Overview

The University Fiscal Policy, Section 805, Part 01 regulates the University's information technology (IT) resources within an atmosphere that encourages free exchange of ideas and a commitment to academic freedom. By adopting this Policy, the University of Tennessee recognizes that all members of the University community are bound by local, state, and federal laws relating to copyrights, privacy, security, and other statutes regarding electronic media.

Purpose

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 of data and privacy of its users, to the extent required or allowed under federal and state law, including but not limited to the Tennessee Public Records Act;
- safeguard the integrity of data and IT resources;
- maintain availability of IT resources within a reasonable time frame;
- preserve UT policies regarding harassment and the safety of individuals;
- minimize University liability from community use of IT resources;
- appropriately respond to claims of infringement of electronically posted copies of copyrighted materials and ensure that the use of electronic communications complies with the provisions of the Policy;
- ensure the free exchange of ideas and support academic freedom.

Scope

The principles described in this document apply to all University of Tennessee computing and networking facilities that are provided for use by users for legitimate purposes relating to the education, research, administration, and outreach activities of the University.

Policy

User Responsibilities

While the University recognizes the role of privacy in an institution of higher learning and every reasonable attempt will be made to honor that ideal, the University cannot promise privacy of information stored on or sent through University-owned information systems and communications infrastructure except for certain records relating to students; research; proprietary, trade secret or patentable materials; or certain medical records. Employees who

receive requests under the Tennessee Public Records Act should not release documents. All requests should be forwarded to the Public Information Officer who will review the request, contact the General Counsel if needed, and oversee any disclosures.

All users are expected to act in a responsible, ethical, and legal manner with the understanding that UT information technology (IT) resources are used in a format that may be accessible by the public. Users should respect other users, including others expectations of privacy and confidentiality, freedom of expression, and intellectual property rights.

Users are required to follow the established guidelines and procedures described in these policies. Although system administrators and designated security officers strive to provide and preserve the security and integrity of files, account numbers, authorization codes, and passwords, security can be breached through actions or causes beyond their reasonable control. Therefore, users are urged to safeguard their data, personal information, passwords, and authorization codes by taking full advantage of file security mechanisms built into the computer's operating system.

Malicious Computer Code

Malicious computer code includes, but is not limited to, computer viruses, Trojans, worms, and hoaxes. Although these are technically distinct forms of code, they are still commonly referred to as viruses and will be treated so in this document.

Computer viruses present a threat to UT'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.

Because of the nature in which viruses propagate themselves within a networked computing environment, all UT users have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. All members of the UT computing community are put at risk without acceptable use practices being exercised by each individual member of the community.

Network connected devices must utilize university approved anti-virus software when available.

To lessen the threat of computer viruses within the UT environment all faculty, staff, and students must adhere to the following practices (when technically possible):

1. A University owned computer is required to have a University approved anti-virus software package installed and running when available.
2. Real time protection (background scanning) should be activated if the computer is attached to the UT network. Full disk scans are to be performed at a minimum of once a week if real time protection is activated.
3. If real time protection is not activated, full disk scans are to be performed once a day.
4. Software virus definitions must be updated and kept current at all times.

User accountability is established through the assignment of a unique user account name (ID) and protected with some form of authentication (e.g., a password). Users are required to protect their account and not share it with others for their use, nor utilize another user's account for any reason, unless authorized to do so by the employee's supervisor. Since passwords are typically the first line of defense to UT IT resources, users should choose passwords carefully and must comply with UT password guidelines for effective password protection. Users are responsible for any electronic messages that are transmitted from their accounts.

Users are expected to report any information concerning instances in which they suspect or have evidence that the above principles have been or are being violated.

If at any time a user receives an electronic communiqué that places the user in peril or leads the user to believe that a criminal act may be pending, the user should immediately report the matter to campus or local authorities.

Reports about suspected violations of these principles should be directed to: abuse@utk.edu, abuse@utmem.edu, or abuse@utsi.edu, as appropriate, regarding inappropriate public behavior and security@utk.edu, security@utmem.edu, security@utsi.edu, as appropriate, for network operations or infrastructure issues. Receipt of incident reports will be acknowledged and investigated in a timely manner.

