Communications Security Establishment
Centre de la sécurité des télécommunications

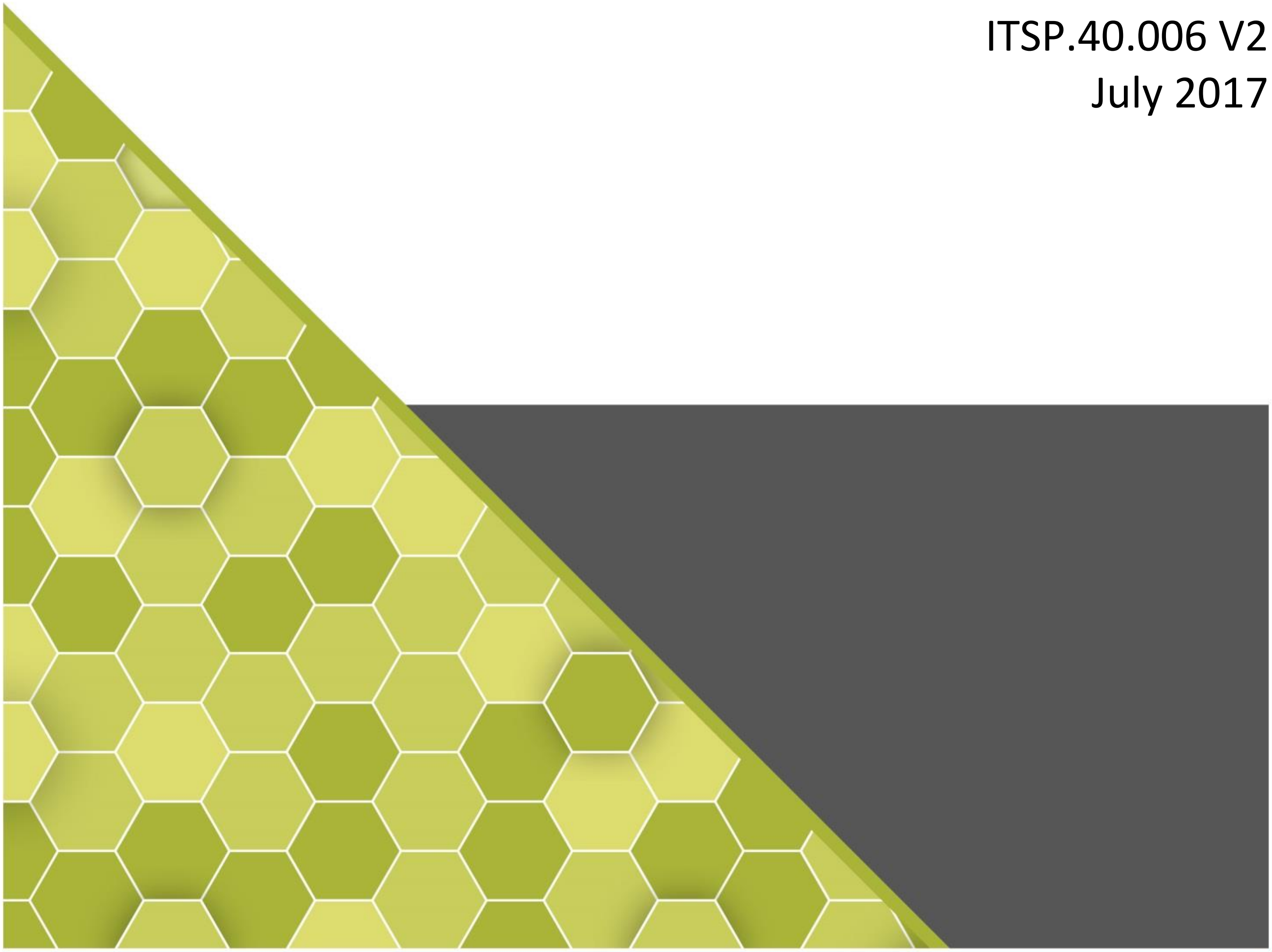
PRACTITIONER SERIES

INFORMATION TECHNOLOGY SECURITY GUIDANCE

IT MEDIA SANITIZATION

ITSP.40.006 V2

July 2017



Canada

FOREWORD

The *ITSP.40.006 v2 IT Media Sanitization* is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

This publication supersedes ITSG-06 Clearing and Declassification of Electronic Data Storage Devices.

Suggestions for amendments should be forwarded through departmental IT security channels to ITS Client Services at CSE.

For further information, please contact CSE by e-mail at ITSclientservices@cse-cst.gc.ca or call (613) 991-7654.

EFFECTIVE DATE

This publication takes effect on (2017-07-07).

[Original signed by]

____

Scott Jones
Deputy Chief IT Security

____

Date

OVERVIEW

The *ITSP.40.006 v2 IT Media Sanitization* publication contains guidance for IT Security for Practitioners and other IT security authorities to help reduce the risk of exploitation of residual data on IT equipment with electronic memory and/or data storage media. This guidance applies to data at all levels of sensitivity. The media to be sanitized may be a discrete item such as a storage device, or it may be part of a network or mobile data processing device.

The normal use of Information Technology (IT) systems and equipment by Government of Canada (GC) departments may result in sensitive data remaining on them at the end of their useful life. This is true even if the user 'deleted' the data. This represents a known vulnerability to departmental data wherein threat actors can exploit life cycled IT media to extract potentially sensitive data that may persist on it, resulting in its unauthorized disclosure.

This guidance incorporates the risk management principles discussed in *ITSG-33 – IT Security Risk Management: A Life cycle Approach* (ITSG-33) [1][1]. With regard to media protection, ITSG-33 describes six security controls ranging from policy to sanitization and transportation. The life cycle process for IT media begins with departmental policies and procedures for the selection, acquisition and management of data processing and storage equipment to meet cost, usability and security requirements. It includes considerations for the eventual end-of-life sanitization and declassification requirements for sensitive data that might reside in the equipment. It concludes with donation or disposal of IT equipment (or destroyed remnants) through departmentally controlled channels to the appropriate organizations that are authorized to receive surplus GC materials.

[1] Numbers in square brackets indicate reference material. A list of references is located the Supporting Content section.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ANNEXES

1 INTRODUCTION

The *ITSP 40.006 v2 – IT Media Sanitization* publication provides guidance on the secure disposal of discrete Media or media components that cannot be easily separated from a system, in order to prevent any data on the Media from being recovered and exploited. Media sanitization refers to the process of converting a single piece of 'sensitive' Media to 'unclassified' so that it will be suitable for reuse or disposal.

The normal business process of the Government of Canada (GC) requires the use of many individual IT Devices or Storage Media (hereafter referred to as **Media**), which is any electronic, electrical, electromechanical equipment designed to store or transmit data that may also then persist on that Media.

This guidance incorporates the risk management principles discussed in ITSG-33 [1] with regard to the life cycle management of Media. ITSP 40.006 V2 was developed in consultation with key stakeholders in government, industry and academia, and is intended for IT Security Managers and IT Security Practitioners responsible for the life cycling of Media that process or store information in GC organizations.

1.1 POLICY DRIVERS

The *Treasury Board Secretariat* (TBS) issues a range of policy instruments designed to establish mandatory requirements and best IT practices for the GC. The following policy instruments are instrumental in strengthening the management of IT assets that may contain sensitive data:

- *Policy on Government Security (PGS)* [2]
- *Operational Security Standard: Management of Information Technology Security (MITS)* [3]
- *Privacy Act* [4]
- *Access to Information Act* [5]
- *Directive on Privacy Practices* [7]
- *Financial Administration Act* [8]
- *Guideline on Acceptable Network and Device Use* [19]
- *Policy on Management of Materiel* [20]

1.2 APPLICABLE ENVIRONMENTS

This guidance specifically applies to the protection of data confidentiality and refers to Media that may contain residual departmental information classified as Low Sensitivity, Medium Sensitivity, or High Sensitivity (defined in section 2.1.1) being life cycled. It provides methods and procedures for the disposal of Media or equipment containing Media for different threat and sensitivity environments.

As part of a risk management framework, it is the department's responsibility to determine the security objectives needed to protect departmental information and services.

1.3 RELATIONSHIP TO THE IT RISK MANAGEMENT PROCESS

This guidance incorporates the risk management principles discussed in ITSG-33 with linkages to the overall life cycle management of Media. The document highlights how the Media sanitization process is an integral component of the overarching departmental program and follows a standard life cycle process as part of the Information System Security Implementation Process (ISSIP) activities in ITSG-33 Annex 2 [1] (Figure 1).

