Policy Administration Procedures

Introduction
The Texas A&M University-Kingsville Information Security Policies provide the operational detail required for the successful implementation of an Information Security program. These policies were developed from and 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 policies have been developed by interpreting HIPAA, 1 TAC 202, PCI, SOX, GLB and other legislation and legal requirements, current and future business needs, technical implementation feasibility, and the campus environment.

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

2. Audience
The Texas A&M University-Kingsville Policy Administration procedures apply to those administrators developing, reviewing, or revising security policies, and to those requesting exceptions to existing policies.

3. Ownership of Security Policies
The Texas A&M University-Kingsville Security Policies are owned by the Texas A&M University-Kingsville Information Resources Manager (IRM). The IRM, or designee, is the only authority that can approve modifications or exceptions to the security policies.

4. Reasons for Change
The security policies were initially developed to the technology neutral, and apply to all aspects of Texas A&M University-Kingsville information resources technology. New technologies, legislation, and administrative law may impact the security policies over time thereby necessitating a periodic review of the various security policies.

5. Security Policy Change Process
Updates to the Texas A&M University-Kingsville security policies, including establishing new policies, modifying existing policies, or removing policies can result from three different processes:

   5.1. At least bi-annually, the Information Security Offices (ISO), or designate, will review the policies for possible additions, revisions, or deletion.
   5.2. When new Information Resources are introduced to Texas A&M University-Kingsville, a security and risk assessment must be performed. The result of this assessment could necessitate changes in the security policies before the new resources are made available for use.
   5.3. Any Texas A&M University-Kingsville information resources user may propose the establishment, revision or deletion of any security policy. The proposals should be directed to the ISO who will evaluate the proposal and make appropriate recommendations to the IRM.

6. Change Distribution and Notification
Subsequent to modifications in the security policies having been approved by the IRM, the following steps will be taken as appropriate to properly document and communicate the modification:

   6.1. The appropriate security web page(s) will be updated with the change
   6.2. Training and other related materials will be updated to reflect the change
   6.3. The changes will be communicated using standard TAMUK communication methods such as E-mail announcements, updated web home page(s), and staff meetings
   6.4. Changes will be communicated to Students and Faculty through the campus wide email system.
7. **Exceptions**
The Texas A&M University-Kingsville security policies provide the techniques and methodology to protect University IR assets. While these policies are technology independent, they remain likely to be impacted by changing technology, legislation, and business requirements.

An exception is the method used to document approved variations from the rules. Examples are:

7.1. Allowing a desktop modem when the policy prohibits modems on networked computers.
7.2. Allowing multiple system administrative users in an academic or training environment.

8. **Exception Process**
The steps for permitting and documenting an exception are:

8.1. A request for an exception is received by the ISO along with a business case justifying the exception
8.2. The ISO analyzes the request and justification and determines if the exception request should be accepted, denied, or needs more investigation
8.3. If more investigation is required, the ISO and IR technical staff determines if there is a solution to the request that does not require an exception.
8.4. If there is no alternative solution, and the induced risk is minimal, the exception may be favorably recommended to the IRM.
8.5. Each exception must be re-examined periodically to determine its continuing need and potential induced risk. This review period must be no longer than 12 months, and may be substantially less depending on the nature of the exception.

9. **Disciplinary Actions**
Violation of this policy 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 Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.