

UNIVERSITY OF TENNESSEE SYSTEM POLICY INFORMATION TECHNOLOGY

POLICY NO.: IT0110 **SUBJECT:** ACCEPTABLE USE OF INFORMATION
TECHNOLOGY RESOURCES

EFFECTIVE: 08/04/2006

OBJECTIVE:

Information technology resources are valuable assets provided to enhance the core functions of the University of Tennessee. The use of the university's information technology resources is a privilege extended to authorized users for education, research, service, and administration. This ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES POLICY (AUP) governs the use of the university's information technology resources in an atmosphere that encourages free exchange of ideas and an unwavering commitment to academic freedom. The university community is based on principles of honesty, academic integrity, respect for others, and respect for others' privacy and property. The university seeks to:

- protect the confidentiality and integrity of electronic information and privacy of its users, to the extent required or allowed under federal and state law, including the Tennessee Public Records Act.
- ensure that the use of electronic communications complies with the provisions of university policy and state and federal law; and
- allow for the free exchange of ideas and support of academic freedom.

The university cannot protect users from the presence of material they may find offensive. The presence of such material must not be represented or construed as an endorsement or approval by the university.

This policy applies to all students, staff, and others, referred to as users throughout this policy, while accessing, using, or handling the University of Tennessee's information technology resources. In this policy, "users" include but are not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities granted access. All "users" are required to be familiar with and comply with this policy.

POLICY:

General Policy

1. All users are expected to act in a responsible, ethical, and lawful manner when using the university's information technology resources.
2. The university's information technology resources are provided for use in conducting authorized university business. Using these resources for personal gain, illegal, or obscene activities is prohibited.
 - a. The prohibition against using the university's information technology resources for personal gain does not apply to:
 - i. Scholarly activities, including the writing of textbooks or preparation of other teaching materials by faculty members, as recognized in the STATEMENT OF POLICY ON PATENTS, COPYRIGHTS, AND LICENSING.
 - ii. Consulting and other activities that relate to the faculty member's professional development or as permitted under university policy. For approved consulting and other activities, see

policies on outside services in campus/institution faculty handbooks.

- b. Minimal personal use of these resources is permitted by this policy, except when such use:
 - i. Is excessive or interferes with the performance of the user's university responsibilities;
 - ii. Results in additional incremental cost or burden to the university's information technology resources;
 - iii. Is otherwise in violation of this policy; or
 - iv. Violates any state or federal law.
 - c. University departments may impose further restrictions upon personal use.
3. Users observing any illegal activities should report their observance to the appropriate university administration. Although not an inclusive list, examples include theft, fraud, gambling, copyright infringement, illegal electronic file sharing, sound or video recording piracy, hacking, and either viewing or distributing illegal pornography.
 4. Abuse of networks or computers at other sites through the use of the university's information technology resources will be treated as an abuse of the university's information technology resource privileges.
 5. State law prohibits the use of university resources for campaign or political advertising on behalf of any party, committee, agency, or candidate for political office. (Tennessee Code Annotated § 2-19-201 et seq.). This prohibition does not prohibit discussion or use of university resources to discuss or examine political topics or issues of public interest so long as the use of university resources does not advocate for or against a particular party, committee, agency, or candidate.
 6. Computer viruses present a threat to the university's computing and networking environment. A virus infection may manifest itself in the loss of data, disruption of computer and server software applications, compromises to the security of the network and connected computers, disruption of network services, and lost faculty, staff, and student productivity. To lessen the threat of computer viruses within the university environment, users must adhere to the following practices (when technically possible):
 - a. All computer systems are required to have a university-approved anti-virus software package installed and running when available.
 - b. Real time protection (background scanning) should be activated if the computer is attached to the university's network. Full disk scans are to be performed at a minimum of once a week if real time protection is activated.
 - c. If real time protection is not activated, full disk scans are to be performed once a day.
 - d. Software virus definitions must be updated and kept current at all times.
 7. The most recent security patches must be installed on the system as soon as technically feasible. The only exception will be when an immediate application would interfere with business and/or operational requirements.
 8. Software such as database software, communications software, and other software with system-level authorization is often the target of hackers. Hackers look for vulnerabilities and attack soon after those vulnerabilities are found. Therefore, these software products should be maintained in the same manner as the operating system software. As new patches are made available, they should be applied and tested just as the operating system patches are handled. This effort can be combined for multiple patches or multiple software products as long as the process is sufficient to test each.

