29.01.99.K1.030 Administrative Access Standard Administrative Procedure

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: March 28th, 2019
Next Scheduled Review: March 2024

Introduction

Technical support staff, security and system administrators at Texas A&M University-Kingsville (TAMUK) 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.

Purpose

The purpose of this procedure is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privileges.

Audience

This procedure applies to individuals that have, or may require, special access privileges to any TAMUK Information Resources.

Administrative Access Procedure

1. TAMUK departments must submit to iTech a list of administrative contacts for their systems that are connected to the TAMUK network.
2. TAMUK departments must request administrative rights through a Helpdesk ticket.
3. All users of administrative access accounts must have account management instructions, documentation, training and authorization.
4. Each individual that uses administrative access accounts must refrain from abuse of privilege and must only do investigations under the directions of the Information Security Officer.

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).
6. Each account used for administrative access must meet the TAMUK Password Procedure.
7. The password for a shared administrative access account must change when an individual with the password leaves the department or TAMUK, or upon a change in the vendor personnel assigned to the contract.
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.
9. When administrative access accounts are needed for internal or external audit, software development, software installation, or other defined need, they:
    a. Must be authorized by department director or higher.
    b. Must be created with a specific expiration date.
    c. Must be removed when work is completed.
10. Supervisors are required to report violations of this procedure to the Chief Information Officer.

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 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
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. 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 Acceptable Use Procedure 29.01.99.K1.010
13. 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