Sam Houston State University
A Member of The Texas State University System
Information Technology Services (IT@Sam)

Technology Incident Management Policy: IT-07

PURPOSE:

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.

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; and complaints of improper use of information technology resources as outlined in the SHSU policies.

SCOPE:

The SHSU Technology Incident Management Policy applies to the ISO, IRM, and Critical Incident Response Team (CIRT).

POLICY STATEMENT:

1. As an incident is identified, pre-defined roles and responsibilities of the SHSU CIRT members take priority over normal duties.
2. The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
3. The ISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
4. 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.
5. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
6. 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.
7. The ISO, working with the IRM, will determine if a widespread SHSU communication is required, the content of the communication, and how best to distribute the communication.

8. 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.
9. IT@Sam Security or Server Management Team will disconnect a server posing an immediate threat to the SHSU network in order to isolate the intrusion or problem and minimize risks.
    a. This can be done without contacting the owner or application administrator if circumstances warrant.
    b. The server will remain disconnected until it is brought back into compliance or is no longer a threat.
10. The Sam Houston State University ISO is responsible for reporting the incident to the:
    a. IRM
    b. Office of Information Technology Services as outlined in TAC 202
    c. Local, state or federal law officials as required by applicable statutes and/or regulations
11. The ISO is responsible for coordinating communications with outside organizations and law enforcement.
12. In the case where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the IRM.
13. In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement including the University Police Department and IT@Sam.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, May 15, 2011
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2015