User Prohibited Activities

9. As stated in **item 1** above, all users are expected to act in a responsible, ethical, and lawful manner when using the university's information technology resources. The following are examples, but are not an exhaustive list of the prohibited activities.
- a. The use of the university's information technology resources to attempt unauthorized use or interference with the legitimate use by authorized users of other computers or networks elsewhere which includes misrepresentation of his or her identity to other networks (e.g., IP address "spoofing") from the university's information technology resources;
 - b. Modification or reconfiguration of the software, data, or hardware of the university's information technology resource (e.g., system/network administration, internal audit) without appropriate authorization or permission;
 - c. Knowingly creating, installing, executing, or distributing any malicious code (including but not limited to viruses, worms, and spyware) or another surreptitiously destructive program on any of the university's information technology resource, regardless of the result;
 - d. "Hacking" into university computers or networks. This activity may be subject to prosecution by state or federal authorities;
 - e. Copyright infringement including illegal file sharing of video, audio, or data;
 - f. Using a computer system attached to university resources to capture data packets (e.g., "sniffer") except for authorized or other official university business that includes teaching and learning activities;
 - g. Launching denial of service attacks against other users, computer systems, or networks;
 - h. Use of the university's information technology resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by state or federal laws is prohibited under this policy;
 - i. Accessing (e.g., read, write, modify, delete, copy, move) another user's files or electronic mail without the owner's permission regardless of whether the operating system allows this access to occur except in cases where authorized by the university;
 - j. Knowingly interfering with the security mechanisms or integrity of the university's information technology resources. Users shall not attempt to circumvent information technology protection schemes or exploit security loopholes;
 - k. Connecting devices (switches, routers, hubs, computer systems, and wireless access points as examples) to the network that are not approved by the central information technology organization at the campus or institution. It should be noted that connecting through a university provided authorization process is considered, by default, to be approved access;
 - l. Connecting any device that consumes a disproportionate amount of network bandwidth;

- m. Intentionally physically damaging or disabling university computers, networks, or software without authorization.

Administrative and Department Requirements

10. Each departmental unit is responsible for security on its computer systems and may apply more stringent security standards than those detailed here while connected to the university's information technology resources; however, they must follow these principles and rules as a minimum or risk losing connectivity to the university's networks and/or use of information technology resources.
11. System administrators are responsible for ensuring that appropriate security is enabled and enforced in order to protect the university's information technology resources.
12. System administrators must make every effort to remain familiar with the changing security technology that relates to their computer systems and continually analyze technical vulnerabilities and their resulting security implications. Stored authentication data (e.g., password files, encryption keys, certificates, personal identification numbers, and access codes) must be appropriately protected with access controls, encryption, shadowing, etc.

Remediation

13. Abuse of university policies, resources, or abuse of other sites through the use of information technology resources may result in termination of access, disciplinary review, expulsion, termination of employment, legal action, and/or other appropriate disciplinary action. Notification will be made to the appropriate university office (e.g., appropriate office for student conduct matters, human resources, general counsel, the police department with campus or institute jurisdiction) or local and federal law enforcement agencies.
14. The position of authority for information technology at the respective campus or institute is authorized to isolate and/or disconnect computer systems from the network while assessing any suspected or reported security incident in order to minimize risk to the rest of the university's network.

Software License Agreements

15. If a software package includes a license agreement that details restrictions on the use of the software, the university expects software users to follow the provisions in these license agreements regarding copying, improvements, number of concurrent users, and similar provisions, even though the university has not signed the license agreements and may not agree to be bound by certain other provisions of the agreements.
16. License agreements differ among software publishers. It is important that users read and understand the license agreement for each software package.
17. Questions about computer software use not addressed by this policy or questions about specific license agreements should be directed to the position of authority for information technology at the respective campus or institute.
18. Each department is responsible and accountable for maintaining records on the license information for the software that they have purchased. The maintenance of records and information related to centrally provided software is the responsibility of the organization that provides it and subject to internal audit review for compliance.

Privacy

19. While the university recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned information technology resources and communications infrastructure.

20. The university reserves the right to preserve or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:
 - a. There is reasonable cause to believe the user has violated or is violating this policy, any campus or institute guideline or procedure established to implement this policy, or any other university policies;

 - b. An account appears to be engaged in unusual or unusually excessive activity;

 - c. It is necessary to do so to protect the integrity, security, or functionality of the university's information technology resources or to protect the university from liability; or

 - d. It is otherwise permitted or required by policy or law.

21. All freedom of information act requests to review or receive copies of university records or information and all subpoenas should be referred to the campus or institute Office of Public/University Relations. The Office of Public/University Relations will review the request, determine the parties that need to be involved in evaluation of the request, and determine whether the information should be disclosed under the Tennessee Public Records Act. Once classified as public, additional review by the Office of Public/University Relations is not necessary. The information owner shall consult the Office of Public/University Relations prior to establishing the classification of the information. Subpoenas with a prohibition on disclosing the existence of the subpoena should be referred to the Office of General Counsel.