

Minnesota State Colleges and Universities

ITS Standard 5.23.B.

Anti-Virus Installation and Management

Part 1. Purpose.

This standard establishes responsibilities for the installation and management of anti-virus software within Minnesota State Colleges and Universities. Computer viruses (including trojans, worms, etc.) represent a substantial risk to the system in terms of time, money, potential data breach or loss. Anti-virus software provides a layer of protection beyond that of the basic security requirement of regularly updating and patching of application and operating systems.

Nothing in this standard 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 standard applies to all users of System technology resources, whether or not the user is affiliated with Minnesota State Colleges and Universities, and to all uses of those resources, wherever located.

Part 3. Definitions.

Subpart A. College or university. College or university, except where specified otherwise, means a System college or university, the Office of the Chancellor, or the Minnesota State Colleges and Universities System.

Subpart B. System. System means the Board of Trustees, the Office of the Chancellor, the state colleges and universities, and any part or combination there of.

Subpart C. User. User means any individual, including, but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using System information technology in any manner, whether or not the user is affiliated with Minnesota State Colleges and Universities.

Subpart D. Must. This word indicates a statement that is an absolute requirement for a compliant implementation.

Subpart E. Should. When the word “should” is used, the statement is recommended, but not required.

Part 4. Responsibilities of All Users

Subpart A. Installation of Anti-virus software

1. Client devices including; desktop and notebook computers, handheld devices, connecting to the system network must have current anti-virus software installed.
2. Servers must have current anti-virus software installed.

3. Anti-virus software must be configured to provide real-time protection.
4. Auto-update should also be activated to provide the most current definition files.
5. If anti-virus software 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.

Subpart B. Exceptions

Each college or university must have a process in place for documenting any exceptions from this standard.

Date of Implementation:	January 1, 2007
Date of Adoption:	July 19, 2006
Related Documents:	Board Policy 5.23, Information Security
Date and Subject of Revisions:	