Centre de la sécurité des télécommunications
Communications Security Establishment

NON CLASSIFIÉ

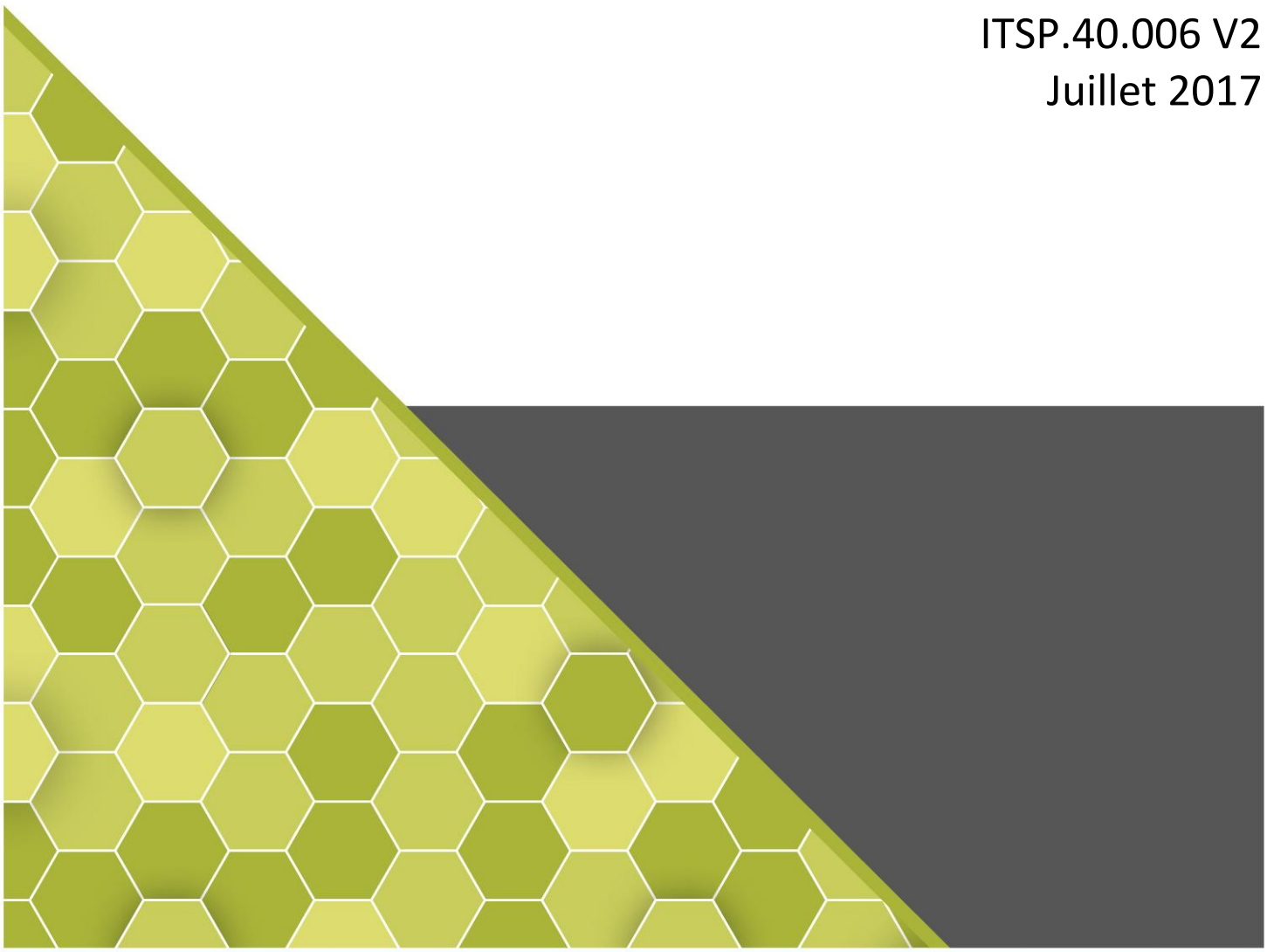
SÉRIE PRATICIENS

CONSEILS EN MATIÈRE DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

NETTOYAGE DES SUPPORTS DE TI

ITSP.40.006 V2

Juillet 2017



Canada

AVANT-PROPOS

L'ITSP.40.006 v2 *Nettoyage des supports de TI* est un document NON CLASSIFIÉ publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST).

Il remplace l'ITSG-06 *Effacement et déclassification des supports d'information électroniques*.

Les propositions de modifications doivent être acheminées aux Services à la clientèle de la Sécurité des TI, du CST, par l'intermédiaire des coordonnateurs de la sécurité des TI du ministère.

Pour obtenir de plus amples renseignements, prière de communiquer avec le CST par courriel, à ITSclientservices@cse-cst.gc.ca, ou par téléphone, au 613-991-7654.

DATE D'ENTRÉE EN VIGUEUR

La présente entre en vigueur le 7 juillet 2017.

[Original signé par]

_____

Scott Jones
Chef adjoint, Sécurité des TI

_____

Date

APERÇU

L'ITSP.40.006 v2 *Nettoyage des supports de TI* fournit des conseils aux praticiens et aux divers responsables de la sécurité des TI dans le but d'atténuer les risques posés par l'exploitation des données résiduelles pouvant subsister dans les dispositifs de TI dotés d'une mémoire électronique ou dans les supports de stockage de données. En outre, ces conseils s'appliquent aux données de tous les niveaux de sensibilité. Un support à nettoyer pourrait être un article discret comme un dispositif de stockage; il pourrait également être une composante réseau ou un dispositif mobile de stockage de données.

À la fin de leur vie utile, l'équipement et les systèmes de technologies de l'information du gouvernement du Canada (GC) peuvent continuer de receler des données sensibles. C'est d'ailleurs le cas même après qu'un utilisateur a effacé toutes les données. Les données présentent ainsi une forme de vulnérabilité qui permettrait à des auteurs de menaces d'exploiter les supports de TI périmés et d'en extraire les données sensibles qui auraient pu subsister, donnant ainsi lieu à des incidents de divulgation non autorisée.

En outre, ces conseils prennent en compte les principes de gestion des risques énoncés dans l'ITSG-33 – *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [1][1]. Pour ce qui a trait à la protection des supports, l'ITSG-33 décrit six contrôles de sécurité visant divers aspects, de la politique au transport en passant par le nettoyage en tant que tel. Dans le cas des supports de TI, le cycle de vie débute par les politiques ministérielles, lesquelles se prolongent dans les procédures de sélection, d'acquisition et de gestion de l'équipement de traitement et de stockage des données, procédures qui doivent répondre aux exigences et aux besoins en matière de coût, d'utilisabilité et de sécurité. En l'occurrence, il tient compte des exigences en matière de nettoyage et de déclassification visant les données sensibles qui auraient pu subsister dans l'équipement. Suivant les mesures de contrôles du ministère, ce cycle se termine avec l'élimination de l'équipement de TI concerné (ou des restes du processus de destruction) ou par le don à des entités autorisées à recevoir du matériel de surplus du GC.

1 Les numéros entre les crochets renvoient à des documents de référence. La liste de ces documents de référence apparaît à la section intitulée Information complémentaire.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ANNEXES

1 INTRODUCTION

L'ITSP 40.006 v2 *Nettoyage des supports de TI* fournit des conseils sur l'élimination sécurisée des supports discrets ou des composants de supports qui ne peuvent pas être aisément séparés de leurs systèmes respectifs. Ces conseils ont pour objet de prévenir l'exploitation de supports périmés qui pourraient être récupérés. Le nettoyage des supports consiste en un processus de conversion de tout support de l'état « sensible » à l'état « non classifié », de façon à le rendre propre à la réutilisation ou à l'élimination.

Les processus opérationnels courants du gouvernement du Canada (GC) requièrent l'utilisation d'un grand nombre de dispositifs de TI ou de supports de stockage (ci-après désignés sous l'appellation « **support** »), ce qui comprend tout équipement électronique, électrique ou électromécanique conçu pour stocker ou transmettre des données susceptibles de subsister dans lesdits dispositifs ou supports.

Les présents conseils prennent en compte les principes de gestion des risques énoncés dans l'ITSG-33 [1] qui ont trait à la gestion du cycle de vie des supports. Préparé en consultation avec des intervenants clés du gouvernement, de l'industrie et des universités, l'ITSP 40.006 V2 s'adresse principalement aux gestionnaires et aux praticiens responsables de la sécurité des TI chargés de superviser le cycle de vie des supports qui sont employés, par les organismes du GC, aux fins de traitement ou de stockage de l'information.

1.1 FACTEURS POLITIQUES

Le *Secrétariat du Conseil du Trésor* (SCT) publie une série d'instruments de politique conçus pour établir les exigences obligatoires et les pratiques exemplaires à respecter au GC. Les instruments de politique énumérés ci-dessous sont des incontournables qui contribuent au resserrement de la gestion des actifs de TI susceptibles de contenir des données sensibles.

- *Politique sur la sécurité du gouvernement (PSG)* [2]
- *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI) [3].
- *Loi sur la protection des renseignements personnels* [4]
- *Loi sur l'accès à l'information* [5]
- *Directive sur les pratiques relatives à la protection de la vie privée* [7]
- *Loi sur la gestion des finances publiques* [8]
- *Ligne directrice sur l'utilisation acceptable des dispositifs et des réseaux* [19]
- *Politique sur la gestion du matériel* [20]

1.2 ENVIRONNEMENTS CONCERNÉS

Les conseils énoncés dans la présente visent à protéger la confidentialité des données et concernent les supports en fin de cycle de vie qui pourraient contenir des résidus d'information ministérielle de divers niveaux : faible sensibilité, moyenne sensibilité et haute sensibilité (voir définitions à la section 2.1.1). On y propose notamment des méthodes et des procédures d'élimination de supports ou d'équipement contentant des supports, et ce, en fonction des contextes de menaces ou des niveaux de sensibilité.

Conformément au cadre de gestion des risques, il incombe à un ministère de définir les objectifs de sécurité qui permettront de protéger son information et ses services ministériels.

1.3 RELATION AVEC LE PROCESSUS DE GESTION DES RISQUES LIÉS À LA TI

Le présent document prescrit l'application des principes de gestion des risques énoncés dans l'ITSG-33 concernant la gestion de l'ensemble du cycle de vie des supports. Il indique également dans quelle mesure le processus de nettoyage des supports constitue une partie intégrale du programme global d'un ministère. De plus, il propose un processus standardisé en matière de gestion du cycle de vie, lequel doit être intégré aux activités décrites dans l'annexe 2 de l'ITSG-33 – Processus d'application de la sécurité dans les systèmes d'information (PASSI) [1] (figure 1).

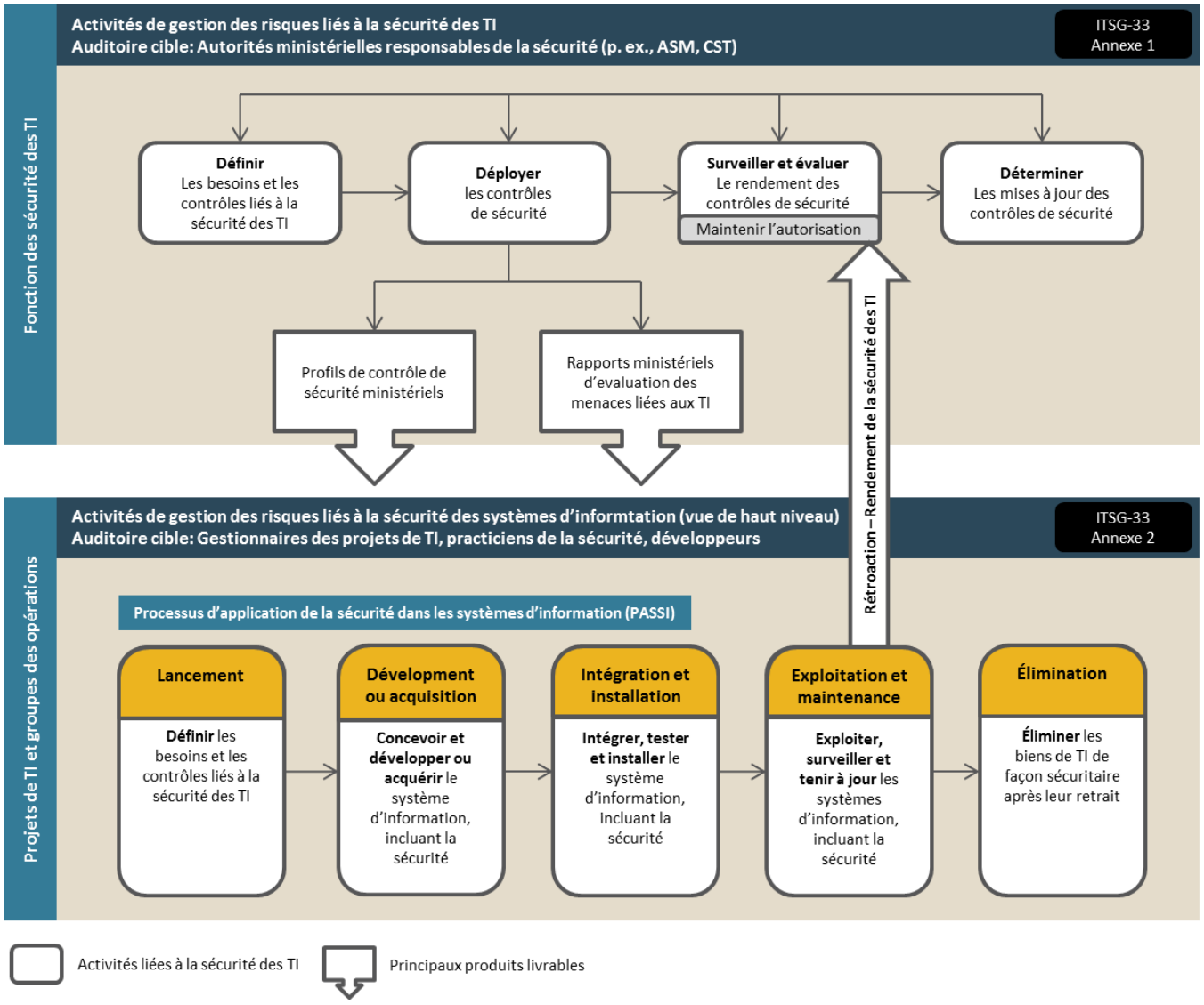


Figure 1 Processus de gestion des risques à la sécurité des TI

Pour chacun des supports concernés, la gestion des risques à la sécurité va bien au-delà de la durée de vie utile du dispositif, puisqu'il est possible que des données classifiées subsistent dans l'une des mémoires, ce qui oblige le ministère concerné à appliquer des mesures de protection ou d'élimination appropriées.

