

THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

INFORMATION TECHNOLOGY

Effective Date: April 1985
Revised Date: April 2001

Page 1 of 8

UT Health Science Center is committed to developing and maintaining a technology infrastructure that supports its mission of teaching, research, patient care and public service in a manner that is unsurpassed. To accomplish and fulfill this commitment, UT Health Science Center has adopted a centrally supported digital network that enables an open flow of information within the University and between the University and the public. This information system is managed through a coordinated infrastructure that decentralizes responsibility for publication and stewardship to the sources of most of the information, the academic and administrative units. Similarly computing administration and the academic and administrative units share responsibility for the hardware and software utilized. Computing and Telecommunications is charged with providing the campus network, information systems and services by serving as an information utility, and by coordinating information technology development, acquisition and implementation within the framework of the institutional mission and institutional policy. Computing and network facilities and services are supported by a hybrid funding model with state funding for University-wide services and an established fee structure for specific functions and services. The UT Health Science Center Planning Committee addresses the allocation of computing resources.

This document sets forth the policy by which computing is structured and utilized to support the UT Health Science Center's mission; affirms UT Health Science Center's commitment to compliance with the Tennessee Computer Crimes Act (enacted into law on April 20, 1983) which prescribes penalties for certain activities related to computer usage; and is in compliance with University Fiscal Policy Statement 05, Section 135. Violations of provisions of this Act are considered to be a crime; and, faculty, staff, and students may be held personally liable for such violation. "Information resources" as used in this document include accesses, computers, computer networks, computer programs, computer software, and computer systems as defined in the Computer Crimes Act. The Act may be found through the UT Health Science Center Homepage.

INFRASTRUCTURE

The infrastructure at UT Health Science Center is a switched fiber optic backbone network (hereinafter referred to as UT Health Science Center Network) that interconnects networks on the campus to the central computing facility and to each other. To maintain an infrastructure sufficient to support the needs of the campus, utilize the infrastructure to the fullest, and provide adequate service to all users:

- 1) Computing and Telecommunications (hereinafter referred to as CT) will oversee maintenance and development of the infrastructure.
- 2) CT will insure that a periodic review of the infrastructure is conducted by an independent, non-vendor-related firm.
- 3) Adequate space and security for wiring and communications closets will be made available within prescribed requirements (see CT Operational Guidelines, Criteria for Communications Closets, on the CT Home Page).
- 4) CT will assure that wiring is maintained at approved standards throughout the campus.
- 5) CT will assure that demands are met for remote site access to the UT system and Internet service. CT will fulfill this responsibility by maintaining a service agreement between the University and an appropriate vendor and by assuring that the services are provided in accordance with that agreement.

SECURITY

Security is defined as the provision of adequate safeguards against threats in order to maintain confidentiality, reliability, availability, and integrity of information resources. University information resources are vital assets, which require protection. CT is responsible for assuring the security of the network operations and applications.

Faculty, students and staff are expected to follow security policy. The circumvention of security controls for information resources is a violation of this policy. Assisting anyone or requesting anyone to circumvent security controls also is a violation of this policy.

All information processing areas used to house information resources supporting mission critical applications must be protected by physical controls that are appropriate for the size and complexity of the operations and the sensitivity of the systems operated at those locations. Physical access to these areas shall be restricted to authorized personnel. Authorized visitors are to be supervised and their entry and exit recorded in a log.

The central computer resource will restrict access to authorized personnel using access locks on machine room doors; daily security audit reporting, monitoring console logs for break-in alarms; restricted access to privileged accounts based on job requirements; and, frequent password changes for privileged accounts.

Those who have access to servers potentially have access to the entire network; therefore, end-users housing servers must protect them by using software which provides password and virus protection, limiting physical access to authorized personnel, restricting modem connection, and allowing CT to test security as necessary.

Each individual should have a unique password. Passwords should not be shared. Passwords should be changed every 90 days on all information resources used for mission critical applications. Passwords for access to systems managed by CT will be issued by CT; these passwords must be changed periodically by the named owner of the account.

End-users should secure their workstations used in sensitive or critical tasks with adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system. Adequate controls are defined as using password protection software and virus protection software (see CT Operational Guidelines, Software Standardization, on the CT Home Page). Also, it is the responsibility of the end user to backup the system as described in CT Operational Guidelines, Backup Procedures, on the CT Home Page. The security controls over the backup resources are as important as the protection of the central resources.

Information resources may be used only for University/work-related purposes. The Tennessee Open Records Act requires that certain records be made available for inspection on request; however, the process of requesting access to such records is by submitting a request to the Office of General Counsel. The Open Records Act does not authorize copying or distribution of records, and it is a violation of this policy to distribute information resources or the output of information resources in any other way.

