29.01.03.Z1.08 Guideline: Incident Management

Approved September 1, 2010
Revised February 13, 2013

Supplements System Regulation 29.01 and TAMU SAP 29.01.03.M1.09

Reason for the Guidelines

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 the actions that can be taken to reduce the risk and drive down the cost of security incidents.

1. Official Guideline

1.1 HSC Computer Incident Response Team (CIRT) members have pre-defined roles and responsibilities which can take priority over normal duties.

1.2 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.

1.3 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.

1.4 The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation.

1.5 The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

1.6 The ISO, working with the IRM, will determine if a widespread HSC communication is required, the content of the communication, and how best to distribute the communication.

1.7 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.
1.8 The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.

1.9 The ISO is responsible for reporting the incident to the:
   - IRM,
   - Department of Information Resources as outlined in TAC 202,
   - Local, state or federal law officials as required by applicable statutes and/or regulations.

1.10 The ISO is responsible for coordinating communications with outside organizations and law enforcement.

1.11 In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the IRM.

1.12 In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and HSC.

2. Disciplinary Actions

Violations of this policy may result in disciplinary action, which may include termination for employees and temporary workers; 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 HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration