Introduction
Computer accounts are the means used to grant access to Texas A&M University-Kingsville Information Resources. These accounts provide accountability for Information Resources usage, an important key to information security.

1. Purpose
The purpose of the Texas A&M University-Kingsville Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

2. Audience
The Texas A&M University-Kingsville Account Management Security Policy applies equally to all individuals with authorized access to any Texas A&M University-Kingsville Information Resources

3. Account Management Policy
3.1. All accounts must be uniquely identifiable using the assigned user name.
3.2. All default passwords for accounts must be constructed in accordance with the Texas A&M University-Kingsville Password Policy.
3.3. All accounts must have a password expiration that complies with the Texas A&M University-Kingsville Password Policy.
3.4. Account holders are required to keep user accounts confidential and must not share their Texas A&M University-Kingsville account(s), or passwords.
3.5. Guest Accounts:
   3.5.1. are required for all individuals who are not students, faculty, or staff of Texas A&M University-Kingsville.
   3.5.2. must have a request and approval that is appropriate for the system or service needed.
   3.5.3. have a maximum lifetime of 180 days.
   3.5.4. are subject to the Acceptable Use Policy, and Information Resource Security Policies.
3.6. System Administrators:
   3.6.1. must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
   3.6.2. must have a documented process for periodically reviewing existing accounts for validity
   3.6.3. are subject to independent audit review
   3.6.4. must provide a list of accounts for the systems they administer when requested by authorized Texas A&M University-Kingsville management
   3.6.5. must cooperate with investigations of security incidents.
   3.6.6. are responsible for removing the accounts of individuals that change roles within Texas A&M University-Kingsville or are separated from their relationship with Texas A&M University-Kingsville.
3.7. Account termination:
   3.7.1. Guest user accounts will be disabled upon expiration.
   3.7.2. Employee accounts will be disabled on their last day of service.
      3.7.2.1. Exceptions may be granted upon request from VP, Dean, or Division Head.
   3.7.2.2. Emeritus faculty are exempt from this provision.
   3.7.3. Student accounts will be disabled upon withdrawal from the university
   3.7.4. Student accounts will be disabled one long semester after graduation

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.