# IT STANDARDS FOR ALL USERS

Approved: June 1, 2016
Reviewed: July 22, 2019
Reviewed: June 24, 2020
Next Scheduled Review: June 24, 2021

---

Contact for Interpretation: Office of Information Security

Parent Procedure: Rule 29.01.99.C1 "Security of Electronic Information Resources"

---

## Summary

---

This procedure defines primary rights and responsibilities for all users of information and information resources that belong to, or under the control of Texas A&M University-Corpus Christi ("university").

This procedure applies to all information and information resources owned or under the control of the university, and to all people ("users") who access those resources and information.

The audience for this procedure is all users.

The purpose of this procedure 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 this university procedure is to provide a set of measures that will mitigate information-security risks.

---

## Definitions

---

Authenticators – account names and passwords, security access cards, tokens, and keys associated with mechanisms that permit 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 – any company, and its employees, not affiliated with Texas A&M University-Corpus Christi, which provides a service to the university.

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.

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

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

Information Security Officer ("ISO") – University employee designated by the President to be responsible for all university 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 information or 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.

Texas Administrative Code 202 ("TAC 202") – information security standards for information resources purchased by agencies and institutions of higher education in the State of Texas.

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

Vendor – see Contractor.

## Procedure

1. ACCEPTABLE USE

1.1. GENERAL

1.1.1. As an institution of higher learning, the university encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. The university 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.

1.1.2. As such, the university 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, university rules and procedures, relevant IT standards, and the university's Student Code of Conduct.

1.1.3. This section addresses, in general terms, the university'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.

1.1.4. Censorship is not compatible with the goals of the university. The university 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 university include obscene material, child pornography, or other violations of the law. Also, the university may block access to content that jeopardizes the security of university information-resources and university information, e.g. websites containing malware.

1.2. ACCEPTABLE USE PROCEDURES

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

1.2.1.1. A user shall use a university information-resource or university information only in the manner authorized by the Owner. For example, if an Owner has authorized a user only to view certain information, then the user is not permitted to edit that information even if the user has the technical ability to do so.

1.2.2. 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 is use that 1) is reasonably related to the user's official duties with respect to the university (e.g., teaching, research, administration), and 2) furthers the university's mission. Permissible incidental use is defined in system policy *33.04, Use of System Resources*.

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

1.2.4. 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).

1.2.5. No indecent or obscene material. Users shall not use university information resources to intentionally access, create, store or transmit material which university 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 university official processes for dealing with academic ethical issues).

1.2.6. Authenticators (e.g., passwords). Users shall neither share their passwords nor accept or use the password of another.

1.2.7. 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 university information resources or from any output produced from such resources. Users shall not use university information resources to promote non-university-related commercial activity or to conduct organized political activity that is inconsistent with the university's tax-exempt status.

1.2.8. 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 university 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 university complies with all legal requests for information and will not hesitate to report a user's use in response to a lawful request.

1.2.9. Hardware and Software. Users shall not 1) use or install unauthorized software or hardware, or 2) make unauthorized changes to university hardware and software.

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

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

1.2.12. Physical Security. Users shall secure unattended portable devices. Users working on publicly-accessible computers shall logout or invoke a password-protected screensaver when leaving the computer.

1.2.13. Security Incident Reporting. Users shall report to the IT Helpdesk any weaknesses in the security of the university's information resources, or any incidents of possible misuse or violation of this or any other policy related to the security of the university's information resources.

## 2. IT PRIVACY

### 2.1. GENERAL

2.1.1. Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users in providing privacy in university information resources.

2.1.2. Users of university information resources have a basic right of privacy in 1) the files they own which are stored or communicated by university information resources, and 2) the activities they perform using university information resources.

2.1.3. However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.

2.1.4. In particular, the university has the right to examine all information stored on or passing through university information resources, and to monitor the activities of any user on university information resources so as to, e.g., ensure business continuity, ensure compliance with law and policy, or conduct authorized investigations.

### 2.2. PRIVACY PROCEDURES

2.2.1. A file may not be accessed, copied, or modified without prior authorization from the file Owner. This general right to privacy is subject to the following exceptions and limitations:

2.2.1.1. The file Owner's right to privacy in their files may be limited by other laws and policy. For example, the Texas Public Information Act may require the disclosure of certain data under certain conditions.

2.2.1.2. A person in the file Owner's chain of command (i.e., the file Owner's supervisor, that supervisor's supervisor, etc.) may access or copy any of the file Owner's files as long as that person

has the authorization of the appropriate dean or vice president, i.e., the dean or vice president in the Owner's chain of command.

