1. GENERAL

Texas A&M University-Corpus Christi 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 preparation for, resistance to, detection of, and recovery from malware.

2. APPLICABILITY

This university procedure applies to all university network information resources.

The purpose of the implementation of this university 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 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.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

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

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions.

4. PREPARATION, PREVENTION, AND DETECTION

4.1. Information resources connected to the university network must be kept up-to-date with security updates from the manufacturer of operating systems and applications.

4.2. Where feasible, host-based firewalls and anti-malware software (e.g. anti-virus, anti-spyware, etc) shall be utilized to protect information resources connected to
the university network. Information resources containing Sensitive Information that cannot implement these safeguards require notification of the Information Resources Manager.

4.3. Email attachments, shared files, and external media storage devices must be scanned for malware before access or execution.

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

4.5. The settings for software that protect information resources against malicious code shall not be altered in a manner that will reduce the effectiveness of the software.

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

4.7. Email servers and gateways must provide protections from malware, spam, and phishing.

4.8. To permit detailed analysis if necessary, malware detection software on any system that contains Sensitive Information, is directly connected to storage containing Sensitive Information, or accesses Sensitive Information through a network connection must be specifically configured to quarantine the detected malware. Quarantined malware on these systems may only be deleted by representatives of the Information Resources Manager.

5. RESPONSE AND RECOVERY

5.1. Malware detected on any system or device that contains Sensitive Information, is directly connected to storage containing Sensitive Information, or accesses Sensitive Information through a network connection must be treated as a security incident and all procedures outlined in University Procedure 29.01.03.C2.08 Incident Response must be followed.

5.2. All reasonable efforts shall be made to contain the effects of malware to a single system or network segment, identify the source of the infection, and mitigate the results to the system and rest of the university network. This may include disconnecting systems or networks from the university network.

5.3. If malware cannot be automatically quarantined or removed by anti-malware software, the system shall be disconnected from the network to prevent further possible propagation of the malware or other harmful impact. The presence of the malware shall be reported to departmental information resources personnel so that
they may take appropriate actions in removing the malware and protecting other systems.

5.4. Departmental information resources personnel should thoroughly document any malware incident noting the source of the malicious code, if possible, the resources impacted, and damage or disruption to information resources. This information should be provided to the Media and Computer Services Helpdesk for consolidation in the University’s Monthly Incident Summary Reports to the Department of Information Resources.

6. CONSEQUENCES FOR VIOLATIONS

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct
- Texas A&M University-Corpus Christi Rule
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Information Security Office

Office of Responsibility: Office of the Associate VP for Information Technology and CIO