Compliance

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:

There is reasonable cause to believe the user has violated or is violating this policy, any campus guidelines or procedures established to implement this policy, or any other University policies;

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

The user has voluntarily made information accessible to the public such as a Web page;

It is necessary to do so to protect the integrity, security, or functionality of the University's IT resources or to protect the University from liability; or

It is otherwise permitted or required by law, such as subpoena or court order.

System administrators or designated security officers will ensure that user authentication is required before access to any restricted UT IT resource is granted. All users of UT IT resources agree to the following rules and responsibilities:

(a) No one shall knowingly or willingly interfere with the security mechanisms or integrity of UT IT resources. Users shall not attempt to circumvent data protection schemes or exploit security loopholes.

(b) No one shall knowingly create, install, execute, or distribute any malicious code or another surreptitiously destructive program on any UT IT resource, regardless of the result.

(c) No one shall interfere with the intended use of UT IT resources. All users shall share computing resources (e.g., bandwidth) in an ethical and fair manner and not unduly interfere with use by other authorized users.

(d) No one shall use UT IT resources to attempt unauthorized use, or interfere with the legitimate use by authorized users, of other computers or networks elsewhere- users are responsible for adhering to the policies and principles of such networks. UT cannot and will not extend any protection to users who violate external network policies. Abuse of networks or computers at other sites through the use of UT IT resources will be treated as an abuse of UT IT resource privileges.

(e) University IT resources are for use in conducting authorized University business. Using these resources for personal gain or illegal or obscene activities is prohibited. This prohibition against using IT resources for personal gain does not apply to 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. Consulting and other activities that relate to the faculty member's professional development and have been approved under the External Activities for Pay Policy are also not included in the prohibition of using IT resources for personal gain. Although not an inclusive list, examples of illegal or obscene use include theft, fraud, gambling, copyright infringement, sound or video recording piracy, and either viewing or distributing child pornography.
Just as minimal personal telephone use is allowed and is sometimes necessary, employees should use the same discretion concerning the University's IT resources. Therefore, minimal personal use of these resources is permitted by this policy except when such use is excessive or interferes with the performance of the user's University responsibilities, results in additional incremental cost or burden to the University's IT resources, or is otherwise in violation of this policy. Further restrictions may be imposed upon personal use by user's supervisor or in accordance with normal supervisory procedures concerning the use of University equipment.

(f) No one shall perform, participate, encourage, or conceal any unauthorized use or attempts of unauthorized use of UT IT resources.

(g) No one shall use a system attached to UT resources to capture data packets (e.g., "sniffer") except for authorized or other official University business without a prior waiver of this policy.

(h) No one shall use UT IT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by state or federal laws.

(i)No one shall launch denial of service attacks against other users, systems, or networks.

(j) No one shall abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a University account.

(k) No one shall connect any computer or network system to any of UT's networks (e.g., direct connection, direct dial-in access) without employing reasonable and available technical and security standards - which, at a minimum, requires user identification and authentication.

(l) No one shall misrepresent his or her identity or relationship to the University for the purpose of accessing or attempting unauthorized access to UT IT resources nor misrepresent his or her identity to other networks (e.g., IP address "spoofing") from UT IT resources.

(m) No user shall access (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.

(n) No one shall use UT IT resources in violation of applicable patent protection and authorizations, copyrights, license agreements, other contracts, state or federal laws, or University rules or regulations.

(o) No one shall modify or reconfigure the software, data, or hardware of any UT IT resource (e.g. system/network administration, internal audit) without appropriate authorization or permission.

(p) No one shall place confidential information in computers without appropriately protecting it. The University cannot guarantee the privacy of files, electronic mail, or other information stored or transmitted on UT IT resources.

(q) No one shall compromise the privacy of others or the confidentiality of the information contained on UT IT resources.

(r) No one shall make nor attempt to make any unauthorized connection to the UT network. Question concerning this site may be sent to the webmaster.

Enforcement

Abuse of UT policies or standards, abuse of UT IT resources, or abuse of other sites through the use of UT 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 appropriate UT office (e.g., appropriate office for student conduct matters, UT Human Resources, UT General Counsel, the police department with campus jurisdiction) or local and federal law enforcement agencies.

Additional Information

Any inquiries relating to this Acceptable Use Policy should be directed to the Security Director.