29.01.99.K1.300 Application Security Standard Administrative Procedure

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: July 8th, 2019
Next Scheduled Review: July 2024

Introduction

The implementation of application security at Texas A&M University-Kingsville (TAMUK) is designed to reduce risks to sensitive and confidential information by providing the appropriate levels of protection as required by state and federal law.

Purpose

The purpose of this procedure is to keep risk to an acceptable level. The University shall ensure that the proper security controls will be implemented for each application. These controls will vary in accordance with the sensitivity and criticality of each application.

Audience

This procedure applies to TAMUK employees and affiliates, including contractors.

Roles and Responsibilities

1. The Information Security Officer (ISO) shall develop enterprise-wide application security standards, procedures and guidelines.
2. Security controls for centralized systems or applications shall be managed by iTech personnel.
3. The information resource owner or custodian shall implement application security in compliance with security standards to have effective controls over applications they directly manage.
4. For hosted applications or applications managed by outsourced contractors, the contractors must implement application security controls consistent with this procedure.

Application Security Procedure

1. Application Security Standards and Implementation Guidelines
   The ISO shall develop and maintain application security standards and guidelines for implementing application security in the production environment.
2. Security integrated within applications
   Systems developed or acquired must have documented security specifications. Applications are required to comply with the Texas Administrative Code (TAC) on "Information Security Standards."
3. Access control
   a. Unauthorized access to electronic information services is prohibited.
   b. Users of various electronic information services are assigned a unique login name or ID to access these resources. Users are required to protect and maintain the confidentiality of their passwords. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate.
4. Application security administrators
   a. Application administrators are designated for administrative applications.
   b. These application administrators will process the appropriate authorization for the applications/information resource systems for which they have responsibility. The application administrators allow for the regular review of access rules granted to each login name in accordance with least privilege policy.

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