State of Minnesota

Enterprise Security Information Sanitization and Destruction Standard

Office of Enterprise Technology

Enterprise Security Office Standard

Version 1.00

State CIO Standard Approval:

Gopal Khanna	<State CIO signature on file with ESO>	06/01/2010
State Chief Information Officer	Signature	Approval Date

Table of Contents

1.0 Standard Statement

Executive branch government entities must implement the requirements in this standard to ensure that:

- Information is properly disposed of in accordance with its classification;
- Electronic data is adequately sanitized when repurposing storage media and equipment;
- Storage media (electronic, paper, microform, etc.) is properly disposed of when end of life is reached; and
- Appropriate documentation is completed and retained in accordance with record retention requirements.

1.1 Disposition Determination

The sanitization and/or disposition of the storage media is at the discretion of the government entity if the entity:

- can ensure storage media has contained only public data (as defined by Minnesota Statutes, Chapter 13 “Data Practices Act”);
- can ensure storage media has been encrypted with full-disk encryption; or
- is repurposing an electronic device internally to either:
  - i) an individual with equal or greater access rights to the same data; or
  - ii) an individual with different or lesser access rights, where the entity can ensure removal of, or otherwise restrict access to, any inappropriate data on the device.

If storage media or an electronic device has contained not public data or data of an unknown classification at any point in its lifecycle and will be leaving organizational control, government entities must use the requirements of this standard to determine proper disposition of the media or device.

See Appendix A for a decision tree to guide proper selection of disposition.

1.2 Shredding of Paper and Microform

All paper and microform (e.g. microfilm, microfiche or other reduced image photo negatives) containing *“Not-Public Data”* will be physically destroyed when no longer needed in accordance with federal, state and organizational records retention requirements. Physical destruction is defined by one of the following means:

- Onsite shredding of paper by an state employee of the owning organization, using a cross cut shredder which reduces paper waste down to 1 x 5 millimeters.
- Onsite/offsite shredding of paper by a National Association for Information Destruction (NAID) certified, state approved service provider (e.g. 3rd party vendor)
- Microform destruction must be performed by a NAID certified, state approved service provider, with a “Micro Media” endorsement, to render the materials legally non-negotiable and indecipherable.

Paper/microform waste deposited in collection containers for destruction must be controlled by any means that precludes access prior to and during the collection and transportation of the waste to the disposal location, whether these services are performed by internal or contracted staff. A documented chain of custody must be maintained throughout the transportation process.

1.3 Sanitization of Electronic Storage Media

If electronic storage media can be properly sanitized (i.e. removing data) according to NIST SP800-88 standards, prior to repurposing, returning, donating, or recycling the device, entities must:

- Perform sanitization using approved software/hardware; or
- Contract out sanitization using a NAID certified, state approved service provider.

Any storage and/or transportation of electronic storage devices prior to sanitization, whether internal or external to the organization, must ensure the confidentiality and security of the information/device and preserve a strict chain-of-custody. When using a NAID certified provider, the provider pickup the storage media directly from the owning organization’s site(s) unless other secured, state run transportation with chain-of-custody documentation can be used (e.g., State Movers).

Media that should be sanitized but can't be due to damage or non-functional status, or that is otherwise not writeable, must be destroyed in accordance with this standards.

Additional guidance for specific media types is listed below (See Appendix B: Information Sanitization and Destruction of Media Types for more detail):.

Portable Storage Media
Sanitize portable storage media in accordance with this standard. However, due to the low-cost and short life of portable media, government entities are discouraged from repurposing portable media.

Examples of portable storage media include, but are not limited to, flash drives, memory cards, magnetic/smart cards, magnetic/optical disks (cd, dvd, floppy, zip), or magnetic tape (reel, tape/video cassette),

Hard-Drives
Computing and communication equipment with fixed/removable drives (whether rotating disk or solid-state storage) and external/portable hard-drives will be reset to the manufacturer's factory default settings and then sanitized.

Examples of devices with hard-drive storage include, but are not limited to, computers/servers, network storage, printers, fax/copy or MFD machines, network/communication devices (e.g. routers, firewalls).

Hand Held Devices
Manually delete all information from the device, including any files/data, configuration/connection information, phone calls/texts sent/received, addresses/contact information, speed dial numbers, pictures, calendar entries, recordings, locations, etc. After deleting all information, perform a full manufacturer's reset back to the factory default settings. When applicable, the device will be removed from the central management server.

