

## STANDARD ADMINISTRATIVE PROCEDURE

### **29.01.99.M1.02 Information Resources – Acceptable Use**

*Approved July 18, 2005*

*Next scheduled review: Currently under review*

*Supplements [University Rule 29.01.99.M1](#)*

#### 1. GENERAL

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. TAMU 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.

#### 2. 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. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual ISAAC report (See [University Rule 29.01.99.M1](#)).

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.

#### 3. DEFINITIONS

3.1 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.

#### 4. PROCEDURES

- 4.1 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 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](#);  
[University Rule 29.01.99.M2, Rules for Responsible Computing](#);  
[University Rule 29.01.99.M3, Incidental Computer Use](#);  
[University SAP 29.01.99.M1.05, Authorized Software](#);  
[University SAP 29.01.99.M1.09, Incident Management](#);  
[University SAP 29.01.99.M1.10, Internet/Intranet Use](#);  
[University SAP 29.01.99.M1.12, Network Access](#);  
[University SAP 29.01.99.M1.14, Password/Authentication](#);  
[University SAP 29.01.99.M1.17, Privacy](#);  
[University SAP 29.01.99.M1.18, Security Monitoring](#); and  
[University SAP 29.01.99.M1.23, Malicious Code](#).

CONTACT: [Information Technology Issues Management of CIS](#)

OFFICE OF RESPONSIBILITY: [Vice President and Associate Provost for Information Technology](#)