TEXAS A&M UNIVERSITY
SAN ANTONIO

29.01.03.00.01.S1 IT Standards for All Users

Approved: August, 2019
Revised: January, 2020
Next Scheduled Review: January, 2025

TABLE OF CONTENTS

1. Summary

These Standards apply to all information resources that belong to or are under the control of Texas A&M University - San Antonio ("institution"), and to all people ("users") who access those information resources.

These Standards define the primary rights and responsibilities of all users.

The audience for these Standards is all users.

The purpose of these Standards is to educate users as to their rights and responsibilities as users.

Users may assume other information-technology roles (e.g., Owner, Custodian) in addition to user. With those other roles come other rights and responsibilities which are detailed in separate documentation called IT Standards for Owners and Custodians.

The purpose of the implementation of these Standards is to provide a set of measures that will mitigate information-security risks.

2. Definitions

Affiliate - An individual, other than a student or employee, with a relationship to the institution such that they receive an account granting access to electronic information resources governed by the institution. Other related terms include contractor and contingent worker.

Authenticator – Password, security access card, USB token, or other thing that verifies a user's identity and permits access to information resources.

Confidential information – Information that is exempted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records are confidential records. Examples of "Confidential" data include but are not limited to: social security numbers, grades, credit card numbers, and personal health records.

Contractor - See affiliate.

Controlled information – Information that is not generally created for or made available for public consumption but that may be subject to public disclosure through the Texas Public Information Act or similar laws. Examples of controlled information include but are not limited to: operational information; personnel records; information security procedures; research; internal communications.

Custodian (of information or an information resource) – A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

ITS - Texas A&M University - San Antonio, Information Technology Services department.

Information resources – 1) Electronic data, and 2) the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Institution - Texas A&M University - San Antonio.

IRM - Information Resources Manager - An institutional role defined by Texas Government Code, Section 2054.071 et seq. Appointed by the institution President, the IRM has management authority over all information resources.

ISO - Information Security Officer – An institutional role defined by Texas Administrative Code, Section 202.71. institution employee designated by the President to be responsible for all institution information-security.

Malware – Software that is designed to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user's information systems, e.g. viruses, spyware.

Owner (of an information resource) – Person or entity authorized to decide which users may access the information resource and how. Not necessarily the owner in the sense of property.

Public information – Public information includes all information made available to the public through posting to public websites, distribution through email, or social media, print publications or other media. This classification also includes information for which public disclosure is intended or required.

Session - A login session, i.e. a user is logged into a computer.

Sponsor - An institution employee who vouches for someone seeking an account.

TAC 202 - Texas Administrative Code, Chapter 202 – information security standards for information resources of Texas state agencies and institutions of higher education.

User – An individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

Vendor – See affiliate.

3. STANDARDS

3.1. General

- As an institution of higher learning, the institution encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. The institution recognizes the importance of information technology to students, faculty and staff in scholarly pursuits, professional development, service activities, personal development and everyday work and class-related activities. In particular, access to networked electronic information (e.g., the Internet) supports the academic community by providing a

link to electronic information in a variety of formats and covering all academic disciplines.

- As such, the institution makes available information resources (e.g., facilities, networks, hardware, software) and information for use by members of the community. Such use must be acceptable, i.e., such use must comply with all relevant law and policy, including federal law (e.g., FERPA), state law (e.g., TAC 202), system policies and regulations, institution rules and procedures, relevant IT standards, and the institution's Student Code of Conduct.
- This document addresses, in general terms, the institution's philosophy about computing use and provides an overview of some of the more important law and policy regarding such use. However, it is the responsibility of all users to ensure that their use complies with all relevant law and policy.
- Censorship is not compatible with the goals of the institution. The institution should not limit access to any information due to its content when it meets the standard of legality and is compatible with authorized use. Forms of expression that are not protected by the First Amendment, and therefore may be subject to censorship by the institution include obscene material, child pornography, or other violations of the law. Also, the institution may block access to content that jeopardizes the security of institution information resources, e.g. websites containing malware.

