# The Division of Information Technology
# University Information Security Standards

**Information Security Standard – Malicious Code (Legacy TAC 202)**
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

## 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 of malicious code.

## 2. Applicability

This standard applies to all University network information resources.

The purpose of the implementation of this standard 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 department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. 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 is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

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

## 3. Definitions

3.1 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.2 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.3 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

3.4 User: An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

3.5 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:

a. Viruses: Pieces of code that attach to host programs and propagate when an infected program is executed.

b. Worms: Particular to networked computers to carry out pre-programmed attacks that jump across the network.

c. Trojan Horses: Hide malicious code inside a host program that appears to do something useful.

d. 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.

e. 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.

3.3 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and

(2) for determining controls and access to information resources

**4. Prevention and Detection:**

4.1 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).

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

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

4.4 Electronic media and mass storage devices will be scanned for malicious code before accessing any data on the media.

4.5 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.

4.6 Software safeguarding information resources against malicious code shall not be disabled or bypassed by end-users.

4.7 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.

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

**5. Response and Recovery:**

5.1 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 accounts.

5.2 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.

5.3 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 the IT Division by contacting the Helpdesk at (806) 651-4357 or at mailto:itsc@mail.wtamu.edu, so that they may take appropriate actions in removing the malicious code and protecting other systems.

5.4 Personnel responding to the incident should have or be given the necessary access privileges and authority to affect the necessary measures to contain/remove the infection.

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

5.6 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.

5.8 Information Technology - Network Services 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 follow the University Incident Management standard administrative procedure to report the incident.

**OFFICE OF RESPONSIBILITY:** Information Technology

**CONTACT:** Chief Information Officer