

STANDARD ADMINISTRATIVE PROCEDURE

29.01.99.M1.23 Information Resources – Malicious Code

Approved July 18, 2005

Revised February 24, 2009

Next Scheduled Review: February 24, 2012

Standard Administrative Procedure Statement

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

Definitions

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Malicious code - Software that is designed to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user's information systems.

Examples of such software include:

- **Viruses:** Pieces of code that attach to host programs and propagate when an infected program is executed.
- **Worms:** Particular to networked computers to carry out pre-programmed attacks that jump across the network.
- **Trojan Horses:** Hide malicious code inside a host program that appears to do something useful.
- **Attack scripts:** These may be written in common languages such as Java or ActiveX to exploit weaknesses in programs; usually intended to cross network platforms.
- **Spyware:** Software planted on your system to capture and reveal information to someone outside your system. It can do such things as capture keystrokes while typing passwords, read and track e-mail, record the sites visited, pass along credit card numbers, and so on. It can be planted by Trojan horses or viruses, installed as part of freeware or shareware programs that are downloaded and executed, installed by an employer to track computer usage, or even planted by advertising agencies to assist in feeding you targeted ads.

Owner of an Information Resource - an entity responsible for:

- a business function; and,
 - determining controls and access to information resources supporting that business function.
-

Responsibilities and Procedures

1. GENERAL

University information resources are strategic assets which, 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. This procedure is intended to provide information to University information resource administrators and users to improve the resistance to, detection of, and recovery from malicious code.

2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all TAMU network information resources.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP 29.01.99.M1.27 Exclusions from Required Risk Mitigation Measures.

The intended audience for this SAP includes all owners, managers, system administrators, and users of University information resources.

3. PREVENTION AND DETECTION:

- 3.1 For each computer connected to the University network, security updates from the manufacturer of the appropriate operating system, and/or application software, must be kept current (e.g, patched and updated).
- 3.2 Where feasible, personal firewall software or hardware shall be installed to aid in the prevention of malicious code attacks/infections.

- 3.3 E-mail attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.
- 3.4 Diskettes and mass storage devices will be scanned for malicious code before accessing any data on the media.
- 3.5 Software to safeguard against malicious code (e.g., anti-virus, anti-spyware, etc.) shall be installed and functioning on susceptible information resources that have access to the University network.
- 3.6 Software safeguarding information resources against malicious code shall not be disabled or bypassed.
- 3.7 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.
- 3.8 The automatic update frequency of software that safeguards against malicious code shall not be altered to reduce the frequency of updates.

4. RESPONSE AND RECOVERY:

- 4.1 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 email.
- 4.2 If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current anti-virus or other control software. (See also University Standard Administrative Procedure [29.01.99.M1.09 Incident Management](#).)
- 4.3 If malicious code cannot be automatically quarantined or removed by anti-virus software, the system shall 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 departmental IR personnel so that they may take appropriate actions in removing the malicious code and protecting other systems.
- 4.4 Personnel responding to the incident should have the necessary system access privileges and authority to affect the necessary measures to contain/remove the infection.
- 4.5 If possible, identify the source of the infection and the type of infection to prevent recurrence.

- 4.6 Utilize anti-viral, anti-spyware, etc. software to execute a complete system scan including the boot sector and all physical drives, to eradicate all malicious code that may be identified.
- 4.7 Any removable media (including diskettes, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.
- 4.8 Departmental IR personnel should thoroughly document the incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information resources.

Related Statutes, Policies, or Requirements

Supplements [University Rule 29.01.99.M1](#)

Contact Office

Contact [Information Technology Issues Management](#) for SAP interpretation or clarification.

OFFICE OF RESPONSIBILITY: [Vice President and Associate Provost for Information Technology](#)