STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.10 Information Resources – Internet and Intranet Use
Approved July 18, 2005
Revised February 24, 2009
Revised March 8, 2013
Revised August 14, 2013
Next scheduled review: August 14, 2018

Standard Administrative Procedure Statement

This Standard Administrative Procedure (SAP) provides procedures to ensure awareness and compliance with applicable statutes, regulations, and mandates regarding the appropriate management and responsible use of information resources.

Definitions

Business Function – a process or operation that is performed routinely to carry out a part of the mission of an organization.

Confidential - information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

Examples of “Confidential” data may include, but are not limited to:

- personally identifiable information, such as a Social Security number (SSN) and/or financial account number;
- student education records;
- intellectual property such as certain intellectual property as set forth in Texas Education Code Section 51.914; or,
- medical records

Information Resources (IR) - the procedures, computer equipment, computing facilities, software and data which are purchased, designed, built, operated and maintained to collect, record, process, store, retrieve, display, report and transmit information.

Owner of an Information Resource – a person responsible for a business function and for determining controls and access to information resources supporting that business function.

Responsibilities and Procedures
1. GENERAL

Texas A&M University (Texas A&M) supports and encourages internet and intranet use for the benefits that such use provides to all users of information resources. University 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 Administrative Procedure (SAP) applies to all Texas A&M information resources.

The intended audience is all users of university information resources.

3. PROCEDURES

3.1. Procedures regarding the protection of information resources against malicious codes; applying web site standards; purchasing over the internet; and, about personal conduct can be found in the following policies and procedures:

- University SAP 25.07.03.M2.01, Purchasing Procedures
- University Rule 29.01.03.M2, Rules for Responsible Computing
- University Rule 29.01.99.M3, Incidental Computer Use
- University SAP 29.01.04.M1.01, Web Accessibility and Usability
- University SAP 29.01.03.M1.09, Incident Management
- University SAP 29.01.03.M1.23, Malicious Code

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

3.3. All confidential or sensitive information transmitted over the Internet must be encrypted.
3.4. Unit Heads, or their equivalent, have the responsibility to ensure that appropriate security practices for university internet and intranet use are implemented in their respective departments.

3.5 All user activity on university information resources assets is subject to logging and review.

3.6 Confidential or sensitive data that is transmitted in an email message must be encrypted. (See SAP 29.01.03.M1.31 Encryption of Confidential and Sensitive Information.)

4. EXCLUSIONS

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this SAP 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 SAP. All exclusions must be in accordance with SAP 29.01.03.M1.27 Exclusions from Required Risk Mitigation Measures.

Related Statutes, Policies, or Requirements

Texas Education Code, Title 3, Chapter 51, Provisions Generally Applicable to Higher Education

University SAP 25.07.03.M2.01, Purchasing Procedures

University SAP 29.01.04.M1.01, Web Accessibility and Usability Procedures

University Rule 29.01.03.M1, Security of Electronic Information Resources

University SAP 29.01.03.M1.02, Acceptable Use

University SAP 29.01.03.M1.09, Incident Management

University SAP 29.01.03.M1.23, Malicious Code

University SAP 29.01.03.M1.27, Exclusions from Required Risk Mitigation Measures

University SAP 29.01.03.M1.31, Encryption of Confidential and Sensitive Information

University Rule 29.01.03.M2, Rules for Responsible Computing

University Rule 29.01.99.M3, Incidental Computer Use
Contact Office

CONTACT: Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY: Associate Vice President for Information Technology & Chief Information Officer