Au niveau du ministère, les activités sont intégrées au programme de sécurité de l'organisation pour planifier, gérer, évaluer et améliorer la gestion des risques à la sécurité des TI.

Les activités visant l'ensemble du système d'information sont intégrées à un cycle de vie de l'information, permettant ainsi de répondre aux besoins opérationnels en matière de sécurité des TI. Il importe que les contrôles de sécurité appropriés soient mis en œuvre et exploités comme prévu. En outre, le rendement des contrôles en place doit faire régulièrement l'objet d'évaluations ainsi que de rapports et, le cas échéant, donner lieu à l'application de correctifs. L'ITSP.40.006 devra être pris en compte pendant les phases énumérées ci-dessous (voir également la *figure 1- Processus de gestion des risques à la sécurité des TI* :

1. préparation
2. développement et acquisition
3. intégration et installation
4. fonctionnement et maintenance
5. élimination

Au reste, ces activités sont décrites en détail à l'annexe 2 de l'ITSG-33 [1].

2 NETTOYAGE – PROCESSUS

La présente section donne un aperçu du processus de nettoyage s'appliquant à divers types de supports employés au GC. L'annexe C apporte certains éclaircissements concernant les normes s'appliquant au nettoyage. En outre, les responsables des ministères devraient consulter les normes du SCT en matière de sécurité opérationnelle ainsi que les lignes directrices du CST pour obtenir de plus amples informations sur la classification et le traitement de l'information protégée ou classifiée.

Par souci de protection de la confidentialité des données résiduelles, le cycle de vie de l'équipement de TI prévoit normalement l'application de procédures de nettoyage lorsque ledit équipement doit être réattribué à de nouveaux utilisateurs ou lorsqu'il doit être éliminé.

Qu'est-ce que le nettoyage?

Le nettoyage est une méthode de déclassification non destructive qui vise à rendre des données irrécupérables tout en veillant à ce que leur support soit réutilisable conformément aux politiques du GC et des ministères en matière de sécurité des TI. Cette pratique permet de garantir la confidentialité des données qui pourraient subsister dans les supports et de minimiser les risques de divulgation non autorisée.

Le nettoyage et l'élimination des supports visent ce qui suit :

1. protéger la confidentialité des données résiduelles qui subsistent dans les supports;
2. répondre aux prescriptions des politiques du GC en matière de gestion et d'élimination des supports de surplus.

Le processus de nettoyage permet la déclassification des supports de stockage de données ou de l'équipement doté de supports de stockage de données, laquelle doit avoir lieu avant toute cessation à des entités autres que le ministère détenteur desdits supports. Habituellement, le nettoyage consistait simplement à effacer les données d'un support ou à détruire ledit support. Avec les technologies actuelles, il est difficile de garantir que l'effacement ou la destruction seront conformes aux politiques ministérielles en matière de sécurité des TI, ce qui se traduit par un alourdissement des procédures et une augmentation du coût de l'équipement requis pour le nettoyage. Pour réduire le coût du nettoyage, on peut désormais avoir recours au chiffrement des supports, particulièrement dans les environnements où les clés cryptographiques peuvent être directement gérées ou sont conservées ailleurs que dans les supports de stockage des données.[2]

Le recours au chiffrement tout au long du cycle de vie d'un support accélère et optimise le processus de nettoyage, et simplifie les exigences visant la destruction des supports en fin de cycle de vie. On conseille aux ministères de chiffrer tous les supports pendant la durée de leur cycle de vie, de façon à protéger la confidentialité des données ministérielles, même après que ces supports ont été déclassés et éliminés.

2 Catégorisation de l'information et des actifs au GC : L'information sensible est classée conformément aux lois régissant l'accès à l'information et la protection des renseignements personnels [4], tandis que le détail de la catégorisation des informations et des actifs sensibles est plutôt fourni dans la documentation opérationnelle du SCT.

Certes, on peut continuer de recourir aux méthodes traditionnelles de réécriture ou de destruction, mais celles-ci s'avèrent plus efficaces lorsqu'elles s'accompagnent de fonctions de chiffrement servant à rendre les données irrécupérables.

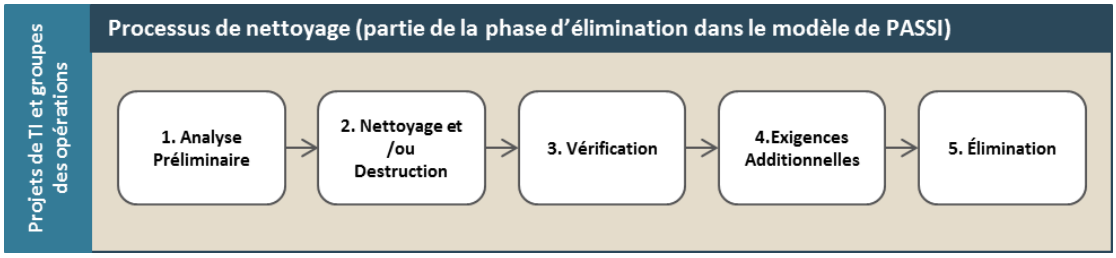


Figure 2 Processus de nettoyage

La Figure 2 – Processus de nettoyage fait état de cinq étapes, lesquelles peuvent être incorporées au processus de nettoyage prescrit par le ministère. Ces étapes sont au nombre des activités du PASSI, qui sont décrites à l'annexe 2 de l'ITSG-33 [1]. En l'occurrence, elles ont lieu pendant la phase d'élimination.

Le cycle de vie des supports de sécurité des TI débute par l'application des procédures d'approvisionnement en équipement. En outre, il prévoit des mesures visant à garantir la sécurité des supports jusqu'à la fin de leur cycle de vie et comprend des procédures menant à la réutilisation ou à l'élimination desdits supports. Une vérification complète visant le déroulement de ces étapes comprend ce qui suit : la mise hors service, une évaluation du niveau de sensibilité des données, l'exécution des mesures appropriées de nettoyage et enfin, la réutilisation ou l'élimination selon les procédures en vigueur.

La figure 3 donne un aperçu du processus de nettoyage des supports de TI.

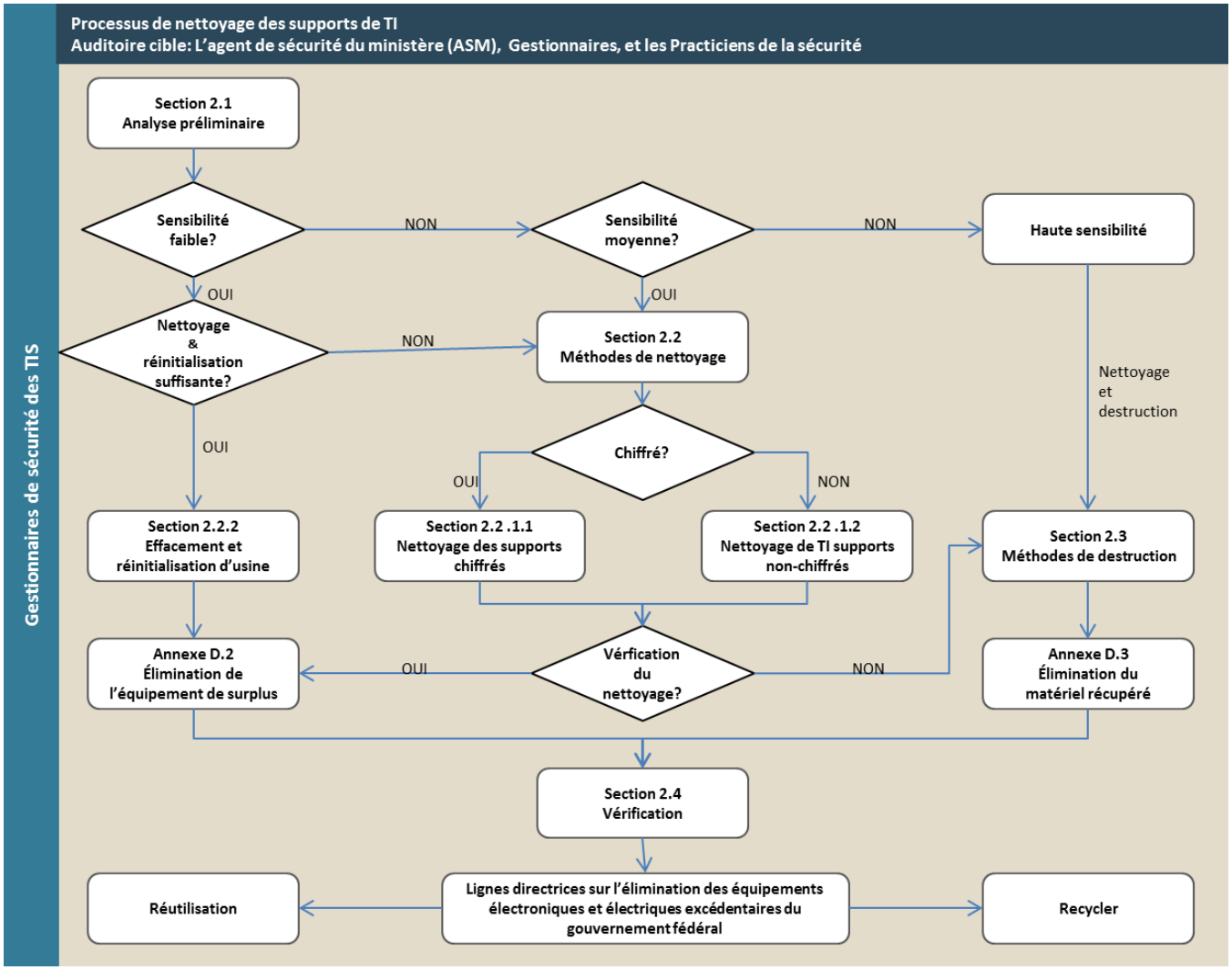


Figure 3 Processus de nettoyage et d'élimination des supports de TI

2.1 ANALYSE PRÉLIMINAIRE

Les ministères procèdent d'abord à une analyse visant à établir le niveau de sensibilité des données stockées dans les supports du ministère. Ce faisant, il faut prendre en compte la catégorisation de sécurité des données enregistrées dans les supports, les stipulations de l'évaluation des menaces et des risques (EMR) ainsi que les divers renseignements dont on dispose sur les menaces éventuelles. Cette analyse permet aux responsables du ministère de déterminer le *type* de nettoyage ainsi que les *méthodes* qu'il conviendra d'appliquer pour respecter les normes en vigueur.

2.1.1 NIVEAUX DE SENSIBILITÉ

Les processus de vidage et de déclassification s'inscrivent dans une approche de gestion des risques qui envisage trois grandes catégories de sensibilité (c.-à-d. faible, moyenne, haute) pour classer les données qui subsistent dans les supports de stockage. [3]

2.1.1.1 FAIBLE SENSIBILITÉ

1. La sensibilité d'un support est considérée comme étant faible lorsque ce support contient des données non classifiées ou protégées. Ce niveau s'applique à la majorité des ordinateurs réseautés dans des systèmes non classifiés, où les fichiers sont conservés dans des serveurs.
2. Les supports à faible sensibilité peuvent être vidés par le recours à diverses méthodes, notamment la réécriture de toutes les données enregistrées. Lorsque le dispositif ne prend pas en charge la fonction de réécriture prévue pour le disque dur (c.-à-d. l'*Advanced Technologie Attachment* [ATA], effacement sécurisé [SE pour *Secure Erase*]), le vidage doit se replier sur la fonction intégrée d'effacement et sur la fonction de réinitialisation d'usine.
3. Lorsqu'il mise sur des méthodes de vidage pour déclassifier un support à faible sensibilité, un ministère devrait prendre en compte le type et le volume des données qui pourraient être récupérées ainsi que la valeur du dispositif susceptible d'être réutilisé ou cédé.
4. La destruction pourrait être désignée dans le cas des supports qui sont non réutilisables ou qui contiennent des volumes importants de données à faible sensibilité qui ne peuvent pas être adéquatement effacées.
5. Suivant les mesures de vidage, et le retrait des marquages et des étiquettes ministérielles, un support devrait être éliminé conformément aux procédures en vigueur, tel qu'il est énoncé à l'annexe D – *Réutilisation et élimination des supports*.

2.1.1.2 MOYENNE SENSIBILITÉ

1. La sensibilité d'un support est considérée comme étant moyenne lorsque ce support contient des données Protégé B ou Confidentiel, et ce, même lorsque ledit support contient des données moins sensibles (c.-à-d. faible ou non classifié).
2. Cette catégorie pourrait également s'appliquer à un support contenant des données allant jusqu'au niveau Secret (sauf lorsque des données concernent la sécurité nationale ou sont classifiées Secret par une entité étrangère). Elle pourrait également, à la discrétion du ministère et conformément à l'énoncé de sensibilité ou à l'EMR, s'appliquer à un support contenant des données allant jusqu'au niveau Protégé C.
3. Lorsque l'on a affaire à un support à moyenne sensibilité qui est chiffré, mais qui ne prend pas en charge un mode admissible de suppression ou dont le nettoyage des données ne peut être acceptablement vérifié, il faut tout de même appliquer la meilleure méthode d'effacement possible puis procéder à l'un des modes de destruction.

