II.C.4. Policy: Southeastern Technical College Computer Use

1.0 Overview

Due to the technological revolution in the workplace, businesses such as Southeastern Technical College (STC) have turned to computer technology as the primary tool used to communicate, perform research, and accumulate information. As the number of users logging on to the college's network at the school or by remote access has increased, so has the possibility of STC's computer resources being mistreated; compromised; or experience unauthorized access, disclosure, destruction, modification, or loss. With easy access to STC's Internet and network resources, it is very important to have a well defined computer use policy. A well defined policy helps protect the end-user as well as STC.

Effective security is a team effort involving the participation and support of every STC employee 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.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at STC. These rules are in place to protect STC as well as its employees, students, and guests. Inappropriate use exposes STC to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, students, contractors, consultants, temporaries, and other workers at STC, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by STC.

4.0 Policy

4.1 General Use and Ownership

1. While STC'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 STC. Because of the need to protect STC's network, users should not expect files stored on STC's computers and/or network to be private.

2. End-users are responsible for exercising good judgment regarding the reasonableness of personal use. Occasional and appropriate personal use is acceptable and permitted by the college. However, this use should be

brief, infrequent, comply with this policy, and shall not interfere with the user’s performance, duties, and responsibilities.

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

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

5. Only the Information Technology Department staff is authorized to provide support, perform installations of new equipment/software, and/or configure devices for the multi-campus network.

6. Any individual associated with STC needing to connect personally owned devices to the college’s network must obtain prior approval from the Information Technology Department.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords should be changed every 90 days.

2. All faculty and staff PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete) when the host will be unattended.

3. Because information contained on portable computers is especially vulnerable, special care should be exercised.

4. Any and all critical information (data, files, etc) should be saved to the network. The IT Department is not responsible for any end-user files not saved to the network.

5. Postings by employees from a STC email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of STC, unless posting is in the course of business duties.

6. All computers that are connected to the STC Internet/Intranet/Extranet, whether owned by an employee, student, third-party, or STC, shall be continually executing approved virus-scanning software with a current virus database.

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

4.3. Unacceptable Use
Under no circumstances is an employee, student, or third-party of STC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing STC-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:

1. 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 STC.

2. 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 STC or the end user does not have an active license is strictly prohibited.

3. 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.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. 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.

6. Using an STC 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.

7. Making fraudulent offers of products, items, or services originating from any STC account.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee, student, or third-party is not an intended recipient or logging into a server or account that the employee, student, or third-party 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.

9. Port scanning or security scanning is expressly prohibited unless prior authorization from the Information Technology Department authorized.

10. Executing any form of network monitoring which will intercept data not intended for the end-user's host, unless prior approval of this activity from the Information Technology Department is authorized.

11. Circumventing user authentication or security of any host, network, or account.

12. Interfering with or denying service to any other host or user other than the end-user’s host (for example, denial of service attack).

13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal and/or network session, via any means, locally or via the Internet/Intranet/Extranet.

14. Providing information about, or lists of, STC employees to parties outside STC.

Email and Communications Activities

1. 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).

2. Any form of harassment via email, telephone, Linc, or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. 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.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within STC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by STC or connected via STC's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Abuse or misuse of computing/information technology services may violate this policy, but it may also violate criminal statutes. Therefore, STC will take appropriate action in response to user abuse or misuse of computing/information technology services. Action may include, but not necessarily limited to, the following:

1. Suspension or revocation of computing privileges. Access to all computing facilities and systems can, may, or will be, denied;

2. Reimbursement to Southeastern Tech for resources consumed;

3. Other legal action including action to recover damages;

4. Referral to law enforcement authorities;

5. Computer users (faculty, staff and/or students) will be referred to the appropriate office for disciplinary action.

6.0 Definitions

Term	**Definition**
End-user	Any person using STC's information systems and/or computers.
Ponzi	Fraudulent investment operation that involves paying returns to investors out of the money raised from subsequent investors.
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Trojan horse	A program in which malicious or harmful code is contained inside.
Virus	A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer.

Adopted: June 25, 2009
Reviewed: February 08, 2010; February 10, 2011; February 09, 2012;