Guideline 5.23.1.5 Security Patch Management

Part 1. Purpose.

Subpart A. This guideline establishes the minimum technical standards for the installation and management of security related software updates within Minnesota State Colleges and Universities (system). Almost all operating systems and many software programs have periodic security patches, released by the vendor, which need to be applied. If security patches and updates are not applied on a regular basis, computer and other network devices are vulnerable to various worms, viruses, trojans, and direct malicious attacks. The result can include breach of data, denial of service, or attacks directed at other entities from the compromised device.

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. Security Patch Identification. Information Technology support staff must stay current on applicable security patches relating to the information technology resources and software for which they are responsible.

Subpart B. Security Patch Installation.

1. **Critical Security Patches**. Critical security patches should be applied as soon as possible and must not exceed 14 days after release.
2. **Non-critical Security Patches**. Non-critical security patches may be applied on a normal maintenance schedule and must not exceed 120 days after release.
3. **Automation**. Procedures should be utilized for security patches whenever available.
4. **Testing.** Security patches should be tested prior to implementation.
5. **Exceptions.** 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.

Part 4. Definitions.

Subpart A. Critical Security Patch. A time-sensitive patch identified by a trusted source (e.g., system office, vendor, security organizations, etc.) Such a patch mitigates a software vulnerability, which if not installed, exposes the system and its users to negative impact. Antivirus definition updates are considered critical security patches.

Subpart B. Data. Information collected, stored, transferred or reported for any purpose, whether in computers or in manual files. Data can include: financial transactions, lists, identifying information about people, projects or processes, and information in the form of reports. Because data has value, and because it has various sensitivity classifications defined by federal law and state statute, it must be protected.

Subpart C. 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 D. Institution. One of the separate entities, or having to do with an organizational entity as described under system.

Subpart E. May. A statement that is optional.

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

Subpart G. Must Not. A statement that is prohibited for a compliant implementation.

Subpart H. Should. A statement that is recommended but not required.

Subpart I. 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: 11/04/09,
Effective Date: 11/04/09,

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.

November 4, 2009 – language in this new guideline was originally adopted as ITS Standard 5.23.C on July 19, 2006, and was implemented January 1, 2007. ITS Standard 5.23.C remained in place until the adoption of System Guideline 5.23.1.5 on November 4, 2009.