3 Catégorisation de l'information et des actifs au GC : L'information sensible est classée conformément aux lois régissant l'accès à l'information et la protection des renseignements personnels [4], tandis que le détail de la catégorisation des informations et des actifs sensibles est plutôt fourni dans la documentation opérationnelle du SCT.

4. Les supports à moyenne sensibilité peuvent être nettoyés par réécriture[4], SE numérique ou effacement cryptographique (CE pour *Crypto Erase*) suivi du retrait des marquages et des étiquettes. Il s'agit là de la méthode à préconiser pour la déclassification des supports susceptibles d'être réutilisés ou recyclés, comme l'indique l'annexe D – *Réutilisation et élimination*.

2.1.1.3 HAUTE SENSIBILITÉ

1. La sensibilité d'un support est considérée comme étant haute lorsque ce support contient des donnée Très Secret, Secret (ayant particulièrement trait à la sécurité nationale ainsi qu'à la sécurité et au renseignement étrangers) ou Protégé C, ou encore lorsque le support a déjà été relié ou connecté à un système contenant de telles données.
2. Les supports à haute sensibilité peuvent être déclassifiés en procédant à la fois au nettoyage (réécriture, SE ou CE, et retrait des marquages ou des étiquettes) et à la destruction (au moyen de méthodes approuvées par la Gendarmerie royale du Canada [GRC]).
3. Le simple recours à « l'effacement » ou à la « destruction » ne suffit pas à garantir que les données ne seront pas récupérées grâce à des technologies de pointe.
   - Ce constat tient à nombre de facteurs, notamment l'erreur humaine, les problèmes d'équipement non relevés ou les supports lacunaires qui n'offrent pas de mécanismes fiables de vérification des effacements.
   - De plus, l'accroissement de la densité de stockage des données associé à l'utilisation de supports de stockages de plus en plus petits fait en sorte qu'il est plus coûteux de broyer le matériel en particules suffisamment petites.
   - Toutefois, lorsqu'elle est combinée à un vidage ou à un nettoyage, une destruction physique, même incomplète, complique grandement la tâche d'un adversaire qui tenterait de récupérer les données subsistant dans le dispositif (voir également la section 2.5.4 – *Destruction : mesures intérimaires et procédures d'urgence)*.
4. La destruction des supports devrait être suivie de l'élimination des restes par des mécanismes contrôlés par le ministère (voir l'annexe D – *Réutilisation et Élimination des supports*).

2.1.2 NIVEAU DE MENACE

Les processus de vidage et de nettoyage des supports suivent une approche axée sur la gestion des risques qui classe les données résiduelles en trois grandes catégories de sensibilité : faible, moyenne, haute.

Pour ce qui a trait à la déclassification et à l'élimination des supports, le choix des procédures et des méthodes de nettoyage repose sur les facteurs suivants :

1. la classification de sécurité attribuée au support (y compris aux données);
2. la plus haute valeur de menace intentionnelle (menace $_{\text{intentionnelle}}$ ou tout simplement Mi) attribuée au support concerné.

4 Réécriture de l'espace libre de la couche logique dans le but de nettoyer les données résiduelles de la couche physique.

Le CST propose une échelle de sept catégories de Mi, chacune représentant divers niveaux de capacité des agents de menaces (voir l'annexe 2 de l'ITSG-33 [1]).

Habituellement, les méthodes de nettoyage devraient permettre ce qui suit :

1. Les supports à faible sensibilité sont sécurisées lorsqu'il s'agit de Mi de catégorie 1 ou 2 (p.ex. les adversaires passifs ou occasionnels comme les « pirates adolescents », lesquels disposent généralement d'outils rudimentaires, notamment des scripts, que l'on peut facilement se procurer dans Internet.
2. Les supports à moyenne sensibilité sont sécurisés lorsqu'il s'agit de Mi de catégorie 1 et 2, à quoi s'ajoutent les catégories 3 et 5 (p. ex. les adversaires plus chevronnés qui disposent de ressources modérément dangereuses).
3. Les supports à haute sensibilité sont sécurisés lorsqu'il s'agit des Mi de catégorie 1, 2, 3, ou 4 à quoi s'ajoutent les catégories 6 et 7 (p. ex. adversaires redoutablement expérimentés disposant de ressources sophistiquées).

2.2 MÉTHODES DE NETTOYAGE

La présente section aborde la question des méthodes de nettoyage des supports. Le nettoyage est une méthode de déclassification non destructive qui vise à rendre des données irrécupérables tout en veillant à ce que leur support soit réutilisable conformément aux politiques du GC et des ministères en matière de sécurité des TI.

Les ministères devraient recourir au nettoyage aux fins de déclassification dans le cas des supports à sensibilité faible à moyenne qui sont susceptibles d'être réutilisés au sein du ministère ou d'être cédés à des organisations non gouvernementales.

Les principales méthodes de nettoyage sont les suivantes :

1. Effacement-réinitialisation : Sans être une méthode de nettoyage en soi, cette solution constitue un équivalent acceptable dans nombre de cas.
2. Réécriture et SE : Procédé courant permettant d'effacer toutes les données.
3. CE : Procédé permettant d'effacer les clés de chiffrement de façon à rendre illisibles les données chiffrées.
4. Démagnétisation : Destruction de la cohérence magnétique des éléments de données enregistrés dans un support magnétique.

Pour obtenir de plus amples informations, prière de consulter l'annexe B – *Normes de nettoyage*.

Certificat cryptographique

Le nettoyage comprend la révocation ou le remplacement de tout certificat cryptographique pouvant résider dans le support.

2.2.1 NETTOYAGE DE SUPPORTS DE TI CHIFFRÉS ET NON CHIFFRÉS

Pendant le nettoyage des supports, on distingue d'abord les données chiffrées de celles qui sont non chiffrées, puisque chacune sera soumise à des procédures particulières en raison de leur nature.

2.2.1.1 NETTOYAGE DES SUPPORTS CHIFFRÉS

Dans le but de protéger les données durant leur cycle de vie, les ministères peuvent instaurer des processus de chiffrement couvrant tout le cycle de vie, tel que le prescrit l'Avis de mise en œuvre de la Politique sur la technologie de l'information (AMPTI) 2014-01 intitulé *Utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada* [9]. Les ministères peuvent opter pour l'instauration du chiffrement pour d'autres supports également; ce chiffrement peut aider les ministères à fournir une protection permanente des données au-delà du cycle de vie des supports.

Un vaste éventail de dispositifs de stockage des données, y compris les disques durs (HDD pour *Hard Disk Drive*), les disques statiques à semiconducteurs (SSD pour *Solid State Drive*) et les disques Flash (clés USB, téléphones intelligents ou tablettes), prennent en charge les fonctions de chiffrement des données utilisateur enregistrées en mémoire. Les dispositifs qui, pendant la durée de leur cycle de vie, ont été soumis au chiffrement grâce à des mécanismes recommandés par le CST sont plus facilement nettoyés et déclassés.

La méthode CE exige que la clé de chiffrement ou la clé de chiffrement de clés soient conservées dans un emplacement connu (p. ex. une puce TPM [*Trusted Platform Module*], un jeton matériel amovible, une carte à puce intelligente) d'où elles pourront être facilement et tangiblement effacées. Même dans les cas où

l'effacement des clés ne peut être positivement prouvé (p. ex. parce qu'elles sont conservées avec les données utilisateur, dans un support Flash qui ne dispose pas d'une fonction vérifiable d'effacement des clés), la méthode CE est tout de même employée, mais devrait néanmoins être suivie d'un vidage de toutes les données. Il s'agit là d'une mesure de protection additionnelle permettant de prévenir les risques que les clés soient récupérées par quelque moyen technologique.

Les étapes de nettoyage visant les supports chiffrés sont les suivantes :

1. suppression de la clé (ou rechiffrement au moyen d'une clé « forte », puis effacement de cette clé forte);
2. vidage du support en guise de mesure de précaution lorsque l'effacement des clés ne peut être vérifié;
3. retrait des marquages ou des étiquettes établissant la propriété du gouvernement ou le niveau de sensibilité des données;
4. enregistrement des étapes de nettoyages exécutées;
5. élimination des supports conformément aux directives et aux normes en vigueur.

2.2.1.2 NETTOYAGE DES SUPPORTS DE TI NON CHIFFRÉS

Les procédures de déclassement des supports qui sont antérieures à l'actuelle politique ministérielle sur le chiffrement ou qui ne sont pas visées par cette politique sont les suivantes :

1. réécriture ou effacement sécurisé d'un support de façon à écraser tous les emplacements de stockage accessibles correspondant à certains motifs;
2. vérification des résultats au moyen d'un échantillonnage représentatif réalisé grâce à des outils d'analyse des supports; cette vérification permet de confirmer la présence ou l'absence de données autres que celles correspondant auxdits motifs;
3. retrait des marquages ou des étiquettes établissant la propriété du gouvernement ou le niveau de sensibilité des données;
4. enregistrement des étapes de nettoyages exécutées;
5. élimination des supports en fin de cycle de vie selon les directives et normes en vigueur.

2.2.2 EFFACEMENT ET RÉINITIALISATION D'USINE

Les méthodes logiques d'effacement et de réinitialisation peuvent être des fonctions propriétaires de certains dispositifs disposant de fonctions de stockage (p. ex. téléphones cellulaires, tablettes, routeurs). Habituellement, les données ne sont pas exactement supprimées; à tout le moins, il est impossible de vérifier si les données ont été intégralement effacées. L'effacement et la réinitialisation d'usine rendent les données inaccessibles depuis l'interface utilisateur du dispositif, laquelle sert à protéger les données contre les accès passifs ou occasionnels.

Cette méthode peut être adéquate pour le nettoyage de dispositifs comme les routeurs, les téléphones cellulaires de base et les téléphones utilisant le protocole Voix sur IP (VoIP pour Voice over *Internet Protocol*) qui contiennent un volume restreint de données d'utilisateur ou de configuration à faible sensibilité.

Les étapes de la méthode d'effacement-réinitialisation applicable à certains médias sont les suivantes :

1. révocation, retrait ou remplacement des certificats cryptographiques;
2. utilisation de la fonction intégrée d'effacement des éléments pointant vers les données utilisateur ou des clés cryptographiques (dans le cas des données chiffrées);
3. réinitialisation d'usine d'un dispositif;
4. retrait des marquages et des étiquettes identifiant l'organisation;

5. élimination selon les directives et normes en vigueur.

2.2.3 RÉÉCRITURE ET EFFACEMENT SÉCURISÉ (SE)

La réécriture et le SE numérique sont des méthodes de nettoyage des supports de stockage aux fins de réutilisation ou d'élimination. Elles sont employées pour nettoyer les supports contenant des données de sensibilité faible à moyenne; elles sont également utilisées conjointement à la destruction physique dans le cas de supports contenant des données à haute sensibilité.

La réécriture et le SE sont :

1. très efficaces pour les supports magnétiques;
2. inefficaces ou inconstants dans le cas de plusieurs supports Flash (mais peuvent tout de même être efficaces dans certains cas);
3. inutilisables pour les supports optiques.

Pour ce qui concerne les supports magnétiques, une seule réécriture est suffisante pour les HDD modernes. Toutefois, une procédure comprenant trois réécritures est recommandée pour les disquettes et les HDD moins récents (p. ex. produits avant 2001 ou comptant un volume de moins de 15 *gigaoctets* [Go]).

Pour ce qui concerne les disques SSD, une double réécriture ou une seule procédure SE est recommandée – si l'une ou l'autre des fonctions est adéquatement prise en charge par le dispositif concerné et pour peu que l'on n'ait pas retiré de ce dispositif des « blocs défectueux » pouvant avoir contenu des données sensibles non chiffrées.

Une vérification positive des résultats est essentielle pour être en mesure de garantir un degré de sécurisation adéquat, particulièrement pour ce qui a trait aux données et aux supports SSD à sensibilité moyenne. Les processus de retrait des données doivent être vérifiés dans chacun des cas, de façon à confirmer la présence ou l'absence des valeurs attendues de nettoyage des données pour l'ensemble d'un large échantillon prélevé dans des zones de stockage réservées aux données. [5]

Les ministères devraient choisir des produits de réécriture qui ont été évalués par une entité indépendante (p. ex. Critères communs) et qui permettent aux utilisateurs de donner de la rétroaction, ce qui permettrait de mieux évaluer le degré d'efficacité des fonctions d'effacement. Des outils distincts devraient être choisis et employés à chacune des étapes de vérification.

2.2.4 EFFACEMENT CRYPTOGRAPHIQUE (CE)

Le nettoyage au moyen du CE est une pratique d'effacement sécurisé des clés de chiffrement employées pour chiffrer les données enregistrées dans un support. Certes, les données restent dans le support, mais sans les clés de chiffrement, ces données demeurent irrécupérables; le support en est ainsi nettoyé.

