Ontario

Unclassified

Government of Ontario IT Standard (GO ITS)

GO-ITS Number 25.20

Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media

Version #: 1.0

Status: Approved

Prepared under the delegated authority of the Management Board of Cabinet

 Last Review Date: 2014-02-06

Copyright & Disclaimer

Government of Ontario reserves the right to make changes in the information contained in this publication without prior notice. The reader should in all cases consult the Document History to determine whether any such changes have been made.

Template Info

Template Name	Template #	Template Version No.	Template Author
GO ITS Template	12.02.10	2.4	Design: PMCoE Boilerplate: SPPB/SCS

Document History

Date	Summary
2013-10-02	Architecture Review Board endorsement
2014-02-06	IT Executive Leadership Council approval

Table of Contents

1. Foreword

Government of Ontario Information Technology Standards (GO ITS) are the official publications on the IT standards adopted by the Ministry of Government Services for use across the government's IT infrastructure.

These publications support the responsibilities of the Ministry of Government Services (MGS) for coordinating standardization of Information & Information Technology (I&IT) in the Government of Ontario.

In particular, GO ITS describe where the application of a standard is mandatory and specify any qualifications governing the implementation of standards.

2. Introduction

2.1. Background and Rationale

Along with the *"Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media Guidelines"*, this standard replaces the former "*Operating Procedures for Disposal, Loss and Incident Reporting of Computerized Devices*".

This standard sets out the processes and procedures that must be followed when disposing of all computerized devices and digital storage media, including the technical procedures that must be used to adequately sanitize and/or destroy them.

Also provided are the steps to take in the event of a lost or stolen computerized device or digital storage media, and guidance for what to do following a report of a security incident or security breach.

Adhering to this standard will ensure that the disposal will be completed in a manner that meets all legislative requirements of the Government of Ontario.

2.2. Target Audience

Applies to all Government of Ontario technology solutions providers and all application development and integration initiatives.

2.3. Scope

2.3.1. In Scope

This document applies to the handling of all government issued computerized devices and digital storage media used to process, store, transmit, and record data/information in the custody or under the control of the Government of Ontario.

The following computerized devices and digital storage media are included in this standard whether they are leased or purchased by the Government of Ontario:

- Desktop computers and all integrated storage;
- Laptop computers and all integrated storage;
- Personal digital assistants and smart phones, (e.g., Blackberry devices);
- Server storage and/or backup arrays;
- Magnetic storage media (e.g., hard disk drives, tapes, cassettes, diskettes);
- Semi-conductor storage media (e.g., USB memory, flash memory cards, solid-state disk drives);
- Optical storage media (e.g., CDs, DVDs, Blu-Ray discs);
- Multi-functional devices with scanner, printer, facsimile and photocopy capabilities as well as legacy devices with any, or all of these capabilities.

2.4. Applicability Statements

2.4.1. Organization

All ministries and clusters are subject to Government of Ontario IT Standards.

All adjudicative and advisory agencies are subject to Government of Ontario IT Standards.

All other agencies that are using OPS information and information technology products or services are required to comply with Government of Ontario IT standards if they are subject to either the *Management or Use of I& IT Directive* or Government of Ontario IT Standards by Memorandum of Understanding.

As new GO IT standards are approved, they are deemed mandatory on a go-forward basis (Go-forward basis means at the next available project development or procurement opportunity).

When implementing or adopting any Government of Ontario IT standards or IT standards updates, ministries, I&IT Clusters and applicable agencies must follow their organization's pre-approved policies and practices for ensuring that adequate change control, change management and risk mitigation mechanisms are in place and employed. For the purposes of this document, any reference to ministries or the Government includes applicable agencies.

2.4.2. Other Applicability

Ministries must ensure that service partners, including other ministries, agencies, jurisdictions, the broader public sector and private sector organizations who use or provide government I&IT resources, are made aware of and adhere to this standard. Reference to this document must be included in contracts and service level agreements where applicable.

