Standard Administrative Procedures Administration Procedure

Introduction
The Texas A&M University-Kingsville (TAMUK) Information Resource Security Standard Administrative Procedures provide the operational detail required for the successful implementation of an information security program. These procedures are based on Security Policy Standards published by the Texas Department of Information Resources (DIR) and the National Institute of Standards and Technology (NIST). In addition these procedures have been developed in accordance with HIPAA, TAC 202, PCI, SOX, GLB, HEOA and other legislation and legal requirements, current and future business needs, technical implementation feasibility, and the campus environment.

Purpose
The purpose of this procedure is to establish rules that govern the drafting, review, modification, and dissemination of the various security procedures, and to provide a mechanism for granting exceptions to these procedures.

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

Ownership of Information Resource Standard Administrative Procedures
TAMUK Information Resource Standard Administrative Procedures are owned by the TAMUK Information Resources Manager (IRM). The IRM, or designee, is the only authority that can approve modifications or exceptions to the security procedures. The Compliance Officer will be notified of all new or changes to existing procedures.

Applicability
The information resource procedures are developed to apply to all aspects of TAMUK information resources technology. New technologies, legislation, and administrative law may impact the information resource procedures over time thereby necessitating a periodic review of the various information resource procedures.

Information Resource Standard Administrative Procedure Changes
1. Updates to the TAMUK information resource procedures, including establishing new procedures, modifying existing procedures, or removing procedures:
   a. At least biennially, senior iTech staff will review the procedures for possible additions, revisions, or deletion.
   b. New technology may result in changes to existing procedures or creation of new procedures.
   c. Removal or obsoleteness of information resources may necessitate the retiring of procedures.
   d. Legislative or business requirements may result in creation of new procedures or changes to existing procedures.
2. Change Distribution and Notification
Information Resource Security Standard Administrative Procedures

29.01.99.K1.005

Standard Administrative Procedures Administration

04/01/2004 - Effective
04/23/2013 - Revised
iTech - Author

a. Subsequent to approval of modifications to information resource procedures, the following steps will be taken as appropriate to properly document and communicate the modification:
   • The appropriate web page(s) will be updated with the change.
   • Training and other related materials will be updated to reflect the change.
   • The changes will be communicated using standard communication methods.
   • Handbooks should reference online publications of information resource procedures.

3. Exceptions
   a. The TAMUK information security procedures provide the techniques and methodology to protect University Information Resources.
   b. A request for an exception is received by the Information Security Officer (ISO) along with a business case justifying the exception.
   c. The ISO analyzes the request and justification and determines if the exception request should be accepted, denied, or needs more investigation.
   d. If more investigation is required, the ISO and technical staff determine if there is a solution to the request that does not require an exception.
   e. If there is no alternative solution, and the induced risk is minimal, the exception may be recommended to the IRM.
   f. Each exception must be re-examined periodically to determine its continuing need and potential induced risk.

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

References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441