Examples of hand-held devices include, but are not limited to, radios, dictation and recording devices, cameras (still, video), cell phones, smart phones, PDA's, barcode or smartcard readers, hand-held printing devices (e.g. receipts, tickets, asset tags), media players, mapping/navigation devices, and many others.

1.4 Destruction of Electronic Storage

If electronic storage devices can't be properly sanitized according to NIST SP800-88 standards, prior to repurposing, returning, donating, or recycling the device, entities must:

- Physically destroy the device using approved hardware; or
- Contract out destruction using a NAID certified, state approved service provider.

It is highly recommended that entities utilize a NAID certified, state approved service provider for destruction to ensure compliance with environmental regulations.

Additional guidance for specific media types is listed below (See Appendix B: Information Sanitization and Destruction of Media Types for more detail):

Portable Media
Portable media will be destroyed by any physical means that prevents reuse and data recovery.

Hard-Drives
For state-owned assets that are at end of life or are no longer functional, or leased assets that are going to be returned due to lease expiration, a state employee of the entity will:

- Reset the device to the manufacturer's factory default settings, then
- Remove the hard-drive and destroy it by any physical means that prevents reuse and data recovery.

Hand-Held Devices
State-owned assets that are at end of life or are no longer functional, will be deposited in a centrally located secure container for destruction by a NAID certified, state approved service provider. Leased devices will be treated no differently than state-owned devices.

Where applicable, the device will also be removed from the central management server.

1.5 Documentation Requirements

A disposition document must be completed for all media sanitized or destroyed, whether performed internally or by a service provider. The document must be kept on record by the owning organization, according to record retention requirements or for one year, whichever is longer.

The disposition document will contain at a minimum the following information:

- Date action was taken
- Action taken (sanitization or destruction)
- Identify whether asset was leased or state-owned (if leased, identify leasing company by name)
- Asset serial number for serialized storage media
- Asset identification (e.g. cell phone, PDA, hard-drive, etc.)
- Name, phone number, organization name and signature of person performing action

In addition, to ensure the security and confidentiality of the information contained on the media, if the media is leaving entity boundaries or control at any point prior to sanitization or destruction, the entity must require the third party to:

- Use appropriate controls (e.g. cases, locks, escort, site pick-up, professional transport, other) to ensure the media is protected from compromise or loss en-route; and
- Employ chain-of-custody inventory processes to document the control of media at all points in transit and/or storage.

2.0 Roles & Responsibilities

2.1 Office of Enterprise Technology (OET) - Enterprise Security Office (ESO)

- Maintain this document
- Provide guidance to government entities on any conflicts or questions pertaining to compliance with this standard
- Provide subject matter expertise to MMD on matters pertaining to this standard and appropriate product selection

2.2 Government Entity

- Maintain a centrally located secure container(s) for the disposal of hand-held devices
- Ensure that all record retention requirements are met before sanitizing or destroying any electronic media, hand-held devices or hard-drives.
- Remove all asset tags from any state-owned equipment prior to destruction or repurposing and that accountable devices and equipment are properly removed from their organization's asset inventory.
- Ensure that any electronic media, hand-held devices, or hard-drives that is undergoing forensic analysis or is a part of any ongoing litigation is not sanitized or destroyed without proper approval.
- Maintain records of media disposition in accordance with this standard and any organizational record retention requirements.

3.0 Related Information

3.1 Reason for the Standard

Having a process for the proper disposition and handling of not public information (as defined by Minnesota Statue, Chapter 13 [Data Practices Act]) is crucial to the prevention of data compromise or disclosure, whether it be unintentional or as a result of a malicious activity. While this standard does not specifically address additional regulatory requirements imposed upon the State, the formal process this standard requires will enable compliance with federal requirements for the disposal of confidential financial and health related data.

Government entity and enterprise procedures for the proper disposition of electronic or paper-based information must have a consistent approach across the Executive branch to avoid confusion amongst state employees, contractors and business partners entrusted with the responsibility of handling state owned information. The requirements defined in this standard are designed to establish the minimum sanitization and disposal requirements and methods for state owned information across the Executive branch.

