Procedure Statement

Texas A&M University-San Antonio (A&M-San Antonio) information resources are strategic assets and must be managed as valuable state resources. Malicious code can disrupt normal operation of University information resources. This Procedure is intended to provide information to administrators and users to improve the resistance to, detection of, and recovery from malicious code.

Reason for Procedure

This Procedure applies to all users of A&M-San Antonio information resources.

The purpose of the implementation of this Procedure 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 are 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 in this Procedure 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).

Official Responsibilities and Procedure

1. PREVENTION AND DETECTION

1.1 Information resources connected to the A&M-San Antonio network must be kept up-to-date with security updates from the manufacturer of operating system and application software (e.g. patched and updated).
1.2 Dedicated firewall hardware and anti-virus software shall be utilized to protect information resources connected to the University network in the prevention of malicious code attacks/infections. Any information resource containing confidential information that cannot implement these safeguards should be reported to the A&M-San Antonio Information Security Officer (ISO) and Information Resource Manager (IRM).

1.3 Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed. Scanning should include files of unknown integrity on any electronic media (i.e. external hard drive, USB memory key, etc.).

1.4 The automatic update frequency of firewall and anti-virus software shall not be disabled, altered or bypassed to reduce the frequency of updates by any user.

1.5 Email servers and gateways must provide protection from malware, spam and phishing.

1.6 Whenever possible, the use of two-factor authentication should be considered and implemented.

1.7 Users are to notify Information Technology Services (ITS) Help Desk in the event they feel that a virus may have infected their equipment.

2  RESPONSE AND RECOVERY

2.1 ITS 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 29.01.03O0.08 Incident Management to report the incident.

2.2 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.

2.3 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.

2.4 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.

2.5 The presence of the malicious code shall be reported to the ITS Help Desk so that they may take appropriate actions in removing the malicious code and protecting other systems.

2.6 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.
2.7 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.

2.8 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.

Non-Compliance

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to A&M-San Antonio information resources, civil, and/or criminal prosecution.

Related Statutes, Policies, or Requirements

DIR Practices for Protecting Information Resources Assets

Family Educational Rights and Privacy Act (FERPA)

Gramm Leach Bliley Act (GLB Act)

Health Insurance Portability and Accountability Act (HIPAA)

Texas Administrative Code (TAC) 202 as amended or supplemented

Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education

TAMU System Policy 29.01 Information Resources

A&M-San Antonio Procedure 29.01.03.O0.08 Incident Management

Definitions
**Accounts** - Information resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

**Confidential Information** - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

**Custodian** - Guardian or caretaker (the holder of data). The agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

**Incident Report** – A formal reporting of a known information technology related incident. This is performed by completing the associated ITS form.

**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 Resources Manager (IRM)** - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.

**Information Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

**Information Technology Services (ITS)** – The designated name for the central Information Technology department for the University.

**ISAAC (Information Security Awareness Assessment and Compliance)** - A web-based system used to assess the security posture of information systems and measure compliance with the Information Security Standards.

**Malicious code** – Software code that infects information resource and allows them 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.

**Mission Critical Information** - Information that is defined by A&M-San Antonio or information resource owner to be essential to the continued performance of the mission of A&M-San Antonio 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 A&M-San Antonio or department.

**Network Scanning** - The process of transmitting data through a network to elicit responses in order to determine configuration state or the presence of security vulnerabilities within an information system.

**Owner** - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

**Production System** - The hardware, software, physical, procedural and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

**Security Incident** - Assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing, disruption or denial of service, altered or destroyed input, processing, storage, or output of information, or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

**Security Incident Reporting System (SIRS)** - The electronic system used for reporting (after the fact, after-action) incidents in compliance with Texas Department of Information Resources (DIR) regulations.

**Security Patch** - A fix or repair to a program that eliminates a known system vulnerability.

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

**Vulnerability** - A weakness or flaw in system security design, implementation, procedures or controls that can cause a violation of the system’s security policy or a security breach if exploited by an attacker.
Contact Office

Finance and Administration, Information Technology Services (210) 784-4357 (HELP)