

Acceptable Use of Information Technology Resources (IT0110)

This document describes guidelines for using The University of Tennessee's computer and Information Technology Resources

DRAFT DATE – 10/18/2007

OBJECTIVE

Users of The University of Tennessee's Information Technology (IT) resources have a responsibility to properly use and protect those resources and to respect the rights of others. The use of the university's IT 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 IT resources in an atmosphere founded on the following principles:

- University Information and IT resources are provided to support the mission of the university. Protecting the confidentiality, integrity, and availability of this information and IT is essential.
- The use of IT is governed by federal and state laws, industry regulations, and university policies and best practices.
- The university seeks to protect the confidentiality 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.
- Users are expected to use IT in a responsible, ethical, and lawful manner. Simply because an action is technically possible does not mean it is legal or appropriate.
- The university seeks to allow for the free exchange of ideas and supports academic freedom.
- The university cannot protect users from the presence of materials they may find offensive. The availability of such material must not be represented or construed as an endorsement or approval by the university.

SCOPE:

Individuals covered

This policy applies to all students, faculty, staff, and others, referred to as "users" throughout this policy, while accessing, using, or handling the university's IT resources. In this policy, "users" includes but is not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities or individuals that are granted access.

Resources Covered

This policy applies to all university IT resources whether individually controlled, shared, stand-alone, or networked. It applies to all computers and communication facilities owned, leased, operated, or provided by the university or otherwise connected to university IT resources. This includes but is not limited to networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers, and any associated peripherals and software, whether used for administration, research, teaching or other purposes. The policy also applies to personally owned devices that are used to store, process, or transmit university information and/or that are connected to university IT resources.

Compliance

Individual units (e.g. campuses or institutes, departments, colleges and divisions) within the university may develop additional IT security requirements, guidelines, and standards so long as they do not have lower standards or requirements than the university's Information Technology Security Strategy, policies, or best practices. Each unit is responsible for security on its systems and may apply more stringent security standards than those detailed here while connected to University of Tennessee IT resources; however, they must follow these principles and rules as a minimum.

Any non-compliance with the university's Information Technology Security Strategy, policies, or best practices must be reported to the Information Security Office (ISO). Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. The ISO will work with University Human Resources and Campus Student Judicial Affairs departments to develop and implement appropriate sanctions for non-compliance with the University's Information Technology Security Strategy, policies, or best practices. Non-compliance issues that cannot be resolved by the ISO will be directed to the Senior Vice President and Chief Financial Officer. Critical non-compliance issues will be directed to the Audit Committee of the Board of Trustees.

GENERAL POLICY

1. All users are expected to comply with university IT security policies and best practices.

University policies can be found from the *University of Tennessee Policy Search Page* at <http://www.tennessee.edu/policy/>. Best practice documents can be found from the *Information Security Office* home page at <http://security.tennessee.edu/>.

PRIVACY

2. User privacy:

The university provides electronic resources to users to facilitate the advancement of the university's mission. The university will not routinely monitor an individual user's electronic data, software, or communication files. However, there should be no expectation of privacy for any information stored, processed, or transmitted, on university IT resources.

As required by state law, the University hereby notifies users that email maybe a public record and open to public inspection under the Tennessee Public Records Act unless the email is covered by an exception, such as personally identifiable student information, proprietary information, or trade secrets, to the Act. See Information Classification Policy: IT 0115, sections 2 & 3.

3. University rights:

Although, as stated above, users file's and communications will not be routinely monitored, users should be aware that any activity on systems and networks may be monitored, logged, and reviewed by university approved personnel or may be discovered in legal proceedings. In addition, all documents created, stored, transmitted, or received on university computers and networks may be subject to monitoring by systems administrators.

In addition, the university reserves the right to access, monitor, review, and release the contents and activity of an individual user's account(s), including email. The university may access such accounts on any university-owned IT resources and any non-university-owned IT resources on university property that are connected to university networks. This action may be taken to maintain the network's integrity and the rights of others authorized to access the network. Additionally, this action may be taken if the security of a computer or network system is threatened, other misuse of university resources is suspected, or the university has a legitimate business need to review such. This action will be taken only after obtaining approval from the Information Security Office or another authorized university office (e.g. Office of General Counsel, Audit and Consulting Services), or when compelled by subpoena or court order.

USER RESPONSIBILITIES

4. Users will:
 - a. Be responsible for following university policies and best practices to maintain the confidentiality, integrity, and availability of computer systems and information on all devices under their control.
 - b. Make regular backups of information and files as appropriate.
 - c. Control and secure physical and network access to IT resources and data.
 - d. Properly log out of sessions.
 - e. Monitor access to their accounts. If a user suspects that their account has been compromised or that there has been unauthorized activity on their accounts, they are to report it and change passwords immediately.
 - f. Install, use, and regularly update virus protection software.
 - g. Abide by the password protection best practices specified for each IT resource.
 - h. Use only the password and privileges associated with their computer account(s) and utilize those account(s) only for the purposes for which they were authorized.
 - i. Respect and honor the rights of other individuals, with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright and use of IT resources.

