# Use of Electronic Information Resources

**Original Implementation:** July 25, 2002
**Last Revision:** April 24, 2018

## STATEMENT

Stephen F. Austin State University (SFA) supports the responsible use of its electronic information resources. SFA's information resources include, but are not limited to, computers, servers, wired and wireless networks, computer-attached devices, network-attached devices, voice systems, cable systems and computer applications. The use of information resources is for SFA academic activities, research and public service. Access to SFA's information resources is, however, a privilege. All users of information resources should act responsibly to maintain the integrity of these resources. Furthermore, all users will abide by all existing SFA codes of conduct as well as local, state and federal statutes. SFA reserves the right to limit, restrict or extend privileges and access to its resources.

## RESPONSIBILITIES

- It is the responsibility of all individuals using SFA's information resources to protect the privacy of their account(s). Personal account information should not be released to friends, relatives, roommates, etc. Users are responsible for the security of their passwords.
- All individuals using SFA information resources are prohibited from using a computer account for which they are not authorized, or obtaining a password for a computer account not assigned to them.
- The owner or designated assignee of a computer that is attached to the SFA network is responsible for both the security of the computer system and for any intentional or unintentional activities from or to the network connections. Owners or designated assignees are responsible for all network activity originating from their equipment, regardless of who generates it.
- Any person operating a network-intensive application or a defective computer that causes network overload will be notified, and steps will be taken to protect other users and the overall SFA network. This may include disconnecting the defective computer system from the network until the problem is resolved. If the condition is an imminent hazard to the SFA network or disrupts the activities of others, the defective computer system or the subnet to which it is attached may be disabled without notice. The operator of the defective computer system will be expected to follow instructions from information security staff for securing the machine.
- Any person using e-mail should not send unnecessary e-mails, attachments, or messages locally or over the network.

- The content of any files or services made available to others over the network is the sole responsibility of the person with ownership of and/or administrative authority over the computer providing the service. It is this person's responsibility to be aware of all applicable federal and state laws, as well as SFA policies. This person will be liable for any violations of these laws and policies.
- It is the responsibility of every person using SFA's information resources to refrain from engaging in any act that may seriously compromise, damage, or disrupt the operation of computers, terminals, peripherals, or networks.
- Users should refrain from using an IP address not specifically assigned to them and should not attempt to create unauthorized network connections or unauthorized extensions, or re-transmitting any computer or network services.
- All email messages of a personal nature sent by faculty, staff, and retirees using an SFA email address must contain the following disclaimer: "The views and opinions expressed in this message are my own and do not necessarily reflect the views and opinions of Stephen F. Austin State University, its Board of Regents, or the State of Texas."
- All breaches of system security will be reported immediately to the information security officer.

## INFRACTIONS

Examples of infractions include, but are not limited to:

- Circumventing or attempting to circumvent data protection schemes or exploiting security vulnerabilities.
- Running programs that attempt to identify passwords, weaknesses in the SFA system, or other security codes.
- Attempting to monitor or tamper with another user's data communications or network traffic, or reading, copying, changing, or deleting another user's files or software..
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place an excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses and worms.
- Using SFA computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized), fundraising or advertising on behalf of non-SFA organizations, reselling of SFA computer resources and using SFA's name in an unauthorized manner.
- Engaging in unlawful communications, including threats of violence, obscenity, child pornography and harassing communications.
- Attempting to alter any SFA computing or networking components (including, but not limited to, switches, routers and data/phone/cable TV wiring) without authorization or

beyond one's level of authorization.

- Failing to comply with requests from appropriate SFA officials to discontinue activities that threaten the operation or integrity of computers, systems, networks, or otherwise violate this policy.
- Tampering with network components, blocking communication lines, interfering with the operational readiness of a computer, creating/operating, or providing unsanctioned servers such as personal Web servers, Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), Bootstrap Protocol (BOOTP), or File Transfer Protocol (FTP) servers, or delivering unsanctioned streaming audio, video, high bandwidth gaming, or high bandwidth video conferencing.

## PENALTIES

Misuse of computing, networking, or information resources may result in the loss of computing privileges, as well as disciplinary action.

## PRIORITIES

When demand for computing resources exceeds available capacity, priorities for their use will be enforced. The priorities for use of computing resources are:

- Highest: Uses that directly support the educational, research and service missions of SFA.
- Medium: Uses that indirectly benefit the education, research and service missions of SFA, as well as reasonable and limited personal communications.
- Lowest: Recreational use, including game playing and general browsing.
- Forbidden: Uses listed in the Infractions section of this policy, as well as breaches of the Responsibilities section not specifically listed under the Infractions section.

SFA may enforce these priorities by restricting or limiting usages in circumstances where their demand and limitations of capacity impact or threaten usages of higher priority.

## IMPLIED CONSENT & LIABILITY RELEASE

All individuals with access to SFA computing resources are responsible for their appropriate use. Such use constitutes an agreement to comply with applicable SFA policies and regulations, with applicable city, state, and federal laws and regulations, and with applicable policies of the affiliated networks and systems.

**Cross Reference:** Information Security Management (14.1)

**Responsible for Implementation:** Vice President for University Affairs

**Contact for Revision:** Chief Information Officer

**Forms:** None

**Board Committee Assignment:** Academic and Student Affairs