Sam Houston State University
A Member of The Texas State University System
Information Technology

Cybersecurity Incident Response Policy: IT-07

PURPOSE:

The number of cybersecurity 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 cybersecurity incidents are some of the actions that can be taken to reduce the risk and drive down the cost of cybersecurity incidents.

This policy describes the requirements for dealing with cybersecurity incidents. Cybersecurity incidents include, but are not limited to: malware detections (e.g. virus, worm, ransomware); unauthorized use of computer accounts and information systems; and complaints of improper use of information resources as outlined in Sam Houston State University (SHSU) policies.

SCOPE:

The SHSU Cybersecurity Incident Response policy applies to the Information Security Officer (ISO), the Information Resources Manager (IRM), and the Cybersecurity Incident Handling Team (CIHT) and the Cybersecurity Incident Response Team (CIRT).

POLICY STATEMENT:

1. As an incident is identified, pre-defined roles and responsibilities of the SHSU CIHT and CIRT members take priority over normal duties.

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

3. The ISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident response actions including restoration as defined in the Cybersecurity Incident Response Standard.

4. Whenever a cybersecurity incident is suspected or confirmed, the appropriate procedures identified in the Cybersecurity Incident Response Standard 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 cybersecurity incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

7. The ISO, working with the IRM and CIHT, 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. Information Technology will disconnect an information system or component posing an immediate threat to SHSU to contain the incident and minimize risks.
    a. This can be done on the authority of the ISO without contacting the information system owner or custodian if circumstances warrant.
    b. The information system or component will remain disconnected until it is brought back into compliance or is no longer a threat.

10. The ISO is responsible for reporting the cybersecurity incident as required by law and policy to:
    a. The IRM
    b. The Texas Department of Information Resources and the Texas State University System Office for urgent incidents such as breaches, suspected breaches, or unauthorized exposure in compliance with Texas Government Code 2054.1125
    c. The Secretary of State of Texas if the incident is a breach, suspected breach, or unauthorized exposure involving election data
    d. The Texas Attorney General's Office if the incident is a breach involving at least 250 residents of the state of Texas not later than the 60th day after the date on which the breach was determined.
    e. 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. 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 Information Technology.

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, April 17, 2023
Reviewed by: Heather Thielemann, Information Resources Manager, April, 2023
Next Review: April, 2024