Unauthorized use, alteration, destruction, or disclosure of information resources is a violation of University policy and a computer-related crime, punishable under the Tennessee Computer Crimes Act and federal Copyright Act which are available through the UT Health Science Center Home Page and the CT Home Page. It is safest to assume that activities, which are unlawful in terms of printed material, such as alteration of a signature, are likewise unlawful in terms of online material. Faculty, students, and staff are responsible for knowing and adhering to these statutes.

University-wide Fiscal Policy states that, "Users must recognize that information systems can never be absolutely secure, and the University cannot guarantee the privacy of users, their computer files, or their communications. The University also reserves the right to preserve or inspect for business reasons any information transmitted through or stored in its computers, including electronic mail communications. Such business reasons include, but are not limited to, violations of this policy and any campus guidelines or procedures established to implement this policy, violations of any other University policies, or as required by law. Employee electronic mail may be a public record and may be open to public inspection.

Network traffic will be monitored on a routine basis to identify loads to adequately size the network and to identify usage patterns. CT may monitor specific traffic where there is substantial evidence of a violation of law and may filter spurious traffic that has the potential to adversely affect the system.

Computer software purchased using any University funds is University property and users of this software should protect it as such in accordance with University Fiscal Policy 05, Section 135, Part 02.

University software should not be distributed, sold, taken home for personal use, or copied unless allowed by the software license agreement. It is the responsibility of the user to be aware of the content of software license agreements associated with any software. Fiscal Policy Statement 05, Section 135, Part 02 provides more detailed guidelines related to software copyright compliance and licensing agreements.

HARDWARE AND SOFTWARE

Certain information technology standards have been adopted to insure integrated technology, efficient resource utilization, minimal redundancy, and maximum economies. CT has developed

campus standards for hardware and software that meet campus operational needs and will be supported by CT. These standards are set forth on the CT Home Page. In order to assure effective and efficient implementation of the policy, CT is assigned oversight responsibility for

all purchases of information technology hardware and software. All units should consult with CT to develop an information technology strategy to best meet the needs of their respective units. CT should be contacted for consultation prior to negotiations with vendors or for grants, contracts, collaborations or corporate alliances for acquisition of information technology hardware and software including equipment, computing cycles, programming requirements, and software applications

Hardware

Hardware is defined as the physical aspect of computers, telecommunications, and other information technology. Hardware includes not only the computer monitor and processing unit but also the cables, connectors, power supply units, and peripheral devices such as the keyboard, mouse, audio speakers, and printers.

The UT Health Science Center campus has adopted the Intel based/Intel compatible computing environment as the preferred desktop workstation hardware of choice for administrative systems. CT will provide support for Macintosh hardware.

Standard Hardware. It is very important that hardware be verifiably reliable and efficient and of good quality, therefore, computer hardware should be selected from the standard information technology hardware which is listed on the Computer Acquisition Page (see CT Home Page). It is understood that the standard technology is not always the least expensive. Purchases of standard hardware are covered under the UT Knoxville contract and therefore the bidding process is not required, shipping and handling charges are eliminated, and a three-year maintenance is mandatory with all purchases. Standard hardware is purchased by submitting a Purchasing Requisition to the Purchasing Office.

Due to the fact that non-standard hardware may be incompatible with the network or may have other quality issues, requests for acquisition of personal computer hardware not included on the Computer Acquisition Page is discouraged and requires approval of CT.

Hardware acquisitions of servers and other multi-user devices not included on the standard acquisition list require prior approval of CT.

Servers. In order to be connected to the UT Health Science Center Network, servers must be registered with and meet security requirements of CT. A Server Registration Form is available from the CT Home Page. CT will have administrator access to all

servers connected to the UT Health Science Center Network and will audit these servers for security purposes. If security audit by CT reveals security problems, it may be necessary to disconnect the server from the network. Servers must be protected in accordance with provisions set forth in the "Security" section above.

Modems. Due to the significant risk posed to campus network security, modem connection to the UT Health Science Center Network requires authorization by CT. CT will

review each specific request and make security recommendations based on the individual case.

Software

While the value of equipment such as computer hardware is easily appreciated, the larger investment in less tangible information assets such as software, data and automated processes is critical to the overall success of all UT Health Science Center computing. Computer software is defined as a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system, or computer network.

Electronic Mail. Electronic mail is intended to be a convenient and economical way for the faculty, staff, and students to communicate with one another as well as colleagues at other locations. In order for campus communications to flow smoothly, all users of electronic mail will have University electronic mail accounts. Electronic mail is considered a University-wide service and is therefore supported by state funding. Electronic mail accounts are available from CT by request.

Internet Access. Software providing access to the Internet (World Wide Web) is available from CT. This will enable the user access to specialized plugins. See also "Internet Usage" below.

Standard Software. A listing of standard software is available on the CT Home Page (see CT Operational Guidelines, Software Standardization). CT supports this standard software and works with General Stores to stock the software at an economical price to the University. Software that is not listed as a University standard is not supported by CT. Requests for acquisition of software not included in the listing requires approval of CT.