2.2.1.3. The IRM, his or her designees, and resource Custodians may log, monitor, copy, and examine any information passing through or stored on any university information resource for which they are responsible for reasons including, but not limited to:

2.2.1.3.1. Ensuring compliance with applicable law and policy;

2.2.1.3.2. Ensuring business continuity (e.g., making backups);

2.2.1.3.3. Monitoring network performance and maintenance activities, or;

2.2.1.3.4. Responding to authorized requests for information from, e.g., auditors or investigators.

2.2.1.4. In 2.2.1.2 and 2.2.1.3, the file Owner's authorization still should be sought before altering a file, except, e.g., where it would interfere with an authorized investigation, or in case of an emergency.

2.2.1.5. In response to lawful requests, the IRM may provide to authorized entities (e.g., law enforcement, auditors) access to information transmitted through and stored on university information resources after the notification and written approval of the Vice President of Finance & Administration. Exceptions to this procedure may occur in instances related to federal and state laws.

2.2.2. A user's activities on or with a university information resource may not be tracked or recorded without first obtaining authorization from the user. This right of privacy in activities is subject to the following exceptions:

2.2.2.1. The IRM, his or her designees, and resource Custodians may, without any notification to a user, monitor some or all of the user's activities on relevant information resources for university-business-related purposes, including but not limited to those enumerated in 2.2.1.3. Examples of such monitoring include logging the phone numbers dialed by a user from their desk phone, or recording the web sites a user visited using a university workstation.

2.2.2.2. The university may perform video and audio surveillance as defined in other policy.

2.2.3. Individuals who have special access to information because of their position have the absolute responsibility not to take advantage of that access.

2.2.3.1. Such individuals should access only that information that is relevant to the particular task, and only so much of that information as is necessary to achieve the task

2.2.3.2. If, however, in the course of performing the task such individuals find unrelated evidence of impermissible use or other wrongdoing, those individuals are obligated to report an incident.

2.2.3.3. If an individual inadvertently accesses information (e.g., seeing a copy of a test or homework) that could provide personal benefit, such individual has the responsibility to notify 1) the file Owner, 2) their own supervisor, and 3) the file Owner's supervisor.

2.2.4. Unless otherwise provided for, individuals whose relationship with the university is terminated (e.g., student graduates; employee takes new job; visitors depart) are considered to cede ownership of, and hence the right to privacy in, all their files to the information resource custodian. The university should determine what information is to be retained and delete all other.

2.2.5. Custodians of web sites available to the general public from university information resources shall abide by and ensure that those web sites contain a link to the university's privacy statement located at http://www.tamucc.edu/privacy.htm.

# 1. Access Control

With rare exceptions (e.g. public web sites), a person must possess a TAMUCC *account* to access TAMUCC information-resources and TAMUCC information. An account typically comprises a unique *username*, at least one *authenticator* (e.g., a password), and a set of *permissions* (e.g. the ability read or edit certain files). A *user* is a person to whom TAMUCC has granted an account. For example, TAMUCC gives all employees and students an IslandID account which permits the user to log into many TAMUCC devices and services. When users log into a device, they create a *session*. That session is destroyed when the user logs out or the device is rebooted.

## 1.1. Accounts and Permissions

1.1.1. By default, users are not authorized to create accounts or to modify the permissions associated with any account. Only the Owner of an information-resource or information, or his or her designees, may create an account for that information-resource or information, or modify the permissions associated with that account.

## 1.2. Authenticators (e.g. Passwords)

1.2.1. Users shall not share their authenticators with anyone without the express, prior permission of the TAMUCC Information Security Officer ("ISO").

1.2.2. If a user does share their authenticator without such permission, the user must 1) change or replace the authenticator immediately and 2) notify the IT Helpdesk.

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

1.2.4. If a first user accidentally acquires a second user's authenticator, then the first user shall contact the IT Helpdesk.

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

1.2.6. 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 IT Helpdesk.

1.2.7. Users shall return physical authenticators (e.g., Smartcard) on demand of a supervisor or the token's Custodian, or upon termination of the relationship with the University.

## 1.3. Sessions

1.3.1. 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.

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

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

## 2. University Incidental Use

2.1. Permissible incidental use is defined in Texas A&M System Policy 33.04. The following further restrictions and caveats apply to incidental personal use of the University's information resources and University information:

2.1.1. A user may make incidental use of only those TAMUCC information resources or information to which they have been authorized per section 1.2.1 of Procedure 29.01.99.C1.01 "Acceptable Use and Privacy," and may make only such use as authorized per section 1.2.1.1 of that same Procedure.

2.1.2. Incidental personal use is restricted to the authorized user; it does not extend to family members or other acquaintances.

2.1.3. Storage of personal electronic data (e.g., personal email messages, voice messages, documents) within University information resources must be nominal.

2.1.4. All personal electronic data stored on, processed by, or transmitted by University information resources may be subject to open records requests and may be accessed in accordance with this document and other policy.