2.5. Roles and Responsibilities

2.5.1. Contact Information

Accountable Role:
Title: Head – Cyber Security Strategy, Risk Management & Architecture Branch
Ministry/Cluster: Ministry of Government and Consumer Services
Division: Cyber Security Division

Responsible Organization(s):
Ministry/Cluster: Ministry of Government and Consumer Services
Division: Cyber Security Division
Branch: Cyber Security Strategy, Risk Management & Architecture Branch

Support Role (Editor):
Ministry/Cluster: Ministry of Government Services
Division: Cyber Security Division
Branch: Cyber Security Strategy, Risk Management & Architecture Branch
Job Title: Security Policy and Standards Unit

Name: Tim Dafoe
Phone: 416-327-1260
Email: Tim.Dafoe@ontario.ca

3. Technical Specification

3.1. Disposal of Computerized Devices and Digital Storage Media

3.1.1. Disposal of Functioning Computerized Devices & Digital Storage Media

All functioning computerized devices and digital storage media (e.g., cassettes, tapes and traditional hard drives) must have the entirety of any integrated magnetic storage capacity overwritten using software approved by the Government of Ontario. Simply reformatting or deleting recorded data is not an acceptable sanitization process for any type of storage media.

All functioning optical and semi-conductor storage media (e.g., CDs, DVDs, Blu-Ray discs, solid-state drives, flash memory, USB sticks) must be destroyed in accordance with this standard. Overwriting with third party software is not considered an acceptable sanitization process for semi-conductor and optical storage media. Additionally, if the semi-conductor storage capacity cannot be reliably removed from the device and the device is not vendor serviceable, then the entire device must be destroyed.

3.1.2. Disposal of Non-Functioning Computerized Devices & Digital Storage Media

Non-functioning computerized devices and/or digital storage media (e.g., cassettes, tapes and traditional hard drives) cannot be overwritten but must be crushed at the user's site and then sent for destruction. If on-site crushing is not possible (e.g., by reason of geographical distance) then the device or media must be transferred under a secure chain of custody to the destruction service provider's site where its destruction must be witnessed.

Non-functioning optical and semi-conductor storage media (e.g., CDs, DVDs, Blu-Ray discs, solid-state drives, flash memory, USB sticks) must not be over-written. Over-writing with third party software is not considered an acceptable sanitization process for semi-conductor and optical storage media.[1] The media must be crushed at the user's site, and then sent to the service provider for destruction. If on-site crushing is not possible, then the device or media must be transferred under a secure chain of custody to the destruction service provider's site where its destruction must be witnessed.

Additionally, if the semi-conductor storage capacity cannot be reliably removed from the device and the device is not vendor serviceable, then the entire device must be sent to the destruction service provider's site under secure chain of custody where its destruction must be witnessed.

[1] Reliably Erasing Data from Flash-Based Solid State Drives. Michael Wei, Laura M. Grupp, Frederick E. Spada and Steven Swanson. 9th USENIX Conference on File and Storage Technologies (Fast'11), Feb.2011.

3.1.3. Certification

A certification of completion must be made available to the program manager. The certificate is required to confirm that the sanitization and/or the destruction process was successfully completed.

Certificates must be retained by the program manager for three years for audit purposes.

The completed certificate must contain the following details at a minimum:

- Person's name who requested the sanitization and/or destruction;
- Person's name who witnessed the destruction;
- A description of the device (e.g., USB key, hard drive, smart phone, etc.)
- Any unique identifier (e.g., serial number);
- The date the process was performed;
- The method of destruction (e.g., pulverization, cross-cut shredding);
- The name and address of the service provider who performed the process;
- The signature of the service provider.

3.1.4. Magnetic Storage Media Overwriting Process

Software must be used which can over-write the data/information by writing "1" and "0" data bits on all sectors, blocks, tracks, file allocation tables, and any unused disk space.

To ensure the effectiveness of this method and to overcome a documented track-edge phenomenon, the over-write process must apply three separate over-writing passes to ensure that the data cannot be reconstituted.[2] In accordance with the RCMP over-write criteria, the first pass must write all "1"s or all "0"s to the media; the second pass must write the opposite of the first pass; and, the third pass must apply a pattern that the technician operating the software can read to verify the results. The technician must verify that there are no sectors that were not over-written.

3.1.5. Physical Destruction Process

All computerized devices or digital storage media must be destroyed using a process that absolutely ensures the recorded information on the device or media is rendered totally and permanently inaccessible.