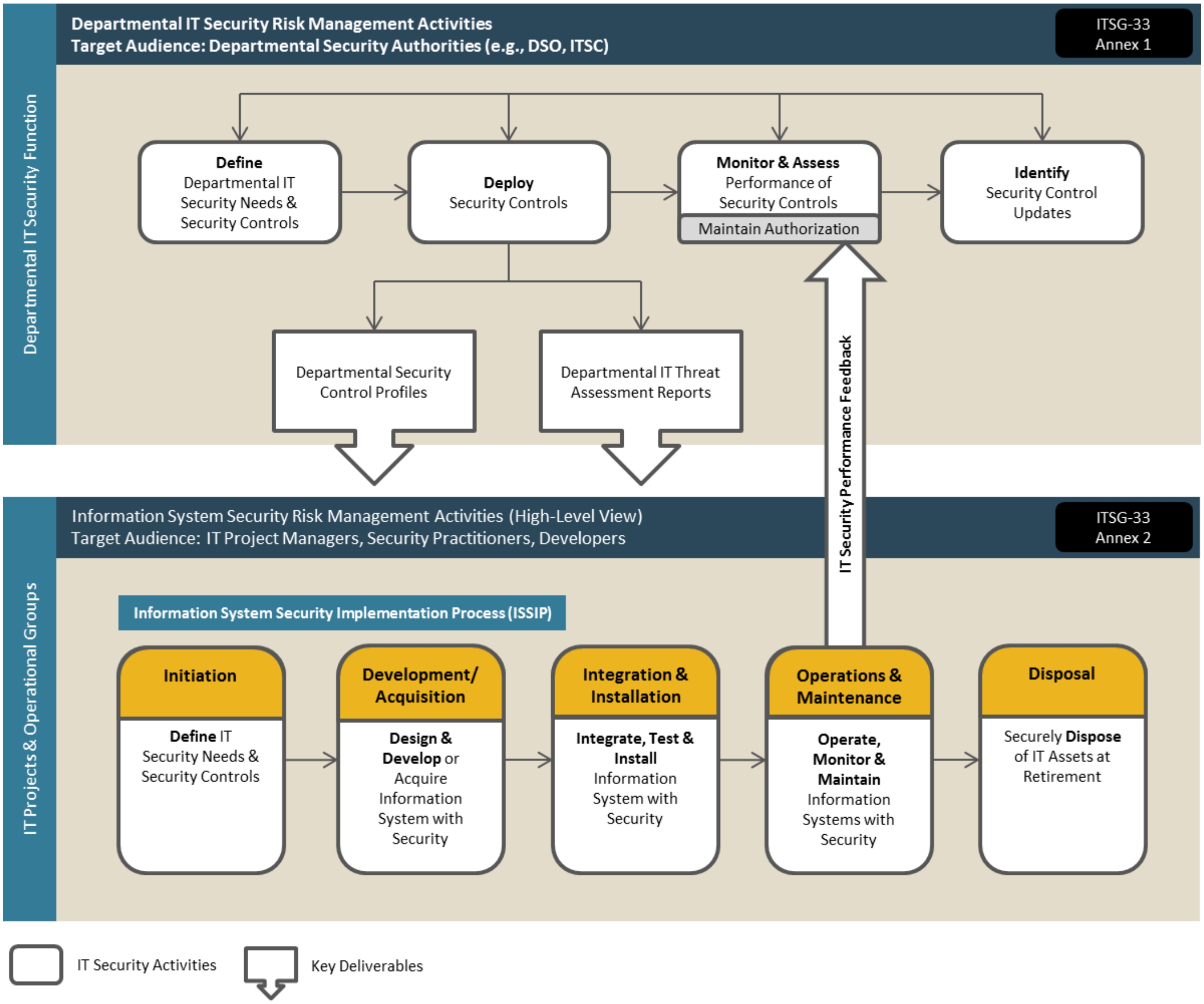

Departmental IT Security Function
Departmental IT Security Risk Management Activities
Target Audience: Departmental Security Authorities (e.g., DSO, ITSC)
ITSG-33 Annex 1
Define Departmental IT Security Needs & Security Controls
Deploy Security Controls
Monitor & Assess Performance of Security Controls
Maintain Authorization
Identify Security Control Updates
Departmental Security Control Profiles
Departmental IT Threat Assessment Reports
IT Security Performance Feedback
IT Projects & Operational Groups
Information System Security Risk Management Activities (High-Level View)
Target Audience: IT Project Managers, Security Practitioners, Developers
ITSG-33 Annex 2
Information System Security Implementation Process (ISSIP)
Initiation
Define IT Security Needs & Security Controls
Development/ Acquisition
Design & Develop or Acquire Information System with Security
Integration & Installation
Integrate, Test & Install Information System with Security
Operations & Maintenance
Operate, Monitor & Maintain Information Systems with Security
Disposal
Securely Dispose of IT Assets at Retirement
IT Security Activities
Key Deliverables

Figure 1 IT Security Risk Management Process

Security risk management for a specific Media device extends beyond the useful life of the device since classified data may persist on the device and require departmental protection or secure disposal.

Departmental level activities are integrated into the organization’s security program to plan, manage, assess and improve the management of IT security-related risks faced by the organization.

Information System level activities are integrated into an information system life cycle to ensure IT security needs of supported business activities are met. It is very important that appropriate security controls are implemented and operating as intended. Continued performance of the implemented security controls is assessed, reported on, and issues are addressed. ITSP.40.006 will need to be considered during the following phases as seen in *Figure 1- IT Security Risk Management Process*:

1. Initiation
2. Development/Acquisition
3. Integration and Installation
4. Operations and Maintenance
5. Disposal

These activities are described in detail in Annex 2 of ITSG-33 [1].

2 SANITIZATION – PROCESS

This section provides an overview of the sanitization process for Media types used in the GC. Detailed explanation about the various sanitization standards is provided in Annex C, and departments should consult the relevant TBS operational security standards and CSE guidelines for more detailed information on the classification and handling of Protected and Classified information.

The normal life cycle of IT equipment usually requires sanitization processes to be followed when the equipment is to be re-provisioned for other users and/or prior to disposal of the equipment, in order to ensure the confidentiality of residual data on the media.

What is Sanitization?

Sanitization is a non-destructive declassifying method to make data non-recoverable while leaving the Media in a re-usable condition in accordance with departmental and GC IT security policy. This ensures the continuing confidentiality of residual data on the Media and minimizes the threat of unauthorized disclosure.

Media sanitization and disposal is done to:

1. Protect the confidentiality of any residual data on the Media
2. Comply with GC policy for the management and disposal of surplus Media

The sanitization process allows for the declassification of data storage media, or equipment containing data storage media, permitting its release outside the department. Historically, Media sanitization consisted of simply erasing the data on the Media or physically destroying the Media. Current Media technology is more difficult to verifiably erase and/or destroy in accordance with departmental IT security policy—this translates into a longer sanitizing effort or higher equipment costs. To reduce sanitization costs, media encryption has emerged as a preferred option, particularly in environments where cryptographic keys can be directly managed or are stored separately from the data storage media.[2]

Encryption throughout the life cycle of the Media facilitates fast and effective sanitization and eases the destruction requirements at the end-of-life of the Media. Departments are advised to routinely encrypt all Media, throughout their life cycle, to protect the ongoing confidentiality of departmental data after Media decommissioning and disposal.

Traditional overwriting and destruction methods may still be used, but they are more effective in combination with underlying encryption to make data non-recoverable.

[2] Categorization of Information and Assets in the GC: Sensitive information is broadly categorized according to federal *Access to Information and Privacy (ATIP) laws* [4], while the specific details for categorizing sensitive information and assets are provided in TBS operational.

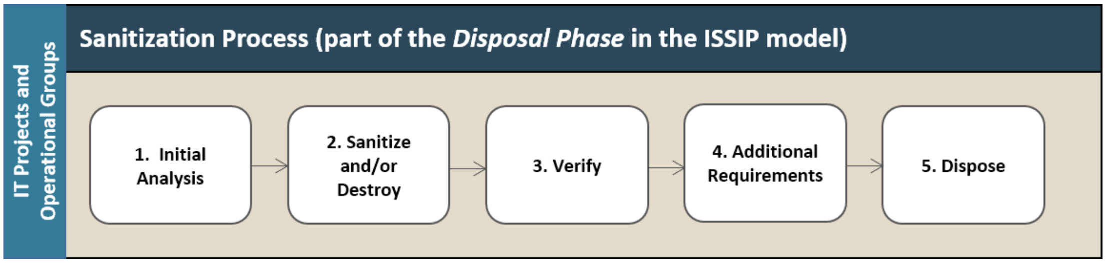

IT Projects and Operational Groups
Sanitization Process (part of the Disposal Phase in the ISSIP model)
1. Initial Analysis
2. Sanitize and/or Destroy
3. Verify
4. Additional Requirements
5. Dispose

Figure 2 Sanitization Process

Figure 2 –Sanitization Process includes the five key steps that can be integrated into a departmental sanitization process, and these steps are prescribed by the ISSIP activities found in ITSG-33 Annex 2 [1], and take place during the Disposal Phase.

The IT Security Media life cycle process, starting with equipment procurement using established procedures, involves safeguarding the Media's security throughout its useful life and includes end-of-life procedures involving reuse or disposal. A complete audit of these steps includes: its withdrawal from active service, an assessment of its data sensitivity, the execution of appropriate sanitization procedures, and finally its reuse or disposal through approved channels.

Figure 3 provides an overview of the IT Media Sanitization process.

