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

Malicious Code Policy: IT-24

PURPOSE:

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

SHSU information technology 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 technology resources are critical to the operation of the University. Malicious code can disrupt normal operation of university information technology resources.

The number of information technology resource 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 decrease the cost of security incidents.

SCOPE:

The SHSU Malicious Code Policy applies equally to all individuals utilizing SHSU information technology 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:

The following requirements shall be adhered to at all times to ensure the protection of SHSU information technology resources:

Prevention and Detection:

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

- 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.
- Software to safeguard against malicious code (e.g. antivirus, anti-spyware, etc.) shall be installed and functioning on susceptible information technology resources that have access to the University network.
- All information technology 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 a part of an approved research or academic program.
- All information technology resource users are prohibited from knowingly propagating malicious programs including opening attachments from unknown sources.
- Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.
- Flash drives, external hard drives, and other mass storage devices will be scanned for malicious code before accessing any data on the media.
- Software safeguarding information technology resources against malicious code should not be disabled or bypassed by end-users.
- The settings for software that protect information technology resources against malicious code should not be altered in a manner that will reduce the effectiveness of the software.
- 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.

Response and Recovery:

- 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.
- If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current antivirus or other control software.
- If malicious code cannot be automatically quarantined or removed by antivirus 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 Information Technology Services by contacting the Service Desk.
- Personnel responding to an incident should be given the necessary access privileges and authority to afford the necessary measures to contain/remove the infection.

- If possible, identify the source of the infection and the type of infection to prevent recurrence.
- 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.
- IT@Sam Services personnel should thoroughly document the incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information technology resources and submit to the Information Security Officer to be included in the Department of Information Resources Security Incident Reporting System.

DEFINITIONS:

Information Security Officer (ISO): Officer designated to administer the university Information Security Program.

Malicious Code: A term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.

Mitigate: The elimination or reduction of the frequency, magnitude, or severity of exposure to risks in order to minimize the potential impact of a threat.

Security Incident: A single event or a series of unwanted or unexpected events that involve information security (see definition of "information security event"), causing harm or threatening information assets and requiring non-routine preventative or corrective action.

Virus Protection Software: Software that is designed to prevent viruses, worms and Trojan horses from getting onto a computer, as well as remove any malicious code that has already infected a computer.

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, January 30, 2015
Approved by:	President's Cabinet, February 6, 2012
Next Review:	November 1, 2016