Incident Management Policy

Introduction
The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, 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.

1. Purpose
This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the E-Mail Policy, the Internet Policy, and the Acceptable Use Policy.

2. Audience
The Texas A&M University-Kingsville Incident Management Policy applies equally to all individuals that use any Texas A&M University-Kingsville Information Resources.

3. Incident Management Policy
   3.1. Texas A&M University-Kingsville Computer Incident Response Team (CIRT) members have pre-defined roles and responsibilities which can take priority over normal duties. The CIRT team consists of the Associate CIO, ISO, Security Analyst, Network Analyst, and Microcomputer Technicians.
   3.2. Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
   3.3. The Information Security Officer (ISO) is responsible for notifying the Information Resources Manager (IRM) and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
   3.4. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
   3.5. The appropriate technical resources from the CIRT are responsible for monitoring such that any damage from a security incident is repaired or mitigated and that the vulnerability to a particular threat is eliminated or minimized where possible.
   3.6. The ISO, working with the IRM, will determine if a widespread University communication is required, the content of the communication, and how best to distribute the communication.
   3.7. The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability being exploited by a specific threat or set of threats.
   3.8. The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
   3.9. The Texas A&M University-Kingsville ISO is responsible for reporting the incident to the:
       3.9.1. IRM
       3.9.2. Department of Information Resources as outlined in TAC 202
       3.9.3. Local, state or federal law officials as required by applicable statutes and/or regulations

3.10. The ISO is responsible for coordinating communications with outside organizations and law enforcement.
   3.11. In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the IRM.
   3.12. In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and Texas A&M University-Kingsville.

4. Incident Reporting: Violations of this policy must be reported to ISO and CIO.
5. **Disciplinary Actions**

Violation of this policy 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 Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.