

**ADMINISTRATIVE PROCEDURES**

|  |  |
| --- | --- |
| **50.04 Information Security – Malicious Codes & Malware** | **Revised: May 17, 2022** |

1. GOVERNING REGULATIONS

This procedure is governed by System Regulation [29.01.03](http://policies.tamus.edu/29-01-03.pdf) Information Security and Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, [Rule 202.75](http://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75) Information Resources Security Safeguards.

2. PURPOSE

Malware includes viruses, worms, trojans, adware, keyloggers, and any unauthorized code to circumvent information security. This procedure establishes a process for prevention, detection, response, and recovery from the effects of malware.

3. PREVENTION AND DETECTION

3.1 Personal computers (desktops, laptops, tablets), workstations and servers, regardless of network connectivity status, shall be safeguarded against malware by installing agency approved endpoint protection software, Microsoft security updates, patches, and other vendor-provided software updates.

3.2 Personal computers are configured to automatically download the security updates and patches from Microsoft and endpoint protection updates.

3.3 For personal computers that have remained inactive for more than a month (for example, idle laptop computers), security updates and patches as well as endpoint protection updates must be installed manually.

3.4 The settings for software that protect information resources against malware should not be altered in a manner that will reduce the effectiveness of the software.

3.5 The automatic update frequency of software that safeguards against malware must not be altered to reduce the frequency of updates.

3.6 While endpoint protection updates are configured to download automatically, it is suggested that end users check to ensure their computer has received the latest endpoint protection updates at least once a week.

3.7 In addition, specialized software installed on computers will be controlled and managed by its owner for protection against malware by installing vendor-recommended patches and updates.

3.8 E-mail attachments or shared files transmitted or received will be scanned for malware before they are opened or accessed.

3.9 Discs, flash drives, external drives and other storage media will be scanned for malware before accessing data on the device.

4. RESPONSE

4.1 Reasonable efforts will be made by the user to contain the effects of a personal computer or storage device that is infected with malware. This includes disconnecting the computer from the network, disabling e-mail, and contacting the IR Department for further guidance.

4.2. If malware is discovered, or believed to exist, then IR Department staff, the Information Security Officer, or other designated staff will be notified immediately.

5. RECOVERY

IR Department staff or designated staff will utilize the following the recovery procedures:

5.1 Isolate the infected computer/device.

5.2 Identify the source of the infection and the type of infection to determine the proper course of action and prevent recurrence.

5.3 Utilize endpoint security software and execute a complete system scan including all physical drives, to eradicate all malware that may be identified.

5.4 If the infection cannot be eradicated, then the computer must be completely reimaged.

5.5 Any removable media (discs, flash drives, external drives, etc.) recently used on infected machine shall be scanned prior to opening and/or executing any files contained therein.

5.6 The security incident should be documented, the Information Security Officer notified, and included in the monthly security incident report to the Texas Department of Information Resources.

CONTACT: [Information Resources Department Head](mailto:cbryan@tfs.tamu.edu), (979) 458-6607