5 Vérifier la réécriture ou le SE au moyen d'un échantillon prélevé dans tout l'espace du support; une couverture globale de 10 % sur 2 000 zones de mémoire constitue le minimum recommandé. Le document du NIST (États-Unis) *Guidelines for Media Sanitization* fournit des conseils additionnels concernant ce processus de vérification. [18]

Le nettoyage des supports au moyen du CE convient aux HDD chiffrés, aux disques SSD ainsi qu'aux dispositifs de stockage de type Flash – pour peu que le chiffrement ait été utilisé depuis le tout début du cycle de vie du support.[6]

Employée comme suit aux fins de nettoyage, le CE constitue un équivalent au processus de réécriture et SE, qu'il s'agisse d'un support à autochiffrement ou d'un support auquel on a ajouté, après l'acquisition, une fonction de chiffrement global du support :

1. emploi d'une cryptographie homologuée FIPS 140-2;
2. utilisation de chiffrement tout au long du cycle de vie du support;
3. gestion sécurisée du mot de passe et de la clé de chiffrement;[7]
4. destruction vérifiable ou effacement sécurisé du mot de passe et de la clé de chiffrement. [8]

Une version améliorée, *CE Enhanced,* fait appel au rechiffrement de toutes les données dans le support et l'attribution d'une clé forte aléatoire *à utilisation unique* qui est sécuritairement effacée après utilisation.

Pour veiller à ce que les clés cryptographiques soient assurément effacées, celles-ci doivent être stockées dans la *Trusted Platform Module* (TPM), laquelle est disponible dans les plateformes fixes comme les ordinateurs de bureau et les ordinateurs portables, ou dans les jetons matériels amovibles et les cartes à puce intelligente que l'on retrouve dans les dispositifs portables, notamment les téléphones intelligents et les tablettes.

Suivant la procédure de CE, une étape additionnelle peut être ajoutée pour vider le support par la réécriture ou l'effacement sécurisé de toutes les zones de stockage accessibles. La combinaison du CE et du vidage est particulièrement efficace pour les supports Flash, puisque ceux-ci sont particulièrement difficiles à analyser aux fins de vérification des résultats de la CE ou de la procédure de vidage.

2.2.5 PARTICULARITÉS DU NETTOYAGE DES SUPPORTS SSD FLASH

Les processus de réécriture et de SE, ainsi que les outils de vérification connexes, fonctionnent bien pour les HDD, mais ne conviennent pas à la plupart des dispositifs Flash comme les supports SSD[9]. Voici pourquoi :

1. Les contrôleurs Flash sont conçus avec une fonctionnalité de répartition de l'usure qui redirige automatiquement toutes les commandes d'écriture de données de façon à sous-utiliser des zones de mémoire, ce qui a pour effet de freiner le processus de nettoyage et de l'empêcher d'atteindre toutes les zones de la mémoire[10].

---

6 Si le support n'est chiffré qu'à la fin de son cycle de vie, la CE serait tout de même en mesure de nettoyer toutes les zones de stockage inscriptibles, mais n'aurait aucune incidence sur les données qui n'auraient pas été antérieurement chiffrées et qui pourraient subsister dans des « blocs défectueux » retirés.

7 La CE exige des mots de passe forts ainsi qu'une gestion rigoureuse des clés de façon à réduire les risques de découverte du mot de passe ou de récupération technique.

8 De nombreux produits ne prennent pas en charge l'effacement vérifiable de la clé de chiffrement. Si elle peut être récupérée au moyen de technologies d'analyse informatique, cette clé permettra de déchiffrer les données enregistrées dans le support.

9 Le *Non-Volatile Systems Laboratory* (NVSL) de l'University of California San Diego (UCSD) a publié des articles de recherches sur les difficultés posées par le nettoyage des supports SSD. [17]

10 Les cellules de mémoire Flash ne peuvent prendre en charge qu'une quantité restreinte de cycles d'écriture de données avant d'atteindre le point de saturation et, par conséquent, de défaillance. La fonction Flash de répartition de l'usure permet de prolonger la durée de vie d'un dispositif en veillant à ce que les commandes d'écriture de données soient toujours réparties également entre toutes les cellules de stockage.

2. Il conviendra de postuler que les supports SSD ne sont pas conçus pour exécuter des commandes d'effacement *Advanced Technology Attachment* (ATA) ou qu'ils ne permettent pas aux outils de réécriture de cibler certaines zones de stockage.
3. Dès lors qu'ils ont été utilisés pendant un certain temps, les supports SSD peuvent contenir des données récupérables dans des blocs défectueux retirés qui ne sont pas atteignables par les processus d'effacement ou de rechiffrement.
4. Les dispositifs Flash ne prennent probablement pas en charge la fonction d'accès direct à la mémoire aux fins de vérification.

Dans le cas des dispositifs non chiffrés, les ministères devraient, dans la mesure du possible, recourir à la réécriture ou au SE pour nettoyer toutes les zones de stockage.

1. Il conviendra également d'employer les outils et l'interface livrés avec le dispositif pour vérifier le processus de nettoyage et pour déceler la présence de blocs retirés non nettoyables[11] (voir l'annexe C – Outils de nettoyage).
2. Avant de réutiliser un dispositif de stockage de données non chiffrées qui n'a pas encore été assurément nettoyé, un ministère devrait envisager les risques d'atteinte à la confidentialité et à la vie privée que posent les données résiduelles.

2.2.6 DÉMAGNÉTISATION

La démagnétisation consiste en l'application d'une force magnétique pour supprimer toutes les données enregistrées sur une bande magnétique, un HDD, une disquette ou une carte à bande magnétique.

Dispositifs SSD

Les dispositifs SSD (y compris les dispositifs Flash ainsi que les composantes Flash des disques magnétiques hybrides) ne sont pas touchés par la démagnétisation et ne peuvent donc pas être nettoyés par cette méthode.

Ainsi, lorsqu'ils sont judicieusement choisis, convenablement utilisés et entretenus conformément aux directives du fabricant, les appareils de démagnétisation approuvés effacent toutes les données des disques magnétiques pour lesquels ils ont été conçus.[12]

Pour l'effacement des données, les bandes magnétiques et les disquettes nécessitent un degré de magnétisation plutôt faible et peuvent être ultérieurement réutilisées. Ainsi, la démagnétisation est considérée comme une forme de nettoyage non destructive des bandes magnétiques.

Pour ce qui a trait aux HDD modernes, le nettoyage exige une force de démagnétisation considérable. En outre, cette méthode endommage les mécanismes du disque au point de rendre ce dernier inutilisable. Par conséquent, la démagnétisation est plutôt considérée comme un mode de destruction dans le cas des HDD.

Pour ce qui concerne les données extrêmement sensibles, il conviendra de procéder à un nettoyage avant la démagnétisation; il conviendra également de procéder à la destruction après ladite démagnétisation. De cette façon, on atténue les risques de compromission attribuables à des incidents qui surviendraient pendant le

11 Un bloc retiré constitue un ensemble non adressable de zones-mémoires qui ne peut pas être vidé.

12 Le CST applique la liste des codes énumérés dans la liste U.S. NSA/CSS *Degausser Evaluated Products List*. [10]

transport du matériel vers le site de démagnétisation ou à des problèmes de démagnétisation qui pourraient passer inaperçus.

2.3 MÉTHODES DE DESTRUCTION

Après le nettoyage (par réécriture, SE ou CE) d'un support, un ministère peut conclure à la nécessité de procéder à une destruction physique dudit support, soit en raison d'un échec à l'étape de vérification du nettoyage soit parce que le support avait contenu des données hautement sensibles.

Les méthodes de destruction physique couramment employées par les ministères sont de moins en moins efficaces et doivent être combinées à des mesures complémentaires de nettoyage. En effet, la massification du recours à des supports dotés de mémoires toujours plus denses et sans cesse miniaturisés, de même que les percées technologiques donnant lieu au perfectionnement des méthodes de récupérations des données résiduelles incitent à la plus grande prudence. La destruction devrait être précédée de mesures adéquates de chiffrement ou d'effacement (pour prévenir la lecture de fragments du support) et de mesures de retrait des étiquettes et des identifiants externes (pour éviter d'attirer l'attention sur les restes de supports). L'élimination des supports ne doit être exécutée que selon les directives en vigueur (pour en savoir davantage sur les normes de la GRC en matière de nettoyage des supports, voir l'annexe B – *Normes de nettoyage*).

La destruction constitue la dernière étape de déclassification des supports répondant aux critères suivants :

1. ne se prêtent ni au don ni à la réutilisation commerciale;
2. contiennent des données à sensibilité moyenne qui auraient résisté aux mesures de nettoyage ou auraient échoué à l'étape de vérification de nettoyage;
3. contiennent des données à haute sensibilité, qu'il y ait eu nettoyage du support ou non.

La nécessité de détruire un support repose sur des facteurs de sécurité des TI, comme l'effacement des données avant la destruction et le niveau de sensibilité résiduelle suivant l'effacement. Il convient également de prendre en compte certains facteurs environnementaux, comme le débit, le bruit et la formation de poussières nocives, qui sont associés à l'utilisation des outils de destruction.

Pour ce qui a trait aux supports sensibles, la destruction devrait être précédée, dans la mesure du possible, par des mesures de nettoyage. Les mesures de destruction sont généralement les suivantes : le déchiquetage, la désintégration, le broyage, l'écrasement, l'incinération et la démagnétisation des supports magnétiques.[13] Prière de consulter le *Guide d'équipement de sécurité* (GES) G1-001 [11], de la GRC pour en savoir davantage sur les exigences et sur les produits de destruction approuvés.

Les trois sections suivantes portent sur l'application des méthodes de destruction.

2.3.1 DÉCHIQUETAGE, DÉSINTÉGRATION ET BROYAGE

Les déchiqueteuses de bureau emploient un mécanisme de coupe qui sert à réduire un matériau en pièces de formes et de tailles diverses. Les déchiqueteuses sont généralement employées pour détruire le papier, mais elles peuvent également servir à déchiqueter les supports minces, notamment les disques compacts (CD pour *Compact Disc*) et les disques vidéonumériques (DVD pour *Digital Video Disc*). La GRC approuve diverses déchiqueteuses selon les supports à traiter (en fonction de la taille et de la forme des résidus de déchiquetage). [11]

13 La démagnétisation n'a aucun effet sur les supports statiques à semiconducteurs (c.-à-d. SSD, Flash) ou sur les supports optiques.

Les dispositifs de désintégration et de broyage emploient un ensemble de lames ou de marteaux rotatifs qui réduisent le matériel en fragments de formes et de tailles diverses. Au point de sortie, ces dispositifs sont généralement munis d'écrans déviateurs qui ramènent les pièces de trop grande taille pour qu'elles soient traitées de nouveau. La GRC approuve les désintégrateurs, les broyeurs et les broyeurs à marteaux en fonction de facteurs comme la taille de l'écran déviateur, la taille des fragments, le type de support et le niveau de sensibilité des données. La GRC permet également l'utilisation d'autres types d'équipement dotés d'écrans approuvés.

Le broyage de l'équipement consiste en l'application d'une force de compactage dans le but de rendre les composants de mémoire inaccessibles. Les mâchoires de broyage peuvent avoir des pointes ou des « dents » de formes particulières qui servent à appliquer une force de broyage additionnelle aux puces-mémoire électroniques d'un dispositif en cours de destruction.

2.3.2 INCINÉRATION ET FUSION

L'incinération mène à la destruction totale d'un support. On peut y avoir recours pour la destruction de supports de tout niveau de sensibilité.

La fusion est un processus par lequel le matériel est porté à une température inférieure au point d'inflammabilité des matériaux, mais assez élevée pour en causer la fonte. La fusion est une méthode efficace de nettoyage des HDD.

Nota

Compte tenu des règlements en matière d'environnement, il se peut que l'équipement et les services d'incinération ou de fusion des matériaux composés ne soient pas disponibles.

2.3.3 MEULAGE DES SURFACES ET MOLETAGE

Le meulage des surfaces et le moletage sont des procédés de broyage qui ne détruisent pas intégralement les supports.

1. *Le moletage* consiste en l'utilisation de rouleaux de pression pour déformer les CD, les DVD ou les disques Blu-ray de façon à les étirer et à les courber légèrement, ce qui détruit les éléments de données (c.-à-d. les creux et les plats optiques). Ce procédé strie profondément ou endommage irrémédiablement la surface d'un disque, et ce, des deux côtés.
2. *Le meulage de surface* pulvérise la couche porteuse d'informations réduisant ainsi les CD optiques à l'état de simples morceaux de plastique transparent, qu'il s'agira ensuite de recycler ou d'éliminer.

2.4 VÉRIFICATION

Le nettoyage des supports doit absolument être vérifié de façon à garantir la confidentialité des données ministérielles enregistrées dans ces supports. On compte deux types de vérification :

- vérification de chacun des emplacements de mémoire;
- vérification d'un échantillon représentatif des emplacements de mémoire.

Le degré d'efficacité du nettoyage varie selon les technologies caractérisant les supports. Il arrive que les processus traditionnels de nettoyage s'avèrent inefficaces et que les procédures de vérification du nettoyage soient difficiles, voire impossibles à réaliser.

Il convient alors d'adopter des méthodes de nettoyages qui se prêtent aisément aux procédures de vérification.

2.5 EXIGENCES ADDITIONNELLES

2.5.1 RETRAIT DES MARQUAGES ET DES ÉTIQUETTES

Les supports sur lesquels des informations sensibles ont été enregistrées exigent un étiquetage en bonne et due forme, tel que l'indique la PSG. Le retrait de toute étiquette indiquant le niveau de sensibilité des données conservées dans un support donné constitue une part importante du processus de nettoyage. Cette mesure permet de limiter toute attention préjudiciable au support ou aux données pouvant subsister suivant l'élimination.

2.5.2 EXIGENCES EN MATIÈRE DE RÉTENTION DES DONNÉES ET DE VÉRIFICATION

Les ministères et les organismes doivent tenir compte des exigences politiques et juridiques concernant la période de rétention des données et la vérification permettant d'approuver, le cas échéant, l'effacement ou la destruction du support. Ces exigences sont les suivantes :

1. exigences juridiques relevant des lois fédérales qui régissent l'AIPRP pour ce qui a trait à la rétention des documents publics;
2. exigences relevant des politiques du SCT en matière de gestion de l'information pour ce qui a trait à la conservation des documents gouvernementaux (voir l'annexe D – *Réutilisation et élimination des supports*);
3. exigences de sécurité visant la rétention des données admissibles en preuve aux fins d'une enquête ou d'une procédure judiciaire;
4. exigences de vérification de sécurité visant la rétention des registres de destruction et d'élimination des supports, de l'information et de l'équipement du gouvernement.