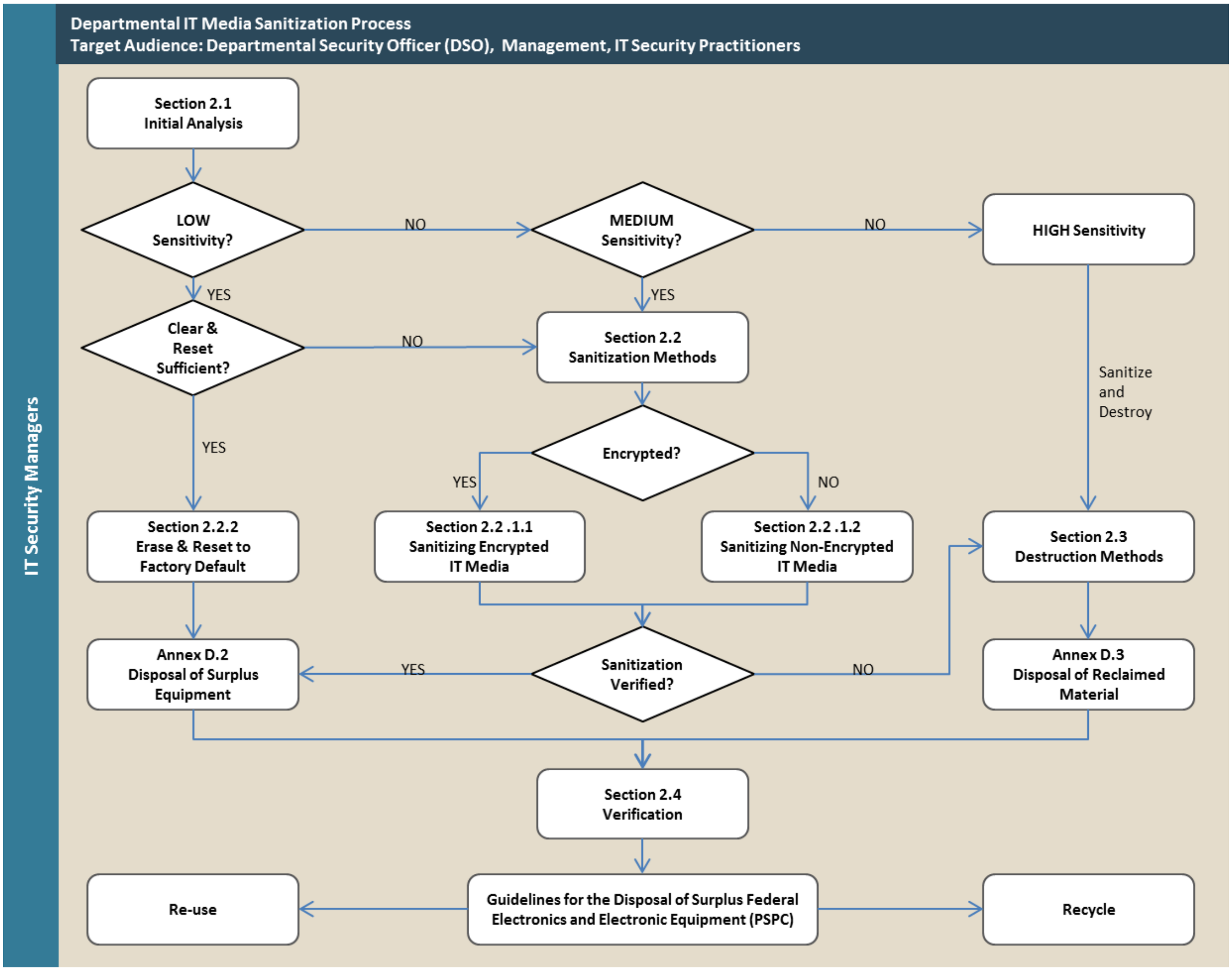

Departmental IT Media Sanitization Process
Target Audience: Departmental Security Officer (DSO), Management, IT Security Practitioners
IT Security Managers
Section 2.1 Initial Analysis
LOW Sensitivity?
NO
MEDIUM Sensitivity?
NO
HIGH Sensitivity
YES
YES
Clear & Reset Sufficient?
NO
Section 2.2 Sanitization Methods
Sanitize and Destroy
YES
Encrypted?
YES
NO
Section 2.2.2 Erase & Reset to Factory Default
Section 2.2 .1.1 Sanitizing Encrypted IT Media
Section 2.2 .1.2 Sanitizing Non-Encrypted IT Media
Section 2.3 Destruction Methods
Annex D.2 Disposal of Surplus Equipment
YES
Sanitization Verified?
NO
Annex D.3 Disposal of Reclaimed Material
Section 2.4 Verification
Re-use
Guidelines for the Disposal of Surplus Federal Electronics and Electronic Equipment (PSPC)
Recycle

Figure 3 IT Media Sanitization & Disposal Process

2.1 INITIAL ANALYSIS

Departments perform an initial analysis to determine the level of sensitivity of the data stored on the department’s Media. Other considerations are the security categorization of the data stored on the Media, the departmental Threat and Risk Assessment (TRA), and available threat information. This analysis allows the department to determine the *type* of sanitization best suited and the preferred *method* to employ to achieve the sanitization goals.

2.1.1 LEVELS OF SENSITIVITY

The clearing and declassification process utilizes a risk-management approach that considers three broad ranges of sensitivity (i.e. low, medium, high) for data that may persist on IT storage media.[3]

2.1.1.1 LOW SENSITIVITY

1. Media has low sensitivity when it contains only Unclassified or Protected A data. This level applies to the majority of networked computers on unclassified systems where files are centrally stored on servers.
2. Low-sensitive Media can be cleared using several methods, including overwriting all stored data. If the device does not support the native overwriting feature found on the hard disk itself (i.e., Advanced Technology Attachment [ATA] Secure Erase [SE]), the clearing is done by using built-in erase features and then resetting the device to factory default conditions.
3. When relying on clearing methods to declassify low-sensitive media, departments should consider the type and quantity of data that may be recovered after clearing and the value of the device for reuse/donation.
4. Destruction may be indicated for media that has no re-use value or that contains significant quantities of low-sensitive data that cannot be adequately cleared.
5. Following the clearing action and the removal of departmental markings or labels, the media should be disposed of through departmentally controlled channels as discussed in *Annex D - Reuse and Disposal of Media*.

2.1.1.2 MEDIUM SENSITIVITY

1. Media has medium sensitivity when it contains any Protected B or Confidential data, even where the media might contain data of lower sensitivities (i.e., low or Unclassified sensitivity).
2. This category may also apply to Media containing some data up to Secret (except when it relates to national security or foreign secret classifications) or may include data up to Protected C, at departmental discretion and in accordance with a Statement of Sensitivity (SoS) or a Threat Risk Assessment (TRA).
3. In the case of medium-sensitive Media that is unencrypted and does not support an acceptable erasure method, or that cannot be satisfactorily verified to confirm sanitization of all user data, a best effort to apply an erasure method should be performed, followed by certain destruction.
4. Medium-sensitive media may be sanitized by logical overwriting[4], digital SE, or Crypto Erase (CE), along with the removal of departmental markings or labels. This is the preferred method of declassifying Media that has value for reuse and recycling as discussed in *Annex D - Reuse and Disposal of Media*.

[3] Categorization of Information and Assets in the GC: Sensitive information is broadly categorized according to federal *Access to Information and Privacy (ATIP) laws* [4], while the specific details for categorizing sensitive information and assets are provided in TBS operational.

[4] Overwrite free space at the logical layer in order to clean residual data at the physical layer.

2.1.1.3 HIGH SENSITIVITY

1. Media has high sensitivity when it contains any data that is classified Top Secret, Secret (especially with respect to national or foreign security and intelligence), or Protected C, or if the Media has ever been attached or connected to a system that contains such data.
2. Highly sensitive media may be declassified by a combination of sanitization (overwrite, SE or CE, and removal of markings or labels) and destruction (using Royal Canadian Mounted Police (RCMP)-approved methods).
3. Simply "erasing" or "destroying" of the media does not ensure that the data cannot be recovered using advanced laboratory techniques.
   - This is due to several factors, including human error, unnoticed equipment problems, and inadequate design of some media to provide verifiable support for erasure methods.
   - In addition, increasing data storage density in combination with physically smaller storage media that make it costlier for destruction equipment to achieve the required secure remnant particle sizes.
   - However, when combined with clearing or sanitization, even incomplete physical destruction will add a layer of complication to an adversary's attempts at recovering any data left on the device (see also *2.5.4 – Interim or Emergency Destruction*).
4. Destruction of the media should be followed by disposal of the remnants through departmentally controlled channels refer to *Annex D - Reuse and Disposal of Media*.

2.1.2 LEVEL OF THREAT

The Media clearing and declassification process is based on a risk-management approach that considers three broad ranges of sensitivity (low, medium, high) for data that may be on the Media.

For the declassification and disposal of Media, the selection of sanitization methods and processes is based on:

1. The security classification assigned to the Media (including its data).
2. The highest Deliberate Threat (Threat $_{\text{Deliberate}}$, or simply Td) value assigned to the Media.

The CSE defines seven categories of Td, each with an increasing level of threat-agent capability (refer to ITSG-33 Annex 2 [1]).

In general, sanitization methods should ensure that:

1. Low-sensitive media will be secure against Td categories 1-2 (e.g. passive or casual adversaries such as "script kiddies", who are generally unsophisticated attackers and are able to use publicly available attack tools, such as scripts).
2. Medium-sensitive media will be secure against Td categories 1-2 and, additionally, 3-5 (e.g. more sophisticated adversaries with moderate resources).
3. High-sensitive media will be secure against the same Td categories as in low and medium-sensitivity with the addition of Td 6-7 (e.g. extremely sophisticated adversaries with abundant resources).

2.2 SANITIZATION METHODS

This section discusses methods of media sanitization. Sanitization is a non-destructive declassifying method to make data non-recoverable while leaving the Media in a re-usable condition in accordance with departmental and GC IT security policy.

Departments should use sanitization to declassify low-to-medium sensitive devices that may have value for reuse within the department or donation to organizations outside the department.

The main sanitization methods are:

1. Erase-and-Reset: Although not a true form of full sanitization it is equivalent in some cases.
2. Overwrite and SE: Traditional processes to remove all data.
3. CE: Process to remove encryption keys in order to make encrypted data unreadable.
4. Degaussing: Destruction of the magnetic coherence of data elements on magnetic IT media.

For additional detailed information, please refer to *Annex B – Sanitization Standards*.

Cryptographic Certificates

Sanitization includes revoking or replacing any cryptographic certificates that may be stored on the device.

2.2.1 SANITIZING OF ENCRYPTED AND NON-ENCRYPTED IT MEDIA

When sanitizing media we are looking at data that could be either encrypted or non-encrypted, which have different implications and as such different procedures to follow.

2.2.1.1 SANITIZING ENCRYPTED IT MEDIA

In order to protect data during its life cycle, departments can institute life cycle encryption processes as mandated by the TBS IT Policy Implementation Notice (ITPIN) 2014-01 *Secure Use of Portable Data Storage Devices within the Government of Canada* [9]. Departments may choose to institute encryption for other Media as well; such encryption can assist departments to provide for continuing protection of the data beyond the life cycle of the media.

A wide range of data storage devices, including Hard Disc Drives (HDD), solid-state drives, and flash-based devices from thumb-drives to smartphones and tablets, are able to support the encryption of all user data that is stored in their memory. Devices encrypted throughout their life cycle using CSE-recommended solutions are easily sanitized and decommissioned.

The CE requires the encryption key or key-encryption key to be stored in a known location (e.g. Trusted Platform Module (TPM) chip, removable hardware token, smartcard) where it can be targeted for erasure and verification. Even in cases where key erasure cannot be positively verified (e.g. because it is stored with the user data in flash-based media that does not include a verifiable key-erase function), CE is still used but should also be followed by clearing all data. This is an additional safeguard against the possibility of forensic recovery of the key following disposal.

