities to investigate suspected illegal activities. A request to monitor the activities of a suspected abused account may be obtained from the CIO.

If the University inadvertently discovers messages or data files within its network that leads it to suspect the presence of illegal activities or activities that violate University policies, then the University will be free to use that discovered information to pursue investigations or to inform the appropriate authorities.

User Right to Privacy

Users are advised to consider the public nature of information they disseminate on the Internet through the World Wide Web. Information in a home page is published and available to everyone who can get to the World Wide Web. Students must not assume that their information is restricted to only a close circle of friends, or even the campus community.

The University will not impose any restraints on, nor make any effort to monitor the content of, communications other than those imposed by applicable Federal, State or local laws, including laws regarding the right to privacy and laws which prohibit defamatory material. Users of the University's information systems are advised that their communications are subject to such laws and that the consequences of violations can be severe.

APPROVED BY COMPUTER ADVISORY COMMITTEE
07-06-00

I. General

A. Chain Letters

The writing and forwarding of chain letters is considered a violation:

> **Use of electronic mail and other network communications facilities to harass, offend, or annoy other users of the network is forbidden.**

Chain letters are clearly an annoyance to most users in addition to being a waste of technical resources and potentially illegal (see Ponzi Schemes below). Users who receive unsolicited chain mail should report the incident to the Aggie Help Desk in Computing and Information Technology. Users who forward chain mail should be aware that their usernames appear in the forwarding path.

Ponzi schemes are against the law. A Ponzi scheme is a form of chain letter that requests recipients to send money to people on a list. The US Supreme Court has determined that Ponzi schemes are inherently fraudulent. The US Criminal Code, 18 USC 1341-1346, prohibits the use of mail or wire in any attempt to defraud. Note that under the wire fraud statutes, the attempt to defraud is a violation, and all who are involved in the attempt, whether intentionally or not, may also be in violation.

B. Spamming

Spam is generally defined as unsolicited bulk email – "unsolicited" because recipient did not ask for it and "bulk" because spammers send the same message to hundreds of unwilling recipients at he same time. Everyone pays for spam. Spam uses up limited bandwidth and slows down the university network and Internet. Spam clogs up mailboxes and disrupts Internet service. Accordingly, unsolicited bulk emailing is considered a violation:

> **Use of electronic mail and other network communications facilities to harass, offend, or annoy other users of the network is forbidden.**

APPROVED BY COMPUTER ADVISORY COMMITTEE
07-06-00

IV. Sanctions for Policy Violations

Alleged violations of this policy shall be processed according to the judicial processes outlined in the University Faculty Handbook, the Human Resources (HR) Manual and the Student Handbook. North Carolina Agricultural and State University treats access and use violations of computing facilities, equipment, software, information resources, networks, or privileges seriously and may also prosecute abuse under appropriate state and federal statues.

Misuse of Computing and Information Resource Privileges

If, in the best judgment of the system administrator, the action of one user threatens other users or if a system or network for which the system administrator is responsible is in grave, imminent danger of crashing, sustaining damage to its hardware or software, or sustaining damage to user jobs, the system administrator should act quickly to protect the system and its users. In the event that he or she has had to inspect user files in the pursuit of this important responsibility, he or she **must** notify, as soon as possible, his or her own administrative officer or other individual designated by that administrative officer of his or her action and the reasons for taking that action. The administrative officer needs to be certain that one of the following are also notified as soon as practical (ordinarily within one business day): the user or users whose files were inspected; the user's supervisor, project director, administrative officer, or academic advisor.

In cases in which the user is not available in a timely fashion, in which the user is suspected of malicious intent to damage a computer system, or in which notifying the user would impede a sensitive investigation of serious computer abuse, the system administrator may inspect the information in question so long as he notifies his or her own administrative officer or other individual designated by the administrative officer of his or her actions and the reasons for taking those actions. The administrative officer needs to be certain that the user's supervisor, project director, administrative officer, or academic advisor is notified of the situation. In the case of suspected malicious intent, the administrative officer may also need to refer the matter to the appropriate University judicial body or to the University Police.

A system administrator may find it necessary to suspend or restrict a user's computing privileges during the investigation of a problem. The system administrator should confer with his or her administrative officer or other person designated by that administrative officer before taking this step. A user may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the appropriate University grievance process, or by petition to the Chief Information Officer (CIO).