All service providers must be currently registered with Ontario Shared Services – Supply Chain Ontario and be a qualified vendor on the official Government of Ontario vendor of record list.

[2] Track-edge phenomena refers to data remnants that can remain at track edges. The read/write heads do not always pass concentrically over the exact center of the original bit pattern – mostly due to mechanical and electric variables and tolerances. The result is that residual "track edges" of the original bit patterns are left on the disk platter even through the bulk of the track will have been over-written. (*Government of Canada ITSG-06 "Clearing and Declassifying Electronic Data Storage Devices*".).

The following devices or media must be sent directly to the destruction service provider under a secure chain of custody, and the destruction process must be witnessed.

- Any computerized devices, when storage capacity cannot be reliably removed or otherwise sanitized;
- Semi-conductor storage media (e.g., USB memory, flash memory cards, solid-state disk drives);
- Non-functional magnetic storage media (e.g., hard disk drives, tapes and cassettes, diskettes) where the information recorded is high sensitivity and where it cannot be confirmed with certainty that all of the information is encrypted.

3.1.6. Encryption

Information that has been encrypted by a corporately managed OPS service does not need to be over-written. Only the keys used to encrypt and decrypt the encrypted information must be over-written.

If all of the information on any device or media has not been encrypted, then the device or media must be over-written to avoid any risk of unauthorized disclosure of unencrypted information.

Advice to users about how to report a security incident or a lost or stolen device may be found in the associated document "*Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media Guidelines".*

3.1.7. User Support Group

Procedures must be developed and administered within the Infrastructure Technology Services Division (ITS) that support all information users in their responsibility to securely dispose of and/or to report security incidents involving computerized devices and digital storage media.

The procedures must be administered by a first point of contact (FPOC) within ITS. The FPOCs must be positioned to provide all or part of the necessary services required by this standard, and must be sufficiently knowledgeable that they can point users to other service providers or program areas who can offer further direction or guidance if additional services, assistance or information are required.

3.1.8. Lost or Stolen Computerized Devices or Digital Storage Media

Although the Information Security and Privacy Classification Policy requires that encryption be implemented when any personal or high sensitivity information is stored on a device or media, a privacy breach may still happen if those rules are not followed and a device and/or media is lost or stolen.

Users must report any lost or stolen computerized devices and/or digital storage media, (or any part thereof) to their respective managers and to the OPS IT Service Desk immediately.

The OPS IT Service Desk must log the incident and advise the user to report any suspected privacy breach in accordance with the Guide to Managing Privacy and Privacy Breaches. This involves notifying the Program Manager of the area affected by the breach, their ministry FOI Coordinator and the Delegated Decision Maker responsible for the area involved in the privacy breach (notify the Program Area Director if there is no Delegated Decision Maker) . The Service Desk should also provide users with instructions about how to order a replacement computerized device or digital storage media, if required.

Also, if there is a way to remotely delete all government information stored on a missing device (e.g., a Blackberry device), that process must be performed immediately.

3.1.9. Security Incident Reporting

Procedures must be in place within ITS to log and process security incidents reported to them by users. The procedures must document all details about the incident and be escalated to the Cyber Security Operations Centre (CSOC) within Cyber Security Branch at CSOC@Ontario.ca or 416-327-2100.

The following is a table of security incident examples. This table is presented here as a broad sampling of the types of incident reports that the OPS IT Service Desk may be informed of, and need to log.

