Texas A&M University System Standard – Internet/Intranet Use

Standard Statement

This standard provides procedures to ensure awareness and compliance with applicable statutes, regulations, and mandates regarding the appropriate management and responsible use of information resources.

Definitions

Confidential Information - information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act. Refer to the Data Classification Standard under Regulation 29.01.03 for additional information.

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 Resource Owner - an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Responsibilities and Standards

1. GENERAL

   SO information resources are strategic assets of the State of Texas and thus must be managed as valuable state resources. This procedure is established to achieve the following:

   1.1 To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

   1.2 To establish acceptable practices regarding the use of information resources; and,

   1.3 To educate individuals who may use information resources with respect to their responsibilities associated with such use.

2. APPLICABILITY

This Standard (standard) applies to all SO information resources.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The intended audience is all users of SO information resources.

3. STANDARDS

3.1 Standards regarding the protection of information resources against malicious codes; web site standards; purchases over the internet; and, personal conduct can be found in the following policies and standards:

- *Responsible Computing*
- *Incidental Computer Use*
- *Incident Management*
- *Malicious Code*

3.2 No confidential information shall be made available via SO Web sites without ensuring that the material is accessible to only authorized individuals or groups.

3.2.1 All confidential information transmitted over external networks must be encrypted. See the Data Classification Standard under Regulation 29.01.03 Information Security.

3.2.2 Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

3.3 Directors or their equivalent have the responsibility to ensure that appropriate security practices for SO internet/intranet use are implemented in their respective departments.

Contact Office

Contact The Texas A&M University System Chief Information Officer for standard interpretation or clarification.

OFFICE OF RESPONSIBILITY**:** The Texas A&M University System Chief Information Officer