Guide opérationnel de la sécurité matérielle
GSMGC-010 (2022)

Préparé par :
Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sécurité ministérielle
Direction générale – 73, promenade Leikin, Ottawa (Ontario) K1A 0R2

Publication diffusée le : 2022-12-05
Mise à jour :

Avant-propos

Le Guide opérationnel de la sécurité matérielle GSMGC-010 (2022) est une publication NON CLASSIFIÉE, diffusée avec l'autorisation du principal organisme responsable de la sécurité matérielle de la Gendarmerie royale du Canada (GRC). Bien qu'il soit NON CLASSIFIÉ, l'accès au présent guide et son utilisation devraient être limités aux ministères et organismes du gouvernement du Canada (GC).

Les suggestions de modifications et les autres renseignements peuvent être envoyés au principal organisme responsable de la sécurité de la GRC par courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Reproduction

Date d'entrée en vigueur

La date d'entrée en vigueur du guide opérationnel de la sécurité matérielle GSMGC-010 (2022) est le 2022-12-05.

Registre des modifications

Nº de la modification	Date	Auteur	Résumé de la modification

Remarque : Le principal organisme responsable de la sécurité matérielle de la Gendarmerie royale du Canada (POSM de la GRC) est autorisé à apporter des modifications.

Remerciements

Le présent guide, publié avec l'approbation du Secrétariat du Conseil du Trésor (SCT), remplace la Norme opérationnelle sur la sécurité matérielle publiée par le SCT, qui a été annulée le 28 juillet 2019.

Table des matières

1. Introduction

La GRC, en tant que principal organisme responsable de la sécurité matérielle (POSM) pour le gouvernement du Canada (GC), est responsable de fournir des conseils et des orientations sur toutes les questions concernant la sécurité matérielle.

1.1. Objectif

Le présent guide vise à fournir aux employés du GC des renseignements sur les mesures de sécurité matérielle de référence. Pour obtenir des renseignements détaillés, les employés devraient consulter leurs politiques, normes et lignes directrices ministérielles en matière de sécurité, ainsi que la Politique sur la sécurité du gouvernement (PSG), l'annexe C de la Directive sur la gestion de la sécurité (DGS) et d'autres Guides des POSM de la GRC afin de mettre en œuvre les mesures appropriées pour contrer les menaces qui pèsent sur les employés, les biens et la prestation des services du gouvernement et assurer une protection uniforme pour le GC.

Le guide contient les mesures de contrôle de sécurité requises (indiquées par l'emploi du mot « doit »), conformément aux politiques et aux règlements, ainsi que des mesures recommandées (indiquées par l'emploi du mot « devrait »).

Les mesures de sécurité matérielle de référence sont conçues pour offrir une protection contre les types courants de menaces auxquels les ministères et organismes pourraient être exposés. Certains ministères et organismes ou activités opérationnelles peuvent être confrontés à des menaces différentes en raison de la nature de leurs activités, de leur emplacement ou de l'attrait de leurs biens. Nous citons comme exemples les établissements policiers ou militaires, les services de santé, les laboratoires, les installations de recherche sur des matières délicates, les musées, les guichets de service au public, les bureaux situés dans des zones de forte criminalité, et les bureaux situés en pays étrangers.

Les dispositions relatives à l'entreposage, à la transmission et à la destruction des renseignements classifiés et protégés et d'autres biens s'appliquent aux installations gouvernementales et non gouvernementales.

1.2. Application, rôles et responsabilités

Tous les ministères et les organismes sont responsables de la protection des employés, des biens et de la prestation des services dans leur domaine de responsabilité. Les directives fournies dans le présent document constituent les exigences minimales. Il incombe aux ministères et organismes de valider ces exigences en fonction des besoins de leur ministère en matière de sécurité.

Les ministères locataires doivent informer les ministères gardiens de leurs exigences en matière de sécurité pour le choix de l'emplacement et des aménagements des locataires. (Voir la section 7 pour en savoir plus.)

Les ministères gardiens doivent fournir les services de sécurité considérés comme nécessaires par le gardien pour assurer la protection des installations et en assurer le financement en regard de l'évaluation des menaces et des risques (EMR) qui a été réalisée par le gardien ou pour celui-ci. Cette responsabilité comprend la mise en œuvre et l'intégration de mesures pour assurer la sécurité de base de l'immeuble (p. ex., portes extérieures et éclairage), les systèmes du bâtiment (p. ex., ascenseurs, systèmes mécaniques et électriques) ainsi que la sécurité des personnes (p. ex., escaliers, avertisseurs d'incendie et gicleurs). Les gardiens doivent en outre intégrer à l'infrastructure de base des immeubles les exigences de sécurité (de base et accrues) dont les locataires assurent le financement.

Ce guide devrait être employé pour appuyer la prise de décisions concernant les installations du GC et ne se rapporte pas uniquement aux lieux de travail à distance ou de télétravail. D'autres guides peuvent être nécessaires pour évaluer pleinement la sécurité à distance ou en télétravail et peuvent être consultés sur la page Principal organisme responsable de la sécurité matérielle – Gendarmerie royale du Canada (rcmp-grc.gc.ca).

