Guideline 5.23.1.6 Vulnerability Scanning

Part 1. Purpose.

Subpart A. This guideline establishes the minimum technical standards for vulnerability scanning within Minnesota State Colleges and Universities (system). Vulnerability scanning is a process by which devices connected to system information technology resources are probed in an attempt to identify security-related issues.

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

Part 2. Applicability. This guideline applies to all information technology resources connected to any system network. This includes but is not limited to those located in residence halls, wireless devices, and devices on public networks such as libraries, whether or not they are owned or operated by the system. This does not include system information technology resources not directly connected such as a system owned or managed laptop connected at a user's home on a private Internet connection. Institutions may adopt additional requirements, consistent with this guideline and policy 5.23, for information technology resources under their control.

Part 3. Guidelines.

Subpart A. Vulnerability Scans. Information Technology support staff must stay current on applicable security patches relating to the information technology resources and software for which they are responsible.

1. **Frequency.** Institution IT staff must schedule quarterly vulnerability scans of information technology resources for well-known or high-risk exposures. Scans should be performed more frequently than this, and these more-frequent scans are not restricted to the requirements set forth in this guideline.
2. **Scan Depth.** Scheduled vulnerability scans should include probes of services, operating systems, and applications to identify weaknesses in configurations, missing patches, default passwords, and other common vulnerabilities that could be exploited by intruders. The institution CIO may specify parameters for scans beyond the minimums defined in this guideline.
3. **Authenticated Scans.** Scans of system-owned devices should include authenticated access to services and applications that would not be accessible without authentication.
4. **Scanning Infrastructure.** Scanning devices must be connected and configured such that it allows scanning all networks and systems. This should include permitting traffic

from scanning devices through network access control lists. This additional access may be configured such that it is only in effect during full scans.

5. **Public or Isolated Networks.** Scheduled vulnerability scans may exclude information technology resources that are physically isolated or that have no access to internal networks that are routed directly outside the institution's networks. Examples of public-only networks may include public-access wireless, conference rooms, etc. A physically isolated network has no connection to, or device shared with, any other network.
6. **Non-managed Resources.** Scans may exclude information technology resources which are not owned or managed by the institution or which are not logically or physically connected to a system network.
7. **Payment Processing Networks.** Scheduled vulnerability scans may be required for payment processing systems. These scans must meet payment card industry data security standards.
8. **Personal Data and Service Outages.** Scheduled vulnerability scans should not intentionally search the content of personal electronic files or cause service outages.
9. **Ad Hoc Scans.** Scans should also be performed on all new systems and significantly modified existing systems. Scans should be completed as early as feasible in the system development lifecycle and must be completed prior to the system being placed into production or on the system network.
10. **Exceptions.** Each institution should follow their exception documentation process if vulnerability testing interferes with system availability. Excepted information technology resources should be reviewed manually for vulnerabilities.

Subpart B. Authorization. The Institution CIO must designate authorized individuals to perform scans of devices and networks in their institution. Vulnerability scanning must only be conducted by authorized individuals.

Subpart C. Reporting. Reports are considered confidential security information and are subject to the Minnesota Government Data Practices Act (MGDPA), Minnesota State Statutes §13, and may be subject to other privacy laws depending on the content of the data. Reports may be disseminated and must be limited to only those with a need to know.

Subpart D. Operational Precautions.

1. **Privacy.** Institutions must respect the privacy of individuals and other institutions, pursuant to board policy, system procedures, system guidelines and all applicable laws.
2. **Service Disruption.** Scans that may impact service availability should be conducted during maintenance windows. Scans may omit tests that may interrupt service.

Part 4. Definitions.

Subpart A. Access. Approved authorization to view, modify or delete system information/data. Access shall be authorized to individuals or groups of users depending on the application of law, system policy or guideline. Technical ability to access information is not necessarily equivalent to legal authority.

Subpart B. Assessment. As used in this document, an assessment is either a vulnerability scan or a penetration test.

Subpart C. Authorized Individual. Employee, consultant, volunteer or other individual who is approved and allowed access to information within the system to perform an activity on behalf of an institution. The individual may have access to any class of information, according to policy.

Subpart D. Availability. Assurance that information technology resources are accessible to authorized users when needed.

Subpart E. Confidentiality. Assurance that information technology resources are accessible only as authorized.

Subpart F. 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 G. Information Resources. Data collected, created, received, maintained or disseminated by any Minnesota State Colleges and Universities user, regardless of its form, storage media, security classification, or conditions of use.

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

Subpart J. May. A statement that is optional.

Subpart K. Minnesota Government Data Practices Act (MGDPA). Per Minnesota State Statutes §13, MGDPA regulates the collection, creation, maintenance and dissemination of government data in state agencies, statewide systems, and political subdivisions. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is a federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

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

Subpart M. Not Public Data. Data that is considered confidential, private, nonpublic or protected nonpublic data as defined in the MGDPA or any other relevant state or federal statute or system legal guideline. For examples of data classifications, see standard 5.23.E, Notice of Breach of Security, Part 4: Reporting a Suspected Breach.

Subpart N. Penetration Testing. A method of evaluating the security of a computer system or network by simulating an attack by a malicious user. The process involves scanning for potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

Subpart O. Public Data. Information/data that is available to the general public according to Federal and State laws, regulations or State Statutes.

Subpart P. Risk. Denotes the exposure to potential loss or harm as a function of probability of loss or harm and the impact because of loss or harm.

1. **High Risk.** A high probability of loss or harm paired with a severe impact to operations or security as a result of loss or harm. May also include high/low or low/high pairings.
2. **Medium Risk.** A moderate probability of loss or harm paired with a moderate impact to operations or security as a result of loss or harm. May also include high/low, low/high, medium/low, or low/medium pairings.
3. **Low Risk.** A low probability of loss or harm paired with a low impact to operations or security as a result of loss or harm. May also include medium/low or low/medium pairings.

Subpart Q. Scan. An active analysis of an information technology resource for any particular software or hardware configuration.

1. **Authenticated Scan**. A scan utilizing credentials, authenticating the scanning device and allowing the scan to gather additional information.
2. **Basic Scan.** A scan performed without credentials, gathering less information, and in some cases, returning results that are not verified to be accurate.

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

Subpart S. Should Not. A statement that is not recommended, but which may be followed if circumstances warrant.

Subpart T. 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.

Subpart U. User. Any individual, including but not limited to, students, administrators, faculty, employees, volunteers, and other authorized individuals using system information resources, whether or not the user is affiliated with the system.

Subpart V. Visibility. Visibility is a relative measure of where an asset resides within a network, and what other assets can reach that specific asset.

Subpart W. Vulnerability Scan. A process that identifies security issues of information technology resources. Using specific tools that communicate with devices connected to the institution's network, each system is scanned in an attempt to identify security related issues. These issues may include missing or weak passwords, insecure software installations, missing patches, service packs, software with known security issues, and malicious software installed on information technology resources. The result of this process is generally a risk-based report that outlines vulnerabilities, allowing ITS staff to address and mitigate or remedy each vulnerability in a timely manner.

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: 05/04/10,

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.