Texas A&M University System Standard - Acceptable Use

Standard 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. The System Offices (SO) has developed other rules and procedures that address acceptable use of information resources.

Reason for Standard

The purpose of this standard 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 Rule/ Responsibilities/ Process

1.   APPLICABILITY

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

      The purpose of the implementation of this standard is to provide a set of measures that will mitigate information security risks associated with acceptable use of SO 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 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 for this standard administrative procedure includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of SO information resources.

2.   STANDARDS

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

System Policy 07.01 Ethics Policy, TAMUS Employees;
System Policy 21.04, Control of Fraud, Waste and Abuse;
System Policy 33.04, Use of System Resources;
System Regulation 29.01.02, Use of Licensed Commercial Software;
SO Standard Rules for Responsible Computing;
SO Standard Incidental Computer Use;
SO Standard Authorized Software;
SO Standard Incident Management;
SO Standard Internet/Intranet Use;
SO Standard Network Access;
SO Standard Password/Authentication;
SO Standard for Privacy;
SO Standard for Security Monitoring; and
SO Standard for Malicious Code.

For interpretation or clarification, contact the Texas A&M University System Chief Information Officer.

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