CEHD Information Security Procedure
IS-12 Use of Non-TAMU Equipment on Campus

Procedure Statement

The Texas A&M campus network is shared resource that is critical to the entire campus community. As such, it is important that all devices that connect to the network are reasonably secure to prevent them from spreading malware within the campus. This document provides best practices that should be followed by everyone who brings non-TAMU owned computing devices on campus. In some cases, TAMU-IT will block access to devices that violate these guidelines.

Note. This procedure is for temporary use of non-TAMU equipment on campus such as bring your personal laptop to work. For more permanent situations where the computer will be left on campus and performs on-going university work, the computer should comply with all relevant computer configuration requirements as listed in IS-6.

Official Procedure and Responsibilities

1. The computer should use an operating system that is still supported by its vendor.

   See https://tamu.teamdynamix.com/TDClient/KB/ArticleDet?ID=33372 for end-of-life information for Windows and MacOS X.

2. Critical and security related patches for the operating system and software should be up to date (within a month of release).

3. The computer should have working anti-virus software that is kept up to date with the latest virus definitions.

   3.1 CEHD employees can install Sophos (the anti-virus software used by CEHD) on personal equipment. Contact Technology Services for a copy of the software. Sophos also provides a free home version at https://home.sophos.com/.

   3.2 A&M provides a copy of McAfee (at no charge) through software.tamu.edu

   3.3 Any other AV software can be obtained and used as long as it is actively maintained by the vendor.

4. The computer should NOT use peer to peer file sharing software (e.g., Torrent, LimeWire, Kazaa) while on campus.