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.

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

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.

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 29.01.99.S1.27
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 SO information resources.

2. PROCEDURES

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

- **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 Rule 29.01.99.S2, Rules for Responsible Computing;
- SO Rule 29.01.99.S3, Incidental Computer Use;
- SO SAP 29.01.99.S1.05, Authorized Software;
- SO SAP 29.01.99.S1.09, Incident Management;
- SO SAP 29.01.99.S1.10, Internet/Intranet Use;
- SO SAP 29.01.99.S1.12, Network Access;
- SO SAP 29.01.99.S1.14, Password/Authentication;
- SO SAP 29.01.99.S1.17, Privacy;
- SO SAP 29.01.99.S1.18, Security Monitoring; and
- SO SAP 29.01.99.S1.23, Malicious Code.

---

**Related Statutes, Policies, or Requirements**

**Supplements**  
**SO Rule 29.01.99.S1**

**Contact Office**

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