29.01.99.K1.200 Systems Development Procedure

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

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. By implementing appropriate security procedures, blocking unnecessary access to networks, computers and applications, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents at Texas A&M University-Kingsville (TAMUK).

Purpose

The purpose of this procedure is to describe the requirements for developing and/or implementing new systems and software applications at TAMUK.

Audience

This procedure applies to all individuals that use develop and implement University Information Resources.

Systems Development Procedure

1. ITS is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for TAMUK system and software projects. All software developed inhouse which runs on production systems must be developed according to the SDLC. At a minimum, this plan should include preliminary analysis or feasibility study; risk identification and mitigation; system analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical TAMUK information.

2. All production systems must have designated owners for the critical information they process. ITS must perform annual risk assessments of production systems to determine whether the controls employed are adequate.

3. All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. An administrator must be assigned for all production systems to grant and revoke access according to guidelines in the Account Management Procedure.

4. Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions.

5. All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

6. Violations of this procedure must be reported to the Information Security 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: ITS
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404