Portable computing devices such as smart phones, tablets, laptop computers, USB memory (aka thumb drives) are becoming convenient, powerful and easy to use. Their small size and functionality are making these devices more desirable to replace traditional desktop devices in a wide number of applications. Portable computing devices also introduce risk to personal privacy and University data. This document outlines guidelines regarding the use of these portable computing devices in the Texas A&M University-San Antonio (A&M-San Antonio) computing environment.

This Procedure applies to all users of A&M-San Antonio information resources.

The purpose of this Procedure is to provide a set of measures that will mitigate information security risks associated with portable computing devices connected to the A&M-San Antonio network. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this Procedure based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

1. Portable computing devices must be password-protected using the security feature provided on the tool, and there should be no sharing of portable computing device passwords.
2. Whenever possible, sensitive or confidential A&M-San Antonio data should not be stored on portable computing devices. In the event that there is no alternative to local storage, such data must be encrypted using University-approved encryption techniques. Assistance with protecting or encrypting information is available by contacting the Information Technology Services (ITS) Help Desk.

3. Remote access to A&M-San Antonio systems must utilize approved techniques when transmitting or receiving sensitive or confidential information.

4. Unattended portable computing devices shall be kept physically secure using means appropriate to the potential risk associated with the device. This may include storing the device in a locked office, desk drawer, or filing cabinet, or securing the device via a cable lock system.

5. Device and information resource owners will ensure that any portable computing device within their area of responsibility is being managed and used in accordance with all applicable University acceptable use Rules and Procedures.

6. ITS reserves the right to inspect any system or equipment connecting to the network and disconnect as necessary for business or other risk related reasons.

7. Users possessing portable computing devices with access to sensitive information must comply with 29.01.03.O0.13 Encryption of Confidential and Sensitive Information.

8. The University is not responsible for the recovery or maintenance of personal content to include but not limited to music or pictures files that may be lost while the device is issued to the employee. It is the responsibility of the individual to recover any files stored on the device upon transfer or termination of employment.

9. Users are prohibited from using University owned portable computing devices to access inappropriate or obscene material.

10. ITS will provide limited support for applications or software on portable computing devices not adopted universally by the University.

11. Internet connectivity will be accessible on campus via the wireless network for authorized users. Some ITS applications may not be compatible or accessible through portable computing devices.

---

**Non-Compliance**

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship.
in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to the University information resources, civil, and/or criminal prosecution.

Related Rules

DIR Practices for Protecting Information Resources Assets

Family Educational Rights and Privacy Act (FERPA)

Gramm Leach Bliley Act (GLB Act)

Health Insurance Portability and Accountability Act (HIPAA)

Texas Administrative Code (TAC) 202 as amended or supplemented

Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education

TAMU System Policy 29.01 Information Resources

A&M-San Antonio Procedure 29.01.03.O0.13 Encryption of Confidential and Sensitive Information

A&M-San Antonio Procedure 29.01.02.O0.17 Network Access

Definitions

Accounts - Information resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

Confidential Information - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

Custodian - Guardian or caretaker (the holder of data). The agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.
**External Storage Media** - Portable devices that are not permanently fixed inside a computer and are used to store data. These include, but are not limited to, USB thumb drives, CDs, DVDs, external hard drives, memory cards, etc.

**Incident Report** – A formal reporting of a known information technology related incident. This is performed by completing the associated ITS form.

**Information Resources (IR)** - 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)** - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.

**Information Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

**Information Technology Services (ITS)** – The designated name for the central Information Technology department for the University.

**Mission Critical Information** - Information that is defined by A&M-San Antonio or information resource owner to be essential to the continued performance of the mission of A&M-San Antonio or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of A&M-San Antonio or department.

**Owner** - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

**User** - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner’s rules and procedures.

---

**Contact Office**

Finance and Administration, Information Technology Services (210) 784-4357 (HELP)