



## STANDARD ADMINISTRATIVE PROCEDURE

### 29.01.03.M0.02 Information Resources – Acceptable Use

*Approved August 27, 1997*

*Revised March 24, 2011*

*Revised October 15, 2013*

*Revised July 23, 2018*

*Revised September 13, 2021*

*Next scheduled review: September 13, 2026*

---

#### SAP Statement

---

Acceptable Use procedures provide guidance for the appropriate use of Texas A&M University (Texas A&M) information resources.

---

#### Definitions

---

Abuse – excessive or improper use of a resource, intentional destruction, diversion, manipulation, misapplication, or misuse of resources.

Breach of Security - unauthorized access to information resources or information resources technologies and/or release of password or other confidential information related to computer security.

Custodian of an Information Resource - a person responsible for implementing owner-defined controls and access to an information resource. Custodians may include university employees, vendors and any third party acting as an agent of or otherwise on behalf of the university and/or the owner.

Fraud – any intentional act or omission designed to deceive others and resulting in the victim suffering a loss and/or the perpetrator achieving a gain (i.e., a willful or deliberate act or failure to act with the intention of obtaining an unauthorized benefit, such as money or property, by deception or other unethical means). For purposes of this SAP, fraud and fraudulent activities include, but are not limited to, such things as:

- theft of any system asset including money, tangible property, time, trade secrets and intellectual property;
- embezzlement;

- bribery/rebate/kick-back;
- misappropriation, misapplication, destruction, removal or concealment of university property;
- forgery, alteration or falsification of documents; and/or
- conflicts of interests.

Harmful Access - creating a computer malfunction or interruption of operation; alteration, damage, or destruction of data; or, injection of malicious software.

Information Resources - the procedures, computer equipment, computing facilities, software and data which are purchased, designed, built, operated and maintained to collect, record, process, store, retrieve, display, report and transmit information.

Unauthorized Access – gaining access to a computer, network, storage medium, system, program, file, user area, or other private repository, without the express permission of the owner.

Owner of an Information Resource (owner) - a person responsible for a business function and for determining controls and access to information resources supporting that business function.

Waste – intentional or unintentional, thoughtless or careless expenditure, consumption, mismanagement, use or squandering of resources to the detriment of the organization. Waste also includes incurring unnecessary costs as a result of inefficient or ineffective practices, systems or controls.

---

## **Official Procedure/ Responsibilities/ Process**

---

### **1. GENERAL**

Texas A&M recognizes the importance of information resources and facilities to students, faculty and staff in scholarly pursuits, professional development, service activities, personal development and every day work and class-related activities.

- 1.1. Use of these resources and facilities is a privilege and requires that individual users act in compliance with University Rules. The university may provide users with a university account that permits the use of information resources and facilities within guidelines established by Texas A&M. Users must respect the integrity of information resources and facilities, respect the rights of other users and comply with all applicable laws (local, state, federal and international), System Policies, System Regulations, University Rules and contractual agreements. The university reserves the right to limit, restrict, or deny computing privileges and access to its facilities for those who violate, or who are under investigation for allegedly violating, local, state, federal and international laws, System Policies, System Regulations, University Rules, or contractual agreements.

- 1.2. As an institution of higher learning, Texas A&M encourages, supports and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. Access to networked computer information in general and to the Internet in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. As with any resource, it is possible to misuse information resources or facilities and abuse access to the Internet. The following sections address, in general terms, Texas A&M University's philosophy about use of information resources and facilities. Additional information can be found in Texas A&M University System Policies and Regulations, Texas A&M University Rules and Student Rules.

## 2. PRIVACY

- 2.1. While there is no expectation of privacy beyond that which is expressly provided by applicable privacy laws, the privacy of data will be maintained to the extent possible in the course of all custodial operations and access. Personnel (non-owner) will not access data except for authorized business purposes, including but not limited to the normal operation and maintenance of university information resources. In such circumstances, the confidentiality of user data will be protected to the extent possible and will not be divulged except to authorized university officials (see [Texas A&M Information Security Control AC-5 Separation of Duties](#)). Contents of electronic files will be examined or disclosed only when authorized by their owners, approved by an appropriate university official, or required by law (see [University SAP 29.01.03.M0.09 Information Resources - Privacy](#)).
- 2.2. Information created, stored or transmitted on university information resources may be subject to disclosure under the Texas Public Information Act or through legal or administrative proceedings.

## 3. COPYRIGHT LAWS

All members of the university community should be aware that copyright laws apply to the electronic environment. Users should assume that works communicated through a network are subject to copyright laws unless specifically stated otherwise. Utilization of any electronically transmitted information should be within the "fair use" principle unless permission of the copyright owner is obtained.

