Texas A&M University System Standard - Exclusions from Required Risk Mitigation Measures

Standard Statement

The purpose of this standard is to provide a process that facilitates a resource owner's appropriate application of exclusions to the provisions of information technology standards and preserves the overall integrity and consistency of the state of System Office security.

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 Standards

1. GENERAL

   This standard is primarily related to the security of information resources provide measures that mitigate risks to those resources. There may also be other or additional measures that will provide appropriate mitigation. 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 resource owner may determine that the implementation of some or all of the risk mitigation measures provided in a standard is 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 standard is to provide a process that facilitates a resource owner's appropriate application of exclusions to the provisions of a standard and preserves the overall integrity and consistency of the System Office's security posture.

2. APPLICABILITY

This standard applies to all resource owners, their designees and standards related to the security of information technology resources.

3. STANDARDS

3.1. Exclusions are of two types:

3.1.1 An exclusion may be granted to address the specific 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 Broader exclusions may be issued to address circumstances that span the System Office and related systems as a whole. Requests for exclusions of this type may come from any person, or may be initiated by the Texas A&M University System Chief Information Officer or designee. Exclusions of this type will be documented in each standard to which the exclusion applies.

3.2 Exclusions requested by the information resource owner must be submitted through the exclusion request. The request must contain the following:

3.2.1 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 Texas A&M University System 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 Texas A&M University System 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 The request for the exclusion will be fully documented in the risk management system in the form of a risk management decision by the information resource owner or their designee.

Contact Office

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

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