Acceptable Use of Information Resources

Original Implementation: October 29, 2018
Last Revision: None

Contents

POLICY STATEMENT 1
SCOPE 1
DEFINITIONS 1
RESPONSIBILITIES 3
GENERAL 3
CONFIDENTIALITY AND SECURITY OF DATA 4
SOFTWARE COPYRIGHT 4
EMAIL 5
INCIDENTAL USE OF INFORMATION RESOURCES 5
REQUIREMENTS FOR PORTABLE AND REMOTE COMPUTING 6
ACCOUNT AND PASSWORD MANAGEMENT 6
IMPLIED CONSENT & LIABILITY RELEASE 6
COMPLIANCE 6

POLICY STATEMENT

Stephen F. Austin State University (SFA) supports the responsible use of its information resources. This policy ensures all SFA employees accessing SFA Information Resources are aware of the duties and responsibilities in place to protect SFA Information Resources. The use of Information Resources is provided for the purpose of supporting the mission of SFA. All SFA employees should act responsibly to maintain the integrity of SFA Information Resources. All SFA employees will abide by all existing SFA codes of conduct as well as applicable local, state and federal statutes.

SCOPE

All SFA employees granted access to or use of SFA Information Resources must be aware and agree to abide by the acceptable use requirements set out in this policy.

DEFINITIONS

Confidential Data (Category I) – Data that is considered confidential and must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public

Information Act, Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act) and other constitutional, statutory, judicial, and legal requirements. For more information and examples see the Informational Technology Services (ITS) Policy Handbook located on the ITS website.

Chief Information Security Officer (CISO) – Staff member responsible for providing and administering the overall information security program for the university.

Data – Information which is recorded, regardless of form or media, and used to support the mission of the university, whether in an administrative, teaching or research capacity. Data may be saved or transmitted in hard copy (printed or written), digital/electronic (including video, audio, images) or other formats.

Data Classification – Data is classified as Category I (confidential), Category II (protected) or Category III (public), with each category subject to its own protection requirements and processes. More information, including definitions, protection requirements and examples of data are included in the ITS Policy Handbook.

Data Owner – The university employee responsible for the administrative function supported by the Information Resource or the individual upon whom responsibility rests for carrying out the program using the Information Resources. A listing of Data Owners is contained in the ITS policy handbook.

Information Resources – The procedures, equipment, facilities, software, and data that are designed, built, operated, purchased, and maintained to create, collect, record, process, store, retrieve, display, and transmit information. This may include, but is not limited to, any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, mobile devices, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (e.g., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and hosted services.

Mobile Device – General term for any handheld computing device or smartphone such as tablet, e-reader, smartphone, PDA or portable music player with smart capabilities and which runs a mobile device operating system, i.e. non-enterprise operating system.

Portable Computer – A laptop, notebook, or Surface Pro, which is capable of running on enterprise operating system.

Protected Data (Category II) – Data that may be subject to disclosure or release under the Texas Public Information Act but requires additional levels of protection. For more information and examples see the ITS Policy Handbook.

Public Data (Category III) – Information intended or required for public release by the Texas Public Information Act. For more information and examples see the ITS Policy Handbook.

User – An individual who is authorized by the Data Owner to access the Information Resource, in accordance with the Data Owner's procedures and rules. The User is any person who has been authorized by the Data Owner or SFA representative to access, read, enter, or update that information whether done individually or through facilitation or responsibility for an automated application or process. The User is the single most effective control for maintaining adequate security.

RESPONSIBILITIES

Chief Information Security Officer (CISO)

- Reviews the Acceptable Use Policy annually to ensure consistency with all applicable rules, regulations, and federal/state/local laws.
- Reviews and approves the contents of compliance training related to Acceptable Use Policy.
- Administers the overall information security program.

Human Resources

- Ensures the materials and acknowledgements are included and recorded during the course of the compliance training. Maintains records of training and notifies users of training requirements.

Data Owner

- Authorizes access to the Information Resource.
- In the event that the Data Owner is also the User, then the Data Owner is also responsible for compliance with User responsibilities as specified below.

User

- Reviews and acknowledges understanding and acceptance of the Acceptable Use Policy during annual security training.
- Uses the Information Resource only for the purpose specified by the Data Owner.
- Complies with controls established by the Data Owner.
- Prevents any prohibited disclosure of Category I or Category II data. This data may be disclosed pursuant to a court order or other legal finding as directed by the CISO and General Counsel.

GENERAL

1. SFA Information Resources are provided for the purpose of supporting the mission of SFA. However, Users are permitted to use SFA Information Resources for use that is incidental to the User's official duties to SFA (Incidental Use) as permitted by this policy.
2. Users have no expectation of privacy regarding any SFA data residing on SFA owned computers, servers, or other information resources owned by, or held on behalf of, SFA.
3. Users have no expectation of privacy in regard to any personal information stored by a User on SFA Information Resource including SFA email accounts.
4. Users will exercise responsible, ethical behavior when using SFA's Information Resources. SFA reserves the right to limit, restrict or extend privileges and access to its resources.

