



## State of Minnesota CIO POLICY

### Enterprise Storage Media Sanitization Policy *Enterprise Security Policy 2008-03*

#### *Policy Statement*

All government entities in the executive branch of Minnesota State Government will develop, implement, test, and maintain a process for the sanitization of storage media.

#### *Reason for the Policy*

To define a minimum requirement to ensure that any data collected, created, received, maintained, or disseminated by any state government entity regardless of storage media or conditions of use (collectively referred to as *government data*), which is classified anything other than public, is properly removed from a government entity's storage media resources prior to it being surplus, internally transferred (repurposed), traded-in (lease-end), replaced, or the storage media must be properly destroyed.

To prevent unauthorized use or misuse of *government data* and promote the security of information resources within the state's government entities.

To foster compliance with all applicable regulations dealing with the confidentiality of personally identifiable information. This includes regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act, among others.

This policy supersedes the Department of Administration's informational bulletin 03-01 (Data Removal from Surplus Computers).

#### *Approval History*

Document version 1.0, effective on approval date.

Signature: <Signature on File with Enterprise Security Office>  
Gopal Khanna, State Chief Information Officer (CIO)

October 2<sup>nd</sup>, 2008  
Approval Date

*Who Should Know about this policy*

Agency Heads, Chief Information Officers, and Chief Information Security Officers, and their designees who are responsible for the management of procurement, delivery, movement, maintenance, repurposing, recovery, and disposal of storage media assets.

Any third party contracted by a government entity to handle/process, transmit, store, or dispose of *government data* or handle storage media on behalf of the state.

This policy is offered as guidance to local government, higher education, K-12, or other government related entities.

*Related information*

[Minnesota Statutes 16E](#). Office of Enterprise Technology

*Contacts*

[State Chief Information Security Officer](#)

*Applicability and Exclusions*

This policy is applicable to all government entities in the executive branch of Minnesota State Government that surplus, transfer, trade-in, otherwise dispose of, or replace storage media, which stored *government data*, be it owned or leased by, or on loan to the government entity.

This policy is applicable to any arrangement with third parties who surplus, transfer, trade-in, otherwise dispose of, or replace storage media that stored *government data*.

This policy is offered as guidance to local government, higher education, K-12 or other government related entities.

*Definitions*

**Assets:** Something of either actual or intrinsic value to the state. Assets can be logical or physical in nature and can be classified as information (physical or electronic), systems, software, hardware, facilities, or people.

**Storage Media:** Any device that can store (temporarily or permanently) government data in an electronic format (e.g., Hard Drives, CD's, DVD's, Thumb Drives, Floppy Disks, Tape

Backups, *Volatile and Non-Volatile Memory*, Cell Phones, Handheld Devices, printers and copiers, etc.).

**Government Entity:** As used in this document it refers to what is covered by Minnesota Statute [16E.03, Subdivision 1\(e\)](#), which includes any office, department, division, bureau, board, commission, authority, district, or agency of the executive branch of the Minnesota State Government.

**Government Data:** All data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use.

**Intrinsic Value:** The value of an asset to the business or government entity that is above and beyond its material or depreciated value.

**Nonvolatile Memory:** A general term for all forms of solid state (no moving parts) memory that do not need to have their memory contents periodically refreshed. This includes all forms of read-only memory (ROM) such as programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), and flash memory. It also includes random access memory (RAM) that is powered by a battery.

**Sanitization:** The removal of data so that it is unrecoverable from a given media form to a level commensurate with the sensitivity of the information.

**Software:** Applications and services such as operating systems, database applications, networking software, office applications, custom applications, etc. that process, store, or transmit *government data*.

**State Data:** See *Government Data*

**System:** Information systems that process and store *government data* that is a combination of software, hardware and any host, client or server.

**Volatile Memory:** A general term for all form of solid state (no moving parts) memory that do have their memory contents periodically refreshed or lost when power is interrupted. This is primarily referred to as random access memory (RAM) that is not powered by a battery.

*Roles & Responsibilities*

### **Enterprise Security Office**

1. Manage this policy and related standard.
2. Develop a standard that defines the requirements for the data sanitization processes.
3. Review all exceptions to this policy.
4. Periodically evaluate this policy and related standard for effectiveness.
5. Periodically evaluate the government entity-level processes related to data sanitization

for effectiveness and compliance to the Enterprise policy and standard.

6. Provide approval process for government entity-level sanitization/disposal tools or processes not covered by the data sanitization standard.

**Government Entity**

1. Implement and manage entity-level data sanitization processes that comply with this policy and related standard.
2. Periodically evaluate entity-level processes for data sanitization effectiveness.
3. Define additional entity-level requirements for data sanitization as necessary.

*Standards/Procedures*

Enterprise Security Standard on Sanitization of Electronic Media

*Forms and Instructions*

Not applicable

*Appendices*

Not applicable