IT STANDARDS FOR ALL USERS

Approved: June 1, 2019
Reviewed: June 1, 2020
Next Scheduled Review: June 1, 2021

Contact for Interpretation: Chief Information Officer
Parent Procedure: Procedure SAP 29.01.03.T0.01 IT Acceptable Use

1. University Incidental Use

1.1. 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:

1.1.1. A user may make incidental use of only those University information resources or University information to which they have been authorized.

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

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

1.1.4. 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. (See Information Resource Privacy, below.)

2. Protection of Confidential and Controlled Information.

2.1. Users should constantly strive to minimize 1) the amount of confidential and controlled information stored on all their computing devices and 2) the transmission of such information to others.

2.2. Users shall not store confidential or controlled information on a portable computing device (e.g., laptop, smartphone, USB storage device) or a non-University computing device (e.g., home workstation, Internet host) unless absolutely necessary.

2.3. Users shall encrypt confidential and controlled information before 1) storing such information stored on a portable device or on a non-Tarleton State University-owned device, or 2) transmitting such information over a non-Tarleton State University-owned network, e.g. the Internet.

2.4. Before a user may transfer confidential or controlled information to another institution of higher education, contractor, or other third party, that third party must affirm that they will protect the transferred data in accordance with the conditions imposed by the information owner, which conditions will contain, at a minimum, the conditions specified in this procedure.

2.5. 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 includes email and text messages. Users should contact the University's Records Officer for more guidance.

2.6. Users shall not perform mass file deletions without supervisory approval.

3. Authenticators (e.g. Passwords)

3.1. Users shall not share their authenticators with anyone.

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

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

3.4. Users shall not store or transmit their passwords in clear-text. Stored/transmitted passwords must be encrypted.

3.5. If a user doubts the security of one of his or her own authenticator, 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.

3.6. 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.

4. Security Incident Reporting

4.1. Users shall report security incidents to the IT Helpdesk (ext. 9885). helpdesk@tarleton.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 University 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 University information-resource:

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

5.2.2. Software for which the user does not have a valid license;

5.2.3. Software for which the vendor is no longer supplying security patches;

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

5.3. Users shall not make the following software changes on a University 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 University 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. Connect the device to a non-University network, or change how the device connects to the University network (i.e., change from a wired connection to wireless or vice versa);

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

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

5.4.5. Attach personally-owned devices to a University network without University approval or in a manner different from what the University approved;

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

Remote Access: Users remotely accessing an information resource (e.g., via VPN or Remote Desktop) shall use only those remote access methods that have been approved by ITS.

6. CONSEQUENCES FOR VIOLATIONS

6.1. 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.

6.2. 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.

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

6.3.1. Texas A&M System Policy

6.3.1.1. 01.03 Appointing Power and Terms and Conditions of Employment

6.3.1.2. 07.01 Ethics Policy, TAMUS Employees

6.3.1.3. 32.02 Discipline and Dismissal of Employees

6.3.1.4. 32.02.02 Discipline and Dismissal Procedure for Non-faculty Employees

6.3.1.5. 33 Employment, Standards of Conduct

6.3.1.6. 33.04.01 Use of System Resources for External Employment