2.5.3 OUTILS DE NETTOYAGE

Prière de consulter l'annexe C – *Outils de nettoyage* pour obtenir de plus amples détails concernant le nettoyage des supports et la vérification.

2.5.4 DESTRUCTION : MESURES INTÉRIMAIRES ET PROCÉDURE D'URGENCE

Pour ce qui a trait à la destruction, les mesures intérimaires et les procédures d'urgence consistent à endommager un support donné. L'endommagement peut être couramment utilisé soit comme procédures d'urgence ou comme mesure provisoire de sécurité ministérielle visant les supports qui seront ultérieurement expédiés aux installations sécurisées de destruction.

L'endommagement nécessite le recours à des outils (p. ex. étau/presse, marteau, cloueuse, perceuse électrique, dispositif à impact focalisé) pour causer des dommages physiques et ciblés au support de stockage, et ce, dans le but d'entraver, de retarder ou d'empêcher la récupération des données provenant d'un support nettoyé.

Les dispositifs miniatures ou à mémoire Flash peuvent être détruits en les frappant à plusieurs reprises avec un marteau. Même si elle ne garantit pas la destruction de la puce-mémoire, cette méthode peut efficacement entraver les tentatives de récupération. Le fait de mêler les fragments du support endommagé à des restes de supports de TI non sensibles peut entraver davantage les tentatives de récupération des données.

2.5.5 SERVICES COMMERCIAUX DE DESTRUCTION ET DE RECYCLAGE

Avant d'être envoyés à un service externe de destruction, les supports devraient être nettoyés ou rendus inopérationnels (voir la section 2.5.4 – *Destruction : mesures provisoires et procédures d'urgence*). Lorsqu'il ne peut être nettoyé avant l'expédition, le support doit être transporté et entreposé conformément aux exigences correspondant à son niveau de sécurité, après quoi il faut procéder à une destruction authentifiée.

Lorsqu'il s'agit de confier la destruction à un service externe, il convient de suivre les consignes suivantes :

1. consulter la Sous-direction de la sécurité ministérielle de la GRC pour obtenir des conseils concernant le choix d'un fournisseur et les exigences s'appliquant à l'équipement de destruction;
2. vérifier la validité des habilitations de sécurité du fournisseur et des installations auprès de la Direction de la sécurité industrielle canadienne (DISC) de Services publics et Approvisionnement Canada (SPAC);
3. vérifier la validité des clauses contractuelles portant sur la sécurité, y compris sur la façon dont le fournisseur est en mesure de certifier la destruction et l'élimination du matériel concerné.

2.6 ÉLIMINATION PAR LES MÉCANISMES EN VIGUEUR

La préparation et le transport des supports et du matériel sont régis par les politiques ministérielles, lesquelles sont énoncées dans l'annexe D – *Réutilisation et élimination des supports*.

Prière de consulter les *Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral* ainsi que la Stratégie de gestion des déchets électroniques, de SPAC.

2.7 CHAÎNE DE POSSESSION

Les organismes du GC doivent disposer d'une chaîne de possession pour tous les supports provenant d'équipement de TI déclassé et pour tous les supports qui sont arrivés en fin de cycle de vie et qui sont prêts à être nettoyés et éliminés.

Disposer d'une chaîne de possession signifie que les autorités compétentes du ministère doivent toujours tenir un registre chronologique indiquant qui a été en possession de chacun des supports et ce qu'il est advenu de ces supports. Ce processus débute lorsqu'un support est appelé à subir un nettoyage. Il se poursuit pendant le nettoyage, durant le transport vers le récipiendaire du don ou le site d'élimination, et ne se termine qu'une fois l'élimination ou le don accomplis.

3 RÉSUMÉ

En cours d'utilisation normale, un support peut contenir des données sensibles, et ce, jusqu'à la fin de son cycle de vie. La confidentialité des données s'expose ainsi à certaines vulnérabilités dont les ministères doivent tenir compte lorsqu'il est temps d'éliminer l'équipement comportant des supports de TI.

Le nettoyage des supports est un processus sécurisé et vérifiable servant à garantir la confidentialité des données résiduelles se trouvant sur lesdits supports. Ce processus est régi par voie de politiques du GC et vise la gestion et l'élimination des supports en surplus. Il répond également aux principes de gestion des risques énoncés dans l'ITSG-33 – *La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie*, où il est notamment question des contrôles de sécurité qu'il convient d'appliquer.

Certes, certains produits sont déjà dotés de fonctions d'effacement ou de réinitialisation, mais ces outils de nettoyage ne devraient être employés que sur les supports contenant de faibles volumes de données à faible sensibilité.

Pour ce qui a trait aux supports contenant des données dont le niveau de sensibilité est plus élevé, la présente fournit de plus amples détails, pour veiller à la protection permanente des données ministérielles au-delà du cycle de vie desdits supports. Les supports qui ont été chiffrés pendant la durée de leur cycle de vie peuvent être aisément nettoyés.

Les supports non chiffrés nécessitent un traitement plus approfondi de façon à garantir la confidentialité des données résiduelles – les ministères pourraient donc stipuler que la seule façon de garantir la confidentialité des données serait de détruire physiquement lesdits supports.

Les exigences juridiques et politiques visant la rétention des données et la vérification doivent être prises en compte par le ministère concerné; il convient également de tenir un registre faisant état des mesures de nettoyage et d'élimination.

3.1 COORDONNÉES ET ASSISTANCE

Les ministères qui, dans le cadre de leurs activités opérationnelles, sont appelés à nettoyer des supports peuvent demander conseil auprès des Services à la clientèle de la STI, aux coordonnées suivantes :

Téléphone : 613-991-7654
Courriel : itsclientservices@cse-cst.gc.ca

4 CONTENU COMPLÉMENTAIRE

4.1 ABRÉVIATIONS, ACRONYMES ET SIGLES

Terme	Définition
AIPRP	Accès à l'information et protection des renseignements personnels
ALB	Adressage logique en bloc
AMPS	Avis de mise en œuvre de la politique sur la sécurité
ASM	Agent de sécurité du ministère
ATA	Advanced Technology Attachment (*Integrated Drive Electronics* (IDE) /ATA)
CD	Disque compact (*Compact disk*)
CF	Carte Flash
CST	Centre de la sécurité des télécommunications
DRAM	Mémoire vive dynamique (*Dynamic Random Access Memory*)
DVD	Disque vidéonumérique (*Digital Video Disc*)
EMR	Évaluation des menaces et des risques
GC	Gouvernement du Canada
GES	Guide d'équipement de sécurité (GRC)
Go	Gigaoctet
GPS	Système mondial de localisation (*Global Positioning System*)
GRC	Gendarmerie royale du Canada
HDD	Disque dur (*Hard Disc Drive*)
MFD	Appareil multifonction (*Multi-Function Device*) [c.-à-d. imprimante, photocopieur, télécopieur]
Mi	Menace intentionnelle
MMC	Carte multimédia (*Multimedia Card*)
NSA	National Security Agency [É.-U.]
NVSL	Non-Volatile Systems Laboratory [University of California in San Diego –UCSD]
OPE	Ordinateurs pour les écoles
PSG	Politique sur la sécurité du gouvernement
RAM	Mémoire vive (*Random Access Memory*)
SATA	Serial ATA [pour HDD]
SCSI	Interface SCSI (*Small Computer System Interface*)
SCT	Secrétariat du Conseil du Trésor
SD	Secure Digital
SE	Effacement sécurisé (*Secure Erase*)

SPAC	Services publics et Approvisionnement Canada [anciennement TPSGC]
SRAM	Mémoire vive statique (*Static Random Access Memory*)
SSD	Disque statique à semiconducteurs (*Solid-State Drive*)
TI	Technologie de l'information
TPM	Trusted Platform Module
TPSGC	Travaux publics et Services gouvernementaux Canada [voir également SPAC]
UCSD	University of California San Diego [É.-U.]
VoIP	Protocole Voix sur IP

4.2 GLOSSAIRE

Terme	Définition
Agent de menace	Organisation ou individu qui constituent intentionnellement des menaces; entité (naturelle ou autre) pouvant constituer une menace accidentelle.
ATA	*Advanced Technology Attachment* (ATA) : Norme visant les interfaces pour HDD (y compris les anciens Parallel ATA ainsi que la version plus récente, Serial ATA) de même que d'autres dispositifs de stockage de données.
ATA Secure Erase (SE)	Méthode servant à effacer le contenu de HDD et de disquettes. Depuis 2001, cette méthode est utilisable moyennant une commande de micrologiciel interne lancée depuis les HDD ATA. Elle permet la réécriture de tous les secteurs de données et de n'y inscrire que des « 0 » binaires.
Déclassifier	Étape administrative à laquelle il est établi qu'un support ne contient plus aucune information sensible après avoir été nettoyé conformément aux directives en vigueur.
Destruction sécurisée	Destruction de supports ayant contenu des données. Cette destruction est accomplie par au moins une des méthodes approuvées qui – en soi ou combinées à une procédure d'effacement – détruit l'information ou modifie suffisamment un support pour que l'information ne soit plus récupérable.
Effacement cryptographique (CE)	Processus de nettoyage consistant à effacer la clé de chiffrement qui est employée sur un support chiffré pour rendre les données illisibles.
Effacement cryptographique (CE) amélioré	Processus de nettoyage consistant à rechiffrer des supports au moyen d'une clé de chiffrement aléatoire forte, puis à effacer de toute trace de cette clé, de façon à garantir que les données sont illisibles.
Effacement sécurisé	Processus numérique de nettoyage qui fait appel à des commandes et des outils de l'industrie – notamment ATA *security erase* (SE) – pour effacer adéquatement tous les emplacements accessibles de la mémoire d'un dispositif de stockage de données; le cas échéant, ce processus comprend la réécriture de chacun des secteurs d'un support magnétique ou encore l'effacement des blocs d'un support statique à semiconducteurs.
EMR	L'évaluation des risques et des menaces (EMR) est le processus par lequel on identifie et caractérise les risques et les menaces qui pèsent sur les actifs de TI et à la suite duquel on recommande ou met en place des contrôles de sécurité additionnels dans le but d'atténuer les risques trop importants pour être tolérés.
ISO	Organisation internationale de normalisation (*International Standards Organization*).
Mémoire flash	Forme de mémoire non volatile qui est couramment employée comme moyen de stockage de

	données dans les appareils électroniques et l'équipement de TI commerciaux (p. ex. jeton USB, SSD, SD).
Mémoire non volatile	Composantes (mémoire ou stockage de données) qui conservent les données indéfiniment (p. ex. HDD, mémoire Flash, etc.).
Mémoire volatile	Éléments de la mémoire d'un support qui perdent les données enregistrées dès que ce support n'est plus alimenté en électricité (p. ex. RAM).
Menace	Occurrence ou acte intentionnels ou accidentels pouvant s'avérer préjudiciables ou compromettants pour des personnes, des informations, des actifs ou des services.
Nettoyage	Le nettoyage est une méthode de déclassification non destructive qui vise à rendre des données irrécupérables tout en veillant à ce que leur support soit réutilisable conformément aux politiques du GC et des ministères en matière de sécurité des TI. Cette pratique permet de garantir la confidentialité des données qui pourraient subsister sur les supports et de minimiser les risques de divulgation non autorisée.
Nettoyage sélectif	Type de nettoyage qui ne vise que certains fichiers ou certains éléments de données (à ne pas confondre avec le « nettoyage de support » qui consiste à effacer l'intégralité des données enregistrées dans un support.
Réécriture	Processus de nettoyage logique qui consiste à écrire des motifs préétablis de données sur tous les emplacements de stockage adressables d'un support de stockage TI dans le but d'écraser les données déjà enregistrées.
Support de TI	Supports et dispositifs à mémoire TI ou à stockage de données
TPM	Trusted Platform Module (ISO/IEC 11889) Le sigle TMP désigne « [...] une puce informatique sécurisée pouvant emmagasiner [...] des clés de chiffrement. » (*Trusted Computing Group*).
Vidage	Application de techniques logiques dans le but de nettoyer les données de tous les emplacements de stockage adressables aux fins de protection contre les techniques non invasives de récupération des données. En l'occurrence, il s'agit d'une méthode de remplacement par de nouvelles valeurs (réécriture) ou, lorsque la réécriture n'est pas prise en charge, d'utilisation d'une option de menu permettant de procéder à la réinitialisation d'usine du dispositif concerné. [18]

4.3 DOCUMENTS DE RÉFÉRENCE

Numéro	Titre et auteur
1	Centre de la sécurité des télécommunications (CST). *ITSG-33 – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2012.
2	Secrétariat du Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement (PSG)*, 1er juillet 2009.
3	Secrétariat du Conseil du Trésor. *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI),* non daté.
4	*Loi sur la protection des renseignements personnels* [en ligne]. [Ottawa] : Ministère de la Justice, 10 septembre 2015 [cité le 29 septembre 2015]. Disponible à cette adresse : http://laws-lois.justice.gc.ca/fra/lois/p-21/
5	*Loi sur l'accès à l'information* [en ligne]. Ottawa, Ontario, Canada : Ministère de la Justice, 5 avril 2016 [cité le 1er novembre 2016]. Disponible à cette adresse : http://laws-lois.justice.gc.ca/fra/lois/A-1/
6	Secrétariat du Conseil du Trésor. *Politique sur les conflits d'intérêts et l'après-mandat*, avril 2012.
7	Secrétariat du Conseil du Trésor du Canada. *Directive sur les pratiques relatives à la protection de la vie privée*, mai 2014
8	*Loi sur la gestion des finances publiques* [en ligne]. Ottawa, Ontario, Canada : Ministère de la Justice, 11 octobre 2016 [cité le 1er novembre 2016]. Disponible à cette adresse : http://laws-lois.justice.gc.ca/fra/lois/F-11/
9	Secrétariat du Conseil du Trésor. *Utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada (Avis de mise en œuvre de la Politique sur la technologie de l'information [AMPTI] 2014-01)*, mai 2014
10	National Security Agency, gouvernement des États-Unis. *Degausser Evaluated Products List*, novembre 2015
11	Gendarmerie royale du Canada. *Guide d'équipement de sécurité (GES) (G1-001)*, non daté. (Nota : L'accès est réservé aux ministères et organismes du gouvernement du Canada.)
12	Secrétariat du Conseil du Trésor. *Stratégie de gestion des déchets électroniques* (2010) et Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral (v2.0), non daté.
13	Centre de la sécurité des télécommunications (CST). ITSB-112. *Questions de sécurité relatives à l'utilisation de supports amovibles pour les renseignements Protégé C et classifiés*, août 2014.
14	National Cyber Security Centre (NCSC, Royaume-Uni) *Overwriting Tools for Magnetic Media,* février 2016.
15	Secrétariat du Conseil du Trésor. *Directive sur l'aliénation du matériel en surplus*, novembre 2016.