Security Incident Examples

Security Incident	Description	Impact
Phishing, spear-phishing or whaling	An attempt to obtain sensitive or personal information by sending emails that masquerade, manipulate and/or deceive users into believing the request for information is legitimate. Spear-phishing is more targeted. Perpetrators research their targets or use social engineering techniques and then include some personal information or account details in their request hoping to get even more sensitive information from a user. Whaling aims for high-value information or assets and often targets high-level executives.	Unauthorized access is gained to personal or sensitive information for fraudulent purposes including identity theft, financial loss or invasion of privacy.
Social engineering	Manipulation of trusting individuals by someone who misrepresents him/herself as a person authorized to request information. The perpetrator then uses the information they obtain to gain trust and appear as an “insider” to others in the same organization who may be able to provide additional sensitive information (spear-phishing).	Perpetrators gain unauthorized access to offices, file storage areas or computer rooms to obtain confidential documents, HR information, trade secrets or other organizational intelligence needed to perform more sophisticated thefts or attacks.
Introduction of a virus, malicious code, spying or virtual key-logging software or scare-ware	Introduction of unauthorized software in the form of code, scripts, and active content for malicious intent such as spying or key-stroke logging. Scare-ware uses aggressive advertising practices usually in the form of pop-up windows, to trick users into believing that their computers are infected with malware. Then they try to convince users that purchasing their rogue application will get rid of the virus.	Confidential information such as logon IDs and passwords may be captured by key-logging software and used to gain unauthorized access to IT systems. Network and system response time can degrade and disruptions or complete denial of normal operations can cause loss of employee productivity. Unsaved work or data may be lost as viruses take over IT systems.
Spam	Bulk or junk emails such as advertising, training	Costs multiply as junk

Security Incident	Description	Impact
	opportunities, pharmaceutical products and dating sites flood IT networks and systems.	email takes up expensive storage space on servers. Employee productivity is reduced as networks and systems become unavailable for legitimate users. Technical and human resources are wasted trying to store and manage the increased email load.
Website or system has been breached or hacked	A government website or system has been accessed, modified or defaced by an unknown person.	Results range from simple inconvenience to financial or other hardship to the public who are denied valuable services and information on government Internet sites and other IT systems.
Distributed Denial of service attack (DDOS)	A multitude of compromised systems simultaneously attack a single target to cause denial of service for legitimate users of the targeted system.	Results in flooding IT systems with fake service requests causing degradation or total denial of service to authorized users of targeted systems.
Botnet	A collection of compromised computers connected to the Internet. When a computer is compromised by an attacker, code within the malware commands it to become part of a botnet. The "botmaster" or "bot herder" controls these compromised computers via standards based network protocols such as IRC and http.	Could cause denial of service attack against a remote OPS server or computer.
Port Scanning	An attack that sends client requests to a range of server port addresses on a host, to find and attack an active port.	Perpetrators gain unauthorized access to IT systems by identifying and attacking active ports causing expensive service disruption and denial.
P2P File Sharing	A series of peer-to-peer communication protocols for file sharing.	Results in degradation of bandwidth, and a violation of the terms of

Security Incident	Description	Impact
		service within the OPS.
Inappropriate use of I&IT resources	Use of information technology resources for unacceptable activity.	Consumes costly service space and information technology resources.
Lost or stolen IT assets	Lost or stolen computerized devices or digital storage media bearing government information.	Results in loss of expensive computerized devices or media, and unauthorized disclosure of personal or sensitive information,(unless the device or media has been encrypted).
Compromise of “username and password”.	Knowledge and/or use of a confidential username and password combination by someone other than the owner.	May result in unauthorized access to information and information systems plus embarrassment or inconvenience if emails are sent using the stolen logon ID and password combination.
Network intrusion	An unauthorized security breach of the government system.	Could cause loss of confidentiality, integrity or availability of government information and IT systems.

4. Related Standards

4.1. Impacts to Existing Standards

Identify any Standards that reference or are referenced by this Standard and describe the impact.

GO-IT Standard	Impact	Recommended Action
None	None	None

4.2. Impacts to Existing Environment

Impacted Infrastructure	*Impact*	*Recommended Action*
None	None	None

5. Compliance Requirements

This standard complies with the Government of Ontario's requirements and legislative obligations to maintain the confidentiality and integrity of data/information by restricting access to personal and sensitive information to prevent the creation and subsequent distribution of unauthorized copies and/or manipulated versions.

The following governance documents provide the direction to comply with this standard:

- Management and Use of Information & Information Technology (I&IT) Directive (July 25, 2011);
- Information Security & Privacy Classification Policy (June 2006);
- Information Security & Privacy Classification Operating Procedures (June 2006).

These documents provide additional context for compliance:

- Acceptable Use of Information and Information Technology (I&IT) Resources (March 2011);
- Disposal, Loss and Incident Reporting of Computerized Devices & Digital Storage Media Guidelines (October 1, 2013);
- GO-IT standards 25.x series.

