Administrative Access Policy

Introduction
Technical support staff, security and system administrators may have special access account privilege requirements compared to typical users. The fact that these administrative accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

1. Purpose
The purpose of the Texas A&M University-Kingsville Administrative Access Policy is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privileges.

2. Audience
The Texas A&M University-Kingsville Administrative Access Policy applies to all individuals that have, or may require, special access privileges to any Texas A&M University-Kingsville Information Resources.

3. Administrative Access Policy
3.1. Departments must submit to iTech a list of administrative contacts for their systems that are connected to the Texas A&M University-Kingsville network.
3.2. Departments must request administrative rights.
3.3. All users of administrative access accounts must have account management instructions, documentation, training and authorization.
3.4. Individuals with administrative rights must refrain from abusing those privileges. Investigations of abuse are conducted under the direction of the Information Security Officer.
3.5. Each individual that uses administrative access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
3.6. Each account used for administrative access must meet the Texas A&M University-Kingsville Password Policy.
3.7. The password for a shared administrative access account must change when an individual with the password leaves the department or Texas A&M University-Kingsville, or upon a change in the vendor personnel assigned to the contract.
3.8. In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the system in an emergency situation.
3.9. When administrative accounts are needed for software installation or other defined need, they:
   3.9.1. Must be authorized by department director or higher.
   3.9.2. Must be created with a specific expiration date.
3.10. Supervisors are required to report violations of this policy to the Information Security Officer.

4. Disciplinary Actions
Violation of this policy may result in disciplinary action up to and including 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.