IT STANDARDS FOR ALL USERS

Approved: June 1, 2016
Reviewed: March 26, 2018
Next Scheduled Review: March 26, 2019

Contact for Interpretation: Office of Information Security

Parent Procedure: Procedure 29.01.99.C1.01 “IT Acceptable Use and Privacy”

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 or in Procedure 29.01.99.C1.01 "IT Acceptable Use and Privacy" should contact the ISO at iso@tamucc.edu.

7. DEFINITIONS

7.1. See TAMUCC Procedure 29.01.99.C1.01 "IT Acceptable Use and Privacy" for definitions.

8. CONSEQUENCES FOR VIOLATIONS

8.1. 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.

8.2. 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.

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

8.3.1. Texas A&M System Policy

8.3.1.1. 01.03 Appointing Power and Terms and Conditions of Employment

8.3.1.2. 07.01 Ethics Policy, TAMUS Employees

8.3.1.3. 32.02 Discipline and Dismissal of Employees

8.3.1.4. 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees

8.3.1.5. 33 Employment, Standards of Conduct

8.3.1.6. 33.04.01 Use of System Resources for External Employment

8.3.2. Texas A&M University-Corpus Christi Rule

8.3.2.1. 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments

8.3.2.2. 13.02.99.C1 Student Disciplinary Proceedings