In addition, this standard is issued in compliance with the Management Board of Cabinet Procurement Directive (v1.1, October 2012; s7, ss.14), specifically, "Ministries must remove all confidential, personal and sensitive data from IT equipment prior to disposing of the equipment."

Compliance with this standard is mandatory.

5.1. Implementation and Metrics

The intention of the OCCIO is to advertise and promote this standard as being a mandatory component throughout government. However, in order to effectively manage its implementation, ministries, clusters and applicable agencies are expected to adopt and monitor compliance to this standard.

6. Acknowledgements

Consulted
As part of the development of this standard, the following individuals were included and have been indicated by name. Their opinions were sought by two-way communications and in meetings.

Organization Consulted (Ministry/Cluster)	Division	Branch	Date
Brian Savard	ITS		Jan.17, 2012
David Douglas	IPA	FOI Privacy	Dec. 11, 2011
Mano Pancharatnam	OCCIO	CSB – Security Design	Various
Tim Dafoe	OCCIO	SPEA – Security Policy	Various
Bob Rutherford	OSS	Supply Chain Management	Various
John Lorenc	OCCIO	CSB – CSOC	Various
Michael Harrington	OCCIO	CSB – CSOC	Jan. 18, 2012
Raj Mistry	OCCIO	SPEA – Policy	Feb. 10, 2012
Jim O'Neill	ITS	Desktop Services	May 29, 2012
Sheila Sullivan	ITS	Desktop Services	May 29, 2012
Kevin Varga	OSS	Surplus Asset Management	Various
Bert Umbertinesi	OSS	Surplus Asset Management	Dec.20, 2012
Fil Stabile • Ravilya Rafikova	ITS		Nov. 2012
Rick Provenzano	ITS		Nov. 2012
Frank Grimaldi • Joe Coady	ITS		Nov. 2012
Mark Elliott • Gordon Budd	ITS		Nov. 2012
Zelko Holjevac	ITS		Nov. 2012
Deborah Hendricks	ITS		Nov. 2012
Jennifer Stewart	ITS		Nov. 2012
Wynnann Rose	ITS		Nov. 2012
Conrad Brown	ITS		Nov. 2012
Wade Jones	ITS		Nov. 2012
Jackie Jones	ITS		Nov. 2012
Roland Deutsch • Christopher Brown • Walter Kish • Dave Bourgeois • Leslie Stickie • Vanessa Rodricks	ITS		Nov. 2012
Stephen Milling • Fraser Duff • Evan Woodhead	Health Services I&IT Cluster		Sept. 30, 2013

Committee/Working Group Consulted	Date
ITS Senior Management	March 12, 2012
Architecture Review Board	October 2, 2013

7. Recommended Versioning and/or Change Management

Changes (i.e., all revisions, updates, versioning) to the standard require authorization from the "responsible" organization(s).

Once a determination has been made by the responsible organization to proceed with changes, IT Strategy, Policy and Enterprise Architecture Branch of IT Strategy and Cyber Security as custodians of the I&IT Rules Refresh Plan will coordinate and provide assistance with respect to the approvals process.

The approval process for changes to standards will be determined based on the degree and impact of the change. The degree and impact of changes fall into one of two categories:

Minor updates *- require confirmation from ARB, and communication to stakeholders and ITELC. Changes are noted in the "Document History" section of the standard. Minor updates generally consist of:*

- Editorial corrections (spelling, grammar, references, etc.) made with the intention to eliminate confusion and produce consistent, accurate, and complete work.
- Formatting changes (due to template updates or to improve readability of document).
- Documented organizational changes e.g. renaming of committees, approved transition of committee responsibilities, approved reporting relationship changes.

Standard revisions *- require consultation with stakeholders, ARB endorsement, and ITELC approval. Standard revisions consist of any updates to the I&IT Rules Refresh Plan that are not considered minor and may:*

- represent new standard or significant revision to an existing standard
- represent a major version change to one or more specifications
- impact procurement
- require configuration changes to current solutions
- impact other standards
- respond to legislative, policy or procurement changes

7.1. Publication Details

All approved Government of Ontario IT Standards (GO ITS) are published on the OCCIO Intranet web site. Please indicate with a checkmark below if this standard is also to be published on the public, GO ITS Internet Site.

