Guideline 5.23.1.3 Data Sanitization

Part 1. Purpose.

Subpart A. This guideline establishes the minimum technical standards for the removal of institutional data from electronic information technology assets owned by the Minnesota State Colleges and Universities (system). This institutional data may include information classified by the institution's administration; information protected by federal or state laws; information that could lead to identity theft, institutional embarrassment, or loss of personal privacy; and licensed software or restricted intellectual property.

Subpart B. As storage and media devices are decommissioned, re-purposed, or re-allocated, the institutional data must be effectively removed from the storage media or the media must be destroyed. This removal process has been called data removal, data sanitization, data destruction, or other similar terms. In this guideline we will use data sanitization for compatibility with federal guidelines.

Subpart C. 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 system information technology resources, such as computer equipment and/or storage media, and other electronic media capable of data retention that may contain institutional data. This guideline establishes minimum requirements for data sanitization. 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. All information technology resources must be sanitized before being re-purposed, removed, donated, sold, or disposed of. Sanitization must remove or destroy all data and information resources in such a manner that the data cannot be retrieved, even partially, by conventional means or commercially available processes.

Subpart B. Record retention schedules must be complied with prior to any media sanitization. The authorized system or institutional official(s) must refer to system procedure 5.22.1, *Acceptable Use of Computers and Information Technology Resources*, Part 7, *Application of Government Records Laws*, Subpart B, *Record Retention Schedules*, and other applicable requirements.

Subpart C. Removal and destruction of any (or potential) institutional data shall be based on standards and practices as they are documented in the National Institute of Standards and Technology document, NIST 800-88, Guidelines for Media Sanitization.

Subpart D. A record should be maintained detailing the sanitization procedure applied to system-owned information technology resources. The record should include the:

1. unique property identification,
2. time and date,
3. description of the information technology resource,
4. disposition of the information technology resource,
5. procedure employed to remove and/or destroy the information, and
6. individual executing the procedure.

Subpart E. The appropriate method of data sanitization is determined by the type of physical media containing the data. The authorized system or institutional official(s) may take guidance from the NIST 800-88, Guidelines for Media Sanitization. Minimum sanitization methods and suggested tools for various media types can be found in Appendix A of NIST 800-88. Acceptable methods of data sanitization are as follows:

1. **Clearing.** Clearing, also known as overwriting, preserves the media for re-use after the data sanitization process.
    a) The clearing process must replace written data with random values at all addressable locations.
    b) Media can be effectively cleared by one overwrite using currently available sanitization technologies.
    c) Deleting files, re-imaging and formatting are not acceptable methods of clearing.
2. **Purging.** Purging is a stronger method of sanitization that protects magnetic media against a laboratory attack.
    a) Executing the firmware *secure erase* command (for ATA drives only) is an acceptable method for purging.
    b) Degaussing is a typical method of purging where the degaussed media is not expected to be re-used.
3. **Destruction.** Proper physical destruction protects against laboratory attacks. Acceptable methods of destruction are as follows:
    a) **Disintegration, pulverization, melting, and incineration.** These are designed to completely destroy the media and therefore any data it contains. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.
    b) **Shredding.** Shred size of the refuse should be small enough to ensure reasonable assurance, relative to the data's confidentiality, such that the data cannot be reconstructed.

Subpart F. Contracted Secure Disposal. Electronic media disposal service companies that contract with the system should be certified by the National Association for Information Destruction, Inc. (NAID certified).

Subpart G. Most computers and mobile devices, including but not limited to cell phones, copiers, MP3 players, and digital cameras, contain some form of storage media and should be handled accordingly. The institution must consider what institutional data the onboard storage may contain and destroy that data according to these standards. If the existence of internal storage cannot be reasonably ruled out, then the device must be destroyed.

Subpart H. Any questions or issues regarding data sanitization, such as procedures for media types not described within this guideline, must be directed to the authorized system or institutional official.

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 equivalent to legal authority.

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

Subpart C. Authorized System or Institutional Official. For those seeking access to not-public information, or access to centrally-supported systems, it is the person designated by the Chancellor, Director or Department Head to function in an authorization role for information/data access purposes. In some cases, the employee's Supervisor may function as the designee. In other cases, a key contact is named. Also see "Supervisor".

Subpart D. Clearing. Overwriting process on digital media to make it unreadable using normal access methods.

Subpart E. 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 F. Degaussing. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.

Subpart G. Destruction. Destruction of media includes: disintegration, incineration, pulverizing, shredding, and melting. Information cannot be restored in any form following destruction.

Subpart H. Information Resources. Data collected, created, received, maintained or disseminated by any system user, regardless of its form, storage media, security classification, or conditions of use.

Subpart I. Information Technology Resources. Facilities, technologies, and information resources used for system 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 J. Institution. A system college or university, the system office, or the system as a whole.

Subpart K. May. A statement that is optional.

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

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

Subpart N. Overwrite. Writing patterns of data over existing data stored on a magnetic medium.

Subpart O. Purge. Media sanitization process that protects the confidentiality of information. Degaussing is considered a typical method of purging.

Subpart P. Sanitization. The process of removing data from storage media, providing reasonable assurance that the data may not be easily retrieved and reconstructed.

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

Subpart R. Should Not. A statement of practices that are not recommended but which may be followed.

Subpart S. System. Referring to the Board of Trustees, the system office, the state colleges and universities, and any part or combination thereof.

Subpart T. System or Institutional Information. Information collected, maintained, stored, reported or presented in any format, on any medium, by any unit or entity within the system.

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

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: 02/09/09,
Effective Date: 03/09/09,

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.