

Minnesota State Colleges and Universities

ITS Standard 5.23.C.

Security Patch Management

Part 1. Purpose.

This standard establishes responsibilities for the installation and management of security related software updates within Minnesota State Colleges and Universities. Almost all operating systems and many software programs have periodic security patches released by the vendor that need to be applied. If critical patches and updates are not applied on a regular basis, computer and other network devices are vulnerable to various worms, viruses, Trojans, and direct hacker attacks. The result can include breach of data, denial of service, or attacks directed at other entities from the compromised device.

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. Critical security patches. Critical security patches are time sensitive patches identified by trusted sources (e.g., Office of the Chancellor, vendor, security organizations, etc.) as required to mitigate potential negative impact to the System and its users. Anti-virus definition updates are considered critical security patches

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

Subpart F. Must Not. This phrase indicates a statement that is an absolute prohibition for a compliant implementation.

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

Subpart H. Should Not. The phrase “should not” is used in statements of practices that are not recommended, but which may be followed if circumstances warrant.

Subpart I. May. The word “may” means that an item is completely optional.

Part 4. Responsibilities of All Users.

Subpart A. Installation of Security Patches.

1. Computers and other devices attached to the system networks must be regularly maintained by the application of security patches. Critical security patches must be applied as soon as possible, not to exceed 14 days after release. Other security patches not designated as critical may be applied on a normal maintenance schedule.
2. If the application of security patches is not feasible, alternate risk mitigation techniques must be implemented. The risk mitigation alternative selected should be in proportion to the risk. Alternate risk mitigation techniques are considered exceptions.
3. Automated patching procedures should be utilized for critical security patches whenever available.
4. Security patches should be tested prior to implementation.

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:	