Texas A&M University-San Antonio

29.01.03.O0.12 Internet/Intranet Use
Approved: June 12, 2014
Next Scheduled Review: June, 2019

Procedure Statement

Texas A&M University-San Antonio (A&M-San Antonio) supports and encourages internet and intranet use for all users of information resources. Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas and must be managed as valuable state resources. This Procedure is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;
- To establish acceptable practices regarding the use of information resources; and,
- To educate individuals who may use information resources with respect to their responsibilities.

Reason for Procedure

This Procedure applies to all users of University information resources.

The purpose of this Procedure is to provide a set of measures that will mitigate information security risks associated with Internet/Intranet use. There may also be other or additional measures that department heads or deans will provide to further mitigate risk. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and the 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).
Official Responsibilities and Procedure

1. All Internet and Intranet usage by University employees, authorized vendors, business partners, students, and guests must adhere to federal and state laws, as well as, Texas A&M University System and University policies, rules, and procedures.

2. Users are responsible for their account(s). Users should make appropriate use of the system(s) and network-provided features to ensure computer resources are protected.

3. Users must not use another user’s account or password without proper authorization. Individual password security is the responsibility of each individual user.

4. Users are prohibited from using any form of electronic media (e.g. email or web resource) to harass, intimidate, or otherwise annoy another person/group.

5. University Internet or Intranet access may not be used for personal gain or solicitations.

6. All activity may be subject to logging and review.

7. No University mission critical or confidential information shall be made available via University websites or public websites without ensuring that the material is accessible to only authorized individuals or groups.

8. ITS and/or other department heads in control of information resources are required to ensure that all systems and software accessing the Internet and Intranet are up-to-date with security patches and the system’s protection software are maintained.

9. Downloading games, music, movies or any other non-business software or materials may be restricted by ITS for network performance purposes.

10. All sensitive material transmitted over external networks must be encrypted.

11. Any security violations, and unauthorized use pertaining to this Procedure, shall be reported according to the ISO and/or the IRM.

12. Incidental use of Internet/Intranet access is subject to A&M-San Antonio Procedure, 29.01.03.O0.02, Acceptable Use for Information Technology. Incidental use definitions apply to all Internet/Intranet activities to include downloading.
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)
- **TAMU System Policy 29.01 Information Resources**
- **Texas Administrative Code (TAC) 202** as amended or supplemented
  - **Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education**
- **A&M-San Antonio Procedure 29.01.01 Information Resources – State Web Sites**
- **A&M-San Antonio Procedure 29.01.03 Electronic Information Services Access and Security**
- **A&M-San Antonio Procedure 29.01.03.02 Acceptable Use for Information Technology**
- **TAMU System Policy 07.01 Ethics**

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.

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.

Internet - A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies and colleges.

Intranet - A private network for communications and sharing of information similar to the Internet, but accessible only to authorized users within an organization. An organization’s intranet is usually protected from external access by a firewall.

Logon ID - A unique account name that is required as the first step in logging into a secure information resource. A logon ID typically must be associated with a user password to obtain access to the information resource.

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 procedures and rules.

Contact Office

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