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

Malicious Code Policy: IT-24

PURPOSE:

This policy is intended to provide information to university information resource administrators and users to improve the resistance to, detection of, and recovery from the effects of malicious code.

Sam Houston State University (SHSU) information resources are strategic assets that, as property of the State of Texas, must be managed as valuable State resources. The integrity and continued operation of university information resources are critical to the operation of the University. Malicious code can disrupt normal operation of university information resources.

SCOPE:

The SHSU Malicious Code Policy applies equally to all individuals utilizing SHSU information resources (e.g., employees, faculty, students, alumni, agents, consultants, contractors, volunteers, vendors, temps, etc.).

This policy does not apply to approved faculty research and academic programs where students and instructors develop and experiment with malicious programs in a controlled environment.

POLICY STATEMENT:

1. All desktops and laptops connected to the SHSU network must use SHSU approved virus protection software and configuration.

2. Each file server attached to the SHSU network must utilize SHSU approved virus protection software and must be setup to detect and clean viruses that may infect file shares.

3. Software to safeguard against malicious code (e.g., antimalware, anti-spyware, etc.) shall be installed and functioning on susceptible information resources that have access to the University network.

4. All information resource users are prohibited from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.) unless approved by the Information Security Officer.

5. All information resource users are prohibited from knowingly propagating malicious programs including opening attachments from unknown sources.

6. Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.

7. Flash drives, external hard drives, and other mass storage devices shall be scanned for malicious code before accessing any data on the media.

8. The settings for software that protect information resources against malicious code should not be altered in a manner that will reduce the effectiveness of the software and should include the minimum configuration:

    a. Regular scheduled scans
    b. Enabled real-time scans

9. The automatic update frequency of software that safeguards against malicious code should not be disabled, altered, or bypassed by end-users to reduce the frequency of updates.

10. All reasonable efforts shall be made to contain the effects of any system that is infected with a virus or other malicious code. This may include disconnecting systems from the network or disabling service.

11. If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current antimalware or other control software.

12. If malicious code cannot be automatically quarantined or removed by antimalware software, the system should be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to IT by contacting the Service Desk.

13. Personnel responding to an incident should be given the necessary access privileges and authority to afford the necessary measures to contain/remove the infection.

14. If possible, identify the source of the infection and the type of infection to prevent recurrence.

15. Any removable media (including flash drives, external hard drives, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.

16. IT personnel should thoroughly document the incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information resources and submit to the Information Security Officer.

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, February 6, 2012
Reviewed by: Heather Thielemann, Information Resources Manager, June, 2023
Next Review: June, 2024