STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.27 Exclusions from Required Risk Mitigation Measures

Approved January 7, 2009
Revised April 17, 2012
Revised August 14, 2013
Next Scheduled Review: August 14, 2018

Standard Administrative Procedure Statement

All owners and custodians of information technology resources are expected to adopt and adhere to Texas A&M University information resource rules and Standard Administrative Procedures (SAP). However, there may be situations where strict adherence to a University information resource rule or SAP would significantly impair the conduct of business and presents a low risk. The purpose of this SAP is to provide a process that documents an information resource owner's application of a requested exclusion to an information technology rules or SAP.

Definitions

Information Resource Owner – A person responsible for:

- a business function, and
- determining controls and access to information resources supporting that business function.

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.

Responsibilities and Procedures

---

1. GENERAL

   Rules and Standard Administrative Procedures (SAP) relating to the security of information resources provide measures that mitigate risks to those resources. However, there may be other, or additional, measures that will also appropriately mitigate 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.

Texas Administrative Code 202 – Information Security Standards recognizes the potential need for flexibility and discretion in the application of risk mitigation measures. The information resource owner may determine that the implementation of some or all of the risk mitigation measures provided in a rule or SAP are not essential for an information resource and/or environment. Risk assessment and business functions provide the criteria for making such risk management decisions.

The purpose of this SAP is to provide a process that facilitates an information resource owner's appropriate application of exclusions to the provisions of a SAP and preserves the overall integrity and consistency of the University's security posture.

2. APPLICABILITY

This SAP applies to all information resource owners, their designees and standard administrative procedures related to the security of information resources.

3. PROCEDURES

3.1. Exclusions are of two types:

3.1.1 A system specific exclusion may be granted to address the circumstances or business needs relating to an individual program or department. Requests for exclusions of this type are to be initiated by the information resource owner or their designee.

3.1.2 An enterprise-wide exclusion may be issued to address circumstances that affect the University as a whole. Requests for exclusions of this type may be initiated by any person, office or department, or by the Associate Vice President for Information Technology & Chief Information Officer or designee. Exclusions of this type will be documented by referencing the rule or SAP to which the exclusion should apply.

3.2 Exclusions requested by the information resource owner must be submitted through the exclusion request form found at the Texas A&M IT, http://cio.tamu.edu/Risk_Management_Policy/Risk_Management_and_Compliance/Risk_Management/Exclusion_Request.php. The request must include the following:

3.2.1 The provision for which the exclusion is sought.

3.2.2 A statement defining the nature and scope of the exclusion in terms of the data included and/or the class of devices included.

3.2.3 Risk management rationale for the exclusion.

3.3 Each request will be reviewed by the Associate Vice President for Information

Technology & Chief Information Officer or designee. After any questions or concerns are addressed, the requestor will be notified as to whether the request was approved or denied. A record of all requests and results will be maintained by the Office of the Associate Vice President for Information Technology & Chief Information Officer or designee.

3.4 If the request is denied, a rationale for the denial will be supplied to the requestor.

3.5 If the request is approved:

3.5.1 The information resource owner may be required to apply compensating security controls to mitigate any risk resulting from the exclusion.

3.5.2 An expiration date for the exclusion will be supplied to the requestor.

3.5.3 Exclusions will be documented in ISAAC by the information resource owner or their designee.

Related Statutes, Policies, or Requirements

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: Associate Vice President for Information Technology & Chief Information Officer