Account Management Procedure

Introduction

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

Purpose

The purpose of this procedure is to establish the rules for the creation, monitoring, control and removal of user accounts.

Audience

This procedure applies to individuals with authorized access to any TAMUK Information Resources.

Account Management Procedure

1. All accounts must be uniquely identifiable using the assigned user name.
2. All default passwords for accounts must be constructed in accordance with the TAMUK Password Procedure.
3. All accounts must have a password expiration that complies with the TAMUK Procedure.
4. Account holders are required to keep user accounts confidential and must not share their TAMUK account(s), or passwords.
5. Guest Accounts:
   a. are required for all individuals who are not students, faculty, or staff of TAMUK.
   b. must have a request and approval that is appropriate for the system or service needed.
   c. have a maximum lifetime of 180 days.
   d. are subject to the Acceptable Use Procedure, and Information Resource Security Procedures.
6. System Administrators:
   a. must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
   b. must have a documented process for periodically reviewing existing accounts for validity
   c. are subject to independent audit review
   d. must provide a list of accounts for the systems they administer when requested by authorized TAMUK management
   e. must cooperate with investigations of security incidents.
   f. are responsible for removing the accounts of individuals that change roles within TAMUK or are separated from their relationship with TAMUK.
7. Account termination:
   a. Guest user accounts will be disabled upon expiration.
   b. Employee accounts will be disabled on their last day of service.
      1) Exceptions may be granted upon request from Vice President, Dean, or Division Head.
      2) Emeritus faculty are exempt from this provision.
   c. Student accounts will be disabled upon withdrawal from the university
d. Student accounts will be disabled one long semester after graduation

Disciplinary Actions
Violation of this procedure 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 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