16	Ordinateurs pour les écoles, *Innovation, Sciences et Développement économique Canada* [en ligne]. Ottawa, Ontario, Canada : Innovation, Sciences et Développement économique Canada, 12 mai 2015 [cité le 1er novembre 2016]. Disponible à cette adresse : https://www.ic.gc.ca/eic/site/cfs-ope.nsf/fra/accueil
17	Non-Volatile Systems Laboratory (University of California in 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*, décembre 2014.
19	Secrétariat du Conseil du Trésor. *Ligne directrice sur l'utilisation acceptable des dispositifs et des réseaux*, non daté.
20	Secrétariat du Conseil du Trésor. *Politique sur la gestion du matériel*, novembre 2006.

Annexe A Dispositifs à support relatif à la TI

A.1 Supports magnétiques

Les dispositifs suivants stockent les données sur des bandes magnétiques :

1. disques durs (HDD pour Hard Disk Drive) – y compris les Integrated Drive Electronics/Advanced Technology Attachment (IDE/ATA) et les interfaces SCSI;
2. disquettes;
3. bandes magnétiques y compris les bandes magnétiques sur bobines, les cassettes, les cassettes VHS, etc.;
4. réseau de stockage (SAN pour *Storage Area Network*);
5. disques Zip;[14]
6. cartes magnétiques.

Les dispositifs magnétiques sont couramment utilisés pour le stockage de quantités considérables de données. Ils sont dotés d'un support d'enregistrement consistant en un mince film déposé sur une surface, notamment un disque de plastique ou un ruban. Les données sont stockées sous forme de zones magnétiques miniatures, sur la surface d'un film composé d'alliages spéciaux qui peuvent retenir fermement les zones magnétiques, et ce, pendant de longues périodes. La fermeté avec laquelle le support peut retenir le magnétisme et la petitesse des zones magnétiques contribue à accroître la densité des données.

Les dispositifs à supports magnétiques peuvent être nettoyés par le recours à la réécriture de tous les secteurs contenant des données utilisateur. En l'occurrence, des données non sensibles remplacent les données originales. Une seule réécriture est suffisante, sauf dans le cas des HDD produits avant 2001, lesquels en nécessitent trois. Ils peuvent également être effacés grâce à des produits approuvés pour la démagnétisation.

A.2 Supports optiques

Au nombre des supports de stockage des données, on compte les suivants :

1. disques compacts (CD) – ce qui comprend les disques à lecture seulement de même que les variantes inscriptibles ou réinscriptibles;
2. disques vidéonumériques (DVD);
3. disques Blu-ray.

Les disques optiques sont couramment utilisés pour le stockage des fichiers de données ou des fichiers audio et vidéo. C'est grâce à des technologies laser qu'il est possible d'inscrire des données sur les disques optiques ou de lire les données inscrites. Les CD peuvent être nettoyés par le recours au meulage de la surface. Toutefois la majeure partie des autres types de disques optiques exigent une solution plus dommageable comme le broyage ou la désintégration.

14 Le disque Zip est un dispositif à disquette de haute capacité mis en marché en 1994 par l'entreprise Iomega Corporation.

A.3 Supports statiques à semiconducteurs

Les supports qui misent sur les supports statiques (c.-à-d. semiconducteurs électroniques) utilisent des mémoires volatiles (les données enregistrées sont perdues dès que le support n'est plus alimenté en électricité) ou des mémoires non volatiles et conservent les données même lorsque l'alimentation est coupée).

A.3.1 Volatile

Au nombre des dispositifs à mémoire volatile, on compte les suivants :

1. mémoire vive (RAM);
2. mémoire vive statique (SRAM);
3. mémoire vive dynamique (DRAM).

Les dispositifs à mémoire volatile sont couramment employés pour doter l'équipement informatique et réseautique de mémoires à accès rapide. Ces dispositifs misent sur des technologies à semiconducteurs pour enregistrer des données. Ils sont considérés comme étant volatiles dans la mesure où ils ne peuvent conserver les données lorsqu'ils ne sont plus alimentés en électricité. Ils peuvent être nettoyés par la simple interruption du courant d'alimentation et, s'il y a lieu, par le retrait des piles pouvant permettre à la mémoire de conserver les données.

Nota

En cas de doute concernant l'interruption de l'alimentation interne de la mémoire vive dans l'équipement hautement sensible en cours de déclassement, il convient de simplement retirer la mémoire vive.

A.3.2 Non volatile

Au nombre des dispositifs à mémoire non volatile servant au stockage des données, on compte les suivants :

1. disques électroniques SSD – en divers facteurs de forme;[15]
2. dispositifs USB Flash (c.-à-d. clés USB, cartes mémoire Flash);
3. cartes Secure Digital (SD);
4. cartes multimédia (MMC);
5. cartes Flash (CF);
6. dispositifs de communication et de réseau contenant de la mémoire et des espaces de stockage de données.

Les technologies à mémoire non volatile sont fiables lorsqu'il s'agit de conserver toutes les données indéfiniment sans recours à un courant électrique. Elles sont couramment utilisées pour permettre à de nombreux appareils de stocker des données : ordinateurs, imprimantes, routeurs et autres dispositifs réseau, dispositifs portables de stockage de données, téléphones intelligents, tablettes, et autres produits commerciaux allant des appareils photo aux dispositifs GPS.

15 La technologie SSD est disponible en divers facteurs de forme, notamment Serial ATA (SATA), mSATA (PCIe et mini PCIe), Disk-on-a-Module (DOM), mini-DIMM, MO-297, etc.

Flash est la plus utilisée des technologies, dans la mesure où elle peut servir de principal support de stockage. Dans certains cas, elle peut servir à des fins spéciales ou fournir un stockage d'appoint, notamment dans le cas des disques durs hybrides.[16]

D'autres formes de mémoire électronique non volatile ont été mises au point, mais sont peu susceptibles d'être employées dans le contexte du GC. Voici quelques exemples : technologies à mémoire magnéto-optique, magnétorésistante ou nanomagnétique.

16 Le disque dur hybride allie la technologie magnétique HHD traditionnelle à celle de la mémoire à semiconducteurs. Il peut nécessiter une procédure de nettoyage plus complexe qui saura traiter les composants FLASH séparément des disques magnétiques.

Annexe B Normes de nettoyage

B.1 Applicabilité des méthodes de nettoyage

Employées seules (voir 2.2 – *Méthodes de nettoyage*) ou combinées à des méthodes d'endommagement ou de destruction physiques, les méthodes de nettoyage sont applicables à une grande diversité de supports et de dispositifs.

Tableau 1 Applicabilité des méthodes de nettoyage

Méthode	Applicabilité
NETTOYAGE	
Effaçage et réinitialisation	Routeurs, téléphones VoIP, télécopieurs, téléphones cellulaires, et autres dispositifs
Réécriture et SE	HDD, certains disques SSD et certains dispositifs Flash
Méthodes CE	HDD, tous les SSD et autres dispositifs Flash
Démagnétisation *(non destructive)**	Bandes magnétiques, cartes magnétiques et disquettes
DESTRUCTION	
Déchiquetage, désintégration, meulage et déformation	Tous les supports (utilisation d'équipement approuvé par la GRC)
Incinération et fusion	Tous les supports (recours à des installations approuvées par Environnement Canada)
Meulage des surfaces et moletage	Disques optiques
Démagnétisation (destructive)*	HDD (utilisation de produits de démagnétisation approuvés par le CST)

* La démagnétisation peut être destructive ou non destructive suivant la force de démagnétisation employée et le type de support à démagnétiser.

B.2 Exigences et normes en matière de nettoyage

Dans la section qui suit, un tableau fait état d'exigences tirées de normes homologuées par le CST et la GRC et régissant le nettoyage ou la destruction de supports aux fins de déclassification.

Le nettoyage par réécriture, SE ou CE est généralement suffisant dans le cas de supports à faible ou moyenne sensibilité. Toutefois, une évaluation des menaces et des risques (EMR) ou une politique ministérielle pourraient exiger une destruction (après l'effacement) dans le cas de certains supports à moyenne sensibilité. Pour ce qui a trait aux supports à haute sensibilité, la destruction est généralement requise, mais un nettoyage préalable peut réduire le degré de destruction requis en rendant quasi impossible la tâche de récupération (par un adversaire) de données significatives à partir des fragments résiduels.

Nota : *Les procédures de nettoyage et de vérification pourraient s'améliorer si les fabricants de dispositifs de TI arrivaient à développer des produits compatibles avec les méthodes d'effacement sécurisé.*

De plus, les spécifications concernant la taille des fragments (voir tableaux) sont appelées à changer en raison de nouveaux développements dans les technologies de stockage des données et dans les produits de destruction. Pour obtenir les plus récentes spécifications, prière de consulter le GES [11] de la GRC.

Retrait des marquages et des étiquettes

Le processus de nettoyage comprend le retrait des marquages et des étiquettes qui se trouvent sur un support et qui pourraient indiquer le niveau de sensibilité (pour le GC) des données stockées antérieurement ou révéler l'identité du propriétaire. Le retrait des étiquettes et des autres indicateurs de sensibilité du GC permet de freiner la curiosité que pourraient susciter les restes de supports.

B.3 Tableaux sur les exigences en matière de nettoyage

La présente section comprend une série de tableaux qui font état des exigences en matière de nettoyage, et ce, pour divers types de supports ou de dispositifs dotés de supports.

Le tableau suivant s'applique à tous les supports de stockage de données.

Tableau 2 Exigences en matière de nettoyage visant l'ensemble des supports de stockage de données

Sensibilité	Exigence	Nota
FAIBLE (Non classifié, Officiel, et Protégé B)	1) Utilisation d'outils et de méthodes de nettoyage (y compris la réécriture, SE ou CE) ou utilisation des fonctions de réinitialisation ou de vidage fournies par le fabricant 2) Vérification des résultats	A
MOYENNE (Protégé B et Confidentiel)	1) Nettoyage (réécriture, SE ou CE amélioré) et vérification attentive des résultats du nettoyage 2) Lorsqu'il n'est pas possible de nettoyer ou de vérifier : procéder à la destruction du support	A, C
HAUTE (Très secret, Secret et Protégé C)	1) Nettoyage 2) Destruction	A, B

Nota :

A. Élimination : Don ou élimination des supports nettoyés ou détruits conformément aux *Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral* [12].

B. Supports dont le contenu est Protégé C ou Secret : Les données Protégé C peuvent avoir un niveau moyen de sensibilité pouvant donner lieu, à la discrétion du ministère, à une certaine procédure de sécurité correspondant à un énoncé de sensibilité et une EMR; toutefois, on juge normalement que le niveau de sensibilité est haut sur le plan du stockage et des exigences de sécurité.

Un ministère peut, à sa discrétion, attribuer une sensibilité moyenne à des données Secret qui n'ont pas trait à des intérêts nationaux. Les données Secret qui portent sur des intérêts nationaux (p.ex. défense et renseignement) ou qui sont marquées d'une classification Secret provenant d'un gouvernement étranger ou allié (p. ex. OTAN Secret) ont toujours un haut niveau de sensibilité.

C. **CE :** Le CE peut être utilisé en toute confiance lorsque l'emplacement de la clé de chiffrement est connu (p. ex. enregistrée dans une puce TPM ou dans un jeton matériel amovible) et qu'il peut aisément être l'objet d'un effacement et d'une vérification des résultats de l'effacement.

Lorsque l'effacement de la clé ne peut être vérifié, le CE devrait être suivi d'un vidage de façon à réduire les risques que la clé de chiffrement (et les données) soit récupérée par quelque moyen d'analyse avancée.

B.3.1 Supports optiques

Les exigences suivantes s'appliquent aux CD, aux DVD et aux disques optiques Blu-ray.