1.3. Considérations relatives à la technologie de l'information

En raison de l'évolution constante des menaces et de la convergence de la sécurité matérielle et de la sécurité des technologies de l'information, il est crucial d'évaluer le risque associé à l'utilisation des applications et/ou des logiciels connectés à un réseau qui servent à faire fonctionner l'équipement et à le prendre en charge dans les édifices à accès contrôlé du gouvernement du Canada. Quelques exemples de ces applications ou de ces logiciels de commande peuvent comprendre, entre autres, l'éclairage de sécurité, les barrières de périmètre, les portes, le chauffage, la ventilation et la climatisation, etc.

Avant de mettre en place une application et/ou un logiciel pour commander et/ou automatiser certaines fonctions de l'édifice, la sécurité ministérielle demande qu'une évaluation et autorisation de sécurité (ESA) soit effectuée. Cette ESA garantira le maintien de l'intégrité et de la disponibilité des composants contrôlés par les applications et/ou les logiciels, ainsi que l'atténuation de tout risquent mis en évidence. Il est fortement recommandé de commencer le processus d'ESA tôt pour s'assurer du respect de l'échéancier de livraison du projet. Pour plus d'information sur le processus d'ESA, consultez la sécurité ministérielle.

2. Coordonnées

Pour obtenir de plus amples renseignements, veuillez communiquer avec la GRC aux coordonnées suivantes :

Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
73, promenade Leikin, arrêt postal n° 165
Ottawa (Ontario)
K1A 0R2
Adresse de courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronymes

Acronyme	Signification
TVCF/EVCF	Télévision en circuit fermé/Matériel vidéo en circuit fermé
CST	Centre de la sécurité des télécommunications
PCAM	Prévention du crime par l'aménagement du milieu
DGS	Directive sur la gestion de la sécurité;
FFPA	Federal Fire Protection Association
(EASI)	Évaluation et autorisation liées à la sécurité des installations
GC	Gouvernement du Canada
ZHS	Zone de haute sécurité
POSM	Principal organisme responsable de la sécurité (matérielle)
ZT	Zone de travail
PDIR	Protection, détection, intervention et rétablissement
PSG	Politique sur la sécurité du gouvernement
ZP	Zone d'accès public
GRC	Gendarmerie royale du Canada
ZA	Zone d'accueil
SCIF	Installation renfermant des informations sensibles cloisonnées (pour *Sensitive Compartmented Information Facility*)
AI	Aire insonorisée
COS	Centre des opérations de sécurité
ZSS	Zone de sécurité SIGINT
PES	Pièces d'entreposage sécuritaire
ZS	Zone sûre
SCT	Secrétariat du Conseil du Trésor
EMR	Évaluation de la menace et des risques

4. Glossaire :

Terme	Définition
Actif	Actifs matériels ou immatériels du gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale.
Disponibilité	Se dit de l'information utilisable sur demande au soutien des opérations, des programmes et des services.
Exigences sécuritaires de base	Dispositions obligatoires de la Politique sur la sécurité du gouvernement, des normes opérationnelles connexes et de la documentation technique.
Biens classifiés	Biens dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national.

Informations classifiées	Informations dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national.
Compromission	Divulgation, destruction, suppression, modification, interruption d'accès ou utilisation de renseignements ou de biens non autorisée.
Contrôle de l'accès	Assurer l'accès autorisé aux biens à l'intérieur d'une installation ou de zones d'accès restreint, en effectuant le triage des visiteurs et du matériel aux points d'entrée par les membres du personnel, les gardes ou de façon informatisée et, lorsque requis, en surveillant leur déplacement à l'intérieur de l'installation ou des zones d'accès restreint en les escortant.
Gardien	Le ministère responsable de l'administration d'un immeuble attribué à d'autres ministères au titre de l'exécution de programmes gouvernementaux.
Escorte	Personne possédant une cote de sécurité appropriée qui est responsable de la surveillance continue de personnes n'ayant pas une cote de sécurité dans les secteurs où une cote de sécurité ou un statut seraient normalement exigés.
Installation	Une installation peut être un bâtiment (en tout ou en partie) et peut comprendre son site ou son terrain, ou peut être une zone ou une construction qui n'est pas un bâtiment (par exemple, champs de tir, champs agricoles).
Intégrité	L'exactitude et l'intégralité des biens, et l'authenticité des transactions.
Surveillance continue	Surveillance sur une base continue pour confirmer qu'il n'y a pas eu infraction à la sécurité.
Surveillance périodique	Surveillance périodique, mais régulière pour confirmer qu'il n'y a pas eu d'infraction à la sécurité. La fréquence et la diligence de la surveillance périodique sont fondées sur les recommandations d'une évaluation des risques.
Intérêt national	Concerne la défense et le maintien de la stabilité sociale, politique et économique du Canada.
Besoin de connaître	Le principe selon lequel il est nécessaire pour une personne d'avoir accès à des renseignements et de les connaître afin de pouvoir exécuter ses tâches.
Renseignements protégés	Renseignements dont la compromission risquerait vraisemblablement de porter préjudice à un intérêt non national.
Biens protégés	Biens dont la compromission risquerait vraisemblablement de porter préjudice à un intérêt non national.
Zone d'accès restreint (ZAR)	Aire de travail (site ou édifice) au sein d'un ministère où l'accès est restreint aux individus autorisés. Cela comprend la zone de travail, la zone de sécurité et les zones de haute sécurité définies dans le document de référence : Guide pour l'établissement des zones de sécurité matérielle G1-026.
Locataire	Un ministère qui occupe un immeuble du gouvernement fédéral administré par un autre ministère ou une société d'État.