5. SFA may access and monitor its Information Resources for any purpose consistent with the university's duties and/or mission without notice.
6. All Users must comply with applicable SFA Information Security policies at all times.
7. Users shall not circumvent SFA computer or information security measures.
8. Users should report misuse of SFA Information Resources or violations of this policy to their supervisors, the CISO or EthicsPoint.
9. The unauthorized deletion or alteration of information or data of others, misuse of system resources, and misuse of system resources by others are prohibited.
10. The owner or designated custodian of a computer that is attached to the SFA network is responsible for the security of the computer.
11. Users are responsible for any activities to or from the network connections and all network activity originating from their equipment.
12. All employees who access SFA information resources must complete compliance and security awareness training annually.

CONFIDENTIALITY AND SECURITY OF DATA

1. Users shall access SFA data only to conduct authorized university business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access.
2. Users shall maintain all records containing SFA data in accordance with the university's Records Retention Policy and Records Management Guidelines.
3. SFA data can only be stored or processed on cloud services provided or sanctioned by ITS. Storing or processing SFA data in a personally obtained cloud service is prohibited.
4. Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official SFA duties.
5. All SFA confidential data must be stored on university provided equipment purchased by SFA or cloud services sanctioned by ITS.
6. All computers connecting to a SFA network must run security software provided by the ITS as necessary to properly secure SFA Information Resources.
7. Devices determined by ITS to lack required security software or otherwise pose a threat to SFA Information Resources may be immediately disconnected by the Information Security Office from a university network without notice.
8. Confidential data stored on portable storage devices must be encrypted.

SOFTWARE COPYRIGHT

1. Software provided through the university for use by SFA employees will be used on computing equipment only as appropriate to the specific software licenses and will not be copied except as specifically permitted by the software license, e.g., to create a backup copy.
2. SFA employees may not use unlicensed or unauthorized copies of software on university-owned computers or any computer connected to the university network.

3. The user is responsible for ensuring and documenting via a license agreement or proof of purchase that the software used on the computer is licensed.
4. The user is responsible for ensuring and documenting the number of software license/s purchased are not exceeded and do not violate copyright law.
5. The university may audit software on university-owned equipment without notice.

EMAIL

1. Emails sent or received by Users in the course of conducting SFA business are considered SFA data that are subject to state records retention and security requirements.
2. Users are to use SFA provided email accounts, rather than personal email accounts, for conducting SFA business. The assigned SFA email account is considered an official method of communication from SFA, and all SFA employees are responsible for the email message content.
3. 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."
4. The following email activities are prohibited when using a SFA provided email account:
    a. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a business related purpose.
    b. Accessing the content of another User's email account except:
        i. As part of an authorized investigation;
        ii. As part of an approved monitoring process; or
        iii. For other purposes specifically associated with the User's official duties on behalf of SFA.
    c. Sending or forwarding any email that is suspected by the User to contain computer viruses.
    d. Any use prohibited by applicable SFA policy.
5. Email access will be removed on the last day of employment, unless special authorization has been granted by the appropriate SFA staff.

INCIDENTAL USE OF INFORMATION RESOURCES

1. Incidental Use of SFA Information Resources must not interfere with a User's performance of official SFA business, result in direct costs to SFA, or expose SFA to unnecessary risks.
2. A User's incidental personal use of a SFA Information Resources does not extend to the User's family members or others regardless of where the Information Resources are physically located.
3. Incidental Use to conduct, support, or promote the User's outside employment, including self-employment, is prohibited.
4. Incidental Use for purposes of political lobbying or campaigning is prohibited.
5. Files not related to SFA business or in support of the SFA mission may not be stored on network file servers.

REQUIREMENTS FOR PORTABLE AND REMOTE COMPUTING

1. All electronic devices including personal computers, smart phones or other devices used to access, create or store SFA Information Resources, including email, must be password protected in accordance with SFA requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.
2. SFA issued mobile computing devices must be encrypted and must have a lock screen enabled.
3. Unattended portable computers, smart phones and other computing devices must be physically secured.
4. All remote access to networks owned or managed by SFA must be accomplished using a remote access method approved by the Information Security Office, as applicable.
5. SFA employees should utilize information security best practices when using personal computing devices to conduct SFA business.

ACCOUNT AND PASSWORD MANAGEMENT

1. SFA issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.
2. Each User is responsible for all activities conducted using the User's account or other credentials.
3. 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.
4. 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.

IMPLIED CONSENT & LIABILITY RELEASE

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

COMPLIANCE

All SFA employees are required to comply with this policy. SFA reserves the right to deny, limit, restrict or extend privileges and access to its Information Technology Accounts and Systems.

Cross Reference: 1 Tex. Admin. Code Ch. 202; Information Security Management (14.1); ITS Policy Handbook

Responsible for Implementation: Vice President for University Affairs

Contact for Revision: Chief Information Security Officer

Forms: None

Board Committee Assignment: Academic and Student Affairs