Standard to be published on both the OPS Intranet and the GO ITS Internet web site (available to the public, vendors etc.)	✓

8. Requirements Levels

Within this document, certain wording conventions are followed. There are precise requirements and obligations associated with the following terms:

Must	This word, or the terms "REQUIRED" or "SHALL", means that the statement is an absolute requirement.
Should	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore the recommendation, but the full implications (e.g., business functionality, security, cost) must be understood and carefully weighed before choosing a different course.

9. Appendices

9.1. Normative References

- Freedom of Information and Protection of Privacy Act (FIPPA) (1990);
- Personal Health Information Protection Act (PHIPA) (2004);
- Archives and Recordkeeping Act (2006).

http://www.e-laws.gov.on.ca/navigation?file=browseStatutes&reset=yes&menu=browse&lang=en
Informative References

Corporate Directives, Policies, Standards and Guidelines

- Corporate Policy on Information and Information Technology (I&IT) Security (June 16, 2011);
- Information Security & Privacy Classification Policy (June 2006);
- Information Security & Privacy Classification Operating Procedures (June 2006);
- Acceptable Use of Information and Information Technology (I&IT) Resources Policy March 2011);
- GO-IT Standard 25.12 Use of Cryptography (November 2012).

http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadPagesByRefId_Content)/cpd2008.10.06.16.24.55.RXL_page?open

- Guidelines for the Protection of Information When Contracting for Services (December 2008);
- Taking the Right Steps - A Guide to Managing Privacy and Privacy Breaches (April 18, 2007);
- Guide to Privacy Impact Assessment (PIA) Process and Tools for the Ontario Public Service (October 2012).

https://intra.sse.gov.on.ca/inetwork/pages/default.aspx

10. Implementation Roles and Responsibilities

Following are the roles and responsibilities of the five major groups primarily responsible for developing, implementing, utilizing, and supporting the internal processes and procedures required to ensure compliance with this standard.

Program Manager

A Program Manager is the ministry employee accountable for the successful operation of the ministry program that creates or collects information held in the custody or under the control of the Government of Ontario.

Program Managers are responsible for:

- Ensuring that all computerized devices and/or digital storage media are sanitized before they are de-provisioned;
- Ensuring that a secure chain of custody exists to protect any non-functioning devices and/or storage media bearing high sensitivity information before it is sent for destruction;
- Obtaining and retaining a copy of the sanitization and/or destruction certificate;
- Ensuring that all employees read and follow the Disposal, Loss and Incident Reporting of Computerized Devices and Digital Storage Media Guidelines.

Infrastructure Technology Services Division

Infrastructure Technology Services (ITS) manages and delivers information and information technology services to the Ontario Public Service, including the OPS IT Service Desk and the Desktop Services program areas.

Infrastructure Technology Services (ITS) is responsible for:

- Establishing and maintaining the procedures and services necessary to help users who need to dispose of, or report security incidents involving computerized devices and/or digital storage media;
- Ensuring that the sensitivity classification level of information involved in a loss or theft of computerized devices or digital storage devices is captured as part of the documented security incident report;
- Ensuring that all vendors of record, including those responsible for securely sanitizing all computerized devices and/or digital storage media, comply with the technical requirements of this standard;
- Ensuring that program managers have access to sanitization and/or destruction certificates of completion;
- Assisting the program manager in their responsibility to ensure a secure chain of custody for computerized devices and digital storage media for destruction;

- Ensuring the OPS IT Service Desk functions as first point of contact for security incident report and device and media disposal/destruction requests.

Ontario Shared Services - Surplus Asset Management

The Ontario Shared Services (OSS) Division manages the OSS Surplus Assets Management Group (SAM) which is responsible, under the Procurement Directive, for secure disposal of surplus moveable assets owned by the Government of Ontario. These assets include, but are not limited to – multi-functional devices not purchased under the current vendor of record, old servers that were purchased outside the ITS process, and hard drives from multi-functional devices which have been leased under the current vendor of record but which are non-functioning and have been removed by the vendor for disposal by the program manager.