Accès non autorisé	Accès à des renseignements ou à des biens par un particulier qui n'a pas fait l'objet d'une enquête de sécurité du personnel exigée ou ne satisfait pas aux critères du « besoin de connaître », ou les deux.

5. Types de conditions de menace

Les menaces suivantes sont communes à tous les ministères et organismes gouvernementaux. Divers événements, accidentels ou intentionnels, peuvent provoquer la matérialisation de ces menaces et causer des préjudices.

5.1. Violence liée au travail

En raison de tâches ou de situations liées au travail auxquelles ils sont exposés, les employés peuvent faire l'objet de menaces, verbales ou écrites, ou d'actes de violence physique (p. ex. voies de fait telles que définies dans le Code criminel, intimidation et harcèlement) commis par d'autres employés ou des membres du public. Des menaces liées au travail peuvent survenir sur le lieu de travail ou à l'extérieur alors que les employés sont en service ou hors service.

Le Code canadien du travail (CCT) tient compte du problème de la violence et exige que les employés soient adéquatement protégés. L'employeur (GC) reconnaît aux employés le droit d'être à l'abri de ce type d'actions afin qu'ils puissent accomplir leur travail en toute sécurité. Le règlement sur la prévention de la violence établit la méthode requise d'intervention face aux actes internes et externes de violence et les rôles obligatoires des parties sur le lieu de travail. Les ministères et organismes doivent respecter tous les règlements et toutes les lois lorsqu'ils établissent des procédures. Pour de plus amples renseignements, les ministères et organismes devraient consulter leurs groupes des Relations de travail et des Ressources humaines, le CCT et le Code criminel au besoin.

5.2. Perte de la confidentialité

La divulgation non autorisée de documents protégés ou classifiés peut se produire :

- Accidentellement, par perte ou par négligence de la part d'employés ayant eu accès aux renseignements;
- Intentionnellement, de la part de personnes ayant un accès autorisé aux renseignements (c'est-à-dire ayant fait l'objet d'un contrôle sécuritaire approprié et ayant un besoin de connaître);
- Intentionnellement, de la part de personnes qui obtiennent un accès aux renseignements sans y être autorisées, de quelque manière que ce soit (par exemple, le ciblage de renseignements protégés et classifiés par des criminels, des terroristes ou des services de renseignements étrangers).

Le préjudice causé à l'intérêt national ou aux intérêts privés/non nationaux augmente en fonction du caractère sensible de l'information divulguée. Le préjudice peut comprendre des dommages à la défense et à la stabilité économique, sociale ou politique du Canada, la compromission des intérêts d'autres gouvernements, des atteintes à la confidentialité, des

pertes financières ou liées à la responsabilité, des pertes de confiance envers le GC ou la diminution de l'efficacité du gouvernement. La divulgation non autorisée de renseignements secrets ou protégés C entraîne un préjudice supérieur à la divulgation non autorisée de renseignements protégés A ou B. En outre, certains renseignements protégés ou classifiés peuvent être plus attrayants que d'autres renseignements de la même classification de sécurité et peuvent, par conséquent, nécessiter une protection supérieure à la protection de base requise pour la catégorie d'information. Pour de plus amples renseignements sur la classification de la sécurité, consultez l'annexe J de la DGS.

5.3. Entorse à la disponibilité

Le vol, la fraude, le vandalisme, les cyberattaques et les activités malveillantes, la perte ou l'endommagement accidentel ou intentionnel par des employés ou des membres du public de même que les événements naturels (comme une panne de courant, un incendie ou une inondation) constituent des menaces potentielles pesant sur des biens, qui peuvent priver le gouvernement de leur utilisation et perturber la prestation de programmes et de services. La perte financière ou patrimoniale subie par les Canadiens en fonction du coût de remplacement ou du caractère unique des objets en cause constitue un autre genre de répercussions. Le préjudice augmente selon l'importance des biens pour les Canadiens et pour le gouvernement du Canada.

5.4. Perte d'intégrité

Les cyberattaques et les activités malveillantes, le sabotage intentionnel ou les erreurs attribuables aux employés ou aux systèmes peuvent causer une inexactitude de l'information ou la perte de renseignements, altérer l'utilisation prévue de ceux-ci et entraîner une perte d'authenticité. Ce type d'attaque peut porter atteinte à un intérêt national ou personnel. Parmi les répercussions possibles figurent également la responsabilité à l'égard des conséquences possibles, la perte financière, la perte de confiance envers le gouvernement, ainsi que l'incapacité temporaire ou prolongée de gouverner adéquatement. Les dommages augmentent proportionnellement à la classification des renseignements et des biens.

