STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.02 Information Resources – Acceptable Use

Approved July 18, 2005
Revised April 27, 2010
Revised August 14, 2013
Next scheduled review: August 14, 2018

Standard Administrative 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. Texas A&M University has developed other rules and procedures that address acceptable use of information resources.

Reason for SAP

The purpose of this SAP is to identify those relevant policies and procedures that pertain to aspects of acceptable use.

Definitions

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.

Official Procedure/ Responsibilities/ Process

1. APPLICABILITY

   This Standard Administrative Procedure (SAP) applies to all University information resources.

   The purpose of the implementation of this SAP 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 will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

The information resource owner or designee (e.g., custodian, user), 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*.

The intended audience for this standard administrative procedure includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

2. PROCEDURES

2.1 The procedures determining acceptable use of University information resources are addressed in the following System Policies/Regulations and University Rules/SAPs:

System Policy *07.01 Ethics Policy, TAMUS Employees*;
System Policy *10.02, Control of Fraud, Waste and Abuse*;
System Policy *33.04, Use of System Resources*;
System Regulation *29.01.02, Use of Licensed Commercial Software*;
University Rule *29.01.03.M2, Rules for Responsible Computing*;
University Rule *29.01.03.M3, Incidental Computer Use*;
University SAP *29.01.03.M1.12, Network Access*;
University SAP *29.01.03.M1.14, Password/Authentication*;
University SAP *29.01.03.M1.17, Privacy*;
Texas A&M Information Security Control CM-11 *User Installed Software;*
Texas A&M Information Security Control IR-6 *Incident Reporting*;
Texas A&M Information Security Control SC-8 *Transmission Confidentiality and Integrity*;
Texas A&M Information Security Control SI-4 *Information System Monitoring*; and
Texas A&M Information Security Control SI-3 *Malicious Code Protection*

Related Statutes, Policies, or Requirements

Supplements University SAP *29.01.03.M0.01, Security of Electronic Information Resources*

Contact Office

CONTACT: Office of the Chief Information Security Officer.

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