OIS 31 – Standard for Protection Against Malware

I. STANDARD STATEMENT

A significant threat to UTSA data and computing resources is the propagation of malware (malicious software) through network connections.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. With the goal of data integrity, reliability and system performance, the University Technology Solutions (UTS) manages a virus protection program for all UTSA-owned computers, including home computers and portable computing devices. Because of the critical nature of malware protection, UTS will establish and maintain a baseline of protection that must be met by computer users and systems administrators.
    1. All workstations, whether connected to the network or standalone, must use data protection software approved by UTS.
    2. The data protection software must not be disabled or bypassed.
    3. The data protection software must not be altered in such a manner that the effectiveness of the software is diminished.
    4. The software's automatic feature must not be altered to reduce the frequency of updates.
    5. All UTSA servers attached to the network must utilize UTS-approved data protection software.

6. Email gateways must utilize UTS approved email virus protection software in accordance with UTS rules for the setup and use of the software.
7. Procedures for handling malware are established in the Standard for Incident Response.

Title: OIS 31 – Standard for Protection Against Malware
Effective Date: December 1, 2013
Last Revised: August 4, 2020