Application Software. CT will assist areas in analyzing systems to determine whether commercial software packages will sufficiently meet computing application needs. If existing commercial software is not available to meet system requirements, in-house development will be considered.

Development Priorities. While it is preferred to purchase application software when available, CT is committed to developing state-of-the-art systems. CT will maintain an application development and technology support staff for the purpose of developing and supporting computing applications and resources on campus.

Application requests are prioritized by Deans and Vice Chancellors within their area of responsibility. The Planning Committee is responsible for addressing the priorities on a campus-wide basis and for allocation of funding and computing resources in response to needs of the campus.

Internet Usage.

This section establishes rules governing use of University of Tennessee Health Science Center (“UTHSC”) Internet services. The Internet is a powerful communications tool and a valuable source of information. Every individual who uses the UTHSC Internet is expected to conduct themselves honestly and appropriately, and to respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others and all other legal requirements. It should be understood that UTHSC policies apply to an individual’s conduct on the Internet, including but not limited to intellectual property protection, privacy, misuse of University resources, sexual harassment, information and data security and confidentiality. The overall purpose of this policy is to ensure that all individuals use UTHSC Internet services in a productive, ethical and lawful manner while recognizing the rights of academic freedom, freedom of speech and privacy.

An Internet service includes, but is not limited to, FTP, telnet, web browsing, and Usenet newsgroups. This policy applies to any Internet service that is:

- Accessed on or from UTHSC premises; or,
- Accessed using UTHSC computer equipment or via UTHSC access methods.

Policy

1. Employees are strictly prohibited from using UTHSC provided Internet service in connection with any of the following activities:
 - Engaging in illegal, fraudulent, or malicious conduct;
 - Working on behalf of organizations without any business or professional affiliation with UTHSC
 - Using the Internet to break any UTHSC work rule.
 - Obtaining unauthorized access to any computer system;
 - Using another individual’s identity, password or other access privileges without explicit authorization; or,

- Attempting to test, circumvent, or defeat security or auditing systems of UTHSC or any other organization without prior authorization.
2. Internet Services are provided by UTHSC for business use only. Very limited or incidental use of Internet services for personal nonbusiness purposes may be acceptable. However, personal use must be infrequent and must not:
 - Involve any prohibited activity
 - Interfere with the productivity of the employee or his/her coworkers;
 - Consume system resources or storage capacity on an ongoing basis; or
 - Involve large file transfers or otherwise deplete system resources available for business purposes.
 3. UTHSC currently has software and systems in place that can monitor and record all Internet usage. These systems are capable of recording, for each and every user, each World Wide Web site visit and each transfer in and out of our internal networks. Monitoring of UTHSC Internet activity and analysis of usage patterns will be conducted on an ongoing basis. In the event there is a reasonable belief that UTHSC policy has been violated, UTHSC reserves the right to inspect any and all files stored within UTHSC networks to assure compliance with this policy. Employees violating this policy are subject to discipline, up to and including termination of employment.
 4. Employees using UTHSC computer system for the above prohibited purposes also are subject to civil liability and criminal prosecution.

Web Page Development/Ownership

CT maintains the UT Health Science Center World Wide Web Server to aid the instructional, research, and administrative activities of the campus, and to provide access to global electronic resources. The organization of this server is designed to:

- 1) provide information about UT to both the University community and the outside world with clarity and accuracy;
- 2) organize network resources for the use of UT students, faculty, staff, alumni, and others;
- 3) enable members of the UT community to publish their own information, within the general guidelines of the institution, in the manner they deem most appropriate.

Access To Publishing

CT will maintain a UT Health Science Center home page that provides official general information concerning the institution, its organization and its policies and that provides pointers to home pages of UT Health Science Center units.

Any officially recognized UT office, unit, project, program, area, or student organization, as well as any individual faculty, student, or staff member, may publish via the UT Health Science Center Network in accordance with University policies, procedures and guidelines.

UT Health Science Center recognizes the value and potential of personal publishing on the Internet and so allows students to produce personal Web pages. Faculty and staff personal pages are permitted when created by the individual in his/her capacity as a University employee to promote his/her role with the University and its programs. Personal pages published via the UT Health Science Center Network cannot be used for personal gain. The University accepts no responsibility for the contents of these pages and will not undertake to edit or pre-approve these pages; but, does reserve the right to monitor such pages when published through the University servers and to remove any materials that may be disruptive, offensive to others, harmful to morale, or otherwise in violation of University policies and procedures.

University Fiscal Policy Section 175, Part 01 states, "UT cannot protect users from the presence of material they may find offensive. However, such presence must not be represented nor construed as an endorsement or approval by UT."

All units or individuals desiring to publish must register their intent with CT and be in compliance with the UT Network Publishing Guidelines available on the CT Home Page (see CT Operational Guidelines, UT Network Publishing Guidelines).