Introduction

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

Purpose

Department of Information Resources (DIR) of the State of Texas via their Security Incident Reporting System

ii. Level 2 –Incidents that have a small impact on operational functionality but have no impact on the overall business function of TAMUK. Level 2 incidents will be handled by iTech. iTech personnel will continue to monitor the incident after remediation and will report findings to the ISO for as long as deemed necessary. Incident types and quantities will be tracked. Reports will be sent to the DIR of the State of Texas via their Security Incident Reporting Systems.

iii. Level 3 – These are the most severe incidents. They have a major impact on either business or operational functions at TAMUK and may prevent TAMUK from fulfilling its mission. This category also includes incidents that may cause damage to TAMUK's reputation or financial loss. The incident will be handled by the appropriate iTech personnel and all steps taken must be approved by the ISO. iTech personnel will continue to monitor the incident after the threat has been mitigated and must report findings to the ISO for as long as deemed necessary. An incident report will be prepared by the ISO for review by the Chief Information Officer (CIO) and upper administration. Incident types and quantities will be tracked and reported to the DIR of the State of Texas via their Security Incident Reporting System.

b. The following are examples of the categories of iTech security related incidents:

Incident Category	Description	Examples
Level 1	No widespread effect on TAMUK functions	• Minor rule violations by an employee • Detection and removal of viruses or malware

3. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation.
4. The ISO, working with the IRM, will determine if University communication is required and the content of the communication.
5. The ISO will designate appropriate technical resources to communicate new issues or vulnerabilities to the system vendor and work with the vendor to eliminate or mitigate the vulnerability being exploited by a specific threat or set of threats.
6. The ISO is responsible for initiating, completing, and documenting the incident investigation.
7. The ISO is responsible for reporting the incident to the:
    a. IRM
    b. Texas A&M University System
    c. Department of Information Resources as outlined in Texas Administrative Code 202
    d. Local, state, or federal law officials as required by applicable statutes and/or regulations
8. If the incident is caused by a student, faculty or staff member the ISO may recommend disciplinary actions, if appropriate
9. In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and TAMUK.
    a. Any incident that involves criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) must also be reported to the University Police Department.

Disciplinary Actions

11. Texas Administrative Code, Chapter 202
12. 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