3.2 Applicability and Exclusions

This standard is applicable to the government entities in the Executive Branch identified in the Enterprise Security Program Applicability Standard 2009-06. It is also offered as guidance to other government entities outside the Executive Branch.

Agency Heads, Responsible Authorities, Chief Information Officers, Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible for responding to, management of, and reporting on entity security controls must be aware of this standard.

The requirements of this standard must be incorporated into agreements with third parties to ensure proper controls are in place for protection of state information assets.

3.3 Regulatory, Policy, Standards, & Guideline References

Health Insurance Portability and Accountability Act (HIPAA)
Health Information Technology for Economic and Clinical Health Act (HITECH Act)
Federal Information Security Management Act (FISMA)
Payment Card Industry (PCI) Data Security Standard
Minnesota Statutes 2007 Chapter 16E (Office of Enterprise Technology)
Minnesota Statutes, Chapter 13 (Data Practices Act)
Enterprise Security Information Handling Policy
National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization
National Association for Information Destruction (NAID) Information Destruction Policy Compliance Toolkit

3.4 Forms, Templates, and Procedures

Sample Asset Disposal Certification Form
Sample Sanitization Validation Form
Italicized terms can be found in the Enterprise Security Glossary of Terms
Enterprise Security Exception Request Form

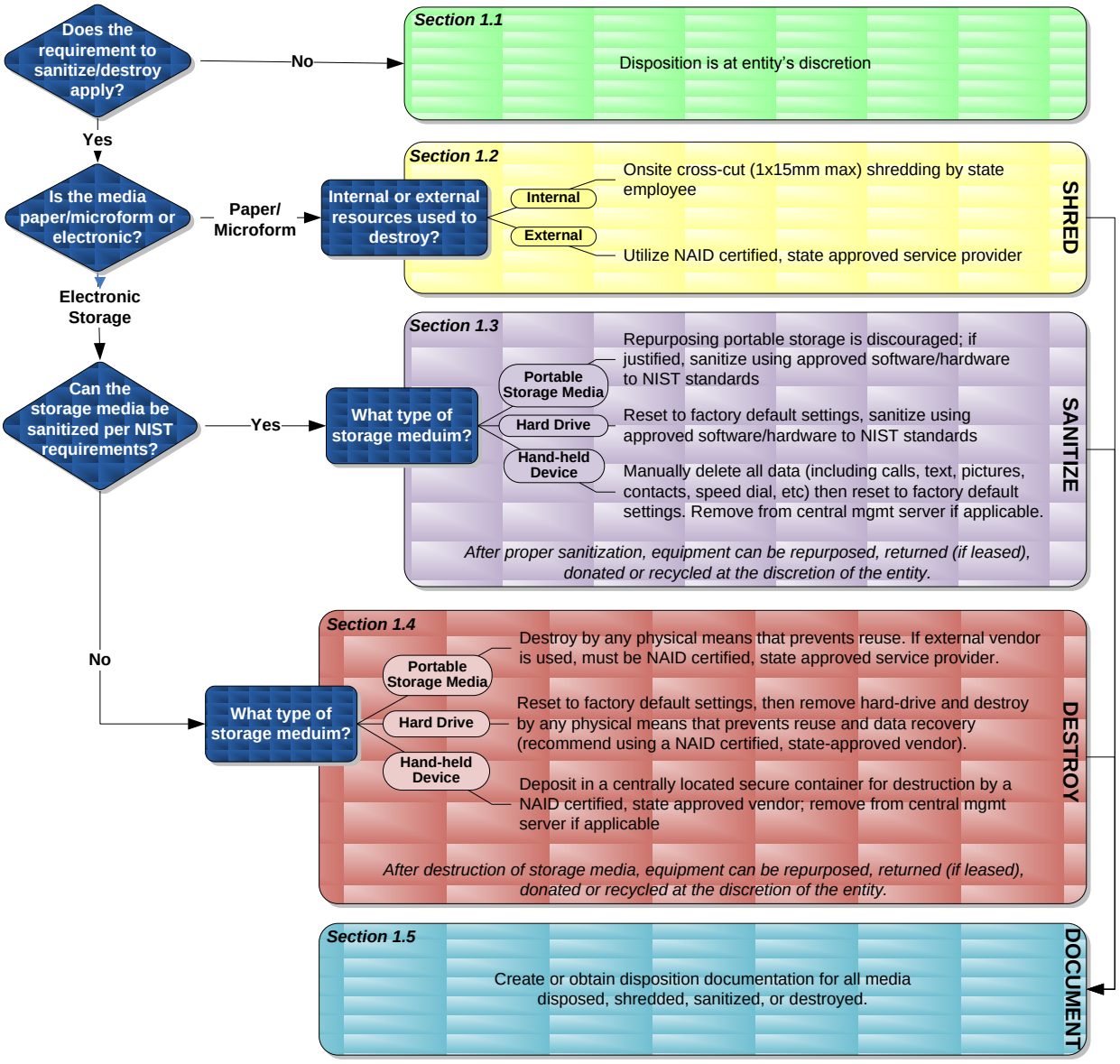
3.5 Compliance

Compliance with this standard is required within 1 year of the approval date of the standard.

Appendixes:

Appendix A: Information Sanitization and Destruction Decision Tree

The following decision tree provides a high level overview of the steps to determine the appropriate disposition of a paper, microform or electronic information storage media.



Appendix B: Information Sanitization and Destruction of Types of Media

There are several methods of media sanitization, each appropriate for different situations and each provide varying levels of protection for the confidentiality of the information contained on the media:

Type	Description
Dispose	Appropriately discarding (e.g. recycling) media without sanitizing first. This method is acceptable only if a loss of confidentiality of the information contained on the media would have no impact on the organization (i.e. public information).