The sanitization steps for encrypted Media include:

1. Erasing the key (or re-encrypting with a strong key then erasing the key used for re-encryption.)
2. Clearing the Media as an additional step when key erasure is not verifiable

3. Removing external markings or labels that indicate government ownership or data sensitivity
4. Documenting sanitization steps performed
5. Disposing of the Media through controlled channels

2.2.1.2 SANITIZING NON-ENCRYPTED IT MEDIA

Decommissioning procedures for Media that pre-dates or does not fall within the scope of current departmental encryption policies include:

1. Overwriting or securely erasing the device to overwrite all accessible storage locations with a known pattern
2. Verifying the results by representative sampling with media analysis tools to confirm the presence or absence of any data other than the expected pattern
3. Removing external markings or labels that indicate government ownership or data sensitivity
4. Documenting sanitization steps performed
5. Disposing of end-of-life Media through controlled channels

2.2.2 ERASE AND RESET TO FACTORY DEFAULT

Erasing and Resetting are logical methods that may be available as a product feature in many storage-capable devices (e.g. cell phones, tablets, routers). Normally, the data is not truly erased, or it might not be possible to verify its erasure. Erase and resetting to factory default settings makes the data inaccessible through the device's standard user interface, which serves to protect the data against passive or casual access.

This method may be suitable for sanitizing devices such as network routers, basic cell phones and Voice over Internet Protocol (VolP) phones that contain limited amounts of low-sensitive configuration or user data.

The erase-and-reset steps for selected Media include:

1. Revoking, removing or replacing any cryptographic certificates
2. Using the built-in erase feature to delete pointers to user data or (in the case of encrypted data) to delete cryptographic keys
3. Resetting the device to factory default
4. Removing organization markings and labels
5. Disposing through controlled channels

2.2.3 OVERWRITING AND SECURE ERASE (SE)

Overwriting and digital SE are methods to sanitize data storage media for reuse or disposal. They are used to sanitize media containing low-to-medium sensitive data; they are also used in conjunction with physical destruction for Media containing highly sensitive data.

Overwriting and SE are:

1. Very effective for magnetic media
2. Ineffective or unreliable for many flash-based media (but may be effective for some)
3. Not used for optical media

For magnetic Media, a single overwrite pass is effective for modern HDDs. However, a triple-overwrite routine is recommended for floppy discs and older HDDs (e.g. pre-2001 or less than 15 *Gigabyte* (GB)).

For solid-state drives, a double overwrite pass or a single SE process is recommended – if either function is adequately supported by the design of the particular device, and if the device does not have retired “bad blocks” that may contain sensitive unencrypted data.

Positive verification of results is essential to provide the needed degree of security, especially for medium-sensitive data and solid-state media. Data removal processes must be verified in each case in order to confirm the presence or absence of the expected sanitization data values across a wide sampling of all data-storage areas.[5]

Departments should select overwrite products that are independently evaluated (e.g. Common Criteria), with user feedback features to help assess the success or failure of erasure tasks. Separate tools should be chosen and used for the verification step.

2.2.4 CRYPTO ERASE (CE)

Sanitization of Media using CE is the practice of securely deleting the encryption key used to encrypt the data on the Media. Although the encrypted data remains on the Media, without the encryption key the data on the Media is unrecoverable and the Media is sanitized.

Media sanitization using CE is suitable for sanitizing encrypted HDDs, solid-state drives, and other flash-based storage devices – providing that encryption has been used from the beginning of the Media’s life cycle.[6]

When used for sanitization as follows, CE is equivalent to overwriting and SE, whether it is a self-encrypting drive or has after-market whole-drive encryption:

1. Use of FIPS 140-2 validated cryptography
2. Employ encryption throughout the life cycle of the Media
3. Securely manage the password and encryption key[7]
4. Reliably destroy or securely delete the password and encryption key[8]

An enhanced version, *CE Enhanced,* involves re-encrypting all of the data on the Media with a strong, random, *one-time* key that is securely deleted after use.

To ensure that cryptographic keys can be reliably erased, they should be stored in the Trusted Platform Module (TPM), which is available on fixed platforms such as desktop or laptop computers, or in a removable hardware token or smartcard, as in the case of portable devices such as smartphones and tablets.

[5] Verify overwriting or SE by representative sampling across the media space; a 10% overall coverage across 2,000 areas of memory is a suggested minimum. The US NIST Guidelines for Media Sanitization has additional guidance about the Verification process. [18]

[6] If the device is not encrypted until the end of its life cycle, CE would still be able to sanitize all writeable storage locations but would have no effect on not-previously-encrypted data that may reside in retired “bad blocks”.

[7] CE requires strong passwords and good key management to reduce the risk of password guessing or technical recovery.

[8] Many products do not support the verifiable erasure of the encryption key. If the key can be recovered using forensics methods, then it can permit the data on the device to be decrypted.

Following the CE procedure, an additional step can be followed to clear the Media by overwriting or securely erasing all accessible storage locations. The combination of CE and clearing is particularly useful for flash-based drives because they are more difficult to analyze in order to verify the results of CE or clearing.

2.2.5 SSD FLASH SANITIZATION CONCERNS

Overwriting and SE processes, and related verification tools, work well for HDDs but are not suitable for most flash-based devices such as Solid-State Drives (SSD)[9]; the reasons include:

1. Flash controllers are designed with a wear-levelling feature that automatically redirects any and all data-write commands to under-utilized areas of memory, which consequently inhibits sanitization processes from reaching all memory spaces[10].
2. SSDs may not be designed to execute the Advanced Technology Attachment (ATA) erase commands or to enable overwriting tools to target specific storage locations.
3. Once they have been in use for a period of time, SSDs may contain recoverable data in retired bad blocks that are not accessible to erasing or re-encrypting processes.
4. Flash-based devices may not support direct memory access for verification processes.

In the case of non-encrypted devices, if possible, Departments should use an overwriting or SE process to sanitize all storage locations:

1. Use available tools and the device's native interface to verify the sanitization process and to determine the presence of retired blocks that cannot be sanitized[11] (refer to *Annex C Sanitization Tools*)
2. Before reusing a non-encrypted data storage device that has not verifiably sanitized, the department should assess the risk of loss of privacy or confidentiality of the residual data.

2.2.6 DEGAUSSING

Degaussing is the application of magnetic force to erase all stored data elements on magnetic tape, HDD, floppy discs and magnetic stripe cards.

Solid-State Devices

Solid-state devices (including all flash-based devices and the flash component of hybrid magnetic drives) are not affected by degaussing and cannot be erased using this method.

When properly selected, used, and maintained in accordance with manufacturer’s direction, approved degaussing machines will erase all data on the specific types of magnetic media for which they are rated.[12]

[9] The University of California San Diego (UCSD) Non-Volatile Systems Laboratory (NVSL) has posted research papers on the issues with SSD sanitization. [17]

[10] Flash memory cells have a limited amount of data write cycles that they can support before reaching a saturation failure point. Flash wear-levelling helps extend the overall life of the device by ensuring that data write commands are always distributed evenly among the entire array of storage cells.

[11] A retired block is un-addressable region of memory locations that cannot be cleared.

[12] CSE follows the ratings in the U.S. NSA/CSS Degausser Evaluated Products List. [10]

Magnetic tape and floppy discs require modest levels of degaussing to remove data, and typically can be reused after they have been degaussed; therefore, degaussing is considered a form of non-destructive sanitization for magnetic tape.

Modern HDDs require extremely high levels of degaussing force to completely remove all data. This action damages the drive mechanism beyond repair; consequently, degaussing is considered a form of destruction for modern HDDs.

In the case of extremely sensitive data, sanitizing prior to degaussing, and physical destruction after degaussing, will help mitigate the risk of compromise due to security incidents during transportation to the degaussing site or undetected problems with the degaussing process.

2.3 DESTRUCTION METHODS

After the Media has been sanitized (by overwriting, SE, or CE), the department may determine a need to physically destroy it, either because the sanitization verification step failed or because the Media had previously contained highly sensitive data.

Physical destruction methods commonly available to departments are not recommended as a stand-alone sanitization method. Their effectiveness is becoming less effective due to the advent of Media with smaller and denser physical memory components, combined with technological advancement in the ability to recover non-sanitized data from memory remnants. Destruction should be preceded by best-effort encryption or erasure (to ensure that Media fragments cannot be read), and removal of external labels and identifiers (to reduce unwanted attention to the Media remnants). Media disposal should only be processed through controlled channels (refer to Annex B - Sanitization Standards for RCMP destruction standards for Media).

Destruction is the final step for declassification of Media that:

1. Has no donation or commercial re-use value
2. Contains medium-sensitive data that failed sanitization efforts or sanitization verification
3. Contains high-sensitive data, whether or not it is sanitized

Requirements for Media destruction are based on IT security factors such as data erasure prior to destruction and the assessed level of residual sensitivity following erasure. This also includes environmental factors such as the through-put rate, noise, and harmful dust generation associated with the destruction product being used.

For sensitive Media, destruction should be preceded by sanitization methods to the extent that this is possible. Destruction methods include shredding, disintegration, grinding, crushing, incineration, and degaussing magnetic media.[13] Refer to RCMP *Security Equipment Guide (SEG)* G1-001 [11] for approved destruction products and requirements.

The application of destruction methods is described in the following three sections.

2.3.1 SHREDDING, DISINTEGRATION AND CRUSHING

Office Shredders use a uniform cutting mechanism to reduce material to small pieces of a specific shape and size. Although typically designed to shred paper, some models may also be used to shred thin Media (e.g.

[13] Degaussing has no effect on solid-state media (i.e., SSD, flash) or optical media.

Compact Disc (CD), Digital Video Disc (DVD)). The RCMP approves individual office shredders for specific Media (based on the desired size and shape of shredding residue). [11]

Disintegrators and grinders use a series of rotating blades or hammers within a closed container to reduce material to random sizes and shapes; they typically use a screen on the output side to stop oversize pieces and to return them for more disintegration. The RCMP approves disintegrators, grinders, and hammer-mills based on screen size and resulting particle sizes specific to the type of Media and the levels of data sensitivity. The RCMP also allows for the use of other equipment that uses the approved screen size.

Crushing equipment applies compaction forces to make memory components inaccessible. The crushing jaws may have protuberances or an array of 'teeth' with specific geometries, in order to apply additional crushing force to electronic memory chips within a device that is being destroyed.

2.3.2 INCINERATION AND MELTING

Incineration involves the total destruction of the media. It can apply to any Media at all levels of sensitivity.

