Information Security - Media Disposal Standard

Document Identifier:	0758
Version:	1.3
Owner:	Bobby Singh

Document Control

The electronic version of this document is recognized as the only valid version

Document Location:	eHealth Ontario Information Security Library
Review Frequency:	This document will be reviewed on an annual basis.
Document Prime* **Enquiries relating to this document should be referred to the responsible Document Prime.*	Marc Stefaniu Sr. IT Security Consultant

Approval History

Approver(s)	Title	Approved Date
Bobby Singh	Director, Information Security	29 October 2008
Karen Waite	Chief Privacy and Security Officer	11 September 2009

Revision History

Version No.	Version Date YYYY-MM-DD	Summary of Change	Changed By
1.0	2008-10-29	Initial release	Marc Stefaniu
1.1	2008-11-04	Updates based on Michael Power input	Marc Stefaniu
1.2	2008-11-09	Updates based on input from Mugino Saeki	Marc Stefaniu
1.3	2009-09-11	Changed classification from low to unclassified	Denise Shih

Table of Contents

1 Purpose/Objective 1

2 Scope of Application 1

3 Standard Requirements 2

3.1 Process documentation 2
3.2 Identification, tracking, recording and reporting 2
3.3 Accountability 3
3.4 Storage 4
3.5 Loss of Media 4
3.6 Disposal 4

4 Responsibilities 4

4.1 Director, Operations 5
4.2 Director, Corporate IT 5
4.3 Director, Information Security 6
4.4 Manager, Facilities 6
4.5 Director, Procurement 7
4.6 Employees, Contractors, Consultants and Others 7

5 Appendix A 8

References and Associated Documents 8

5.1 Related Policies 8

1 Purpose/Objective

Protection of confidential information throughout its entire life cycle is a regulatory requirement and a major business imperative for eHealth Ontario ("the Agency").

This Information Security Standard Practice (the "Standard") outlines the mandatory requirements and establishes roles and responsibilities required to ensure appropriate disposal of specific categories of information technology ("IT") storage media, such as hard disk drives ("HDDs") and magnetic tapes.

The objective of the Standard is to ensure that media disposal is controlled in a manner that prevents accidental or intentional disclosure of any type of business information, including Personal Information ("PI") and Personal Health Information ("PHI"), that may be stored on the specified media.

2 Scope of Application

This Standard applies to HDDs and tapes decommissioned for any business or technical reason from IT equipment used in all eHealth Ontario facilities, including Markham Computing Centre ("MCC"), Streetsville Computing Centre ("SCC"), all downtown office locations and any third party site where eHealth Ontario-owned assets are in use.

This Standard does not cover:

- HDDs or tapes that are removed from IT equipment, but deemed reusable;
- CD or DVD media, PDAs, microfiche/microfilm and USB memory sticks.

These types of media require less stringent controls for disposal, and will be covered in a subsequent version of this Standard.

The HDDs and tapes may come from IT equipment such as application or database servers, email servers, data storage servers, firewalls, routers, switches, desktop computers and laptops.

The HDDs and tapes involved may come out of IT equipment owned by eHealth Ontario, clients or vendors. The disposal of HDDs and tapes owned by clients and vendors is executed at the request/instruction of the client or vendor, as a supplemental eHealth Ontario service.

Refer to **Appendix A** for other related eHealth Ontario policies and Standards.

3 Standard Requirements

3.1 Process documentation

To ensure consistency of operations and clear accountabilities, detailed disposal processes and procedures must be followed as specified in Section 4.

Separate process documentation must be developed for media items:

a) used in production or development and test environments, and located in MCC and SCC or in downtown office locations, and

b) used by Corporate IT and located at MCC, SCC or in downtown office locations.

Where possible, roles/functions within the disposal process (for instance, execution of degaussing and recording of the serial number of degaussed items, or recording and shipping) shall be segregated, to minimize opportunities for fraud and theft.

Process design must include expected time lines, so that impacted media are destroyed in a timely fashion, reducing the risk of inappropriate use.

Final disposal does not necessarily require shipping to a third party vendor for scrapping. Any solution for final disposal, after degaussing and applying physical damage, is entirely at the decision of the Agency's Facilities department, and could use disposal processes similar to other decommissioned IT equipment.

3.2 Identification, tracking, recording and reporting

The responsible roles (see Section 4) must produce and retain records pertaining to each stage of the disposal process. The records must be detailed enough to enable accurate tracking of disposable HDDs and tapes from the time they are removed from IT equipment, until confirmed degaussed, physically damaged and disposed. These records need to remain available for internal or external audits or compliance verification programs. Records older than five years may be destroyed.

The records shall be maintained and archived:

- by IT Operations for media removed from production and development servers located at MCC and SCC; and
- by Corporate IT for media removed from laptop and desktop computers.

