South Texas College

Guidelines for the Acceptable Use of Information Resources

Division of Information Services and Planning (IS&P)

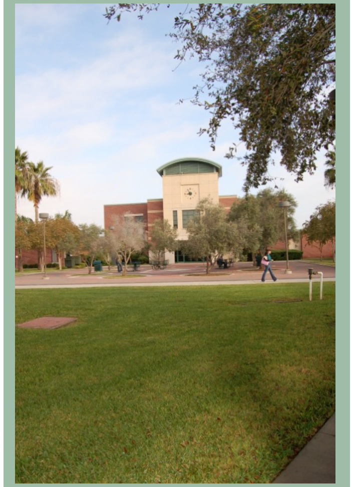
Information Security Office

956-872-2335

Email:
infosec@southtexascollege.edu

Mission Statement

The Information Security Office (ISO) develops and maintains an information security program that safeguards the college's information resources and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss.



Introduction, Overview and Scope

These guidelines, under the authority of South Texas College Policy #4712 titled Information Resources Security, outline the acceptable use of South Texas College's information resources and provide users with basic knowledge and general rules for proper, fair, efficient and effective use of those resources. These rules are in place to protect students, employees and the college. Inappropriate use exposes STC to risks including virus attacks, compromise of network systems and services, and legal issues.

The intent of the Acceptable Use Guidelines is not to impose restrictions that are contrary to the institutions established culture of openness, trust and integrity. STC endeavors to protect employees, students and the institution from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of everyone at the college who deals with information resources.

It is the responsibility of every user of information resources to know these guidelines and to conduct their activities accordingly.

These guidelines apply to all users, including but not limited to: students, employees, contractors, consultants, temporaries and guests, including all personnel affiliated with third parties, whether on campus or from remote locations. Additional usage guidelines may apply to information resources provided or operated by individual units of STC or to users within specific units.

General Guidelines

Ownership
Information resources, including but not limited to: computers, computer accounts, printers, networks (LAN, WAN, wireless and Internet gateways), software, storage media (flash drives, diskette), messaging systems, Personal Digital Assistant devices (PDAs), audio and video conferencing, facsimile machines, and the telephone and voice mail systems, are the property of South Texas College. These resources are to be used for school business in serving the interests of the institution, its faculty, staff and students in the course of normal operations. Users have no property rights to computer resources or the information contained therein.

Access to Information Resources
Access to information resources is solely for the furtherance of the educational, operational and professional goals of the college. All information resources including hardware, software, databases and all computerized information and data entered on, or developed with, are either owned by licensors or directly owned by STC.

South Texas College may restrict access to computers and network systems when presented with evidence of the violation of STC policies or procedures, federal or state laws, or when it is necessary to protect the college against potential legal liability. STC reserves the right to limit access to its informational resources, and to remove or limit access to material stored on its information resources.

Usernames and passwords provide users with access to specific information and system resources, based on the needs of their job function or role. Under no circumstances are users to share usernames and passwords with anyone else, unless requested to do so by a system administrator for the purpose of troubleshooting a system issue. Sharing of this information will be construed as circumventing the college's security practices and procedures, and will expose that user to risk of disciplinary action. Authorized users are responsible for the security of their passwords and accounts.

Connecting Personal Equipment to the College's Network
No one is allowed to connect any personal computer, laptop, or other device onto the college's wired network. Exceptions to this rule must be addressed to the chief information officer or chief information officer security officer.

Wireless connectivity is provided to all students, faculty and staff to promote mobile learning. The college provides limited support for personal wireless technology and users are expected to understand how to configure and operate their devices accordingly.

All wireless computers connecting to the STC's network are required to have current and automatically-updating antivirus software. Files which are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect computer viruses and prevent their propagation.

South Texas College reserves the right to restrict or suspend wireless access to individuals and locations found in violation of any provisions set forth in these guidelines.

STC
South Texas College

Email and Communication Activities

The following activities are strictly prohibited:

- Sending unsolicited email messages unrelated to college functions, 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 address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding chain letters or other pyramid schemes of any type.
- Use of unsolicited email originating from within the 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.
- Encryption devices which are not approved by IS&P will not be allowed on any electronic resources.

Privacy Expectations

Electronic Communications

The college respects user privacy and will make reasonable efforts to maintain the integrity and effective operation of its electronic communications systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information.

Because of the nature and technology of electronic communications, STC can assure neither the privacy of an individual user's use of the college's electronic communications resources nor the confidentiality of particular messages that may be created, transmitted, or received.

Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, modified, or stored by others. Furthermore, others may access electronic communications as authorized under college policies.

The electronic communications of users may be subject to the Public Information Act in the same way that printed or typed letters and memos are.

Therefore, users are strongly encouraged to consider any and every electronic communication they produce, send or receive with college resources as public and official communiqué in the execution of their official job duty.