6. Approche en matière de sécurité matérielle

L'approche adoptée par le gouvernement en matière de sécurité matérielle s'ajoute à d'autres aspects de la PSG. Elle est fondée sur la théorie selon laquelle les zones interne et externe des installations du GC peuvent être conçues et gérées de manière à créer des conditions qui, conjuguées à des mesures particulières de protection de la sécurité matérielle, réduiront les risques de violence à l'égard des employés, assureront une protection contre l'accès non autorisé, permettront de déceler les tentatives ou les cas réels d'accès non autorisé, et entraîneront le déclenchement d'une intervention efficace.

Les stratégies de sécurité matérielle sont axées sur le concept de protection, de détection, d'intervention et de rétablissement; une conception reposant sur une série de zones clairement reconnaissables; un contrôle de l'accès aux zones d'accès restreint; la capacité d'accroître la sécurité pendant les urgences et les situations de menace accrue.

6.1. Protection, détection, intervention et rétablissement (PDIR)

Les ministères et les organismes doivent s'assurer que leur stratégie en matière de sécurité matérielle comprend des éléments identifiables de protection, de détection, d'intervention et de reprise des activités (PDIR). Pour de plus amples renseignements, reportez-vous au Guide de la GRC G1-025 intitulé Protection, détection et intervention de la GRC.

6.1.1. Protection

La protection est assurée par des obstacles matériels, procéduraux et psychologiques visant à exercer un effet dissuasif ou à retarder l'accès non autorisé.

6.1.2. Détection

La détection comporte l'utilisation d'appareils, de procédures et de systèmes adéquats visant à signaler l'occurrence ou la tentative d'accès non autorisé.

6.1.3. Réponse

La réponse consiste à mettre en œuvre des mesures pour s'assurer que les incidents de sécurité sont traités immédiatement. Ces incidents sont ensuite signalés aux responsables de la sécurité concernés. Ainsi, des mesures correctives immédiates et à long terme sont prises en temps opportun.

6.1.4. Rétablissement

La reprise des activités renvoie à la restauration des niveaux entiers de prestation de services suivant un incident.

6.2. Hiérarchie des zones

Les ministères et les organismes doivent veiller à ce que l'accès aux biens protégés et classifiés, ainsi que leur protection respectent une hiérarchie des zones clairement reconnaissable. Il y a cinq zones : accès public, accueil, travail, sécurité et haute sécurité.

6.2.1. Zone publique (ZP)

Zone où le public peut circuler librement et qui entoure habituellement un immeuble gouvernemental ou en fait partie. Parmi les exemples de ZP, citons les terrains entourant un bâtiment ou les corridors publics et les vestibules d'ascenseurs dans les immeubles à locataires multiples.

6.2.2. Zone d'accueil (ZA)

Zone où la transition d'une zone d'accès public à une zone à accès restreint est délimitée et contrôlée. Elle est située généralement à l'entrée de l'immeuble ou des locaux où survient le premier contact entre le public et le ministère. Il peut s'agir de zones dans lesquelles ont lieu des interactions avec les gardiens de sécurité, dans lesquelles des services ministériels sont fournis ou dans lesquelles des renseignements sont échangés. L'accès des visiteurs peut être limité à certaines heures de la journée ou pour des raisons précises.

6.2.3. Zone de travail (ZT)

La zone de travail est une zone dont l'accès est limité au personnel qui y travaille et qui est soumis à des contrôles de sécurité appropriés, ainsi qu'aux visiteurs dûment escortés. Une ZT doit être indiquée par un périmètre reconnaissable et nécessite une surveillance périodique. Les ZT sont un bureau à aire ouverte typique ou un local des installations électriques typique.

6.2.4. Zone de sécurité (ZS)

La zone de sécurité est une zone dont l'accès est limité au personnel autorisé qui détient une cote de sécurité valide et de niveau approprié ainsi qu'aux visiteurs autorisés et dûment escortés. Une ZS doit être indiquée par un périmètre reconnaissable et nécessite une surveillance continue (c.-à-d. jour et nuit, sept jours sur sept). Les ZS sont des zones où des renseignements et des biens secrets sont traités ou entreposés.

6.2.5. Zone de haute sécurité (ZHS)

La zone de haute sécurité est un secteur auquel l'accès est limité au personnel autorisé qui détient une cote de sécurité valide et de niveau approprié ainsi qu'aux visiteurs autorisés et dûment accompagnés. Elle doit être balisée par un périmètre aménagé selon les caractéristiques recommandées dans l'EMR et faire l'objet d'une surveillance continuelle (c.-à-d. 24 heures sur 24, sept jours sur sept), et les détails relatifs à l'accès à ce secteur doivent être consignés et faire l'objet de vérifications. Les ZHS sont soit des zones où des biens de grande valeur sont manipulés, soit des zones où des renseignements et des biens très secrets sont traités et stockés.

Les ZT, les ZS et les ZHS sont appelées zones d'accès restreint. L'établissement d'une hiérarchie de zones permet aux ministères et aux organismes :

- D'entreposer dans la même installation des renseignements ou des biens de

classification différente ou soumis à des menaces différentes;
- D'instaurer divers niveaux de contrôle d'accès pour protéger divers niveaux d'information et de biens;
- De réduire les coûts en traitant et en détruisant des renseignements et des biens de différents niveaux dans une même installation;
- De sélectionner les zones qui se rapportent au travail effectué et d'omettre les zones lorsqu'elles ne sont pas requises;
- Avec une planification appropriée, de changer de zone d'une période à l'autre (c.-à-d. de faire passer une ZT pendant les heures de travail à une ZS pendant les heures de fermeture).