## 3. Protection of TAMUCC Information

3.1. Sharing of TAMUCC Confidential Information.

3.1.1. Users **should** constantly strive to minimize the amount of TAMUCC confidential information they share with others.

3.1.2. Users **shall not** share TAMUCC confidential information with another entity unless authorized by the information's Owner;

3.2. Transmission of TAMUCC Confidential Information. Users:

3.2.1. **May** transmit **encrypted** TAMUCC confidential information over any network, including the Internet, provided the encryption is at least as strong as AES 128-bit.

3.2.2. **May** transmit **unencrypted** TAMUCC confidential information **only**:

- within the TAMUCC network or with approved devices and services listed on it.tamucc.edu/approved, or;
- over the Internet if the user is certain that the transmission session is encrypted from end-to-end (e.g. SFTP, HTTPS).

3.2.3. All other transmission of TAMUCC confidential information is prohibited.

3.3. Storage of TAMUCC Confidential Information. Users:

3.3.1. **Should** constantly strive to minimize the amount of TAMUCC confidential information they store on all devices;

3.3.2. **May** store **encrypted** TAMUCC confidential information on **any device or service**, provided the encryption is at least as strong as AES 128-bit;

3.3.3. **May** store **unencrypted** TAMUCC confidential information on:

- any TAMUCC-owned device or service;
- any device or service listed on it.tamucc.edu/approved;
- any personally-owned device that has whole-disk encryption (e.g. BitLocker, FileVault) enabled;

3.3.4. **Shall not** store TAMUCC confidential information on any device or service that does not satisfy one of the conditions listed above.

3.4. 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 University's Records Retention Officer for more guidance.

## 4. Security Incident Reporting

4.1. Users shall report security incidents to the IT Helpdesk (x2692, ithelp@tamucc.edu)

4.2. The University Marketing and Communications office shall handle all interactions with public or private media related to any security incident involving University information resources and sensitive information. All University employees must refer any questions about these issues to this office.

4.3. 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.

## 5. Hardware and Software

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

5.2. Users shall not install or use the following software on a TAMUCC information-resource:

5.2.1. No valid license. Software for which the user does not have a valid license (including using personally-licensed software for business purposes).

5.2.2. 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.

5.2.3. Blacklisted. Software which is widely recognized by the information-security community as malicious.

5.2.4. Peer-to-Peer Filesharing. P2P filesharing software e.g. BitTorrent.

5.2.5. Security Software. Software for disabling, circumventing, or testing security measures, e.g., vulnerability scanners, password crackers, and packet sniffers.

5.2.6. Anti-Virus/Anti-Malware. TAMUCC installs anti-virus/anti-malware on all its machines. Users shall not install additional anti-virus/anti-malware applications.

5.2.7. Encryption. Proprietary encryption software or encryption software that is weaker than AES 128-bit.

5.2.8. Cryptocurrency Mining. Any software for the mining of cryptocurrencies such as Bitcoin.

5.3. Users shall not make the following software changes on a TAMUCC information-resource unless they are also a Custodian of the information resource and the change is authorized:

5.3.1. Replace the operating system or boot the device from another operating system;

5.3.2. Disable or modify University anti-malware and other security software;

5.3.3. Turn off whole disk encryption;

5.3.4. Change the domain to which the machine is attached;

5.3.5. Modify the network-interface configurations, e.g. IP address, protocols.

5.4. Users shall not make the following changes to TAMUCC hardware unless they are also a Custodian of the information resource and the change is authorized:

5.4.1. Replace or remove internal hardware components, e.g. network card, hard drive, etc.;

5.4.2. Format a University hard drive or other mass storage device;

5.4.3. Attach network extending devices (e.g., access points, routers) to the University network;

5.4.4. Modify, in any way, University network devices (e.g. routers, firewalls), or network cabling other than station cables.

## 6. EXCEPTIONS

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

## 7. CONSEQUENCES FOR VIOLATIONS

7.1. 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 University procedure, and may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and University policies.

7.2. Individuals found in violation of this University Procedure are subject to loss of access privileges to University information resources (e.g. servers, workstations, email, etc.) In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

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

7.3.1. Texas A&M System Policy

7.3.1.1. 01.03 Appointing Power and Terms and Conditions of Employment

7.3.1.2. 07.01 Ethics Policy, TAMUS Employees

7.3.1.3. 32.02 Discipline and Dismissal of Employees

7.3.1.4. 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees

7.3.1.5. 33 Employment, Standards of Conduct

7.3.1.6. 33.04.01 Use of System Resources for External Employment

7.3.2. Texas A&M University-Corpus Christi Rule

7.3.2.1. 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments

7.3.2.2. 13.02.99.C1 Student Disciplinary Proceedings