Melting is a process whereby material is heated to a temperature that is less than its flash point but high enough to melt it. Melting is an effective process for sanitizing HDDs.

Note

Due to environmental regulations, equipment/services for incineration or melting of mixed materials may not be available.

2.3.3 KNURLING AND SURFACE GRINDING

Knurling and surface grinding are processes that do not destroy the Media completely.

1. *Knurling* involves the use of pressure rolling to deform CD, DVD, or Blu-ray discs to an elongated and slightly curled shape, in order to destroy all data elements (i.e. optical pits and lands). It also deeply scores and/or defaces the surface on both sides of the disc.
2. *Surface Grinding* reduces the information-bearing layer of optical CDs to a fine powder, leaving behind a transparent plastic disc suitable for recycling or disposal.

2.4 VERIFICATION

It is essential that the sanitization of the Media be verified to ensure the confidentiality of departmental data on the Media. There are two types of verification:

- Verify every memory location
- Verify a representative sampling of memory locations

Sanitization effectiveness varies with different Media technology. Legacy sanitization processes may be ineffective and the verification of the sanitization process may be difficult or not possible.

If Media verification cannot be performed, use an alternative sanitization method that can be acceptably verified.

2.5 ADDITIONAL REQUIREMENTS

2.5.1 REMOVAL OF MARKINGS AND LABELS

Media used to store sensitive information requires appropriate labelling according to the PGS. An important part of the sanitization process is the removal of any labelling indicating the sensitivity of the data previously resident on the Media. This reduces unwanted attention to the Media device or its residue following disposal.

2.5.2 DATA RETENTION AND AUDIT REQUIREMENTS

Departments and agencies need to address legal and policy requirements for data retention periods and audit before approving the erasure or destruction of Media. This includes:

1. Legal requirements under federal ATIP laws regarding the retention of public records
2. Policy requirements under relevant TBS information management policies regarding the keeping of government records (refer to *Annex D – Reuse and Disposal of Media*)
3. Security requirements for retention of data that could be required as evidence in investigative or legal proceedings
4. Security audit requirements for retention of records of destruction and disposal of government media, information, and equipment

2.5.3 SANITIZATION TOOLS

Refer to *Annex C – Sanitization Tools* for an explanation of tools and processes used in Media sanitization and verification.

2.5.4 INTERIM OR EMERGENCY DESTRUCTION

Interim and emergency destruction methods involve damaging the Media. Damaging may be routinely used as an interim departmental security measures prior to shipping the Media to a secure destruction facility, or as an emergency security procedure for sensitive Media at imminent risk of acquisition or access by unauthorized parties.

It involves the use of tools (e.g. vice/press, hammer, nail gun, electric drill, focussed high-impact device) to cause localized physical damage to a storage device in order to delay, impede or discourage the recovery of data on the sanitized Media.

Miniature or flash memory devices can be destroyed by repeatedly hitting them with heavy blows from a sledgehammer; while this may not destroy the actual memory chip in the Media, it can effectively impede recovery attempts. Mixing the fragments of the destroyed Media with remnants of non-sensitive IT media can further impede attempts at data reconstruction.

2.5.5 COMMERCIAL DESTRUCTION AND RECYCLING SERVICES

Prior to shipment to an external destruction service provider, departments should sanitize Media or render it non-functional (refer to Section *2.5.4 Interim or Emergency Destruction*). If the Media cannot be sanitized prior to shipment, it needs to be transported and stored in a secure manner commensurate with its sensitivity, followed by a witnessed destruction.

When considering an external destruction service, departments should:

1. Obtain advice regarding selection of a provider, and equipment requirements, from the RCMP Departmental Security Branch (DSB).
2. Confirm facility or contractor security clearance requirements from Public Services and Procurement Canada (PSPC) Canadian Industrial Security Directorate (CISD).
3. Validate contract security clauses, including how the service provider certifies the destruction and disposal of the destroyed materials [12].

2.6 DISPOSAL THROUGH CONTROLLED CHANNELS

The preparation and transport of Media and materials to appropriate disposal centres is governed by departmental policy outlined in *Annex D - Reuse and Disposal of Media*.

Consult the PSPC *Federal Electronic Waste Strategy* and *Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment* [12] for information about the security process and appropriate disposal mechanisms.

2.7 CHAIN OF CUSTODY

GC organizations need to maintain a chain of custody of all Media from decommissioned IT equipment and for all Media when it reaches the end of its useful life and is considered for sanitization and disposal.

Maintaining a chain of custody means that departmental authorities must always maintain chronological documentation showing who has been in possession of the Media, and all actions taken with the media. This process begins when the Media is identified for sanitization, while the Media is being sanitized, during transportation to the authorized donation or disposal site, and up to and including its disposal.

3 SUMMARY

The normal use of Media may result in sensitive data remaining on it at the end of its useful life; this is a known vulnerability to data confidentiality that Departments need to address when disposing of equipment containing IT media.

Media sanitization is a secure and auditable process used to ensure the continuing confidentiality of residual data on the Media. This process is governed by GC policy for the management and disposal of surplus Media and it incorporates the risk management principles discussed in *ITSG-33 – IT Security Risk Management: A Life cycle Approach,* which describes the appropriate security controls.

While some IT products come equipped with built-in erase or reset functions, the built-in sanitization tools should be restricted to Media containing only small amounts of low-sensitive data.

For Media containing more sensitive data, this guidance provides more detailed information to enable the department to provide for the continuing protection of departmental data beyond the life cycle of the media. Media that has been encrypted throughout its life cycle can be easily sanitized.

Non-encrypted Media requires special handling to ensure the confidentiality of residual data – departments may determine that such Media must be physically destroyed to secure the data.

Legal and policy requirements for data retention and audit need to be addressed prior to Media sanitization, and a complete record of sanitization and disposal needs to be maintained by the department.

3.1 CONTACTS AND ASSISTANCE

If your department has identified a requirement for Media sanitization based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

4 SUPPORTING CONTENT

4.1 LIST OF ABBREVIATIONS

Term	Definition
ATA	Advanced Technology Attachment (*Integrated Drive Electronics* (IDE) /ATA)
ATIP	Access to Information and Privacy
CD	Compact Disc
CF	Compact Flash
CFS	Computers for Schools
CSE	Communications Security Establishment
Td	Deliberate Threat
DRAM	Dynamic Random Access Memory
DSO	Departmental Security Officer
DVD	Digital Video Disc
GB	Gigabyte
GC	Government of Canada
GPS	Global Positioning System
HDD	Hard Disc Drive
IT	Information Technology
LBA	Logical Block Addressing
MFD	Multi-Function Device (i.e., printer, copier, fax)
MMC	Multimedia Card
NSA	National Security Agency (US)
NVSL	Non-Volatile Systems Laboratory; University of California San Diego (UCSD)
PGS	Policy on Government Security
PSPC	Public Services and Procurement Canada (formerly PWGSC)
PWGSC	Public Works and Government Services Canada (see also PSPC)
RAM	Random Access Memory
RCMP	Royal Canadian Mounted Police
SATA	Serial ATA (for HDD)
SCSI	Small Computer System Interface
SD	Secure Digital
SE	Secure Erase
SEG	Security Equipment Guide (RCMP)

SPIN	Security Policy Implementation Notice (TBS)
SRAM	Static Random Access Memory
SSD	Solid-State Drive
TBS	Treasury Board Secretariat of Canada
TPM	Trusted Platform Module
TRA	Threat and Risk Assessment
UCSD	University of California San Diego (US)
VoIP	Voice over Internet Protocol

4.2 GLOSSARY

Term	Definition
ATA	*Advanced Technology Attachment* (ATA): a standard type of interface for HDDs (including older Parallel ATA and modern Serial ATA) and other data storage devices.
ATA Secure Erase (SE)	A method to erase HDDs and floppy disks, available through an internal firmware based command on all ATA HDDs since 2001, by overwriting all accessible data sectors with binary 0s.
Clearing	Applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques by overwriting with a new value or, where overwriting is not supported, by using a menu option to reset the device to the factory state. [18]
Crypto Erase (CE)	A sanitization process to erase the encryption key that is used on encrypted Media, in order to make the data unreadable.
Crypto Erase (CE) Enhanced	A sanitization process to re-encrypt previously encrypted Media with a strong random encryption key, followed by erasure of all knowledge of that key, to ensure that the data is unreadable.
Declassify	An administrative step to declare that Media has no remaining information sensitivity after applying prescribed sanitization measures.
Flash Memory	A form of non-volatile memory that is commonly used as data storage in many kinds of consumer electronics and IT equipment (e.g. USB token, SSD, SD).
ISO	International Standards Organization
IT Media	IT memory and data storage media and devices
Non-volatile memory	Data storage or memory components in Media that retain data indefinitely (e.g. HDD, Flash Memory, etc.).
Overwriting	A logical sanitization process to write a fixed data pattern to all user-addressable storage locations of an IT storage medium with the goal of overwriting all previous data.
Redaction	A form of 'data sanitization' that addresses selected data-file elements (not to be confused with 'media sanitization' which must address all data on media).
Sanitizing	Sanitization is a non-destructive declassifying method to make data non-recoverable while leaving the Media in a re-usable condition in accordance with departmental and GC IT security policy. This ensures the continuing confidentiality of residual data on the Media and minimizes the threat of unauthorized disclosure.
Secure Destruction	The destruction of information-bearing media by one or more approved methods that – alone or in

	combination with erasing – destroy the information or sufficiently modify the media so that the information cannot be retrieved.
Secure Erasure	A digital sanitization process that uses tools and industry-standard commands such as ATA security erase (SE) to effectively erase all accessible memory locations of a data storage device, including sector-by-sector overwriting of magnetic media and/or block erasure of solid-state flash media.
Threat	Any potential event or act, deliberate or accidental, that could cause injury or compromise to people, information, assets or services.
Threat Agent	An identifiable organization, individual or type of individual posing deliberate threats, or a specific kind of accidental threat or natural hazard.
TPM	Trusted Platform Module (ISO/IEC 11889). TPM refers to “a computer chip that can securely store... encryption keys” (Trusted Computing Group).
TRA	Threat and Risk Assessment (TRA) is the process of identifying and qualifying threats and risks to IT assets and of implementing or recommending additional security controls to mitigate risks that are deemed unacceptable.
Volatile Memory	Memory elements in Media that lose data after electrical power is removed (e.g. RAM).

