PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.05 Information Resources – Malicious Code
Approved May 26, 2009
Revised November 4, 2014
Revised December 5, 2019
Next Scheduled Review: December 2024

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to provide information to Prairie View A&M University (PVAMU) information resource administrators and users to improve the resistance to, detection of, and recovery from malicious code. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education.

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.

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

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 preprogrammed attacks that jump across the network;
- **Trojan Horses** - hidden 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; and,
- **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 targeted ads.

Official Procedures and Responsibilities

---

1. GENERAL

1.1 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that 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.

1.2 Per the State of Texas control catalog, the information system must implement malicious code protection. (System and Information Integrity (SI)-3)

1.3 The Texas A&M University System's (TAMUS) network infrastructure and other information resources must be continuously protected from threats posed by computer malware and other types of hostile computer attacks. All System-owned and personally owned computing devices that connect to the System network must run all required protection software and adhere to any other protective measures as required by applicable policies and guidelines. (TAMUS Information Integrity Standard)

1.4 There may be additional measures that department heads or deans will implement to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their system administrators where applicable. Each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated ISO.

2. APPLICABILITY

2.1 This UAP applies to all PVAMU network information resources. The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of university information resources.

3. PROCEDURES

3.1 Prevention and Detection

3.1.1 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).

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

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

3.1.4 Storage devices will be scanned for malicious code before accessing any data.

3.1.5 Software to safeguard against malicious code shall be installed and functioning on susceptible information resources that have access to the university network.

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

3.1.7 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.

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

3.2. Response and Recovery

3.2.1 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.

3.2.2 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.

3.2.3 If malicious code is found, the system shall be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact until remediation is complete. The presence of the malicious code shall be reported to the ISO so that the appropriate actions can be taken in removing the malicious code and protecting other systems.

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

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

3.2.6 Utilize anti-virus, 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.

3.2.7 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.

3.2.8 The Office of Information Technology 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 submit the documentation to the ISO.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

Contact Office

Office of Information Resources Management	936-261-9350