Procedure Statement

Privacy policies are mechanisms used to establish the limits and expectations for the users of Texas A&M University-San Antonio (A&M-San Antonio) information resources. The general right to privacy is extended to the electronic environment to the extent possible. Privacy is mitigated by the Texas Public Information Act, administrative review, computer system administration, and audits. Contents of electronic files will be examined or disclosed only when authorized by their owners, approved by an appropriate A&M-San Antonio official, or required by law.

Reason for Procedure

This Procedure applies to electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the University.

The purpose of this Procedure is to provide a set of measures that will mitigate information security risks associated with Privacy Issues. 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).

The intended audience for this Procedure is all users of A&M-San Antonio information resources.
Official Responsibilities and Procedure

1. Privacy of information must be provided to users of A&M-San Antonio information resources consistent with obligations of Texas and federal law and/or secure operations.

2. In the normal course of their duties, custodians may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

3. Electronic files created, sent, received, or stored on University-owned, leased, administered, or otherwise under the custody and control of A&M-San Antonio are not private and may be accessed by authorized employees at any time without knowledge of the information resource owner or owner as required to conduct business related activities. It is the expectation that authorized employees will treat any information viewed or accessed as confidential.

4. To manage systems and enforce security, A&M-San Antonio may log, review, and otherwise utilize any information stored on or passing through its information systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards. For these same purposes, A&M-San Antonio may also capture user activity such as telephone numbers dialed and web sites visited. In the normal course of their duties, system administrators may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

5. In order to protect against hardware and software failures, backups of all data stored on University information resources may be made. System administrators have the right to examine the contents of these backups to gather sufficient information to diagnose and correct problems with system software, hardware, or performance. It is the user’s responsibility to find out retention policies for any data of concern.

6. A wide variety of third-parties have entrusted their information to A&M-San Antonio for business purposes, and all workers at A&M-San Antonio must do their best to safeguard the privacy and security of this information. The most important of these third-parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.

7. The CEO or designee may designate certain individuals or functional areas that may monitor user activities and/or examine data solely to determine if unauthorized access to a system or data is occurring or has occurred. If files are examined, the file owner will be informed as soon as practical, subject to delay in the case of an on-going investigation.
8. Information resource owners or custodians will provide access to information requested by auditors in the performance of their jobs. Notification to file owners will be as directed by the auditors.

9. The University collects and processes many different types of information from third-parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations (e.g., Gramm-Leach-Bliley Act, Texas Administrative Code 206).

10. Individuals who have special access to information because of their position have the absolute responsibility to not take advantage of that access. If information is inadvertently gained that could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

11. Users of A&M-San Antonio information resources shall call the Information Technology Services (ITS) helpdesk or ISO to report any compromise of security which could lead to divulging confidential information including, but not limited to, posting social security and credit card numbers to the Internet.

12. Users shall not attempt to access any A&M-San Antonio data or systems that they do not have authorization or explicit consent from the owner or appropriate employee to access.

---

**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 (HIPPA)
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

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).

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.

**System Custodian** – Guardian or caretaker of the operating system and physical hardware; the person(s) charged with implementing the controls specified by the owner of the system. This custodian is responsible for operating system updates and assisting the Application Custodian with any testing or major changes to the system.

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

---

**Contact Office**

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