OSS SAM is responsible for:

- Managing the destruction of surplus computerized devices and digital storage media as per the Procurement Directive;
- Ensuring that all business partners and vendors of record involved in the destruction of computerized assets and digital storage media bearing government information in the custody and/or under the control of the Government of Ontario, comply with the technical requirements of this standard;
- Ensuring that certificates confirming the completion of the destruction process are provided to all program managers;
- Assisting the program manager in their responsibility to ensure a secure chain of custody for computerized devices and digital storage media prior to destruction;
- Ensuring that all forms related to the disposal or destruction of computerized devices and/or digital storage media include mandatory fields which will confirm the following;
    - The highest sensitivity classification level of any information recorded on the device or media; and,
    - Whether or not the information on the device or media is encrypted.

Cyber Security Branch

The Cyber Security Branch (CSB) of the Ministry of Government Services ensures the needs of a secure e-government environment.

CSB is responsible for:

- Approving all encryption methods for use within the government for the safeguarding of information stored on computerized devices and digital storage media;
- Assisting ITS with the investigation and resolution of security incidents;
- Assisting users to implement security measures and/or strengthen existing security;

IT Strategy, Policy and Enterprise Architecture Branch

The IT Strategy, Policy and Enterprise Architecture Branch (SPEAB) creates and maintains corporate level security policies, standards, guidelines and other related guidance on behalf of the Government of Ontario.

SPEAB is responsible for:

- Communicating this standard and its mandatory requirements OPS-wide;
- Providing interpretation of this standard and advice concerning its contents as required;
- Maintaining this policy and the corresponding guidelines and other related guidance;
- Providing tools to raise awareness about these requirements and help all users meet their obligations to implement them.

11. Glossary

In this document, the following words, terms or expressions mean as follows:

"**control**" means not in the physical possession of data, yet with a legal and/or contractual right to deal with it.

"**compromise**" means to expose, jeopardize or otherwise make vulnerable to danger.

"**custody**" means in the physical possession of the data or information (excluding unsolicited or accidental possession).

"**data**" means any recorded information stored on government issued computerized devices or digital storage media. In all cases, the word "data" also means "information".

"**destruction**" means to render computerized devices or digital storage media unusable by crushing, pulverizing or shredding for the purposes of making the data contained on the device or media permanently inaccessible.

"**information**" means recorded information in any form, in any medium, and at all stages of its life cycle including information created, recorded, transmitted or stored in digital form or in other intangible forms by electronic, magnetic, optical or any other means, but does not include a mechanism or system for creating, sending, receiving, storing or otherwise processing information.

"**integrity**" means the condition of, or requirement for, information that has not been modified or deleted without proper authorization.

"**ministry**' means a ministry of the Government of Ontario and includes all IT clusters and applicable agencies.

"**personal information**" means recorded information about an identifiable individual as per the Freedom of Information and Protection of Privacy Act

"**program manager**" means the program director, their equivalent or delegate, who is ultimately accountable for the successful operation of a program including the confidentiality, integrity, and availability of the recorded information created and/or collected by that program area.

"**safeguard**" means a protective and precautionary security measure intended to prevent a threat agent from causing harm and injury.

"**sanitize**" means a process that makes data permanently inaccessible, and in the context of this document refers to techniques intended to make data permanently inaccessible on magnetic storage media.

"**security breach**" means any act that penetrates the security put in place in order to safeguard data/information.

"**secure chain of custody**" means the unbroken trail of physical security and accountability of a computerized device and/or digital storage media from the time it leaves a secure government site until the moment the data/information on the device or media is either sanitized or the device or media is destroyed.

"**security incident**" any activity that could minimize the security of government data/information or IT systems, or be a prelude to a security breach.

"**semi-conductor**" means an electronic component of a computerized or multi-functional device that exploits the electronic properties of semi-conductor materials.

"**sensitive information**" means information that does not contain any "personal information" as it is defined within the Freedom of Information and Protection of Privacy Act, but must, nonetheless, be secured in accordance with its sensitivity classification level (based on its ability to cause harm and injury if disclosed without authorization).

"**user**" means anyone authorized to access recorded information in the custody or under the control of the Government of Ontario.

"**vendor of record**" means a vendor offering specific goods or services to OPS clients for a defined time period on terms and conditions including pricing, as set out in the governing agreement between the vendor and Her Majesty, in right of Ontario.