HDDs and tapes designated for disposal must be identified by the serial number (if available) assigned by their original manufacturer. In cases where the original

manufacturer serial number is not available, a unique identifier must be assigned to the media marked for disposal.

In addition to the unique identifier, records must identify the type of IT equipment (e.g. server, laptop, etc), the original business use (e.g. hosting EMPI database) and the business ownership of the equipment from which the HDDs or tapes were removed for disposal. This information is needed in case a security incident is triggered by a lost or stolen piece of equipment. The record-keeping tool must be able to link the disposed media to its original IT use. This capability is essential for incident investigations.

Operational and decommissioned hard-drives and tapes are not considered to be capital assets and therefore shall not be reported to or tracked in the Agency's financial reporting systems.

3.3 Accountability

Management accountability for roles and responsibilities must be established for each step of the media disposal process to ensure that all media items are accounted for at all times, that only authorized and qualified personnel handle the media, and that all required process steps are followed without deviation.

Equipment owned by eHealth Ontario

The Director of Operations has the authority to approve the disposal of media items removed from IT equipment used in production in the MCC and SCC data centres.

The Director of Corporate IT has the authority to approve the disposal of media items removed from IT equipment used for Corporate IT services in the data centres or office facilities (e.g. Corporate IT servers, desktop and laptop computers).

Separate procedures should be developed for media owned by eHealth Ontario's clients, in cases where contractual obligations establish special accountabilities for eHealth Ontario

Equipment owned by eHealth Ontario clients or vendors

Media items designated for disposal, removed from IT equipment owned by eHealth Ontario's clients or vendors require approval from the client or vendor authorizing the Agency to dispose of the media.

In cases where eHealth Ontario and clients have entered into a contract, the provisions of that contract with regard to media disposal, if applicable, shall take precedence over this Standard.

The Manager of Facilities has the authority to approve the mode of final disposal of the media, after degaussing and applying physical damage (e.g. bending). Final disposal of

HDDs and tapes must comply with the regulations and requirements of the *Occupational Health and Safety Act*, the *Transportation of Dangerous Goods Act*, the *Environmental Protection Act* and any other rules or regulations that apply.

3.4 Storage

Each eHealth Ontario location must have a secure storage location where items designated for disposal must be stored.

The Director of Operations, the Director of Corporate IT, and the Manager of Facilities shall designate, for each of the eHealth Ontario facilities, the roles that are authorized to access these secure storage locations. Incumbents in these roles shall be assigned to receive, store and release items designated for disposal.

In order to reduce the risks of loss, unauthorized use, or exceeding secure storage capacity, media designated for disposal must be degaussed and physically damaged no longer than two weeks after removal from the original IT equipment, and must be disposed from eHealth Ontario facilities within six months after degaussing and damaging.

3.5 Loss of Media

Lost or stolen HDDs should be treated according to standard IT Operations and Finance processes and procedures as applicable. These processes may include the opening of a ticket with the Enterprise Service Desk (ESD). ESD shall activate the Enterprise Security and Privacy Incident Management (ESPIM) process if applicable criteria are met. If the lost or stolen media are known to hold PI or PHI, then the VP of Privacy and Security must be informed immediately.

3.6 Disposal

All media are subject to the same disposal process, which shall be designed with the assumption that the media contains highly sensitive information.

All HDDs and tape devices designated for disposal must be degaussed and physically damaged before final disposal. Refer to approved Information Disposal Guidelines (see eHealth Ontario's online Policy Library) for recommended products, process requirements or use of third party service providers.

Disposal procedures must include a detailed description of the steps needed to ensure that HDDs and tapes are degaussed and physically damaged in a way that makes data retrieval virtually impossible using commercially available services and technologies.

4 Responsibilities

4.1 Director, Operations

The Director of Operations is responsible for:

- Reviewing, updating or developing processes, procedures and forms as required for the implementation of this Standard, with regard to media designated for disposal at both MCC and SCC data centres;
- Procuring suitable and effective equipment, and providing adequate training for staff charged with the degaussing and physical destruction of HDDs and tapes;
- Ensuring that only authorized and qualified personnel handle HDDs and tapes designated for disposal and that they follow approved degaussing and destruction procedures;
- Assigning individuals who will be responsible for the custodianship of media until it is transferred to Facility Management, an authorized client representative, or an authorized shipping company for delivery to its final disposal site;
- Approving disposal of identified media and ensuring the reason for disposal is recorded in the disposal decision documentation;
- Ensuring that device serial numbers and other identification information are accurately collected, recorded and archived;
- Assigning responsibility within MCC and SCC for the archiving of the disposal records of production media assets;
- Ensuring that media designated for disposal are physically secured, accessible only by a limited number of authorized Data Centre Services personnel, and physically segregated from media used in regular production or as valid spare parts for production equipment;
- Ensuring that specific procedures are developed and implemented to deal with lost, stolen or otherwise unaccounted media items.