L'accès à des zones particulières devrait être fondé sur le principe du « besoin de connaître » et sur les personnes qui détiennent la cote ou l'autorisation de sécurité appropriée. La restriction de l'accès protège les renseignements, les biens et les employés. Consultez le Guide pour l'établissement des zones de sécurité matérielle G1-026.

Le nombre approprié de zones à l'intérieur d'une installation est établi en fonction des besoins du ministère, du nombre de locataires (un ou plusieurs) et du propriétaire/gardien de l'installation (gouvernement fédéral, provincial ou municipal, secteur privé). Pour un immeuble gouvernemental ayant plusieurs locataires, le comité de l'immeuble ou de l'installation chargé de la sécurité (voir la section 7.7.6) devrait établir la hiérarchie des zones dans les aires communes. Le locataire est responsable de délimiter des zones appropriées dans ses locaux.

6.3. Contrôle de l'accès

Les ministères et les organismes doivent contrôler l'accès aux zones d'accès restreint en prenant des mesures de protection qui n'accorderont l'accès qu'au personnel autorisé. Les ministères et les organismes doivent également examiner périodiquement les droits d'accès et supprimer l'accès lorsqu'il n'est plus nécessaire (c.-à-d. lorsqu'un employé quitte ses fonctions ou change de responsabilités, lorsqu'un entrepreneur termine un projet, etc.). Le contrôle de l'accès aux zones d'accès restreint et à d'autres locaux du ministère doit être accordé de sorte qu'il n'aille pas à l'encontre des exigences en matière de sécurité des personnes du Code national du bâtiment du Canada, du Code national de prévention des incendies du Canada et des codes, normes et directives connexes administrées par la Federal Fire Protection Association (FFPA).

La difficulté pour les ministères réside dans la nécessité de concilier un contrôle efficace de l'accès pour le matériel et les personnes non autorisées et un accès facile pour le matériel et les personnes autorisées. Parmi les zones suscitant des préoccupations, mentionnons les entrées des piétons, le contrôle de l'accès des visiteurs, les aires de réception et d'expédition, le stationnement, les locaux techniques, les salles du courrier et les couloirs menant aux zones d'accès restreint.

Parmi les facteurs qui ont une incidence sur la façon de contrôler l'accès se trouvent la taille et l'emplacement de l'installation de même que la nature des activités qui y sont entreprises.

Par exemple, l'exigence de contrôle de l'accès pourrait se traduire par une série de procédures administratives : la signature à l'entrée et à la sortie des visiteurs et la présentation par les employés d'un insigne d'identité au personnel de sécurité, ou un système où les visiteurs doivent signaler leur présence à un employé, qui les accompagnera dans l'installation. Les établissements qui n'abritent qu'un petit nombre d'employés se baseront sur des techniques de reconnaissance personnelle pour identifier les personnes autorisées ou non à pénétrer dans les locaux. Les ministères et les organismes devraient mettre en place des contrôles d'accès électroniques (c.-à-d. accès par carte, NIP ou contrôle biométrique) pour satisfaire aux exigences de contrôle d'accès obligatoire. Une EMR servira à déterminer les moyens efficaces et rentables de contrôler l'accès aux espaces publics et aux installations.

Pour faciliter le contrôle de l'accès aux locaux des ministères, les ministères et les organismes doivent planifier avec soin la manière dont les personnes et le matériel entreront dans leurs locaux. Les ministères et les organismes doivent mettre en place des procédures de détection des colis suspects dès l'arrivée du courrier et des livraisons. La nature et la portée de ces procédures devraient être déterminées par une EMR. Pour de plus amples renseignements, reportez-vous au Guide de la GRC G1-024 intitulé Contrôle de l'accès de la GRC.

6.4. Augmentation de la sécurité en cas d'urgence et de menace

Les mesures de sécurité adoptées pour contrôler l'accès du personnel ou les protocoles de gestion des risques liés aux biens et aux renseignements de nature délicate doivent tenir compte de la nécessité de mettre en œuvre des niveaux plus élevés de préparation durant les situations d'urgence ou caractérisées par un niveau plus élevé de menace. Les ministères et les organismes doivent travailler avec les intervenants à l'élaboration de procédures de sécurité évolutives pour réagir à des situations de sécurité ou d'urgence accrues, comme des intrus armés, des manifestations ou toute menace particulière visant leurs installations ou leur personnel.

La section C.2.3.4 de la DSM sur les contrôles supplémentaires stipule ce qui suit : Mettre en œuvre des mesures supplémentaires, au besoin, pour respecter les exigences en matière de sécurité du ministère ou atteindre un niveau élevé de préparation en cas d'urgence ou de situations de menaces accrues. Ces contrôles supplémentaires comprennent le filtrage du courrier entrant ou des livraisons pour repérer les colis suspects, les espaces de discussion spéciaux, les salles sécurisées, les contre-mesures de surveillance technique, les instructions de destruction d'urgence et les mesures de protection de l'information ou des biens de nature délicate ou précieuse.