4.3 REFERENCES

Number	Reference
1	Communications Security Establishment (CSE). ITSG-33. *IT Security Risk Management: A Life cycle Approach,* December 2012.
2	Treasury Board of Canada Secretariat. *Policy on Government Security (PGS),* 1 July 2009.
3	Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology (MITS),* n.d.
4	*Privacy Act* [online]. [Ottawa]: Department of Justice, 10 September 2015 [cited 29 September, 2015]. Available from: http://laws-lois.justice.gc.ca/eng/acts/p-21/
5	*Access to Information Act* [online]. Ottawa, Ontario, Canada: Department of Justice, 5 April 2016 [cited 1 November 2016]. Available from: http://laws-lois.justice.gc.ca/eng/acts/A-1/
6	Treasury Board of Canada Secretariat. *Policy on Conflict of Interest and Post-Employment*, April 2012.
7	Treasury Board of Canada Secretariat. *Directive on Privacy Practices*, May 2014.
8	*Financial Administration Act* [online]. Ottawa, Ontario, Canada: Department of Justice, 11 October 2016 [cited 1 November 2016]. Available from: http://laws-lois.justice.gc.ca/eng/acts/F-11/
9	Treasury Board of Canada Secretariat. *Secure Use of Portable Data Storage Devices within the Government of Canada (Information Technology Policy Implementation Notice [ITPIN] 2014-01)*, May 2014.
10	National Security Agency, Government of the United States. *Degausser Evaluated Products List*, November 2015
11	Royal Canadian Mounted Police. *Security Equipment Guide (SEG) (G1-001)*, n.d. (Note: Access is restricted to Government of Canada departments and agencies)
12	Public Services and Procurement Canada. *Federal Electronic Waste Strategy (2010), and Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment (v2.0)*, n.d.
13	Communications Security Establishment (CSE). ITSB-112. *Security Considerations for the Use of Removable Media Devices for Protected C and Classified Information*, August 2014.
14	National Cyber Security Centre (NCSC, UK). *Overwriting Tools for Magnetic Media,* February 2016.
15	Treasury Board of Canada Secretariat, *Directive on Disposal of Surplus Materiel*, November 2006.
16	Computers for Schools [online], *Innovation, Science and Economic Development Canada* [online]. Ottawa, Ontario, Canada: Innovation, Science, and Economic Development Canada, 12 May 2015 [cited 1 November 2016]. Available from: https://www.ic.gc.ca/eic/site/cfs-ope.nsf/eng/home
17	Non-Volatile Systems Laboratory, University of California San Diego (UCSD). *Reliably Erasing Data from Flash based Solid-State Drives*, 2011.

18	National Institute of Standards and Technology (NIST). *Special Publication (SP) 800-88 revision 1 (SP800-88r1) Guidelines for Media Sanitization*, December 2014.
19	Treasury Board of Canada Secretariat. *Guideline on Acceptable Network and Device Use*, n.d.
20	Treasury Board of Canada Secretariat. *Policy on Management of Materiel*, November 2006.

Annex A IT Media Devices

A.1 Magnetic Media

Data storage devices that use magnetic media include:

1. Hard Disc Drive (HDD) – including Integrated Drive Electronics/Advanced Technology Attachment (IDE/ATA) and Small Computer System Interface (SCSI)
2. Floppy Disc (FD)
3. Magnetic Tape – including reel-to-reel, cassette, VHS, etc.
4. Storage Area Network (SAN)
5. Zip Disc[14]
6. Magnetic Stripe card

Magnetic media devices are widely used for mass data storage. They are manufactured with a recording medium that is deposited as a thin film on the surface of a base such as a plastic disc or tape. Data is stored in the form of small magnetic regions on the surface film, which is made from special alloys that can strongly retain very small magnetic regions without error for a very long time. The more strongly the recording medium can retain magnetism, the smaller the magnetic regions can be, and the greater the data density.

Magnetic media devices may be sanitized by overwriting all user data with a non-sensitive data pattern, one time (or three times for older HDDs pre-2001). They can also be erased using approved magnetic degaussing products.

A.2 Optical Media

Data storage media that use optical read/write technology include:

1. Compact Disc (CD) – including read-only and writeable or re-writeable variants
2. Digital Video Disc (DVD)
3. Blu-Ray (BD)

Optical discs are commonly used for data, audio and video storage. Data is written to (and read from) optical discs using laser technology. CDs can be sanitized by surface grinding; however, most other optical disks require a more destructive solution such as shredding or disintegration into small pieces.

[14] Zip Disk is a high capacity floppy disk device introduced in 1994 by Iomega Corporation.

A.3 Solid-State Media

Media based on solid-state technology (i.e. electronic semi-conductor) are either volatile (all data is lost when power is off) or non-volatile (all data is retained when power is off).

A.3.1 Volatile

Volatile memory devices include:

1. Random Access Memory (RAM)
2. Static Random Access Memory (SRAM)
3. Dynamic RAM (DRAM)

Volatile memory devices are widely used to provide fast memory in computing and networking equipment. They use semi-conductor technology to contain data. Such devices are volatile in the sense that they cannot retain data in the absence of electrical power. They can be sanitized by the simple act of removing all power, including any internal batteries that might cause the memory to retain data.

Note

If there is doubt concerning the removal of all internal power to RAM in highly sensitive equipment that being decommissioned, consider removing the RAM.

A.3.2 Non-Volatile

Non-volatile memory and data storage devices include:

1. Solid-State Drive (SSD) – in various form factors[15]
2. USB Flash Drive (i.e., thumb drive or memory stick)
3. Secure Digital (SD) card
4. Multimedia Card (MMC)
5. Compact Flash (CF)
6. Communications and Network devices that contain memory and data storage

Non-volatile memory technologies reliably retain all data indefinitely without an external power supply. They are widely used to provide data storage in computers, printers, routers and other networking equipment, as well as portable storage drives, smartphones, tablets, and a wide range of consumer products from cameras to Global Positioning System (GPS) devices.

The main type used today is 'flash' technology, where it may be the main medium for data storage or in some cases may provide supplementary or special-purpose storage such as in hybrid drives.[16]

Other forms of electronic non-volatile memory have also been developed, although they are less likely to be seen in a GC context. Examples include: magneto-optical, magneto-resistive, and nano-magnetic memory technologies.

[15] SSD technology is available in different form factors, including Serial ATA (SATA), mSATA (PCIe and mini PCIe), Disk-on-a-Module (DOM), mini-DIMM, MO-297, etc.

[16] Hybrid drives combine a traditional magnetic HDD with some amount of solid-state memory. They may require additional steps to sanitize the flash component separately from the magnetic disks.

Annex B Sanitization Standards

B.1 Applicability of Sanitization Methods

Sanitization methods, used alone (refer to *2.2 – Sanitization Methods*) or in combination with physical damaging or destruction, may be applied to a wide range of Media and devices.

Table 1 Applicability of Sanitization Methods

Method	Applies to
SANITIZATION	
Erase and Reset	Routers, VoIP phones, fax machines, cellphones, and some other devices
Overwriting and SE	HDD, some Solid-State Drives (SSD), and some other flash-based devices
CE methods	HDD, all SSDs, and other flash-based devices
Degaussing *(non-destructive)**	Magnetic tape, stripe card and floppy disc.
DESTRUCTION	
Shredding, disintegration, grinding and deformation	All Media (using RCMP-approved equipment)
Incineration and Melting	All Media (using facilities approved by Environment Canada)
Knurling and surface grinding	Optical discs
Degaussing (destructive)*	HDD (using degaussing products approved by CSE)

* Degaussing is destructive or non-destructive depending on the degausses' strength/power and the type of magnetic media to be degaussed.

B.2 Sanitization Requirements and Standards

The sanitization requirements tables in the following section are derived from CSE and RCMP endorsed standards for sanitizing and destroying Media to allow its declassification.

Sanitization by overwriting, SE or CE is normally sufficient for low-to-medium sensitive media. However, a Threat and Risk Assessment (TRA) or departmental policy may require follow-up destruction (after erasing) for medium-sensitive media, in some cases. For high-sensitive media, destruction is generally always needed, but prior sanitization will reduce the required degree of destruction by making it extremely difficult for an adversary to recover meaningful data from destroyed remnants.

Note: *Sanitization and verification may improve in the future if IT device manufacturers make advances in the ability of their products to reliably support secure erasure measures.*

In addition, the destruction size specifications shown in these tables may change in the future due to advances in data-storage technologies and available destruction methods. For up-to-date specifications, consult the RCMP *SEG* [11].

Removal of Markings and Labels

Sanitization includes removing any marking and labels from the Media that may indicate GC sensitivity of stored material or prior ownership. Removal of labels and other indicators of GC sensitivity will help prevent unwanted curiosity towards the Media remnants.

B.3 Sanitization Requirements Tables

This section includes a series of Tables that specify the sanitization requirements for different types of Media and devices containing Media.

The following table applies to all data storage media.

Table 2 General Sanitization Requirements for all Data Storage Media

Sensitivity	Sanitization Requirement	Notes
LOW (Unclassified, Official, and Protected A)	1) Use sanitization tools and methods (including overwriting, SE or CE), or use a manufacturer provided Reset or Clearing method 2) Verify the results	A
MEDIUM (Protected B and Confidential)	1) Sanitize (overwrite, SE, or CE-enhanced), and carefully verify the success of the sanitization 2) If unable to sanitize and verify, then follow-up by destroying the media	A,C
HIGH (Top Secret, Secret, and Protected C)	1) Sanitize 2) Destroy	A, B

Notes:

A. **Disposal:** Donate or dispose of sanitized or destroyed media in accordance with the *Guidelines for the Disposal of Federal Surplus Electronic and Electrical Equipment* [12].

B. **Media containing Protected C or Secret:** Data that is designated Protected C may have medium sensitivity for some kinds of security handling, at departmental discretion, in accordance with a statement of sensitivity and a TRA; however, it is normally deemed to have high sensitivity in terms of its physical storage security requirements.

