29.01.03.H0.25 Malicious Code

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

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 the effects of malicious code.

Reason for Regulation

- Required by Texas Administrative Code Section 202
- This Standard Administrative Procedure (SAP) applies to University information resources that store or process mission critical and/or confidential information.
- The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with malicious code. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer (ISO).
- The intended audience for this standard administrative procedure includes, but is not limited to, all information resources data/owners, users, management personnel, students and system administrators.

Procedures and Responsibilities

1. Prevention and detection

    1.1. 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).

    1.2. Where feasible, local firewall software or hardware shall be installed to aid in the prevention of malicious code attacks/infections.

    1.3. Email attachments and shared files of unknown integrity shall be scanned by the local antivirus application for malicious code before they are opened or accessed.

    1.4. Diskettes and mass storage devices will be scanned by the local antivirus application for malicious code before accessing any data on the media.

    1.5. Antivirus software shall be installed to safeguard against malicious code on susceptible information resources that have access to the University network.

    1.6. Software safeguarding information resources against malicious code shall not be disabled or bypassed.

    1.7. 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.

    1.8. The automatic update frequency of software that safeguards against malicious code shall not be altered to reduce the frequency of updates

2. Response and Recovery

    2.1. 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.

    2.2. 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.

    2.3. 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 IR personnel so that they may take appropriate actions in removing the malicious code and protecting other systems.

    2.4. Personnel responding to the incident should have the necessary system access privileges and authority to affect the necessary measures to contain/remove the infection.

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

2.6. 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.

2.7. 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.

2.8. 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

- Texas Administrative Code Section 202

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.

Owner of an Information Resource: an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Information Security Officer (ISO): responsible for administering the information security functions within Texas A&M University-Texarkana and reports to the Information Resources Manager (IRM).

Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

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.

Contact Office

Contact Office: Department of Information Technology, 903-223-3084