3.2. Responsibilities of All Users: Acceptable Use

3.2.1. Summary

All users shall:

- Use resources only in a manner that is authorized, legal, and ethical;
- Report incidents;
- Complete required training;
- Protect passwords and other authenticators;
- Protect sessions;
- Protect confidential information;
- Protect mobile devices;

- Respect copyright;
- Not purchase, acquire, install, use or alter IT-related hardware, software or services without approval from ITS;
- Cooperate with authorized investigations, audits, assessments, etc.

3.2.2. Use institution information resources only in a manner that is authorized, legal, and ethical

Only Authorized Use. A user shall not use or attempt to use an information resource unless and until the Owner of the information resource has authorized such use.

Only Legitimate Institutional Use and Permissible Incidental Use. All use must be either 1) legitimate institutional use or 2) permissible incidental use. Legitimate institutional use 1) is reasonably related to the user's official duties with respect to the institution (e.g., teaching, research, administration), and 2) furthers the institution's mission. Permissible incidental use is defined in system policy *33.04, Use of System Resources* and later on in this document.

No indecent or obscene material. Users shall not use resources to intentionally access, create, store or transmit material which institution may deem to be indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the institution official processes for dealing with academic ethical issues).

Only Lawful Use. All use must comply with all relevant law and policy, including federal law, state law, system policies and regulations, and institution rules, procedures and standards.

Only Ethical Use. All use of information resources must be ethical. (See system policy *07.01, Ethics*).

No private commercial or organized political use. With the exception of the limited purposes described in system regulation *33.04.01, Use of System Resources for External Employment,* users shall not be paid, or otherwise profit, from the use of any resources or from any output produced from information resources. Users shall not use information resources to promote non-institution-related commercial activity or to conduct organized political activity that is inconsistent with the institution's tax-exempt status.

Other Impermissible Use. Users shall not use information resources to purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of information resources; deprive an authorized user access to a information resource; obtain extra resources beyond those allocated; circumvent institution information-security measures. Users shall not otherwise engage in acts against the aims and purposes of the institution as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

3.2.3. Report Incidents

Users shall report to the ITS Service Desk (helpdesk@tamusa.edu, 210-284-4357) any weaknesses in the security of information resources, or any incidents of possible misuse or violation of this or any other policy related to the security of information resources.

The institution Marketing and Communications office shall handle all interactions with public or private media regarding information-resource security incidents. All institution employees must refer any questions about these issues to this office.

If fraud or theft is suspected as part of security incident detection, the person detecting the incident shall follow System Policy 29.04 – Control of Fraud and Fraudulent Actions.

3.2.4. Complete Required Training

Users shall successfully complete all required information-security training by the relevant deadline.

See e.g. System Regulation 33.05.02 *Required Employee Training.*

3.2.5. Protect Passwords and Other Authenticators

Note: "authenticators" includes passwords, keys, access swipe cards, USB tokens, etc.

Users shall not share their authenticators (e.g. passwords) with anyone without the express, prior permission of the ISO.

If a user does share their authenticator without such permission, the user must 1) change or replace the authenticator immediately and 2) notify the ITS Service Desk.

Users shall not ask for, accept, or use the authenticator of another user.

If a first user accidentally acquires a second user's authenticator, then the first user shall contact the ITS Service Desk.

Users shall not store or transmit their passwords in cleartext. Stored/transmitted passwords must be encrypted.

If a user doubts the security of one of his or her own authenticators, the user shall change/replace the authenticator immediately. If a user doubts the security of another user's authenticator, then the first user should contact the ITS Service Desk.

Users shall return physical authenticators (e.g., Smartcard) a) when no longer needed, 2) on demand of a supervisor or the token's Custodian, or 3) upon termination of the relationship with the institution.

3.2.6. Protect Sessions

A user shall not leave a session unattended on an institution computer without enabling a password-protected screensaver.

A user shall not 1) enable or permit the use of the user's session by a person other than the user without the user being present or 2) use a second user's session without the second user being present. For example, a user may not configure remote control software to permit another person to remotely access the user's session without the user being present.