At its discretion, the department can assign a medium sensitivity to Secret data not related to the national interest. Secret data related to the national interest (e.g. defence and intelligence) or that has a foreign or allied government secret classification (e.g. NATOSECRET) is always high sensitivity.

C. **CE:** CE can be used with confidence when the location of the encryption key is known (e.g. stored in TPM chip or in a removable hardware token) and can be targeted for erasure and verification of erasure.

If cryptographic key erasure is not verified, CE should be followed by clearing to reduce the risk that the encryption key (and data) can be recovered through forensic methods.

B.3.1 Optical Media

The following requirements apply to CD, DVD and Blu-Ray optical disks.

Table 3 Sanitization Requirements for Optical Media

Sensitivity	Sanitization Requirement	Notes
All levels	If all contents are file-encrypted, then delete and manage the encryption key prior to destruction.	B
Destruction – *Shredding, Disintegration, Grinding, Melting and Incineration*		
LOW	Cut or break optical disks into pieces and/or severely damage the information-bearing layer of the disc by scraping or scoring.	C
MEDIUM	Reduce discs to small pieces < 40mm^2 (¼ x ¼ “); **or** Grind the surface of the disc to remove the coloured data layer (CDs only).	
HIGH	Reduce discs to small pieces < 10mm^2 (1/8 x 1/8”) or less if the destruction equipment is capable; **or** Grind the disc surface to remove the coloured data layer, leaving only a semi-transparent plastic disc (CDs only).	
Damaging – *Interim and Emergency Destruction*		
All Levels	Damage optical media by scoring the surface and/or break into pieces.	E
Exception		
All Levels	Knurling (high-pressure rolling to stretch and deform optical media surfaces): When using RCMP-approved tools, knurling will make optical discs unreadable, however this method is not approved for declassifying optical media containing highly sensitive information.	N/A

Notes:

A. **Clearing:** N/A

B. **Sanitization:** Sanitization by itself is not practical for optical media that have no reuse value and are easily destroyed

C. **Destruction:** Optical media can clog or damage some destruction equipment. Suitable products to destroy optical media are listed in the RCMP *Security Equipment Guide (SEG)* [11]

D. **Degaussing:** N/A

E. **Damaging:** Inflict severe damage to the media surface (before sending to an approved destruction centre)

F. **Disposal:** N/A

B.3.2 Magnetic Media

The following requirements apply to HDDs, floppy discs, magnetic stripe cards, and magnetic tape (e.g. DAT cartridge, back-up, reel-to-reel, audiocassette, VHS and Beta tape).

Table 4 Sanitization Requirements for Magnetic Media

Sensitivity	Sanitization and Degaussing	Notes
LOW	Sanitize and verify.	A, B, D, F
MEDIUM	Sanitize and carefully verify.	
HIGH	Sanitize, then destroy.	
Destruction – *Shredding, Disintegration, Grinding, Melting and Incineration*		
LOW	If unable to sanitize and verify, then destroy the Media. 1) Discs: reduce to at least two pieces. 2) Tape: reduce to pieces with maximum length < 50mm (2"). 3) Stripe cards: reduce to pieces <140mm^2 (½ x ½ “).	B, C, F
MEDIUM	If unable to sanitize and verify, then destroy... 1) Discs: reduce to pieces (¼ x ¼”). 2) Tape: reduce to pieces (¼”).	
HIGH	Sanitize and then destroy by reducing to pieces (discs <40mm^2 or tape <6mm); **or** If unable to sanitize and verify then reduce to pieces <10mm^2 (1/8 x 1/8”) or smaller.	
Damaging – *Interim and Emergency Destruction*		
All Levels	If unable to overwrite and verify, damage the magnetic discs/platters before sending the media to an approved destruction centre.	E, F

Notes:

A. **Clearing**: Clearing and sanitizing processes for magnetic media are equivalent.

B. **Sanitization**: Overwrite, SE or CE, using validated tools and processes.

C. **Destruction**: See approved destruction products and equivalent disintegrator screen sizes, listed in the RCMP *Security Equipment Guide (SEG)* [11].

D. **Degaussing**: Clear and then degauss. Avoid degaussing low-to-medium sensitive HDDs that have value for reuse or donation. For added assurance, damage or destroy high-sensitive hard-drive platters after degaussing.

E. **Damaging**: Use available tools to inflict damage before transporting the Media to an approved destruction centre (e.g. vise, focused high-impact tool, hammer).

F. **Disposal**: Donate or dispose of sanitized media or destroyed remnants in accordance with the *Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment* [12].

B.3.3 Solid-State and Flash Drives

The following requirements apply to Solid-State Drives (SSD) and USB Flash drives.

Table 5 Sanitization Requirements for Solid-State and Flash Drives

Sensitivity	Sanitization and Degaussing	Notes
LOW	Sanitize if possible **or** Clear and reset.	A,B,F
MEDIUM	Sanitize **and** carefully verify the results. *Non-encrypted USB flash-drives (not cost-effective to sanitize for reuse):* erase and destroy. *Non-encrypted SSD:* erase and destroy if unable to sanitize and verify or if analysis tools reveal that the SSD contains bad or re-allocated sectors that cannot be sanitized.	
HIGH	Sanitize and verify, then destroy.	
Destruction – *Shredding, Disintegration, Grinding, Melting and Incineration*		
LOW	If unsuitable for re-use: Clear, then crush or destroy to pieces < 40mm^{2} in area (e.g. ¼ x¼").	C, F
MEDIUM	If unable to sanitize and verify: Clear, then crush or destroy to pieces < 40mm^{2} in area (e.g. ¼x¼").	
HIGH	Sanitize, then destroy to pieces < 40mm^{2} in area (e.g. ¼ x¼"); or, if unable to sanitize, destroy the device or storage components to particle size < 2mm.	
Damaging – *Interim and Emergency Destruction*		
All Levels	If unable to sanitize, then inflict damage to the storage components before sending the device to an approved destruction centre.	E

Notes:

A. **Clearing**: Clear devices via the built-in erase function for user data or encryption key, then reset to default configuration (and revoke any cryptographic certificates).

B. **Sanitization**: Overwrite, SE or CE, using validated tools and processes.

C. **Destruction**: See destruction products approved for solid-state devices, and equivalent disintegrator screen sizes, listed in the RCMP *Security Equipment Guide (SEG)* [11].

D. **Degaussing**: N/A

E. **Interim**: Use available tools to inflict interim damage before sending to an approved destruction centre (e.g. vise, focused high-impact tool, hammer).

F. **Disposal**: Donate or dispose of sanitized media or destroyed remnants in accordance with federal guidelines [12].

B.3.4 Smartphones and Tablets

The following requirements apply to simple cellphones and smart devices (smartphones and tablets).

Table 6 Sanitization Requirements for Smartphones and Tablets

Sensitivity	Sanitization and Degaussing	Notes
LOW	Clear and reset.	A, B, F
MEDIUM	*Encrypted devices*: sanitize by CE, and verify the key is erased; *BlackBerry and Samsung-Knox based devices*: sanitize by CE, or Clear & Reset; **or** *Other devices*: Clear then destroy.[17]	
HIGH	Clear then destroy (all types).	
Destruction – *Shredding, Disintegration, Grinding, Melting and Incineration*		
LOW	If not suitable for reuse or donation: destroy entire device or storage components to pieces <40mm^2 in area (e.g. ¼ x ¼").	C, F
MEDIUM	If unable to sanitize and verify: destroy entire device or storage components to pieces <40mm2 in area (e.g. ¼ x ¼").	
HIGH	Sanitize, then destroy to pieces <10mm^2 (1/8 x 1/8”); or if unable to sanitize then destroy to particle size < 2mm.	
Damaging – *Interim and Emergency Destruction*		
All Levels	If unable to sanitize, then inflict damage to the screen and interface components before sending the device to an approved destruction centre.	E

Notes:

A. **Clearing:** Clear devices via the built-in erase function for user data or encryption key, then reset to default configuration (and revoke any cryptographic certificates).

B. **Sanitization:** Overwrite, SE or CE, using validated tools and processes.

C. **Destruction:** See destruction products approved for solid-state devices, and equivalent disintegrator screen sizes, listed in the RCMP *SEG* [11].

D. **Degaussing:** N/A

E. **Damaging:** Use available tools to inflict interim damage before transporting the Media to an approved destruction centre (e.g. vise, focused high-impact tool, hammer).

F. **Disposal:** Donate or dispose of sanitized media or destroyed remnants in accordance with the *Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment* [12].

[17] For most smartphones and tablets, the built-in erase function may be suitable for clearing low-sensitive data prior to reuse within the domain or as an interim measure prior to bulk destruction of the device. For BlackBerry and Samsung-Knox based devices, CSE deems their erase-and-reset functions to be reliable to sanitize user data up to and including medium sensitivity.

B.3.5 Network Devices

This applies to Multi-function devices (MFD), Fax machines, VoIP phones, printers, routers and switches.

Table 7 Sanitization Requirements for Network Devices

Sensitivity	Sanitization	Notes
LOW	Fax machines, VoIP phones, Routers and Switches: Clear.	A, F
MEDIUM	MFDs: Sanitize common-criteria evaluated MFDs via the built-in overwrite function; or for non-evaluated MFDs remove and sanitize the storage media. Fax machines: Clear, then destroy. VoIP Phones, Routers and Switches: Clear.	
HIGH	MFDs: Clear, then remove and destroy data storage components. Fax machines: Clear then destroy. VoIP Phones, Routers and Switches: Clear.	
Exception		
All Levels	Volatile Memory (RAM, DRAM, SRAM): sanitize by removing all power for 24 hours (ensure no internal power to the memory).	N/A
Destruction – *Shredding, Disintegration, Grinding, Melting and Incineration*		
LOW	If unsuitable for reuse or donation: Clear, then destroy storage components to pieces <40mm^2 in area (e.g. ¼ x¼").	C, F
MEDIUM	MFDs: if unable to sanitize and verify: Destroy the storage components to pieces <40mm^2 in area (e.g. ¼ x¼").	
HIGH	MFDs: Clear internal storage, then remove and destroy storage components (refer to Annex-B Tables)	
Damaging – *Interim and Emergency Destruction*		
All Levels	Break the device into pieces or inflict severe damage to the storage components, then send the remnants to the approved destruction centre.	E

Notes:

A. **Clearing**: Clear devices via the built-in erase function for user data or encryption key, then reset to default configuration, and revoke cryptographic certificates. This is normally sufficient for network devices that contain configuration data with little or no user data; however, other network devices such as fax machines and MFDs contain user data that require additional measures.