Tableau 3 Exigences en matière de nettoyage visant les supports optiques

Sensibilité	Exigence	Nota
Tous les niveaux	Lorsque l'intégralité du contenu est chiffrée, supprimer et s'occuper de la clé de chiffrement avant la destruction.	B
Destruction – *Déchiquetage, désintégration, broyage, fusion et incinération*		
FAIBLE	Couper ou casser les disques optiques en morceaux et/ou endommager fortement la couche porteuse d'information en éraflant ou en striant le disque.	C
MOYENNE	Réduire les disques en petits morceaux < 40 mm^2 (¼ po x ¼ po); **ou** meuler la surface du disque de façon à éliminer la couche colorée portant les données (CD seulement).	
HAUTE	Réduire les disques en petits morceaux < 10 mm^2 (1/8 po x 1/8 po) ou moins, si l'équipement de destruction en est capable; **ou** Meuler la surface du disque de façon à éliminer la couche colorée portant les données, rendant semi-transparent le disque de plastique (CD seulement).	
Endommagement – Mesures provisoires et procédures d'urgence		
Tous les niveaux	Endommager le support optique en striant la surface et/ou en le cassant en morceaux.	E
Exception		
Tous les niveaux	Moletage (utilisation de rouleaux de pression pour étirer et déformer les surfaces de supports optiques) : lorsque des outils approuvés par la GRC sont utilisés, le moletage rendra les disques optiques illisibles, quoique cette méthode n'est par approuvée pour la déclassification des supports optiques contenant des informations hautement sensibles.	s.o.

Nota :

A. Vidage : s.o.

B. Nettoyage : Le nettoyage en soi n'est pas idéal dans le cas des supports optiques qui n'ont aucune valeur de réutilisation et qui peuvent être aisément détruits.

C. Destruction : Les supports optiques peuvent obstruer ou endommager certains dispositifs de destruction. Les produits qui sont jugés adéquats pour la destruction des supports optiques sont énumérés dans le *Guide d'équipement de sécurité (GES)* [11], de la GRC.

D. Démagnétisation : s.o.

E. Endommagement : Causer de profonds dommages à la surface du support (avant de l'envoyer à un centre de destruction approuvé).

F. Élimination : s.o.

B.3.2 Support magnétique

Les exigences énoncées ci-dessous s'appliquent aux éléments suivants : HDD, disquettes, cartes magnétiques et bandes magnétiques (p. ex. cassettes DAT, bande de sauvegarde, ruban à bobines, cassettes audio, bandes VHS ou Beta).

Tableau 4 Exigences en matière de nettoyage visant les supports magnétiques

Sensibilité	Nettoyage et démagnétisation	Nota
FAIBLE	Nettoyage et vérification	A, B, D, F
MOYENNE	Nettoyage et vérification attentive	
HAUTE	Nettoyage et destruction	
Destruction – *Déchiquetage, désintégration, broyage, fusion et incinération*		
FAIBLE	Lorsqu'il n'est pas possible de nettoyer ou de vérifier : procéder à la destruction du support. 1) Disques : réduire à au moins deux morceaux. 2) Bandes : réduire en lanières d'au plus 50 mm de longueur (2 po). 3) Cartes magnétiques : réduire en morceaux < 140 mm^2 (½ po x ½ po).	B, C, F
MOYENNE	Lorsqu'il n'est pas possible de nettoyer ou de vérifier : procéder à la destruction. 1) Disques : réduire en morceaux (¼ po x ¼ po). 2) Bandes : réduire en morceaux (¼ po).	
HAUTE	Nettoyage et destruction par la réduction en morceaux (disques < 40 mm^2 ou bandes < 6 mm); **ou** Lorsqu'il n'est pas possible de nettoyer ou de vérifier : réduire en morceaux < 10 mm^2 (1/8 po x 1/8 po) ou plus petits.	
Endommagement – Mesures provisoires et procédures d'urgence		
Tous les niveaux	Lorsqu'il n'est pas possible de nettoyer ou de vérifier : endommager les disques/les plateaux magnétiques avant d'envoyer le support à un centre de destruction approuvé.	E, F

Nota :

A. **Vidage** : Les processus de vidage et de nettoyage visant les supports magnétiques constituent des équivalents.

B. **Nettoyage** : Réécriture, SE, CE au moyen d'outils et de processus validés.

C. **Destruction** : Voir les produits de destruction approuvés et les équivalences concernant la taille des écrans de désintégrateurs dans le *Guide d'équipement de sécurité* (GES) [11], de la GRC.

D. **Démagnétisation** : Vidage et démagnétisation. Éviter de démagnétiser les HDD de sensibilité faible à moyenne qui pourraient être réutilisés. Pour accroître le niveau d'assurance : endommager ou détruire les plateaux des disques durs à haute sensibilité après la démagnétisation.

E. **Endommagement** : Utilisation des outils disponibles pour causer des dommages avant le transport du support vers un centre de destruction approuvé (p. ex. étau, dispositif à impact focalisé, marteau).

F. **Élimination** : Don ou élimination des supports nettoyés ou des restes de destruction conformément aux *Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral* [12].

B.3.3 Disques statiques et dispositifs Flash

Les exigences ci-dessous s'appliquent aux disques statiques (SSD) et aux dispositifs USB Flash.

Tableau 5 Exigences en matière de nettoyage visant les disques statiques et les dispositifs Flash

Sensibilité	Nettoyage et démagnétisation	Nota
FAIBLE	Nettoyage si possible **ou** vidage et réinitialisation.	A,B,F
MOYENNE	Nettoyage et vérification attentive des résultats. *Dispositif USB Flash non chiffré (il n'est pas rentable de nettoyer aux fins de réutilisation) :* effacement et destruction. *SSD non chiffré :* effacement et destruction lorsqu'il n'est pas possible de nettoyer ou de vérifier, ou encore lorsque les outils d'analyse indiquent que le SSD contient des secteurs endommagés ou réaffectés qui sont impossibles à nettoyer.	
HAUTE	Nettoyage et vérification, puis destruction.	
Destruction – *Déchiquetage, désintégration, broyage, fusion et incinération*		
FAIBLE	Si impropre à la réutilisation : vidage, puis broyage ou destruction par réduction en morceaux < 40 mm^2 de surface (p. ex. ¼ po x ¼ po).	C, F
MOYENNE	Lorsqu'il n'est pas possible de nettoyer ou de vérifier : vidage, puis broyage ou destruction par réduction en morceaux < 40 mm^2 de surface (p. ex. ¼ po x ¼ po).	
HAUTE	Nettoyage, puis destruction en morceaux < 40 m^2 de surface (p. ex. ¼ po x ¼ po); ou, lorsque le nettoyage n'est pas possible, détruire le dispositif ou les composants de stockage en morceaux dont la taille < 2 mm.	
Endommagement – *Mesures provisoires et procédures d'urgence*		
Tous les niveaux	Lorsqu'il n'est pas possible de nettoyer : causer des dommages aux composants de stockage avant d'envoyer le dispositif à un centre de destruction approuvé.	E

Nota :

A. **Vidage** : Vider les dispositifs au moyen de la fonction intégrée d'effacement pour les données utilisateur ou les clés de chiffrement, puis réinitialiser aux paramètres par défaut (et révoquer tous les certificats cryptographiques).

B. **Nettoyage** : Réécriture, SE, CE au moyen d'outils et de processus validés.

C. **Destruction** : Voir les produits de destruction approuvés pour les dispositifs statiques à semiconducteurs et les équivalences concernant la taille des écrans des désintégrateurs qui figurent dans le *Guide d'équipement de sécurité* (GES) [11], de la GRC.

D. **Démagnétisation :** s.o.

E. **Mesure provisoire** : Utilisation des outils disponibles de façon à causer des dommages en attendant que le support soit envoyé à un centre de destruction approuvé (p. ex. étau, dispositif à impact focalisé, marteau).

F. **Élimination** : Don ou élimination des supports nettoyés ou des restes de destruction conformément aux lignes directrices du gouvernement fédéral [12].

B.3.4 Téléphones intelligents et tablettes

Les exigences ci-dessous s'appliquent aux téléphones cellulaires et aux dispositifs intelligents simples (téléphones intelligents et tablettes).

Tableau 6 Exigences en matière de nettoyage visant les téléphones intelligents et les tablettes

Sensibilité	Nettoyage et démagnétisation	Nota
FAIBLE	Vidage et réinitialisation	A, B, F
MOYENNE	*Dispositifs chiffrés* : nettoyage par CE et vérification de l'effacement de la clé; *Dispositifs compatibles avec BlackBerry et Samsung-Knox* : nettoyage par CE, ou vidage et réinitialisation; **ou** *Autres dispositifs* : vidage et destruction.[17]	
HAUTE	Vidage et destruction (toutes les bandes).	
Destruction – *Déchiquetage, désintégration, broyage, fusion et incinération*		
FAIBLE	Lorsque l'équipement n'est pas propice à la réutilisation ni au don : destruction intégrale du dispositif ou des composants de stockage en morceaux < 40 mm^2 de surface (p. ex. ¼ po x ¼ po).	C, F
MOYENNE	Lorsqu'il n'est pas possible de nettoyer ou de vérifier : destruction intégrale du dispositif ou des composants de stockage en morceaux < 40 mm2 de surface (p. ex. ¼ po x ¼ po).	
HAUTE	Nettoyage et destruction en morceaux < 10 mm^2 (1/8 po x 1/8 po); ou, lorsqu'il n'est pas possible de nettoyer, détruire en morceaux dont la taille < 2 mm.	
Endommagement – *Mesures provisoires et procédures d'urgence*		
Tous les niveaux	Lorsqu'il n'est pas possible de nettoyer : endommager l'écran et les composants d'interface avant d'envoyer le dispositif à un centre de destruction approuvé.	E

Nota :

A. **Vidage** : Vider les dispositifs au moyen de la fonction intégrée d'effacement pour les données utilisateur ou les clés de chiffrement, puis réinitialiser aux paramètres par défaut (et révoquer tous les certificats cryptographiques).

B. **Nettoyage** : Réécriture, SE, CE au moyen d'outils et de processus validés.

C. **Destruction :** Voir les produits de destruction approuvés pour les dispositifs statiques à semiconducteurs et les équivalences concernant la taille des écrans des désintégrateurs qui figurent dans le *GES* [11], de la GRC.

D. **Démagnétisation :** s.o.

17 La plupart des téléphones intelligents et des tablettes comptent une fonction intégrée d'effacement qui pourrait convenir au vidage de données à faible sensibilité en prévision d'une réutilisation de ces appareils. Par ailleurs, cette fonction intégrée pourrait, le cas échéant, servir de mesure provisoire en attendant la destruction intégrale de ces mêmes appareils. Pour ce qui a trait aux dispositifs compatibles avec BlackBerry ou Samsung-Knox, le CST juge que leurs fonctions respectives d'effacement et de réinitialisation sont suffisamment fiables pour le nettoyage des données utilisateur dont le niveau de sensibilité pourrait aller jusqu'à « moyen » inclusivement.

E. **Endommagement** : Utilisation des outils disponibles pour causer des dommages avant le transport du support vers un centre de destruction approuvé (p. ex. étau, dispositif à impact focalisé, marteau).

F. **Élimination** : Don ou élimination des supports nettoyés ou des restes de destruction conformément aux *Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral* [12].

B.3.5 Dispositifs réseau

La présente section s'applique aux dispositifs suivants : appareils multifonctions (MFD), télécopieurs, téléphones VoIP, imprimantes, routeurs et commutateurs.

Tableau 7 Exigences en matière de nettoyage visant les dispositifs réseau

Sensibilité	Nettoyage	Nota
FAIBLE	Télécopieurs, téléphones VoIP, routeurs et commutateurs : vidage.	A, F
MOYENNE	MFD : Pour les MFD évalués selon les Critères communs, le nettoyage se fait au moyen de la fonction intégrée de réécriture; ou, pour les MFD non évalués, retirer et nettoyer le support de stockage. Télécopieurs : vidage et destruction. Téléphones VoIP, routeurs, commutateurs : vidage.	
HAUTE	MFD : vidage, puis retrait et destruction des composants de stockage de données. Télécopieurs : vidage et destruction. Téléphones VoIP, routeurs, commutateurs : vidage.	
Exception		
Tous les niveaux	Mémoire volatile (RAM, DRAM, SRAM) : nettoyer en coupant toute source de courant pendant 24 heures (pour drainer toute source de courant interne pouvant aliment la mémoire).	s.o.
Destruction – *Déchiquetage, désintégration, broyage, fusion et incinération*		
FAIBLE	Lorsque l'équipement n'est pas propice à la réutilisation ni au don : vidage, puis destruction des composants de stockage en morceaux < 40 mm^2 de surface (p. ex. ¼ po x ¼ po).	C, F
MOYENNE	MFD : Lorsqu'il n'est pas possible de nettoyer ou de vérifier : destruction des composants de stockage en morceaux < 40 mm^2 de surface (p. ex. ¼ po x ¼ po).	
HAUTE	MFD : vidage du stockage interne, retrait et destruction des composants de stockage (voir tableaux de l'annexe B).	
Endommagement – *Mesures provisoires et procédures d'urgence*		
Tous les niveaux	Casser le dispositif en morceaux ou causer de profonds dommages aux composants de stockage, puis envoyer les morceaux au centre de destruction approuvé.	E

Nota :

A. **Vidage** : Vider les dispositifs au moyen de la fonction intégrée d'effacement pour les données utilisateur ou les clés de chiffrement, puis réinitialiser aux paramètres par défaut (et révoquer tous les certificats cryptographiques). Cette mesure est généralement suffisante pour les dispositifs réseau contenant des données de configuration et peu de données utilisateur, voire aucune; toutefois d'autres dispositifs réseau comme les télécopieurs et les MFD contiennent des données utilisateur qui nécessitent des mesures additionnelles.

B. **Nettoyage** : Réécriture, SE, CE au moyen d'outils et de processus validés.

C. **Destruction** : destruction des composants de stockage ou des cartes circuit imprimé contenant des composants de stockage, ou de l'intégralité du dispositif au moyen de produits de destruction approuvés et des équivalences concernant la taille des écrans des désintégrateurs qui figurent dans le *Guide d'équipement de sécurité* (GES)[11], de la GRC.

D. **Démagnétisation** : s.o. (sauf pour les HDD qui ont été retirés d'un MFD).

E. **Endommagement** : Utilisation des outils disponibles pour causer des dommages avant le transport du support vers un centre de destruction approuvé (p. ex. étau, dispositif à impact focalisé, marteau).