## 4. CRIMINAL AND ILLEGAL ACTS

Information resources of the university, which include the hardware, software and network environment, shall not be used for illegal activities. Any such use of these resources will be dealt with by the appropriate university authorities and/or other legal and law enforcement agencies. Criminal and illegal use may involve unauthorized access; intentional corruption or misuse of information resources or facilities; theft; obscenity; child pornography; or, illegal discrimination, sexual harassment and related retaliation.

## 5. AUTHORIZED USE

Information resources and facilities are provided by the university to accomplish tasks related to the university's mission. Information resources or facilities may not be used for commercial activities or illegal activities. Incidental personal use of information resources or facilities by employees is governed by the [System Policy 33.04 Use of System Resources](#).

## 6. INCIDENTAL USE

6.1 Incidental personal use of computing resources at Texas A&M University is an exception to the general prohibition against the use of University equipment for anything other than official state business.

6.2 Incidental Use is defined as use that:

6.2.1 is occasional use for personal purposes,

6.2.2 is of minimal time and duration,

6.2.3 results in no additional cost to the university,

6.2.4 does not result in financial gain to the user, and

6.2.5 does not result in a general perception of affiliation between the university and an external organization.

6.3 Incidental Use must not interfere with assigned job responsibilities or be in violation of exiting security or access rules.

6.4 Personal use of University computing resources for consulting, outside employment, or organizations unaffiliated with the University which cannot be categorized as incidental should be guided by System Regulation 33.04.01, *Use of System Resources for External Employment*.

## 7. INDIVIDUAL RESPONSIBILITY FOR USE OF INFORMATION RESOURCES AND FACILITIES

It is expected that all members of the university community will use university resources and facilities in accordance with System Policies and University Rules. Failure to fulfill these responsibilities may lead to the cancellation of computer account(s), disciplinary action by the university and/or referral to legal and law enforcement agencies. In addition to complying with the other provisions of this SAP, individuals using the university's information resources or facilities are required to:

7.1. Use communal resources with respect for others. Disproportionate uses of computing resources can prevent others from using these resources.

7.2. Protect passwords and use of accounts. Individuals are not permitted to use accounts or passwords for which they are not the designated user. (see security control [AC-2](#))

- 7.3. Secure confidential information contained on information resources and do not provide access to any individual who is not authorized to access such information (see security control [DC-2](#)).
- 7.4. Report improper use of information resources and facilities (see security control [IR-6](#)). Improper use of information resources and facilities may include:
  - breach of security;
  - harmful access; or,
  - any other unauthorized access or use.
- 7.5. Comply with the request of an information resource owner or custodian (e.g., system administrator) regarding use of that resource.
- 7.6. Ensure that all software on information resources is used according to its license terms. Unauthorized or unlicensed use of software is prohibited, and subject to disciplinary action (see security control [CM-11](#)).
- 7.7. Report fraud, waste, or abuse using university information resources and facilities in accordance with [System Policy 10.02 Fraud, Waste and Abuse](#).
- 7.8. Report any incidents of illegal discrimination, sexual harassment and related retaliation using university information resources and facilities according to guidelines in [University Rule 08.01.01.M1 Civil Rights Compliance](#).
- 7.9. Report the improper use of university information resources and facilities that may violate other laws and/or university or system requirements in accordance with [University Rule 32.01.99.M1 Complaint Procedures for Electronic Information](#).
- 7.10. Respect the forum (e.g. email lists, social media, public computing facilities) when communicating ideas to others via university information resources (includes access to the Internet). Communications that are threatening, discriminatory, or disruptive may result in administrative and/or disciplinary action.

---

## **Related Policies or Requirements**

---

[System Policy 07.01 Ethics](#)

[System Policy 10.02 Fraud, Waste and Abuse](#)

[System Policy 29.01 Information Resources](#)

[System Policy 33.04 Use of System Resources](#)

[University Rule 08.01.01.M1 Civil Rights Compliance](#)

[University Rule 32.01.99.M1 Complaint Procedures for Electronic Information](#)

[University SAP 29.01.03.M0.09, Information Resources - Privacy](#)

[Texas A&M Information Security Control AC-2 Account Management](#)  
[Texas A&M Information Security Control AC-5 Separation of Duties](#)  
[Texas A&M Information Security Control DC-2 Roles & Responsibilities](#)  
[Texas A&M Information Security Control IR-6 Incident Response](#)  
[Texas A&M Information Security Control CM-11 User Installed Software](#)

---

**Contact Office**

---

Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY:

[Vice President for Information Technology & Chief Information Officer](#)