In general, then, a system administrator should

- protect the integrity of the system entrusted to his or her care
- respect the confidentiality of the information users have stored on the system
- notify appropriate individuals when the above two aims have come into conflict

- assist his or her administrative officer in referring cases of suspected abuse to the appropriate University judicial process.

Judicial Process for Cases of Alleged Misuse of Computing and Information Resource Privileges and Penalties for Misuse of Computing and Information Resource Privileges

If a preponderance of evidence that intentional or malicious misuse of computing resources has occurred, and if that evidence points to the computing activities or the computer files of an individual, CIT has the obligation to pursue **any or all** of the following steps to protect the user community:

- Take action to protect the system(s), user jobs, and user files from damage.
- Notify the alleged abuser's project director, instructor, academic advisor, dean, or administrative officer of the investigation.
- Refer the matter for processing through the appropriate University judicial system. If necessary, staff members from a central computing agency such as Computing and Information Technology as well as faculty members with computing expertise may be called upon to advise the University judicial officers on the implications of the evidence presented and, in the event of a finding of guilt, of the seriousness of the offense.
- Suspend or restrict the alleged abuser's computing privileges during the investigation and judicial processing. A user may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the University's judicial system, through the grievance procedures outlined by the University, or by petition to the Chief Information Officer (CIO).
- Inspect the alleged abuser's files, diskettes, and/or tapes. System administrators must be certain that the trail of evidence leads to the user's computing activities or computing files before inspecting any user's files.

Ordinarily, the administrative officer whose department is responsible for the computing system on which the alleged misuse occurred should initiate judicial proceedings. As the case develops, other administrative officers may, by mutual agreement, assume part of the responsibility for prosecuting the case.

Abuse of computing privileges is subject to disciplinary action. Disciplinary action may include the loss of computing privileges and other disciplinary sanctions up to and including non-reappointment, discharge, and/or dismissal. An abuser of the University's computing resources may also be liable for civil or criminal prosecution.

It should be understood that nothing in these guidelines precludes enforcement under the laws and regulations of the State of North Carolina or county therein, and/or the United States of America.

References

Adapted from the University of Delaware Policy for Responsible Computing. University of Delaware 1994. http://www.udel.edu/eileen/Ecce/policy.approved.html.

University of Delaware Recommended Guidelines for Units Implementing The Policy for Responsible Computing at the University of Delaware. University of Delaware 1993. http://www.udel.edu/eileen/Ecce/guide.020293.html.

Northwestern University Information Technology Policies and Guidelines. Northwestern University, July 1999. http://www.it.nwu.edu/policies/

Section 1 is adapted from *Electronic Rights and Responsibilities at the University of North Carolina at Chapel Hill.* effective August 29. 1994.

Section II is adapted from *Ethics In Computer Usage. at the University of Virginia.* effective July 23. 1996.

Sections III through XI are adapted from the *North Caroling State University Computer and Network User Policy.* effective June 23. 1995.

Section XII is adapted from the *North Carolina State University Computer and Network User Policy: Guidelines and Procedures for Determining Ownership of Computer Software.* effective July 1. 1987.

Section XIII is adapted from the *North Carolina State University Computer and Network User Policy: Web Guidelines.* effective June 23. t995: and *Angelo State University: World Wide Web Policy* (August 23. 1996).

APPROVED BY COMPUTER ADVISORY COMMITTEE
07-06-00

Appendix A

Definition of Terms

Data Owner - The individual of department that can authorize access to information, data, or software and that is responsible for the integrity and accuracy of that information, data, or software. The data owner can be the author of the information, data, or software or can be the individual or department that has negotiated a license for the University's use of the information, data, or software.

System Custodian - The staff employed by a central computing department, such as Computing and Information Technology, whose responsibilities include system, site, or network administration *and* staff employed by other University departments whose duties include system, site, or network administration. System custodians perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. If you have a computer on your desk, you may be acting, in whole or in part, as that system's system custodian.

Users - Someone who does not have system custodian responsibilities for a computer system or network but who makes use of that computer system or network. A user is still responsible for his or her use of the computer and for learning proper data management strategies.

Security Administrator - The individual responsible for carrying out the security policies for the University.