STANDARD ADMINISTRATIVE PROCEDURE

29.01.99. S1.26 Information Resources – Information Security Risk Assessment Reviews

Approved

Next scheduled review:

Standard Administrative Procedure Statement

The purpose of this Standard Administrative Procedure (SAP) is to implement a monitoring process which adequately provides management with assurance that the information on which risk assessment assertions are made is correct. The goal of these procedures is to assist the System Office (SO) with improving the effectiveness of its use of the ISAAC system and the value and accuracy of their information security risk assessments.

Reason

Information security risk assessments are vital procedures for maintaining the security of information resources and meeting legal requirements for protecting confidential information. The purpose and goal of these assessments can only be achieved if the assessments are conducted effectively.

Definitions

Information Security Assessment Awareness and Compliance (ISAAC) - the ISAAC system provides an information security risk assessment methodology and reporting function for TAMU, SO and other TAMUS institutions. (See SO Rule 29.01.99.S1 Security of Electronic Information Resources).

SO ISO – the System Office Information Security Officer

Procedure

1. GENERAL

This Standard Administrative Procedure (SAP) applies to all information security risk assessments that are conducted for SO information resources during the annual ISAAC
assessment process.

The intended audience includes all SO personnel involved in performing, approving, or making risk management decisions related to information security risk assessments.

2. **PROCEDURES**

2.1 After completion of the annual ISAAC assessment process (see Rule 29.01.99.S1 Security of Electronic Information Resources), all assessment reports will be reviewed by SO ISO (i.e., the “primary review”). Based on the primary review, some assessments will be selected for additional review (i.e., a “secondary review”). The selection of assessments for secondary review and the order of these reviews will be predicated on areas of inherent risk (e.g., confidential information, mission critical systems, and/or problematic conditions) or at the direction of the Texas A&M University System Chief Information Officer (or designee).

2.2 The specific process followed for each review will be designed with effectiveness and efficiency as primary goals. Where beneficial and feasible, these reviews may utilize automated software tools to provide confirmation and/or information regarding the configuration and classification (e.g., contains confidential and/or mission critical data) of the information resources.

2.3 The review process shall include where appropriate: notification, information gathering, analysis, and reporting.

3. **GUIDELINES**

Detailed guidelines can be found at the ISAAC website.

---

**Related Statutes, Policies, or Requirements**

SO Rule 29.01.99.S1 Security of Electronic Information Resources

**Contact Office**

Contact  The Texas A&M University System Chief Information Officer for procedural interpretation or clarification

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