5. Users will not:
 - a. Provide access codes to any user not authorized for such access.
 - b. Make use of accounts, access codes, privileges or IT resources to which they are not authorized.
 - c. Tamper, modify, or alter any restrictions or protections placed on their accounts, the university's system, or network facilities.
 - d. Damage university IT resources or other systems using university IT resources.
 - e. Commit copyright infringement including file sharing of video, audio, or data without permission from the copyright owner.
 - f. Introduce, create, or propagate computer viruses, worms, Trojan Horses, or other malicious code to university IT resources.

- g. Obtain extra IT resources or gain access to accounts for which they are not authorized.
- h. Eavesdrop or intercept transmissions not intended for them.
- i. Physically damage or vandalize IT resources.
- j. Attempt to degrade the performance or availability of the system or to deprive authorized users of IT resources or access to any university IT resources.
- k. Misrepresent their identity (e.g., IP address "spoofing", email address falsification, or social engineering).
- l. Send email chain letters or mass mailings for purposes other than official university business.
- m. Use university resources to relay mail between non-university email systems.
- n. Engage in activities that harass, degrade, intimidate, demean, slander, defame, interfere with, or threaten others.
- o. Comment or act on behalf of the university over the Internet without authorization.
- p. Connect devices (switches, routers, hubs, computer systems, and wireless access points as examples) to the network that are not approved by the central IT organization at the campus or institution.
- q. Use any device or application that consumes a disproportionate amount of network bandwidth.

COPYRIGHTS AND LICENSES

- 6. Software may not be copied, installed, or used on university IT resources except as permitted by the owner of the software and by law. Software subject to licensing must be properly licensed and all license provisions (including installation, use, copying, number of simultaneous users, terms of the license, etc.) must be strictly followed.
- 7. All copyrighted information, such as text and images, retrieved from IT resources or stored, transmitted, accessed, or maintained with IT resources must be used in conformance with applicable copyright and other laws. Copied material must be properly credited using applicable legal and professional standards.
- 8. Questions about computer software use not addressed by this policy or questions about specific license agreements should be directed to the position of authority (POA) for IT at the respective campus/institute or their designee.

9. Each department is responsible and accountable for maintaining records of 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.

PERSONAL USE

10. The university's IT resources are provided for use in conducting authorized university business. Using these resources for personal gain, illegal activities, or obscene activities is prohibited.
 - a. The prohibition against using the university's IT 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 (https://my.tennessee.edu/pls/portal/docs/page/aaf/policy/forms/PCL_Policy.pdf).
 - ii. Consulting and other activities that relate to a 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 IT resources;
 - iii. Is otherwise in violation of this policy; or
 - iv. Violates any state or federal law or other university policy.
 - c. University departments may impose more stringent restrictions on personal use.
11. University IT resources may not be used for commercial purposes, except as specifically permitted under other written policies of the university or with the written approval of the Senior Vice President and Chief Financial Officer. Any such commercial use must be properly related to university activities and provide for appropriate reimbursement to the university for taxes and other costs the university may incur by reason of the commercial use.

12. The ".edu" domain on the Internet has rules restricting or prohibiting commercial use; activities not appropriate for the ".edu" domain that otherwise are permissible within the university's IT resources must use other domains.

MISUSE OF IT RESOURCES

13. Users observing any illegal activities should report their observance to the appropriate university administration. Although not an inclusive list, examples include theft, fraud, copyright infringement, illegal electronic file sharing, sound or video recording piracy, hacking, and viewing or distribution of child pornography.
14. Abuse of networks or computers at other sites through the use of the university's IT resources will be treated as an abuse of the university's IT resource privileges.
15. 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 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.

REMEDICATION

Abuse of university policies, resources, or abuse of other sites through the use of IT 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 Information Security Office (ISO), the Position of Authority for Information Technology at Each Respective Campus or Institute (**POA**), and the appropriate university office (e.g., office for student conduct matters, human resources, general counsel, the police department with campus or institute jurisdiction) or local and federal law enforcement agencies.

The **POA** and the ISO are authorized to isolate and/or disconnect computer systems from the network while responding to a suspected or reported security incident to minimize the risk to the rest of the university's network infrastructure. Termination of access may occur without contacting the administrator, user, or custodian of the violating system.

Access to the university's IT resources will only be restored once reasonable assurance has been made to the **POA** or the ISO (whoever approved the initial removal of access) that the incident has been resolved.

It is imperative that the university identifies and responds to abuses in a timely fashion to minimize the impact caused by security vulnerabilities and/or incidents.