An exception to the two previous provisions is when the user's session is being controlled by an authorized ITS employee.

3.2.7. Protect Confidential and Controlled Information

Users must protect confidential and controlled information from unauthorized disclosure, modification, or deletion. See, e.g., Family Educational Rights and Privacy Act (FERPA), Texas Public Information Act (TPIA), and the Payment Card Industry Data Security Standard (PCI-DSS).

1. Sharing of institution Confidential Information.
    a. Users **should** constantly strive to minimize the amount of institution confidential information they share with others.
    b. Users **shall not** share institution confidential information with another entity unless authorized by the information's Owner;
2. Transmission of institution Confidential Information.

a. Users **may** transmit **encrypted** institution confidential information over any network or system, including the Internet, provided the encryption is at least as strong as AES 128-bit.

b. Users **may** transmit **unencrypted** institution confidential information:

   i. Within the university network (e.g. writing to the I: drive);

   ii. Within the university's email system only to other university email accounts*, or;

   iii. Over the Internet **only** if the sender is certain that the transmission session is encrypted from end-to-end (e.g. SFTP, HTTPS).

c. All other transmission of institution confidential information is **prohibited**.

3. Storage of institution Confidential Information.

   a. Users **should** constantly strive to minimize the amount of institution confidential information they store on all devices;

   b. Users **may** store **encrypted** institution confidential information on **any device or service**, provided the encryption is at least as strong as AES 128-bit;

   c. Users **may** store **unencrypted** institution confidential information on:

      i. any institution-owned device or service;

      ii. any personally-owned device that has whole-disk encryption (e.g. BitLocker, FileVault) enabled;

   d. Users **shall not** store institution confidential information on any device or service that does not satisfy one of the conditions listed above.

Users shall not delete information that is protected by records retention laws (e.g., TPIA, System Regulation 61.99.01) or e-discovery requirements. Such information can include email and text messages. Users should contact the institution's Records Retention Officer for more guidance.

* Unencrypted confidential information may be sent over the university email system only if the sender's account and all the recipient accounts are on the university's email

system. For example, if an email is addressed to a university email account but cc'd to a gmail account, then that email cannot contain unencrypted confidential information.

3.2.8. Protect mobile devices

Users shall secure unattended institution portable devices (e.g. laptops, tablets, USB memory devices) by e.g. placing the resources in a locked space, or tethering the resources with a security cable.

3.2.9. Respect Copyright

Intellectual property laws (e.g., copyright) apply to the electronic environment and users shall respect such laws. Users should assume that information (e.g., documents, messages, software) stored on or communicated by institution information resources are subject to copyright unless specifically stated otherwise. Users shall not make unauthorized copies of copyrighted software or other copyrighted materials such as music, films, and textbooks. The institution complies with all legal requests for information and will not hesitate to report a user's use in response to a lawful request.

3.2.10. Do not purchase, acquire, alter, install, or use IT-related hardware, software or services without approval from ITS

Users shall not purchase or otherwise acquire any IT-related hardware, software, or services without ITS approval. This includes desktop software, server software, cloud services, software-as-a-service, online subscription databases, and IT consulting.

Users shall not install or use the following software:

- No valid license. Software for which the user does not have a valid license (including using personally-licensed software for business purposes).
- Unsupported/Vulnerable. Commercial software for which the vendor is no longer supplying security patches (e.g. Windows XP, Adobe Acrobat Basic), or open-source software which has one or more known vulnerabilities.
- Blacklisted. Software which is widely recognized by the information-security community as malicious.
- Peer-to-Peer Filesharing. P2P filesharing software e.g. BitTorrent.
- Security Software. Software for disabling, circumventing, or testing security measures, e.g., vulnerability scanners, password crackers, and packet sniffers.

- Anti-Virus/Anti-Malware. The institution installs anti-virus/anti-malware on all its machines. Users shall not install additional anti-virus/anti-malware applications.
- Encryption. Proprietary encryption software or encryption software that is weaker than AES 128-bit.
- Cryptocurrency Mining. Any software for the mining of cryptocurrencies such as Bitcoin.
- Remote Access. Users must get ITS approval before installing any remote-access software on a workstation.