7. Sécurité dans le choix et la conception des installations

7.1. Introduction

La section C.2.3.1 de la DSM sur la conception de l'environnement des installations stipule ce qui suit : Concevoir, intégrer et gérer les cadres extérieur et intérieur d'une installation pour

mettre en place des conditions qui, de pair avec des mesures de sécurité précises, permettent, dans la mesure du possible, de déceler les tentatives d'accès ou les accès non autorisés, et de déclencher une intervention efficace afin de répondre aux exigences en matière de sécurité du ministère, y compris la surveillance électronique.

Les ministères et les organismes doivent examiner régulièrement leurs installations existantes dans le cadre de leurs activités d'EMR pour déterminer si des mesures de contrôle de sécurité supplémentaires ou modifiées sont nécessaires. Les informations fournies dans ce guide ne concernent pas un type particulier d'installation et ne sont pas exhaustives. Bien qu'elles soient utiles pour les immeubles de bureaux, elles s'appliquent également à d'autres types d'installations comme les installations de co-travail du GC, les entrepôts, les laboratoires, les terrains, les ponts, les quais et les barrages. Tous ces emplacements nécessitent des mesures de contrôle de sécurité uniques pour assurer une sécurité adéquate contre les menaces définies dans ce guide et l'EMR en question.

La PSG et la DSM exigent des ministères et des organismes qu'ils s'assurent que la sécurité est pleinement intégrée dès le début du processus de planification, de sélection, de conception et de modification de leurs installations. Cela peut se faire au moyen du processus d'évaluation et d'autorisation liées à la sécurité des installations (EASI) (reportez-vous au Guide du processus d'évaluation et d'autorisation liées à la sécurité des installations – GSMGC-016). Il est important de veiller à ce que la sécurité soit prise en considération à toutes les étapes de construction ou de modification d'un projet. Une équipe pluridisciplinaire constituée de responsables de la sécurité, de responsables de l'hygiène et de la sécurité au travail, d'experts de l'immobilier et de gestionnaires de programmes et de projets devrait déterminer les critères de sécurité pertinents à adopter pour chaque projet d'après les exigences de sécurité de base et une EMR. Les ministères et les organismes doivent inclure les exigences nécessaires au titre de la sécurité dans tous les plans, les demandes de propositions et les appels d'offres pour les projets de construction ou de modification et intégrer les coûts connexes dans les exigences de financement.

7.2. Planification et sécurité générales

Les gestionnaires de projet, les professionnels des biens immobiliers et de la sécurité devraient utiliser l'information contenue dans cette section lorsqu'ils établissent une stratégie de contrôle de la sécurité pour un projet particulier.

7.2.1. Codes et politiques applicables

Les ministères et les organismes doivent veiller à la conformité des mesures de sécurité matérielle aux règlements, aux codes et aux politiques applicables (c.-à-d. les règlements et codes relatifs au travail, aux incendies, au bâtiment et à l'électricité, ainsi que les politiques connexes en matière de biens immobiliers).

7.2.2. Alimentation de secours

L'alimentation de secours doit être fournie pour les services de base du bâtiment (c.-à-d. fonctionnement partiel des ascenseurs et éclairage de secours). Cette

alimentation doit être appropriée aux installations pour assurer une évacuation sécuritaire en cas d'urgence et protéger les biens du gouvernement. Les besoins en alimentation de secours pour les systèmes de sécurité (c.-à-d. serrures de porte électroniques, TVCF/EVCF, alarmes) seront déterminés par une EMR. À tout le moins, l'alimentation électrique de secours doit être conforme au Code national du bâtiment du Canada et au Code national de prévention des incendies.

7.3. Sécurité du périmètre – Facteurs à prendre en compte dans le choix du site

7.3.1. Servitudes d'accès aux lieux et voies de circulation d'urgence

Pendant le choix de l'emplacement et la négociation du bail, les servitudes à l'intérieur des installations ou attenantes à celles-ci qui pourraient avoir une incidence sur la sécurité du personnel ou la sécurité des biens doivent être examinées. Des servitudes qui permettent aux équipes des services publics, au public ou au personnel des services d'urgence d'avoir accès à des lieux limitent la capacité du locataire de contrôler l'accès. Il peut en résulter que des personnes non autorisées ont accès à l'équipement, aux employés ou aux installations.

7.3.2. Contrôle du périmètre

Le contrôle du périmètre du site devrait être maintenu grâce à l'application des principes de prévention du crime par l'aménagement du milieu (PCAM). Il peut s'agir notamment de garder les intrus en observation au moyen de la surveillance naturelle, de diminuer le crime par le contrôle naturel de l'accès, de créer un sentiment de propriété par le renforcement du territoire, ou d'utiliser des éléments paysagers comme des clôtures, des jardinières et le nivellement du terrain. D'autres mesures de contrôle du périmètre comme le contrôle électronique de l'accès, la TVCF/EVCF, les systèmes d'alarme, les barrières et les clôtures devraient être envisagés.