These responsibilities may be delegated / assigned within the Operations Department, as appropriate.

4.2 Director, Corporate IT

The Director of Corporate IT is responsible for:

- Reviewing, updating or developing processes, procedures and forms as required for the implementation of this Standard, with regard to the disposal of media under the responsibility of Corporate IT, located in any of the eHealth Ontario facilities;
- Procuring suitable and effective equipment, and providing adequate training for staff charged with the degaussing and physical destruction of HDDs and tapes;
- Ensuring that only authorized and qualified Corporate IT personnel handle HDDs and tapes designated for disposal and that they follow approved degaussing and destruction procedures;
- Assigning individuals who will be responsible for the custodianship of media until it is transferred to Facility Management or an authorized shipping company for delivery to final disposal site;

- Approving disposal of identified media and ensuring the reason for disposal is recorded in the disposal decision documentation;
- Ensuring that device serial numbers and other identification information are accurately collected, recorded and archived;
- Assigning responsibility within Corporate IT for archiving the records of disposed Corporate IT media assets;
- Ensuring that media designated for disposal are physically secured, accessible only by a limited number of authorized Corporate IT personnel, and physically segregated from media used in regular production or as valid spare parts for office or production equipment;
- Ensuring that specific procedures are developed and implemented to deal with lost, stolen or otherwise unaccounted media items.

These responsibilities may be delegated / assigned within the Corporate IT Department, as appropriate.

4.3 Director, Information Security

The Director of Information Security is responsible for:

- Developing and maintaining this Standard;
- Providing input and guidelines with regard to methods and tools suitable for erasing all information from disposable media and physically destroying the media;
- Providing input and advice for the development of specific processes, procedures and forms in support of this Standard;
- Participating in the selection of approved vendors for final media disposal, if applicable;
- Participating in security incident investigations related to lost, stolen or otherwise unaccounted media items, in cases where the incidents meet the criteria established in the ESPIM process;
- Updating the Information Security Awareness program to include employees' responsibilities relative to media disposal (see section 4.7).

These responsibilities may be delegated / assigned within the Information Security Department, as appropriate.

4.4 Manager, Facilities

The Manager of Facilities is responsible for:

- Providing secure storage space in each of eHealth Ontario facilities for decommissioned HDDs and tapes and providing access to this secure storage to the custodians appointed by the Director of Operations and the Director of Corporate IT;

- Receiving HDDs, once they have been appropriately degaussed and physically damaged, from either IT Operations or Corporate IT;
- Selecting a service provider/vendor for final media disposal;
- Arranging the shipment of degaussed and damaged media items from any of the SHHA facilities to the vendor selected for final disposal, and providing records and confirmation of the shipment (including equipment identifiers) to IT Operations or Corporate IT, as appropriate.

These responsibilities may be delegated / assigned within the Facilities Department, as appropriate.

4.5 Director, Procurement

The Director of Procurement is responsible for:

- Participating in the selection of and managing the contract with the approved vendor(s) for IT equipment disposal, as applicable;
- Ensuring that the selected vendor(s) complies(comply) with the regulations and requirements of the *Occupational Health and Safety Act*, the *Transportation of Dangerous Goods Act*, the *Environmental Protection Act,* and any other rules and regulations that apply;
- Resolving disputes with vendors regarding equipment receipt issues and discrepancies between eHealth Ontario and vendor records with regard to equipment designated for disposal;
- Notifying the Chief Financial Officer of non-compliance by vendors.

These responsibilities may be delegated / assigned within the Procurement department, as appropriate.

4.6 Employees, Contractors, Consultants and Others

eHealth Ontario's full-time and part-time employees, contractors, temporary employees, consultants, and other resources are responsible for:

- Reporting any problems with their IT equipment to the Enterprise Service Desk, and opening a REMEDY ticket;
- Not opening any piece of IT equipment (whether defective or not), to access and replace the HDDs or tapes, unless their roles are directly related to maintenance and repair of eHealth Ontario's IT equipment;
- Reporting to the Enterprise Service Desk, any piece of equipment, including HDDs or tapes, that seem unattended or abandoned;
- Physically securing any HDD or tape that seems to be abandoned or lost, until authorized eHealth Ontario personnel take possession of the equipment;
- Not trying to access data on found media, or ascertain if any found media item is functional or defective.

5 Appendix A

References and Associated Documents

5.1 Related Policies

Title of Policy
Purchasing and Supply Management Policy
Financial Control Policy
Information Security Policy
eHealth Ontario Privacy and Data Protection Policy
Information Security Operating Directive
Information Classification Standard Practice