Users shall not make the following changes to institution hardware or networks unless they are also a Custodian of the information resource and the change is authorized:

- Create, delete, or modify user accounts;
- Change security parameters;
- Change audit logging;
- Replace the operating system or boot the device from another operating system;
- Disable or modify institution anti-malware and other security software;
- Turn off whole disk encryption;
- Change the domain to which the machine is attached;
- Modify the network-interface configurations, e.g. IP address, protocols.
- Replace or remove internal hardware components, e.g. network card, hard drive, etc.;
- Format a institution hard drive or other mass storage device;
- Attach network extending devices (e.g., access points, routers) to the institution network;
- Modify, in any way, institution network devices (e.g. routers, firewalls), or network cabling other than station cables.

3.2.11. Cooperate with authorized investigations, audits, assessments, etc.

Users shall cooperate with requests related to authorized investigations, audits, assessments, etc. involving institution information resources and users. Users shall answer questions, provide information, and provide logical and physical access to information resources in a prompt manner.

3.3. Rights: Incidental Use & Privacy

Users have no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by e.g. federal law, Texas state law, Texas A&M System policies, institution policies, etc.

Users may use information resources for incidental (i.e. personal) purposes. Incidental use is established in Texas A&M System Regulation 33.04, and further defined by the institution:

- A user may make incidental use of only those institution information resources or information to which they have been authorized.
- A user may not make incidental use of institution controlled or confidential information.
- Incidental use is restricted to the authorized user; it does not extend to family members or other acquaintances.
- Storage of personal electronic data (e.g., personal email messages, voice messages, documents) within institution information resources must be nominal.

Users should be fully aware of the following with regards to their personal incidental use:

- Custodians have the right to perform the following actions, without notice to or consent from any user, for general IT-administration purposes such as capacity planning, billing for services, cybersecurity, business continuity backups, etc:
    - Log any and all user activities (e.g. websites visited, phone numbers dialed, emails sent/received) on the Custodian's resources, and view those logs. Logs are typically retained for at least one year. The institution cannot and does not distinguish personal from institutional activities.
    - Copy and examines any and all data (e.g. Word documents, databases, email files) stored on or processed by the Custodian's resources. The institution cannot and does not distinguish personal from institutional data.

- All data, both institutional and personal, may be subject to disclosure to third parties through e.g. public information requests, audits, law enforcement requests, subpoenas, etc.
- The institution has no obligation to protect or preserve a user's personal files stored on institution information resources. Users are solely responsible for the confidentiality, integrity, and availability of their personal files stored on institution information resources.
- When separating from the institution, users should copy off any personal files they wish to retain and delete any personal files they do not wish the institution to possess.
- Upon a user's separation from the university, any and all user personal files remaining on institution information resources become the property of the user's supervisor or sponsor. The institution has no obligation to either delete personal files or to provide copies of those files to the user.
- Only ITS may review logs and data without obtaining consent from or giving notice to a user, for the purpose of determining the actions of that user. Such investigations must be approved by, at least, the ISO and Compliance Officer.

4. Exceptions

Users seeking an exception to any of the policies in this document should contact the ISO at iso@tamusa.edu.

5. Consequences for Violations

All users, including staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors, are required to adhere to this policy, and may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and institution policies.

The ISO, IRM, and their designees have the authority to:

1. Revoke the access of a user found in violation of these policies;
2. Confiscate and temporarily store any resource found in violation of these policies, and;
3. Review and terminate contracts associated with contractors, consultants or vendors who are in violation of these policies.

Additional guidance may be found but is not limited to, the following policies and rules.

6. Attachments

None

7. Related Authorities

01.03 Appointing Power and Terms and Conditions of Employment

07.01 Ethics Policy, TAMUS Employees

32.02 Discipline and Dismissal of Employees

32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees

33 Employment, Standards of Conduct

33.04.01 Use of System Resources for External Employment

Contact Office

Business Affairs, Information Technology Services (210) 784-4357 (HELP)