Procedure Statement

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources, thus this Procedure is established to:

1. Ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

2. Establish prudent and acceptable practices regarding the use of information resources; and,

3. Educate individuals who may use information resources with respect to their role and responsibilities associated with such use.

Reason for Procedure

This Procedure applies to all Texas A&M University – San Antonio ("The University") information resources.

The purpose of this Procedure is to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. There may also be other or additional measures that division or department heads will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are 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 and approved 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 includes, but is not limited to, all information resources owners, system administrators, and users of University information resources.
1. OWNERSHIP OF ELECTRONIC FILES

1.1. Electronic files created, sent, received, and/or stored on information resources owned, leased, administered, or otherwise under the custody and control of the University are the property of the University.

2. PRIVACY

2.1. Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the University are not private and may be accessed by authorized University employees or processes as needed for data administration or information security purposes, without prior consent or knowledge of the information resources user or owner. This access for employees is in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

3. PROCESS

3.1. Users must report any weaknesses in the University’s computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting their departmental supervisor, University ISO or appropriate Information Technology Services management.

3.2. Users must not attempt to access any resource, data or programs contained on the University’s systems for which they do not have authorization or explicit consent.

3.3. Users must not share their University account(s), password(s), personal identification numbers (PIN), security tokens, or similar information or devices used for identification and authentication purposes.

3.4. Users must not make unauthorized copies of copyrighted software.

3.5. Users must not install and/or use non-standard software without the University Information Technology Services (ITS) management approval unless the software is adopted as a standard, is communicated by Information Technology Services (ITS) as allowable, or is necessary to conduct activities required to perform work related responsibilities.

3.6. Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of information resources; deprive an authorized user access to a University resource; obtain extra resources beyond those allocated; circumvent University computer security measures.

3.7. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system; for example: password
cracking programs, packet sniffers, port scanners or any other non-approved program on University information resources.

3.8. The University information resources must not be used for personal benefit/gain.

3.9. Users must not intentionally access, create, store or transmit material which could be deemed to be offensive, indecent or obscene (other than in the course of academic and/or research activities have the explicit approval of the University through the Office of the Provost).

3.10. Use of a University owned computer outside of the University network must adhere to all the same policies that apply to use from within the University facilities. Employees must not allow family members or other non-employees to access the University computer systems.

4. INCIDENTAL USE

4.1. The University allows for incidental personal use of information resources. User abuse of this privilege may result in the removal of these rights or other disciplinary action. The following restrictions apply to incidental personal use of information resources:

4.1.1. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to approved users; it does not extend to family members or other acquaintances.

4.1.2. Incidental use must not result in direct costs to the University.

4.1.3. Incidental use must not interfere with the normal performance of an employee’s work duties.

4.1.4. No files or documents may be sent or received that may cause legal action against, or embarrassment to the University.

4.1.5. Storage of personal email messages, voice messages, files and documents within the University’s information resources must be nominal.

4.1.6. All messages, files and documents - including personal messages, files and documents - located on the University information resources are owned by the University and may be subject to open records requests in accordance with this Procedure.

5. DISCIPLINARY ACTIONS.

5.1. 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.
6. SUPPORT INFORMATION

6.1. All University employees and other users of campus owned information resources are responsible for managing their use of information resources and their actions relating to information resources security. University employees are responsible for reporting any suspected or confirmed violations of this Procedure to the appropriate information resource owner, departmental supervisor and to the University ISO.

6.2. The use of information resources is intended for officially authorized business purposes. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of information resource utilization, the establishment of effective use, and reporting of non-compliance to management.

6.3. Any data used in an information resource must be protected and properly secured. The fact that the data may be stored electronically does not change the requirement to keep the information protected and properly secured. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted, the data must still be protected and properly secured.

6.4. All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.

6.5. Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized, and controlled.

6.6. All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. University employees and other users of campus owned information resources must abide by all license agreements and must not illegally copy licenses software. The IRM reserves the right to remove any unlicensed software from any computer systems.

6.7. The IRM reserves the right to remove any non-business related or unauthorized software or files from any computer system or network service. Examples of non-business related software or files include, but are not limited to; games, instant messengers, POP email, IMAP email, music files, image files, freeware, shareware, or other resource such as Software as a Service (SaaS) systems that reside in the cloud (such services may be blocked at the firewall to prevent data leakage).
Related Statutes, Policies, or Requirements

TAMU-SA Procedure 29.01.03.O0.01 Electronic Information Services Access and Security

Definitions

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).

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

Information Resource Owner – an entity responsible for:
- A business function; and,
- Determining controls and access to information resources supporting that business function.

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.

Information Resources Manager (IRM) – The IRM ensures that all information resources are acquired appropriately, implemented effectively, and complies with regulations and agency policies. Per requirements of the State of Texas, each agency or institution of higher education must designate an IRM.

Contact Office

Information Technology Services – (210) 784-4357