B. **Sanitization**: Overwrite, SE or CE using validated tools and processes.

C. **Destruction**: Destroy storage components or circuit board containing storage, or entire device, using destruction products and equivalent disintegrator screen sizes listed in the RCMP *Security Equipment Guide (SEG)* [11].

D. **Degaussing**: N/A (except for HDDs that have been removed from MFDs).

E. **Damaging**: Use available tools to inflict damage before transporting the Media to an approved destruction centre (e.g. vise, focused high-impact tool, hammer).

F. **Disposal**: Donate or dispose of sanitized media or destroyed remnants in accordance with the *Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment* [12].

Annex C Sanitization Tools

C.1 Overview

For an effective sanitization process the Department needs technical expertise and a clear understanding of the related security issues. The process includes the application of hardware and/or software tools to the Media to sanitize it in order to reduce its sensitivity to 'Unclassified'.

C.1.1 Tools

Departments use sanitization tools that have been evaluated either in-house or by a third party. For example, some hard-drive overwrite products have been evaluated under the *Common Criteria (CC)*; in addition, the Computers for Schools (CFS), which operates under the oversight of the *Department of Innovation, Science and Economic Development* (formerly *Industry Canada*), has assessed a number of different tools for use.

C.1.2 Training

The operators who perform the work should receive training in the proper application of sanitization procedures. The training should provide necessary skill sets and motivate the operators to meet the exacting technical requirements of this important security task.

C.1.3 Issues

For most types of mass data storage devices, a successful overwriting process will make it difficult or impossible for an attacker to recover data, even in the laboratory. However, due to human error or technical problems, the overwrite process may not be successful:

1. Human error may result from improper use of available sanitization and verification tools or from a lack of adherence to proper procedures when using the tools.
2. Technical problems may arise if the device does not properly support the overwriting of stored data.

Other technical problems are evident:

1. Solid-State Drives (SSD) and flash-based memory devices cannot be completely or reliably overwritten because of their normal design for wear-levelling and the possibility that they may not support ATA Erase commands.
2. HDD design permits sanitization by overwriting but the process may take many hours to complete.

In both cases the alternative process of CE can be performed to effectively sanitize the memory by making it unreadable.

C.2 Products and Tools

A variety of products and tools are available from commercial and on-line sources, or may be developed in-house.

C.2.1 Encryption and Crypto Erase (CE)

Media that has been encrypted throughout its life cycle can easily be sanitized at the end of its life cycle by using a CE method:

1. CE involves erasing the cryptographic key from an encrypted media device.
2. CE-Enhanced involves re-encrypting the encrypted media using a strong, random disposable key and then erasing all knowledge of that key.

A prerequisite to using CE methods to sanitize Media is a departmental policy to:

1. Enforce encryption of Media contents from the beginning of the life cycle of the IT equipment that is involved.
2. Use a FIPS 140 validated cryptography solution that also provides for secure disposal of the encryption key.

In addition to supporting encryption and CE, the solutions should be chosen to adhere to:

1. Treasury Board ITPIN 2014-01 – *Secure Use of Portable Data Storage Devices within the Government of Canada* [9].
2. CSE bulletin ITSB-112 – *Security Considerations for the Use of Removable Media Devices for Protected C and Classified Information* (for classified storage) [13].

C.2.2 Overwriting and Secure Erase (SE)

Departments of the GC use *overwriting* and SE software products to sanitize Media (although not all Media can be erased in this manor). Departments should choose overwrite products that provide user feedback to facilitate process auditing. The National Cyber Security Centre (NCSC, UK) security guidance on *Overwriting Tools for Magnetic Media* [14] provides information on the selection of overwrite products.

Overwrite and SE products are designed to use standard ATA Erase commands, which all HDDs support. But only a limited number of SSDs are designed to properly support such commands, and it is technically difficult to determine which ones can or cannot be erased. Consequently, Departments interested in overwriting SSDs should acquire or develop additional sanitization products to enable operators to assess SSD suitability for overwriting and to examine results.

In addition to lack of support for Erase commands, a given SSD may be unsuitable for sanitization if it contains bad or retired sectors. Such sectors cannot be overwritten in any case and can contain data that may be forensically recoverable after disposal. This is not a concern for devices that have been encrypted throughout their life cycle but needs to be considered when sanitizing devices that were not encrypted.

C.2.3 Verification

Departments should use available tools to verify the results of drive encryption and/or clearing.

Solid-state drives normally only support Logical Block Addressing (LBA). Some models also allow direct examination of physical memory locations, this enables the operator to accurately exam and assess Media content and to correlate extensive memory use with the presence of bad blocks. However, in most cases the department uses additional software tools to examine the device`s memory.[18]

C.3 Considerations for Overwriting Hard Disc Drives (HDD)

This table applies to the use of overwrite tools to sanitize HDDs.

Table 8 Considerations for Overwriting HDDs

Considerations	
#1	Procedures should be documented to ensure adequate controls are enforced to prevent unauthorized modification or subversion of the overwrite software.
#2	Overwrite verification should use a separate, validated application. An overwrite verification utility is used specifically to verify that all addressable locations of the HDD have been overwritten with the prescribed pattern.
#3	Prior to overwriting, the actual disc drive capacity should be calculated, i.e. do not assume the drive has the capacity that is reported by the BIOS, FDISK, CHKDSK, or Windows.
#4	Both the Overwrite and Verification applications must report the actual disc capacity. This is because a complete overwrite of all addressable areas of a HDD is only possible if the overwrite application is 'aware' of the actual capacity.
#5	Disc drives containing bad sectors should not be treated as being overwritten, until verification proves otherwise. An essential performance requirement for verification applications is that they be capable of imaging these reported bad sectors, to allow confirmation that they have been fully overwritten.
#6	Overwrite applications should run from a bootable device.
#7	Use of Documented Procedures and/or Checklists should be enforced when using overwrite applications for sensitive protected or classified situations.
#8	In order to verify that the overwrite software is able to erase all parts of the disc, the operator must correctly calculate the actual capacity of the disc and compare that value to the capacity that is reported by the overwrite software.

[18] The United States government has published guidance on the selection and use of Verification tools, in the NIST Guidelines for Media Sanitization SP 800-88 Rev 1 [18].

Annex D Reuse and Disposal of IT Media

This annex outlines the recommended process and procedures for disposal of electronic data storage media that has ongoing value for reuse or recycling.

D.1 Disposal Records and Reporting

Departments address the legal and policy requirements for data retention and audit before approving the erasure or destruction of Media or equipment containing Media. This includes security audit requirements and the need to maintain a complete record of the disposition of government records, information, and equipment.

The following statements advise departments of the need to maintain records of clearing and sanitization. This includes *destruction*, as indicated in the TBS *Security Policy Implementation Notice* (SPIN) 2011-01 and in the PSPC *Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment* [12].

1. The Departmental Security Officer (DSO) is responsible to ensure that sensitive information is securely handled; including all aspects of collection and storage pending sanitization and/or destruction.
2. Departments are responsible for maintaining detailed 'disposition' records of for all surplus Media.

D.2 Disposal of Surplus Equipment

As set out by TBS via the *Directive on Disposal of Surplus Materiel* [15], the GC Computers for Schools (CFS) program has 'first right of refusal' for all surplus IT equipment from federal organizations. [16]

The department first sanitizes Media/equipment donated to the CFS program in accordance with Treasury Board guidelines on IT security [1]. While the onus is on the departments to ensure that all sensitive information has been removed, the CFS workshops perform additional processes to sanitize the Media to ensure it is suitable for release.

Sensitive Media that cannot be verifiably sanitized must be destroyed.

The CFS workshops are monitored by the Department of *Innovation, Science and Economic Development Canada* (Industry Canada) on behalf of the GC.

D.3 Disposal of Reclaimed Material

To identify the appropriate disposal mechanism, departments should consult the *Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment* [12].

Annex E Health and Safety Issues with Destruction Equipment

This annex outlines health and safety issues with destruction equipment. Before deploying in-house media destruction equipment, departments should consider how to reduce potential health and safety issues associated with the use of the equipment.

E.1 Examples of Potential Hazards

It is hazardous to operate destruction equipment not properly vented through a proper dust collection system. For example, cellphone and smartphone components such as batteries and LCDs may catch fire or release toxic materials when shredded. Furthermore, shredding can cause friction and heat to release toxic dust containing lead from circuit board solder connections and beryllium alloys from flexible conductors.

Note

A study commissioned by PSPC (formerly PWGSC) in 2011 revealed elevated levels of arsenic, lead and chromium near cell phone shredder cabinets.[19]

E.2 Recommendations

The RCMP recommends that shredding equipment be located in a well-ventilated room that provides 15-30 air changes per hour; this is similar to commonly accepted criteria for ventilation of underground parking areas.

The PSPC developed the following recommendations after their 2011 study:

1. Ensure that the shredder's internal HEPA filtered exhaust system is operational during shredder use.
2. Ensure that the weather stripping seal is secure and the cabinet door is closed during shredder use.
3. Attempt to seal the paper ‘waste bag’ to minimize dust and particulate accumulations within the cabinet.
4. Wear HEPA filtered respirator and nitrile gloves when accessing the cabinet, replacing the waste bag, or cleaning the cabinet.
5. Departments should use HEPA filtered vacuum cleaners to remove dust and particulate accumulations within the shredder cabinet because conventional vacuum bags cannot capture fine dust particles from metals.

[19] IAQ Sampling Report 19 April 2011 by Greenough Environmental Consulting – Project No. 26037: the findings from an air and wipe sampling program for lead and metal concentrations in the vicinity of a cellphone shredder in a PSPC facility.