Security Monitoring

To ensure compliance with college policies and state laws and regulations related to the use and security of information resources, Information Security personnel have the authority and responsibility to monitor network traffic and use of information resources to confirm that security practices and controls are adhered to and are effective. STC reserves the right to monitor, filter and/or review, at any time, all Internet utilization via the college's Internet access.

STC further reserves the right to reveal any Internet access related information to any party that it deems appropriate or any to party that it may be required to by law or regulation. This may include law enforcement search warrants and discovery requests in civil litigation.

The use of encryption, the labeling of a communication as private, the deletion of a communication or any other such process or action, shall not diminish STC's rights in any manner.

Emerging Technologies

While these guidelines may not address the specific details of technologies that are yet to be invented or implemented at STC they should be sufficient to allow you to determine the acceptable use of any new or emerging technology.
If you have any questions please contact the IS&P Client Services at 872-2111 for further guidance.

Enforcement

Reporting Violations

If you believe that a violation of these guidelines has occurred, contact the IS&P Client Services at 872-2111 immediately. Under no circumstances should the witness(es) attempt to look through or access the suspect's machine in order to conduct their own personal investigation.

There may be situations when the following additional offices should be contacted:

- 911 if an individual's health or safety appears to be in jeopardy.
- Campus Security Dispatch at 872-2589.
- Office of Human Resources at 872-4448 if violations occur regarding college personnel.

You may also contact the VP of IS&P at 872-3554 if you wish to report an incident but are unable to do so through normal channels.

Sanctions

Any person found to have violated these guidelines might be subject to disciplinary action, up to and including termination of employment or expulsion from school. In addition, there may be cases in which a person may be subject to civil or criminal liability.

Coordination with Other Policies

Users of information resources at STC are advised that other college policies, including those for: Human Resources; faculty, staff and student handbooks; and notably those policies governing copyright and intellectual property compliance, may be related to use of information resources, and that those policies must be observed in conjunction with this policy.

In particular, Board Policy #4712 relating to Information Resources Security as well as the Information Resources Security Guidelines should be referenced in coordination with these guidelines.

Incidental Usage

Information technology resources shall be used in accordance with the following:

- Incidental personal use of Internet access is restricted to college-approved users; it doesn't extend to family members or acquaintances.
- Incidental use must not result in direct costs to STC or interfere with the normal performance of an employee's work duties.
- The streaming of audio or video for personal or recreational use is strictly prohibited. Streaming places an undue and potentially costly burden on college network resources. Examples of prohibited streaming audio include: Pandora, AOL Radio, MSN Radio, and other similar Internet-based radio broadcasts. Examples of prohibited streaming video include: YouTube, Hulu, ABC, CBS, NBC, and other similar broadcasting web sites.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to, the college.
- Storage of personal files and documents within the college's information resources should be nominal. Non-work related files may not be stored on network file servers.
- All files and documents, including personal files and documents, are owned by the college, may be subject to open records requests, and may be accessed by others in accordance with these guidelines.

File Sharing and Copyrighted Materials

Peer-to-Peer (P2P)

P2P applications are designed to allow the worldwide sharing of network bandwidth with anyone using the same software. To maintain network performance P2P is not permitted on the STC network. While there may be legitimate uses for these file sharing programs the vast majority of files shared through P2P technology are copyright-protected works. If you have a legitimate reason for using P2P file sharing you may request an exception on a per-case basis by contacting the IS&P Client Services at 872-2111.

Copyright Infringement

The Recording Industry Association of America (RIAA) and other organizations monitor unlicensed file sharing activity on the Internet on a regular basis. If any of those organizations notify STC about a copyright infringement we are required to take appropriate action. Copyright infringement and unauthorized access to digital materials is subject to disciplinary action by STC and may be grounds for legal action against the user.

Under the terms of the Digital Millennium Copyright Act (DMCA), the college is committed to respond to lawful requests for information and will not protect or defend a user against criminal investigations or lawsuits resulting from intentional copyright infringement.

Offensive Material

Users will not use information resources in a manner that creates a hostile working environment or learning environment (including sexual or other forms of harassment), or that violates obscenity laws. Viewing, transmitting or posting sexually explicit images or any other content deemed to be offensive and inappropriate for academic use is prohibited and may also constitute a violation of college Policy #4212: Sexual Harassment.

Furthermore, users of public terminals or similar facilities at the college should be aware of the public nature of shared facilities and should take care not to display images or play sounds that could create an atmosphere of harassment for others. Similar considerations apply to electronic mail exchanges where the sending of unwanted and/or offensive email or messages may constitute harassment and is in violation of the intended use of the system.

Inappropriate Use

The following activities are, in general, prohibited. Administrative and other authorized users 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). The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

Under no circumstances is a person at STC authorized to engage in any activity that is illegal under local, state, or federal law while utilizing college-owned resources.

