29.01.99.K1.005 Administration of Information Resource Security Standards

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: April 2019
Next Scheduled Review: April 2024

Introduction

The Texas A&M University-Kingsville (TAMUK) Information Resource Security Standards provide the operational detail required for the successful implementation of an information security program. These standards are based on Security Policy Standards published by the Texas Department of Information Resources (DIR), Texas A&M University System (TAMUS) and the National Institute of Standards and Technology (NIST). In addition these standards have been developed in accordance with TAC 202, PCI, Higher Education Opportunity Act (HEOA) and other legislation and legal requirements, current and future business and academic needs, technical implementation feasibility and consideration of the campus environment. All owners and custodians of information technology resources are expected to adopt and adhere to TAMUS and TAMUK information resource rules, procedures and standards.

Purpose

The purpose of this standard is to establish rules that govern the establishment, review, modification, implementation and dissemination of the various security procedures, standards and to provide a mechanism for requesting and granting exceptions to these procedures and standards while preserving the overall integrity and consistency of the University's security posture.

Audience

This standard applies to those administrators developing, reviewing, or revising security procedures and standards, and to those requesting exceptions to existing procedures and standards.

Standard

1. Updates to the TAMUK information resource procedures and standards, including establishing new, modifying existing, or removing procedures or standards:
   a. Periodically, senior iTech staff will review the procedures and standards for possible addition, revision, or deletion.
      i. This review must be completed by review date according to the SAP heading.
   b. The CIO will submit to the University Technology Advisory Committee (UTAC) any new procedures or standards, modifications to existing procedures or standards or removal of existing procedures or standards.
      i. UTAC will make recommendations to the CIO of submitted procedures and standards.
      ii. After changes have been made to meet UTAC's concerns, UTAC will approve procedures and standards.
   c. The CIO will consult with TAMU System CIO and CISO on UTAC-approved procedures and standards.
2. Communication
   a. Subsequent to approval of modifications to information resource procedures or standards, the following steps will be taken as appropriate to properly document and communicate the modification:
      i. iTech will post the approved procedure or standard on JNet and on the iTech webpage.
      ii. A communication plan will be developed.
3. Exceptions
   a. An information resource specific exception may be requested to address the circumstances or business and academic needs relating to an individual program or department. Requests for an exception are to be initiated by the information resource owner.
      i. An exception requested by the information resource owner must be submitted through the exception request form. The request must include the following:
         1. The rule or SAP for which the exception is sought.
         2. A statement defining the nature and scope of the exception and the business or academic justification for the exception request.
         3. Description of any compensating controls implemented to mitigate risk.
   b. The assessment of risk and the application of appropriate mitigation measures are to be determined by the Information Security Officer (ISO) in consultation with the Information Resource Manager (IRM).
      i. The ISO and technical staff will determine if there is a solution to the request that does not require an exception.
   c. The CIO will take the exception request and the ISO's recommendation to the University Technology Advisory Council (UTAC) for discussion and recommendation.
   d. Using the assessment of risk and mitigation measures and the recommendation of UTAC, the CIO will approve or deny the exception request.
      i. If the request is approved:

        1. The information resource owner may be required to apply compensating security controls to mitigate any risk resulting from the exception.
        2. An expiration date for the exception will be supplied to the requestor.
        3. Exceptions will be documented by the ISO.
    - ii. If the request is denied, a rationale for the denial will be supplied to the requestor.
- e. Each exception must be re-examined annually to determine its continuing need and potential risk.
- f. Exceptions to TAMUS policies or regulations must follow the aforementioned standard as well as the following procedure.
    - i. If the exception request is approved by the CIO, the exception will be forwarded to the President for TAMUK review.
        1. If approved, the President will submit the exception to the Chancellor.
        2. If the exception request is denied, the President will return the request to the CIO and to the requester.
    - ii. On an annual basis, exceptions to TAMUS policy or regulation must be reported to the SCISO.

Disciplinary Actions

Violation of this standard may result in disciplinary action which may include termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References

1. Computer Fraud and Abuse Act of 1986
2. Computer Security Act of 1987
3. DIR Practices for Protecting Information Resources Assets
4. DIR Standards Review and Recommendations Publications
5. IRM Act, 2054.075(b)
6. The State of Texas Penal Code, Chapters 33 and 33A
7. Texas Administrative Code, Chapter 202
8. Texas A&M University-System Procedure 29.01.03
9. Texas Administrative Code 206.70a Accessibility
10. Texas Administrative Code 205.50
11. Texas Administrative Code 213.37 Compliance Exceptions and Exemptions
12. Texas Administrative Code 213.17 Compliance Exceptions and Exemptions

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404