Guideline 5.23.1.8 Anti-malware Installation and Management

Part 1. Purpose.

Subpart A. This guideline establishes responsibilities for the installation and management of software to prevent infection by malicious software (malware) within Minnesota State Colleges and Universities (system). Malware, including viruses, trojans, worms, spyware, key-loggers, etc., represents a substantial risk to information technology resources and the system. Anti-malware provides a layer of protection beyond regularly updating and patching applications and operating systems.

Subpart B. Academic Freedom. Nothing in this guideline shall be interpreted to expand, diminish or alter the academic freedom provided under board policy, a system collective bargaining agreement, or the terms of any charter establishing a system library as a community or public library.

Part 2. Applicability. This guideline applies to all system information technology resources. Institutions may adopt additional requirements, consistent with this guideline and board policy 5.23, for information technology resources under their control.

Part 3. Guidelines.

Subpart A. Anti-malware Installation. Information technology resources such as servers, desktop and notebook computers connecting to institution networks must have anti-malware installed.

Subpart B. Hand-held Devices. If anti-malware is available for hand-held devices capable of accessing information technology resources, those devices must have anti-malware installed.

Subpart C. Continuous Protection. Anti-malware must be configured to provide continuous protection.

Subpart D. Updates. Anti-malware should be configured to automatically update and should use the most current definition files.

Subpart E. Exceptions. If anti-malware protection is not feasible, alternate risk mitigation techniques must be implemented. The risk mitigation technique selected should be in proportion to the risk. Alternate risk mitigation techniques are considered exceptions.

Part 4. Definitions.

Subpart A. Continuous Protection. Describes anti-malware software that is constantly active and monitoring information technology resources to identify, prevent, and remove malicious software.

Subpart B. Information Technology Resources. Facilities, technologies, and information resources used for system member information processing, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, and instructional materials. This definition is not all inclusive, but rather, reflects examples of system equipment, supplies and services.

Subpart C. Malicious Software (Malware). Software designed to harm or damage an information technology resource without consent of the resource user.

Subpart D. Must. A statement that is required for a compliant implementation.

Subpart E. Should. A statement that is recommended, but not required.

Subpart F. System. Denotes the Minnesota State Colleges and Universities Board of Trustees, the system office, the state colleges and universities, and any part or combination thereof.

Part 5. Authority. Board policies 1A.1 and 5.23 delegate authority to the vice chancellor to develop system guidelines, consistent with Board policy and system procedure, for the purposes of implementing Board policy 5.23.

Approval Date: 05/17/10,
Effective Date: 05/17/10,

Date and Subject of Revision:

1/25/12 – The Chancellor amends all current system procedures effective February 15, 2012, to change the term "Office of the Chancellor" to "system office" or similar term reflecting the grammatical context of the sentence.

5/17/10 – Language in this new policy was originally adopted as ITS Standard 5.23.B Anti-Virus Installation and Management on July 19, 2006, and was implemented on Jan. 1, 2007. ITS Standard 5.23.B remained in place until the adoption of System Guideline 5.23.1.8 on May 17, 2010.