7.3.3. Aperçu du site, emplacement de l'immeuble et topographie

La conception et l'édification des immeubles devraient faciliter la surveillance naturelle par la police et le public de la zone avoisinante (c.-à-d. des routes ou d'autres bâtiments à proximité), sauf si cette approche n'est pas jugée souhaitable dans le cadre des stratégies ministérielles de protection. Un examen approfondi des statistiques sur la criminalité relative à l'emplacement proposé des immeubles doit être entrepris pour vérifier que l'emplacement est adapté à la fonction prévue des immeubles. Les ministères et les organismes doivent également respecter les exigences du FFPA quant au caractère particulier de l'immeuble en cas d'évacuation d'urgence.

7.3.4. Services d'urgence

La capacité en eau requise pour la lutte contre les incendies et les délais d'intervention efficaces des pompiers et des policiers doivent être pris en considération lors de l'élaboration des stratégies de protection. Ces stratégies

doivent être fondées sur les principes de protection, de détection et d'intervention qui s'appliquent au choix du site, aux installations et aux biens. Des mesures de remplacement ou des mesures supplémentaires en matière de sécurité des personnes et de protection des biens peuvent être nécessaires afin de compenser la lenteur des interventions d'urgence. Les ministères et les organismes doivent obtenir et suivre les directives du FFPA relativement à l'alimentation en eau requise pour lutter contre les incendies.

7.3.5. Occupants des immeubles attenants

Les attenants (occupants, locataires et utilisateurs de l'immeuble) devraient être pris en compte lors du choix du site. Il faudrait notamment tenir compte de l'impact potentiel des occupants des immeubles attenants sur la sécurité des employés du ministère et sur la prestation des services. Il faudrait aussi tenir compte de l'incidence des activités ministérielles sur les occupants des immeubles attenants (qu'ils soient gouvernementaux ou non).

7.3.6. Éclairage du site

L'éclairage devrait être suffisant dans les installations et autour de celles-ci afin de permettre la détection et l'observation des personnes qui approchent des installations, d'exercer un effet dissuasif sur l'activité criminelle opportuniste, de réagir aux autres menaces pour la sécurité (c.-à-d. vandalisme et violence liée au travail) et de soutenir des éléments de surveillance (c.-à-d. surveillance naturelle et TVCF/EVCF). Le choix des niveaux d'éclairage doit être fondé sur le règlement applicable, la technologie photographique et d'autres aspects liés à la sécurité. Consultez le Guide sur les considérations liées à l'éclairage de sécurité – GCPSG-004 de la GRC pour en savoir plus.

7.3.7. Affichage extérieur

Les affiches qui désignent les installations occupées par les ministères et organismes du gouvernement fédéral doivent être conformes au Programme fédéral de l'image de marque. En outre, les installations devraient afficher des renseignements indiquant clairement les points de rassemblement d'urgence du site, ainsi que des indications sur le stationnement, les visiteurs, les employés et les zones de service. Il faut tenir compte de toute condition ou réglementation imposée par les lois provinciales, territoriales ou municipales (c.-à-d. concernant le système de TVCF/EVCF ou pour prouver l'intrusion) lorsque vous utilisez des panneaux pour définir les limites des biens du gouvernement ou établir des zones d'accès restreint conformément à une EMR.

7.3.8. Aménagement paysager

Les éléments de l'aménagement paysager entourant une installation devraient adopter les principes de PCAM et appuyer la stratégie de protection, de détection et d'intervention. Les éléments de sécurité de l'aménagement paysager peuvent comprendre :

- des limites clairement indiquées;
- des clôtures, des murs et d'autres barrières;
- des voies de passage conçues pour faciliter la surveillance naturelle;
- des possibilités limitées de couverture naturelle offertes aux intrus;
- une bonne visibilité des éventuels secteurs à problèmes (c.-à-d. où des activités criminelles risquent de survenir) pour le personnel de sécurité, les employés et le public;
- éviter les matériaux et l'ameublement risquant d'exposer l'immeuble à un plus grand risque dans une situation où la sécurité doit être accrue (c.-à-d. si une manifestation tourne à la violence).

Les principes de la PCAM comprennent également la réduction des possibilités de criminalité grâce à la surveillance naturelle et au contrôle naturel de l'accès, la création d'un sentiment d'appartenance grâce au renforcement territorial et l'utilisation de caractéristiques de l'aménagement paysager comme les clôtures, les jardinières et le nivellement du terrain.

7.3.9. Parcs de stationnement

L'EMR déterminera les mesures de protection nécessaires pour protéger les employés dans les parcs de stationnement sur les installations du GC. Ces mesures de protection peuvent comprendre la mise en place d'un parc de stationnement désigné près de l'installation, l'ajout d'un éclairage de sécurité adéquat, de clôtures de sécurité, d'escortes officielles ou l'installation d'un système de jumelage où les employés sont accompagnés jusqu'à leur véhicule.

7.4. Sécurité de l'entrée

7.4.1. Entrées des piétons et halls d'entrée

Une façon de contrôler physiquement l'accès à une installation ou à ses zones d'accès restreint consiste à aménager des points d'entrée contrôlés. Un point d'entrée canalise la circulation (des employés et des visiteurs) à l'installation d'une manière qui permet que des opérations efficaces de surveillance, de filtrage ou de contrôle soient effectuées par du personnel, par des gardes ou par des moyens automatisés.

