

29.01.99.K1.020

Account Management Standard Administrative Procedure



Effective: April 1, 2004
Revised: October 23, 2012
Revised: October 8, 2019
Next Scheduled Review: October 8, 2024

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 user accounts must be uniquely identifiable using the assigned user name.
 - a. Service accounts are for system-to-system interaction and may not be used for individuals.
 - b. Linux root accounts and Windows administrator accounts must only be used for system administrative processes.
2. All passwords for accounts must be constructed in accordance with the TAMUK Password Procedure 29.01.99.K1.120.
 - a. All accounts must have a password expiration that complies with the TAMUK Procedure.

3. Account holders are required to keep user accounts confidential and must not share their TAMUK account(s), or passwords.
4. Student email and Active Directory accounts are created upon admittance.
5. Affiliated Accounts are required for individuals who need access to TAMUK information resources on an ongoing basis and are not students, faculty, or staff of TAMUK in accordance with the Third Party Access Procedure 29.01.99.K1.210.
 - a. Affiliated Accounts will have a TAMUK email address and may have Banner access.
 - b. Expiration is set to one year. Reactivation requires sponsor approval and completion of required TrainTraq courses.
6. Guest Accounts are temporary accounts requested by departments. The requestor is responsible for maintaining a list of persons using a particular account. Guest accounts do not have TAMUK email accounts or Banner access.
 - a. The requestor must indicate a start and end date for the guest accounts.
 - i. The end date cannot be greater than 180 days from the start date.
7. Library patron accounts are offered to provide access to TAMUK computers and wireless and do not have TAMUK email accounts. Library patron accounts have an expiration date of one year after activation and will be deleted 30 days after expiration.
 - a. Library patron accounts have accounts on Blackboard Transact.
8. Pharmacy accounts are in AD and in systems such as Blackboard Transact, Blackboard Connect, Banner, and Bosscars but do not have TAMUK email.
 - a. Accounts are validated by file submitted by Pharmacy each semester.
 - i. Accounts will be set to expire September 1st and February 1st.
 - ii. Account will be deleted if not in the Pharmacy file.
9. System Administrators:
 - a. Must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
 - b. Must provide a list of accounts for the systems they administer when requested by authorized TAMUK management.
 - c. Must cooperate with investigations of security incidents.
 - d. Are responsible for removing the accounts of individuals that change roles within TAMUK or are separated from their relationship with TAMUK.
10. Account termination:
 - a. Affiliated accounts will be disabled upon expiration and will be deleted 30 days after expiration.
 - b. Employee accounts will be disabled on their last day of service as indicated by Human Resources.
 - i. Exceptions may be requested by the President, Vice President, Dean, or Division Head. Approval for exception may be granted by the Executive Director of Human Resources or the Vice President for Finance.
 - ii. Emeritus faculty are exempt from this provision.
 - iii. Retiree accounts are created in accordance with the Retiree E-mail Standard Administrative Procedure 29.01.99.K1.065.

- iv. Employee AD and email accounts are deleted 13 months after their account expires.
- c. Student AD and email accounts
 - i. Student accounts will be disabled one semester after graduation
 - 1. Alumni accounts are created in accordance with Alumni Email Standard Administrative Procedure 29.01.99.K1.063.
 - ii. Student accounts are disabled when they become inactive in Banner.
 - iii. Student accounts are deleted 2 years after being disabled.
- d. Guest Accounts will be deleted 30 days after account expiration.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. 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
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. System Regulation 29.01.03
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 Acceptable Use Procedure 29.01.99.K1.010
14. Texas Government Code, Section 441

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404