Sanitize	Removal of information sufficient to protect confidentiality against fairly robust attacks (e.g. data recovery tools). Simple deletion is not sufficient to sanitize data. Acceptable methods are: • Overwriting data a minimum of 6 times, using organizational approved and validated technologies, methods or tools; • Executing the secure erase firmware command on a disk drive; or • Degaussing of magnetic media (degaussing is not effective for optical media formats like CD or DVD).
Destroy	The intent is to completely destroy the media beyond any possibility of data recovery. Destruction can be accomplished using a variety of methods including disintegration, incineration, pulverizing, shredding and melting.

The following table provides a summary of acceptable levels of handling to ensure the sanitizing or destruction of various types of information storage media. See NIST SP 800-88 for more definition and detail of acceptable sanitization and destruction methods.

Media Type	Examples	Sanitize	Destroy
Paper		N/A	Cross cut shred *(to particles of 1x5mm in size)*
Microform	microfiche, photo negatives	N/A	Shred or incinerate *(must render the materials legally non-negotiable and indecipherable)*
Hard Drive (rotating disk)	ATA, SCSI, other formats in computers, servers, network storage, printers, external or portable drives, USB flash drives, firewire drives etc	Overwrite, Secure Erase, degauss, or disassemble and degauss the enclosed platters	Disintegrate, shred, pulverize, incinerate
Storage Media (solid-state)	flash drive, memory stick, mp3 player, digital camera, video recorder, phones, PDA, SD card	Overwrite	Disintegrate, shred, pulverize, incinerate
Magnetic Media (Disk, Tape)	floppy or ZIP disk; reel-to-reel, DAT tapes, audio/video cassettes	Overwrite or degauss	Incinerate or shred
Optical Disk	CD, DVD, optical platters	N/A	Optical disk grinding device, incinerate, shred *(nominal edge dimensions of 5mm and surface area of 25 sq. mm when shredding)*

History & Ownership

Revision History – record additions as major releases, edits/corrections as minor

Date	Author	Description	Major #	Minor #
	Rick Ensenbach	Initial Release	1	00

Review History – periodic reviews to ensure compliance with program

Date	Reviewer	Description	Compliance

Approval History – record of approval phases

Phase	Description		Date
SME	Aaron Molenaar Eric Breece Rick Ensenbach Brenda Willard Bernie Kopischke Holly Gustner	Enterprise Security Office Enterprise Security Office Enterprise Security Office Department of Administration, MMD Department of Administration, MMD Department of Administration, TMD	01/12/2010
ISC	Information Security Council Approval		04/07/2010
CIOC	CIO Council Approval		05/20/2010
State CIO	State CIO Approval		06/01/2010

Ownership – current owners of the document

	Owner	Division	Department
Primary	Aaron Molenaar	Enterprise Security Office (ESO)	Enterprise Security Governance
Secondary	Eric Breece	Enterprise Security Office (ESO)	Enterprise Security Governance