Systems and Network Activities

The following activities are strictly prohibited:

- Violations of the rights of any person or institution 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 the college.
- The copying or installation of any copyrighted software for which STC does not have an active license is strictly prohibited.
- Unauthorized access to a particular machine, folder and/or file. Unauthorized access is defined as any person not having the permission via username to the particular machine, folder and/or file.
- Interfering with the intended use or normal operation of information resources, or otherwise harming or damaging college systems, knowingly or unknowingly.
- Deliberately using electronic communications to transfer material of a nature that would seriously impede, interfere with, or otherwise diminish an employee's effectiveness at STC.
- Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Disclosing your user 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.
- Violating policy, rules or other regulations imposed by outside or external information providers while utilizing or accessing those systems with STC resources.
- No person should represent that any personal views contained in any communication emanating from STC equipment are those of the college.
- Effecting security breaches or disruptions of network communication. Security breaches include accessing data of which the person is not the intended recipient or logging into a server or account that the person 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, port or security scanning, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information.
- Executing any form of network monitoring which will intercept data not intended for the person's host, unless this activity is a part of the person'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 person's host (for example, denial of service attacks).
- 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.
- Personnel shall not disclose any confidential or sensitive information unless it is properly required in their jobs, or except as authorized in writing pursuant to security policies. This includes technical and business information, information systems and software development and products and software licenses disclosed on a confidential basis to the institution.

Employee Guidelines

Employees are also expected to follow guidelines presented in this section.

Assignment of Computer Hardware

STC determines the computer system needs of employees and how those needs will be met. The college reserves authority to establish and enforce procedures and rules for employee use of STC-owned computer systems, software, and data.

STC will assign appropriate computer hardware to a position to enable tasks corresponding to the position to be accomplished.

College-owned desktop computer equipment is the exclusive responsibility of IS&P. STC property and desktop computers cannot be taken home, relocated or reassigned without prior approval of IS&P Client Services.

Assignment of Computer Software

The college will attempt to assign appropriate computer software to a position to enable tasks corresponding to the position to be accomplished.

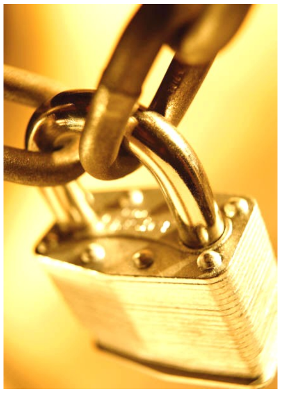
Some software publishers permit employees to have one copy of their software on the college-owned computer and one copy of their software on the employee-owned computer. If a software publisher permits such an arrangement, the employee is still required to obtain permission of IS&P Client Services.

Only college-owned software is to be installed on STC's computers. IS&P Client Services must approve exceptions.

Data Handling & Safeguarding

Data, information, or reports produced using college-owned equipment are the property of STC. Personnel may not use these reports except for internal college business or as required by their job. All college personnel are required to be knowledgeable of and adhere to the Guidelines for the Classification and Management of Electronic Data.

Personnel are directly responsible for applying the appropriate safeguards to adequately protect college data and to exercise the appropriate confidentiality.



Reporting Data Compromise

The college takes the safe guarding of institutional data very seriously. In the event that college data is compromised or devices containing college data (flash drive, diskette) are lost or stolen, it is imperative that personnel immediately report the incident to one of the following: IS&P Client Services, Campus Security, chief information security officer, or chief information officer.

Depending upon the magnitude and sensitivity of the data, the college has a legal requirement to notify the appropriate agencies of the incident. Time is critical in mitigating the impact of data compromise.

Failure to act accordingly is grounds for disciplinary action.

Usage

All PC's, laptops and workstations should be secured with a password protected screensaver with the automatic activation feature set to 15 minutes or less. When the computer will be unattended the user must lock their workstation (ctrl-alt delete and select "Lock Computer") to prevent unauthorized access.

Postings by users from the college email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the college, unless posting is in the course of business duties. Contact Public Relations for sample disclaimers.

Upon the termination of employment or a contractual relationships with STC, or as otherwise requested by appropriate management, personnel must surrender all property and information managed by the college, and must not subsequently disclose any confidential or sensitive information.

Supervisory Authority

Supervisors may encounter the need to inspect the contents of any equipment, files, calendars or electronic communications of their subordinates in the normal course of their supervisory responsibilities. Before doing so; however, supervisors are required to notify and obtain the approval of Human Resources.

The System Administrator shall extract stored electronic communications when requested to do so by authorized supervisory personnel or Human Resources.

Reasons for review include, but are not limited to, system hardware or software problems, general system failure, regular system maintenance, a lawsuit against South Texas College, suspicion of a crime or violation of policy, or a need to perform work or provide a service when the employee is unavailable.

For more information, contact IS&P Client Services at 872-2111 or by emailing isphelp@southtexascollege.edu.