



TMU ACCEPTABLE USE OF TECHNOLOGICAL RESOURCES POLICY

FOCUSING ON THE MISSION AND GOALS OF TMU

This policy defines the boundaries of "acceptable use" of TMU's technological resources, including computers, online classrooms, university internet portals, networks, electronic mail services, electronic information sources, telephones and copiers (technological resources) as detailed below.

The policy is based on the principle that the electronic information environment is provided to support the academic and accreditation goals of TMU including its mission of education, research and service. All other uses are secondary. Technology usage that might threaten the integrity of TMU's network; the actual or perceived safety of others; or any illegal activity is strictly forbidden.

By using TMU's electronic information systems you assume personal responsibility for their appropriate use and agree to comply with this policy, other applicable university policies, and all applicable City, State and Federal laws and regulations.

This policy defines penalties for infractions, up to and including loss of system access, employment termination or expulsion. In addition, some activities may lead to risk of legal liability, both civil and criminal.

Users of electronic information systems are urged in their own interest to review and understand the contents of this policy.

PURPOSE

TMU makes technological resources (including, but not limited to, computer facilities and services, computers, networks, electronic mail, electronic information and data, video and voice services, university internet portals, online classrooms) available to faculty, staff, students, and special guests to support the mission of TMU.

If the demand for technological resources exceeds current capabilities, then priorities for their use will be established and enforced. The priorities for use of university -wide computing resources are:

- High – Uses that directly support the educational and service missions of the University including official electronic communications
- Medium – Other uses that indirectly benefit the education, research and service missions of TMU including reasonable and limited personal communications
- Low – Recreation activities, including personal communications, game playing and recreational Internet browsing
- Forbidden – All unethical or illegal activities that do not represent a faithful Christian witness

TMU may enforce these priorities by restricting or limiting usages of lower priority tasks in circumstances where higher priority tasks are impacted. The Department of Information Technology (IT) diligently works to support the goals of this organization by providing reliable service for the faculty, staff and students of the University.

IMPLIED CONSENT

Each person with access to the University 's technological resources is responsible for his/her appropriate use and by their use agrees to comply with all applicable university and Information Technology policies and regulations, and with applicable City, State, and Federal laws and regulations.

GENERAL STANDARDS

Each person who utilizes the technological resources and computers of the University will display the following basic behavior traits at all times.

- Responsible Behavior. Users shall behave responsibly with all university equipment and computers. Users shall understand the value of this equipment and shall not abuse the equipment in any manner.
- Consistent Behavior. Users shall faithfully display behavior consistent with the mission of the University and a Christian life.
- Respectful Behavior. Users shall respect the rights and property of others, including intellectual property rights.
- Obedient Behavior. Users shall comply with all applicable laws, regulations, and university policies.

ENFORCEMENT AND PENALTIES FOR VIOLATION

Any person who violates any provision of this policy, or other relevant university policies, or of applicable City, State, or Federal laws or regulations may face sanctions up to and including termination or expulsion. Users shall report all suspected violations of these policies to their immediate supervisor.

INTERPRETING THIS POLICY

As technology advances, questions will arise about how to interpret the general standards expressed in this policy. The director of Information Technology, the associate vice president of IT, or the Vice President for Finance and Operations; may periodically update this policy to provide more specific rules that comply with the mission of TMU.

SPECIFIC RULES

The following specific rules apply to all uses of university computing resources. These rules are not an exhaustive list of proscribed behaviors but are intended to implement and illustrate the General Standards for the Acceptable Use of Technological Resources, other relevant university policies, and applicable laws and regulations.

- Content of Electronic Communication. The content of electronic communication (including e-mail, voice mail, etc.) is the property of TMU. Users will communicate in a manner that faithfully represents the mission of the University and a Christian life. Unlawful communications, including threats of violence, obscenity, and harassing communications, are prohibited.
- Personal Business Use. The use of TMU computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized under applicable university policies) is prohibited.

- Personal Identification. All users of TMU's computer resources will be provided a personal user identification name or User ID from IT. This User ID should be treated as confidential and should not be given to anyone who is not authorized to use the University's computer resources.

STRICTLY PROHIBITED

In an effort to protect TMU's computer and network architecture from intentional and unintentional harm, rules have to be established and enforced. These rules are not meant to hinder the users from performing their jobs but are meant to ensure them that the systems and their data will be available when they are needed. The following activities and behaviors are strictly prohibited.

1. Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication;
2. Acquiring or attempting to acquire passwords of others;
3. Using or attempting to use the computer accounts of others;
4. Harassing, threatening or harming individuals or classes of people and/or impeding their activities;
5. Alteration of the content of a message originating from another person or computer with intent to deceive;
6. Using the Internet to view pornographic or morally offensive web sites or the electronic distribution of such material;
7. The use of restricted-access university computer resources or electronic information without or beyond one's level of authorization;
8. The interception or attempted interception of communications by parties not explicitly intended to receive them;
9. Making university technological resources available to individuals not affiliated with this organization without approval of the director of Information Technology or the Vice President for Finance and Operations;
10. Any unauthorized copying or unauthorized use of licensed computer software;
11. Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential under TMU's policies regarding the privacy or the confidentiality of student, administrative, personnel, archival, or other records;
12. Intentionally compromising the privacy or security of electronic information;
13. Intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism, unauthorized use or reproduction, and peer-to-peer file sharing);
14. Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts;
15. Failure to comply with requests from appropriate TMU officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy;
16. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access;
17. Altering or attempting to alter files or systems without authorization;

18. Unauthorized scanning of networks for security vulnerabilities;
19. Attempting to alter any TMU computing or networking components (including, but not limited to routers, switches, and hubs) without authorization;
20. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension of any computer or network services;
21. Intentionally damaging or destroying the integrity of electronic information;
22. Intentionally disrupting the use of electronic networks or information systems;
23. Intentionally wasting human or electronic resources; and
24. Negligence leading to the damage of TMU electronic information, computing/networking equipment and resources.

COMPUTER SOFTWARE

The IT department is responsible for installing all software applications on university owned computers. Additionally, IT maintains a "Software Policy" for TMU. All employees should make themselves familiar with this policy if they have any questions regarding computer software. Each employee is responsible for understanding the rules regarding software as listed in this policy and restated here.

SOFTWARE GUIDELINES

The following software rules are established because TMU is responsible for complying with all software license requirements.

1. All software must be legal, and IT will keep a copy of the Software License on file;
2. No software is to be installed on any university owned computers without the expressed permission of the Director of Information Technology;
3. Users are not allowed to download and install any software (freeware, shareware, or individually purchased) programs without the permission of the Information Technology department.
4. TMU owned software shall not be installed on any non- university owned computers without a legal software license and the permission of the Director of Information Technology.
5. Faculty and Staff members may request the purchase of new software as outlined in the Hardware and Software Policy;
6. All software license agreements, activation keys, and serial numbers should be treated as confidential and should not be shared with anyone outside of the organization.
7. Staff members may not install personally owned software;
8. Faculty members may install personally owned software on a TMU computer if the following conditions are met. (1) Permission is obtained from the Director of Information Technology, (2) The user provides a copy of the proper software license for the software to IT, and (3) The software does not conflict with any of the existing university owned computers, software, or network.