Administrative/Special Access Policy

Introduction
Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access 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/Special Access Policy is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.

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

3. Administrative/Special Access Policy
3.1. TAMUK departments must submit to CIS a list of administrative contacts for their systems that are connected to the Texas A&M University-Kingsville network.
3.2. All users of Administrative/Special access accounts must have account management instructions, documentation, training and authorization.
3.3. Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the directions of the Information Security Officer.
3.4. Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
3.5. Each account used for Administrative/Special access must meet the Texas A&M University-Kingsville Password Policy.
3.6. The password for a shared Administrative/Special 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.
3.7. 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.
3.8. When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
   3.8.1. Must be authorized by department director or higher.
   3.8.2. Must be created with a specific expiration date.
   3.8.3. Must be removed when work is completed.
3.9. Supervisors are required to report violations of this policy to the CIO.

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.