F. **Élimination** : Don ou élimination des supports nettoyés ou des restes de destruction conformément aux *Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral* [12].

Annexe C Outils de nettoyage

C.1 Aperçu

Pour optimiser le processus de nettoyage, un ministère doit disposer d'une expertise technique et d'une compréhension sans équivoque des enjeux de sécurité de circonstance. Le processus comprend le recours à des outils matériels et logiciels de façon à ce que le nettoyage réduise le niveau de sensibilité des supports à « Non classifié ».

C.1.1 Outils

Les ministères emploient des outils de nettoyage qui ont été l'objet d'une évaluation de la part d'intervenants internes ou de tierces parties. Par exemple, certains produits de réécriture de disques durs ont été évalués selon les *Critères communs*; de plus, le programme Ordinateurs pour les écoles (OPE), mis en œuvre sous l'égide du ministère de l'*Innovation, des Sciences et du Développement économique* (anciennement *Industrie Canada*), a également vérifié l'utilisabilité d'un certain nombre de produits.

C.1.2 Formation

Les opérateurs qui exécutent le travail doivent suivre une formation sur la mise en application adéquate des procédures de nettoyage. La formation doit permettre d'acquérir les compétences nécessaires et de motiver les opérateurs à satisfaire aux exigences techniques rigoureuses requises pour cette importante tâche de sécurité.

C.1.3 Difficultés

Pour la plupart des dispositifs de stockage massif de données, la réussite du processus de réécriture rendra difficile, voire impossible, la récupération des données par un adversaire disposant de laboratoires ou d'outils sophistiqués. Toutefois, considérant les possibilités d'erreur humaine ou de problèmes techniques, le processus de réécriture pourrait ne pas fonctionner :

1. L'erreur humaine peut résulter d'une utilisation inadéquate des outils de nettoyage et de vérification ou d'une application lacunaire des procédures en cours d'utilisation des outils.
2. Les problèmes techniques peuvent survenir lorsqu'un dispositif ne prend pas adéquatement en charge le processus de réécriture des données stockées.

D'autres problèmes techniques sont également dignes de mention :

1. Les supports statiques (SSD) et les dispositifs à mémoire Flash ne peuvent pas être réécrits complètement ou de manière fiable, puisqu'ils sont conçus avec une fonctionnalité de répartition de l'usure et en considération du fait qu'ils pourraient ne pas prendre en charge les commandes d'effacement ATA *Erase*.
2. La conception des HDD se prête au nettoyage par réécriture, mais le processus peut durer des heures.

Dans les deux cas, on peut recourir au processus de rechange du CE pour nettoyer efficacement la mémoire et la rendre illisible.

C.2 Produits et outils

Une diversité de produits et outils sont disponibles dans le marché ou en ligne, ou peuvent être conçus et développés en interne.

C.2.1 Chiffrement et effacement cryptographique (CE)

Les supports qui ont été chiffrés pendant la durée de leur cycle de vie peuvent être aisément nettoyés au terme de ce cycle par le recours à la méthode CE :

1. Le CE consiste à effacer la clé cryptographique se trouvant dans un dispositif à support chiffré.
2. Le CE amélioré (*CE Enhanced*) consiste dans le rechiffrement d'un support chiffré au moyen d'une clé jetable et la suppression de tout indice lié à cette clé.

Avant de recourir à la méthode CE améliorée aux fins de nettoyage de supports, les ministères doivent se doter d'une politique énonçant ce qui suit :

1. imposer le chiffrement du contenu des supports pendant la durée du cycle de vie de l'équipement de TI utilisé;
2. employer une solution de chiffrement homologuée FIPS 140 qui fournit également une fonction d'élimination sécurisée de la clé de chiffrement.

En plus de prendre en charge le chiffrement et le CE, les solutions devraient être conformes à ce qui suit :

1. Conseil du Trésor – *Utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada* (AMPTI 2014-01) [9]
2. CST – *Questions de sécurité relatives à l'utilisation de supports amovibles pour les renseignements Protégé C et classifiés* (pour le stockage classifié) (ITSB-112) [13].

C.2.2 Réécriture et effacement sécurisé (SE)

Les ministères du GC emploient des produits logiciels de *réécriture* et de SE pour nettoyer les supports (même si tous les supports ne sont pas forcément effaçables de cette façon). Les ministères devraient plutôt sélectionner des outils de réécriture qui donnent une forme de rétroaction visant à faciliter le processus de vérification. Les conseils en matière de sécurité énoncés dans le document *Overwriting Tools for Magnetic Media* [14], du *National Cyber Security Centre (NCSC, R.-U.),* fournissent de l'information sur le choix des produits de réécriture.

Les produits de SE et de réécriture sont conçus pour employer des commandes standards d'effacement ATA, lesquelles prennent en charge les HDD. Toutefois, il n'y a qu'un nombre limité de SSD qui sont conçus pour prendre adéquatement en charge de telles commandes, et il est techniquement difficile de déterminer lesquels de ces SSD peuvent être convenablement effacés. Par conséquent, les ministères qui envisagent d'utiliser la réécriture sur des SSD devraient acquérir ou développer de nouveaux produits de nettoyage qui permettront aux opérateurs de déterminer dans quelle mesure les SSD se prêtent à la réécriture et à l'examen des résultats.

En plus de ne prendre en charge que partiellement les commandes *Erase*, les SSD peuvent rendre le nettoyage impraticable s'ils contiennent des secteurs défectueux ou retirés. De tels secteurs ne peuvent faire l'objet d'une réécriture et pourraient contenir des données récupérables, même après l'élimination. Cette réalité ne constitue pas un problème pour les dispositifs qui ont été chiffrés tout au long de leur cycle de vie, mais elle doit être prise en compte lorsqu'il est question de nettoyer les dispositifs qui ne sont pas chiffrés.

C.2.3 Vérification

Les ministères devraient utiliser les outils dont ils disposent pour vérifier les résultats du chiffrement ou du vidage du support.

Les supports statiques ne prennent normalement en charge que l'adressage logique en bloc (LBA pour *Logical Block Addressing*). Certains modèles permettent également l'examen direct des emplacements de la mémoire physique, ce qui permet à un opérateur d'analyser minutieusement le contenu des supports et d'établir, le cas échéant, une corrélation entre l'utilisation intégrale de la mémoire et la présence de blocs défectueux. Toutefois, dans la majorité des cas, les ministères ont recours à des outils distincts pour scruter la mémoire des dispositifs.[18]

C.3 Considérations visant la réécriture des disques durs (HDD)

Le tableau suivant porte sur l'utilisation des outils de réécriture aux fins de nettoyage des HDD.

Tableau 8 Considérations visant la réécriture des HDD

Considérations	
#1	Les procédures doivent être documentées pour s'assurer que les mesures de protection sont adéquates et rendent impossible toute modification non autorisée ou toute subversion du logiciel de réécriture.
#2	La procédure de réécriture-vérification devrait s'exécuter au moyen d'une application distincte et validée. Un utilitaire de réécriture-vérification sert plus particulièrement à s'assurer que la réécriture des données a été effectuée dans toutes les zones adressables du disque dur selon le motif prescrit.
#3	Avant la réécriture, la capacité du disque devrait être calculée, c.-à-d. qu'il ne fait pas tenir pour acquis que le disque dispose forcément de la capacité indiquée par le BIOS, le FDISK, le CHKDSK ou par Windows.
#4	Les applications de réécriture et de vérification doivent faire état de la capacité du disque. Cette exigence s'impose, puisqu'une réécriture intégrale de tous les secteurs inscriptibles d'un HDD n'est possible que si l'application de réécriture est en mesure de calculer la capacité réelle.
#5	Les disques durs contenant des secteurs défectueux ne devraient pas être considérés comme ayant été « réécrits » tant qu'une vérification n'a pas été faite. Une exigence essentielle de rendement d'une application de vérification consiste à imager ces secteurs défectueux pour confirmer leur réécriture complète.
#6	Les applications de réécriture devraient être lancées depuis un dispositif de démarrage (*bootable*).
#7	L'utilisation des documents de procédures et des listes de vérification devrait être imposée au moment d'employer des applications de réécriture dans les cas où l'on traite des données protégées ou classifiées.
#8	Pour vérifier si un logiciel de réécriture est en mesure d'effacer toutes les parties d'un disque, l'opérateur doit calculer précisément la capacité réelle du disque et comparer le résultat de ce calcul à la capacité qui est indiquée par le logiciel de réécriture.

18 Le gouvernement des États-Unis a publié un guide sur la sélection et l'utilisation des outils de vérification dans le document du NIST – *Guidelines for Media Sanitization* SP 800-88, Rev 1 [18].

Annexe D Réutilisation et élimination des supports de TI

La présente annexe fait état des procédures et processus et recommandés aux fins d'élimination des supports électroniques de stockage des données qui se prêteraient à la réutilisation ou au recyclage.

D.1 Registres et rapports d'élimination

Les ministères règlent les questions liées aux exigences juridique et politique visant la rétention des données et la vérification avant l'approbation de l'effacement ou de la destruction des supports ou de l'équipement doté de supports. Ces questions concernent notamment les exigences en matière de vérification ainsi que la nécessité de tenir un registre détaillé des mesures d'élimination des documents, de l'information et de l'équipement du gouvernement.

Les énoncés suivants renseignent les ministères sur la nécessité de tenir des registres des mesures de vidage et de nettoyage. Ils concernent également la *destruction*, comme l'indique l'avis de mise en œuvre de la politique sur la sécurité (AMPS) 2011-01, du SCT, ainsi que les *Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral* [12], de SPAC.

1. L'agent de sécurité du ministère (ASM) doit veiller à ce que l'information sensible soit manutentionnée de façon sécurisée, une obligation qui s'applique également à tous les aspects de la collecte et du stockage préalables au nettoyage ou à la destruction.
2. Les ministères ont l'obligation de tenir un registre détaillé des mesures d'élimination visant tous les supports de surplus.

D.2 Élimination de l'équipement de surplus

Comme l'indique la *Directive sur l'aliénation du matériel en surplus* [15], le programme Ordinateurs pour les écoles (OPE) du GC dispose d'un droit de préemption sur tout l'équipement informatique de surplus provenant des organismes fédéraux. [16]

Les ministres procèdent d'abord au nettoyage des supports ou de l'équipement qui sera donné en considération du programme OPE, conformément aux lignes directrices du Conseil du Trésor sur la sécurité des TI [1]. Bien qu'il incombe aux ministères de veiller à ce que toutes les informations sensibles aient été supprimées, les ateliers d'OPE appliquent tout de même des procédures de nettoyage des supports pour que ceux-ci soient fin prêts à être données.

Les supports sensibles dont il est impossible de vérifier le résultat du nettoyage doivent être détruits.

Les ateliers d'OPE sont surveillés par le ministère de *l'Innovation, des Sciences et du Développement économique du Canada* (Industrie Canada) au nom du GC.

D.3 Élimination du matériel récupéré

Pour être en mesure d'identifier les mécanismes d'élimination appropriés, les ministères devraient consulter les *Lignes directrices sur l'élimination des équipements électroniques et électriques excédentaires du gouvernement fédéral* [12].

Annexe E Destruction de l'équipement : questions relatives à la santé et à la sécurité

La présente annexe fait état des questions de santé et de sécurité qu'il faut prendre en compte lorsqu'il s'agit de procéder à la destruction d'équipement. Avant de préparer l'équipement utilisé en interne pour la destruction des supports, les ministères devraient réfléchir à la façon de pallier les dangers que l'utilisation dudit équipement pourrait présenter pour la santé et la sécurité de l'effectif.

E.1 Exemples de dangers potentiels

Il est dangereux d'exploiter de l'équipement de destruction qui ne dispose pas d'un système adéquat de captation des poussières. Par exemple, les composantes de téléphones cellulaires et de téléphones intelligents, notamment les piles et les afficheurs LCD, peuvent prendre feu ou dégager des substances toxiques lorsqu'elles sont broyées. De plus, le broyage ou le déchiquetage donnent lieu à des frictions, donc à de la chaleur, et peuvent ainsi libérer une poussière contenant du plomb provenant des soudures présentes dans les circuits imprimés ou contenant des alliages de béryllium provenant des conducteurs flexibles.

Nota

Une étude commandée en 2011 par SPAC (anciennement TPSGC) a permis de déceler des concentrations élevées d'arsenic, de plomb et de chrome près des armoires où sont rangés les broyeurs à téléphones cellulaires.[19]

E.2 Recommandations

La GRC recommande que l'équipement de broyage ou de déchiquetage soit placé dans une pièce bien ventilée où l'air se renouvelle entre 15 et 30 fois par heure; ce taux de renouvellement de l'air correspond aux critères qui sont généralement appliqués aux espaces de stationnement souterrain.

Pour sa part, SPAC formule les recommandations suivantes :

1. veiller à ce que le dispositif interne d'évacuation par filtrage HEPA du broyeur soit en marche pendant le broyage;
2. veiller à ce que le joint d'étanchéité soit bien en place et que la porte de l'armoire soit fermée pendant l'utilisation du broyeur;
3. tenter d'étanchéiser le sac à rebuts en papier de façon diminuer l'accumulation de poussières et de particules dans l'armoire;

19 Selon un rapport d'analyse de la qualité de l'air intérieur (QAI) produit en avril 2011 par 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*.

4. porter un masque à filtre HEPA et des gants en latex nitrile lorsqu'il faut ouvrir l'armoire, remplacer le sac ou nettoyer l'armoire.
5. Comme nombre d'aspirateurs conventionnels ne sont pas en mesure de retenir les poussières et les particules relâchées par le processus de broyage ou de déchiquetage, il conviendra d'employer des aspirateurs à filtres HEPA pour nettoyer l'armoire du broyeur.