THADDEUS STEVENS COLLEGE OF TECHNOLOGY INFORMATION TECHNOLOGY POLICY	
Subject*:* *Computer Usage Policy & Guidelines*	**Number:**
Effective Date: **Revised:**	**Approved by:**

1 Policy

Thaddeus Stevens College's intentions for publishing a Computer Usage Policy and Guidelines are not to impose restrictions that are contrary to Thaddeus Stevens College established culture of openness, trust and integrity. Thaddeus Stevens College is committed to protecting its employees, students, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Thaddeus Stevens College. These systems are to be used for business purposes in serving the interests of the College, and of our Students and Employees in the course of normal operations.

2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Thaddeus Stevens College. These rules are in place to protect the employees, students and Thaddeus Stevens College. Inappropriate use exposes the college to risks including virus attacks, compromise of network systems and services, and legal issues. This policy is in support of additional IT policies for specific subject matter.

3 Scope

This policy applies to employees, students, contractors, consultants, temporaries, and other workers at Thaddeus Stevens College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Thaddeus Stevens College and non-owned equipment attached to the Thaddeus Stevens network.

3.1 General Use

While Thaddeus Stevens College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the college systems remains the property of Thaddeus Stevens College. Because of the need to protect College's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Thaddeus Stevens College

Employees and Students are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their manager or Department Head.

For security and network maintenance purposes, authorized individuals within the College may monitor equipment, systems and network traffic at any time.

The College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 Security and Proprietary Information

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed every 180 days; user level passwords should be changed every 90 days.

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off (control-alt-delete for Windows XP users) when the PC will be unattended.

Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.

Postings by employees from a College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of “Thaddeus Stevens College of Technology” unless posting is in the course of business duties.

All hosts used by the employees and students that are connected to the College’s Internet/Intranet/Extranet, whether owned by the employee, student or the College, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee or student of Thaddeus Stevens College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Thaddeus Stevens College owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Thaddeus Stevens College
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Thaddeus Stevens College or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using the College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any college account.

- Except with prior explicit written permission from the Office of the President Services, Resources must not be used for commercial purposes or monetary gain.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to Thaddeus Stevens College is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about or lists of the College's employees to parties outside Thaddeus Stevens College.
- Hosting of a Web or FTP Site on the College's network unless this site is a part of the employee's normal job/duty.
- In the event something is not protected does not mean that users have the right to access it. Most information accesses that are not allowed are prevented by mechanisms built into the systems. Computer systems are complex and errors may keep the systems from preventing prohibited access. Such access is STILL PROHIBITED.
- Limited recreational game playing, that is not part of an authorized and assigned research or instructional activity, is tolerated (within the parameters of each department's rules). College computing and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a public computing facility must give up that computing position when others who need to use the facility for academic or research purposes are waiting.

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within College's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the College or connected via the College's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- E-mail and other computer files (collectively, "Files") can never be considered fully private, particularly in light of (i) the open nature of the Internet and related technology and (ii) the ease with which Files may be accessed, copied, and distributed. You are advised to avoid sending messages by e-mail and storing information in computer files that are of a confidential or extremely personal nature (including, but not limited to credit card or social security numbers).

4 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

5 Background

N/A

6 Procedure

The Director of the Computer and Network Services may suspend any person from using the computing and networking facilities for a period not exceeding 28 days (and may recommend additional penalties to the appropriate Vice-President) if after an investigation that person is found to be:

- responsible for willful physical damage to any of the computing and networking facilities;

- in possession of confidential information obtained improperly;
- responsible for willful destruction of information;
- responsible for deliberate interruption of normal services provided by the Computing Network
- responsible for the infringement of any patent or the breach of any copyright;
- gaining or attempting to gain unauthorized access to accounts and passwords
- gaining or attempting to gain access to restricted areas without the permission of the Director
- responsible for inappropriate use of the facilities.

Any employee or student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, suspension, dismissal, or expulsion from the College.

The College reserves the right to take emergency action to safeguard the integrity and security of the computing and networking facilities. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords. The taking of emergency action does not waive the rights of the College to take additional actions under this policy.

7 Duties and Responsibilities

Effective security is a team effort involving the participation and support of every Thaddeus Stevens College employees, students, and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.