



MALICIOUS CODE PROTECTION STANDARD

PURPOSE

The purpose of this standard is to promote a secure computing environment for all students, faculty, staff and affiliates at Hampton University. Computer viruses, worms, Trojans, etc. constitute a major threat to the integrity and performance of the computing operations on campus, including access to sensitive data and the availability of the University network. This standard applies to all computers that are connected to Hampton's network via a University network connection including, but not limited to, a wired connection, a wireless connection, or a VPN connection. This policy encompasses systems which are University-owned, as well as those which simply connect to the Hampton University network.

STANDARD

All computers, which are the property of Hampton, must have the campus-standard endpoint protection client (Symantec) installed and scheduled to perform a local scan weekly (at a minimum). In addition, the anti-virus software and the virus definition files must be kept up-to-date.

To prevent viral propagation to other networked devices or harmful effects to the network, computers infected with viruses, worms or other forms of malicious code may be disconnected from the network until the infection has been removed. All non-University owned computing devices connected to the University network must utilize malware protection software.

Users should not intentionally spread, develop or experiment with malware on the University's network. Intentional spreading of malware includes spreading malicious programs through failure to run malware protection software, undertake proper use of operating systems or software updates or demonstrate due care in opening e-mail attachments or clicking links.

The ATM/Help Desk will install Symantec software on all Hampton University owned desktops and portable computers. It is the responsibility of end-users to either install and maintain antivirus software on their personal computers, or use other means to ensure that their computer is virus free. Computers which are infected with malware may be disconnected from the network until they are verified as "clean."