Incident Management Procedure

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 procedures, 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
The purpose of this procedure is to describe the requirements for dealing with information resource security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems or loss of critical data, as well as complaints of improper use of Information Resources as outlined in the E-Mail Procedure, the Internet Usage Procedure, and the Acceptable Use Procedure.

Audience
This procedure applies to individuals that use any TAMUK Information Resources.

Incident Management Procedure
1. Incidents must be reported to the Information Security Officer (ISO).
2. The Computer Incident Response Team (CIRT) members have pre-defined roles and responsibilities which can take priority over normal duties. Members are appointed by the ISO.
3. The ISO is responsible for notifying the Information Resources Manager (IRM) and the CIRT and initiating the appropriate incident management action.
4. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation.
5. The ISO, working with the IRM, will determine if University communication is required and the content of the communication.
6. 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.
7. The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
8. 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
9. If the incident involves a student, faculty or staff member the ISO will recommend disciplinary actions, if appropriate, to the IRM.
10. In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and TAMUK.
Disciplinary Actions
Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment 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
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
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 Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441