7.4.2. Points d'entrée et de sortie des services publics, mécaniques et électriques

Les points d'entrée et de sortie des services publics (tels que les prises et les conduits d'air, les trappes de toit et l'approvisionnement en eau) doivent être protégés pour garantir que les actifs essentiels, les mesures pour la sécurité des personnes et les programmes ministériels ne soient pas compromis par un accès non autorisé ou non contrôlé.

7.4.3. Zones d'expédition et de réception, quais de chargement et salles de courrier

Dans la mesure du possible, les zones d'expédition et de réception, les quais de chargement et les salles du courrier ne devraient pas être directement liés ou attenants à des zones d'accès restreint ou à l'infrastructure essentielle de l'immeuble (comme les canalisations principales, les systèmes de refroidissement et de chauffage, les systèmes de détection des incendies et les systèmes d'alarme, les circuits électriques, téléphoniques et de transmission de données, ainsi que les autres branchements).

7.5. Sécurité intérieure – Planification

7.5.1. Voies de circulation, corridors intérieurs et vestibules d'ascenseur

Les voies de circulation qui permettent aux employés et aux visiteurs d'accéder aux zones d'accès restreint doivent être soigneusement planifiées. Ainsi, les exigences en matière de sécurité des personnes sont respectées et le contrôle de l'accès aux zones d'accès restreint peut être maintenu.

La planification des activités liées aux renseignements et aux biens protégés et classifiés ainsi que des lieux connexes doit garantir que les mesures de protection requises ne sont pas compromises au cours des situations d'urgence. Par exemple, une ZHS située dans une galerie de communication d'un immeuble de grande hauteur pourrait obliger les personnes non autorisées à la traverser pour accéder à une deuxième cage d'escalier en cas d'urgence. D'autres zones pour lesquelles il faut trouver un équilibre entre la sécurité des personnes et la sécurité matérielle comprennent les vestibules d'ascenseurs, les corridors et les restrictions relatives à l'utilisation de serrures particulières. L'annexe A du Guide de la GRC G1-024 intitulé Contrôle de l'accès, présente les pratiques optimales concernant le zonage et l'aménagement de l'immeuble, la compartimentation, les galeries de communication, l'accès aux sorties, etc.

L'accès des employés et des visiteurs aux zones d'accès restreint devrait être fondé sur les tâches et fonctions de la personne, la cote de sécurité ou le statut de celle-ci et le principe du « besoin de connaître », en tenant compte des possibilités d'observation et d'écoute.

L'aménagement des voies de passage empruntées par les employés pour transporter des biens précieux devrait être planifié de façon à contrer les menaces établies par l'entremise d'une EMR, y compris celles qui sont définies dans la section 5.

Le cas échéant, l'accès aux locaux des locataires depuis les halls d'ascenseurs doit être contrôlé à l'égard des employés, des entrepreneurs, des visiteurs et du personnel de service. Les mesures de protection peuvent varier selon la nature des programmes

ministériels, la superficie des installations des locataires et le nombre de personnes devant avoir accès à un étage donné. Il peut s'agir d'une barrière physique telle qu'un mur, d'un dispositif faisant appel à du personnel, tel qu'un agent de sécurité ou une fonction d'accueil, d'un système de contrôle d'accès électronique ou mécanique comme un clavier ou des clés, ainsi que de procédures de sécurité telles que la restriction de l'utilisation des ascenseurs au personnel autorisé ou encore le recours à des employés pour interpeller les personnes.

7.5.2. Garderies

Lorsque des garderies sont situées dans des installations du GC, il faut tenir compte de la sécurité des locataires et du public en tenant compte des responsabilités du GC. Les garderies ne devraient pas être situées dans les locaux de ministères et d'organismes dont les programmes ou les activités peuvent être interrompus ou faire l'objet de menaces accrues en raison d'événements tels que des protestations ou des manifestations ni dans ceux de ministères et d'organismes susceptibles de traiter avec des clients à haut risque (y compris des personnes potentiellement violentes). Les installations de ministères et d'organismes du GC dans lesquels se trouvent des garderies devraient avoir des sections bien précises dans leurs plans d'urgence pour assurer la protection de la garderie.

7.5.3. Escaliers et ascenseurs

Les escaliers et les ascenseurs ne devraient pas permettre un accès direct aux zones d'accès restreint du locataire ou à l'infrastructure essentielle de l'immeuble. Dans la mesure du possible, les ascenseurs et les monte-charge (y compris ceux des parcs de stationnement et des quais de chargement) devraient déboucher dans une zone publique ou une zone d'accueil, comme le vestibule de l'ascenseur du rez-de-chaussée. Toutefois, les ascenseurs ou les cages d'escalier peuvent s'ouvrir sur l'espace du locataire si cet accès est surveillé en permanence par le locataire ou si l'espace est sécurisé à tout moment.

7.5.4. Toilettes

L'emplacement des toilettes des employés et des toilettes publiques doit tenir compte de la sécurité des employés. Lorsqu'une EMR le recommande, les toilettes des employés ne devraient pas être accessibles à partir des zones publiques ou des zones d'accueil et les toilettes publiques ne devraient jamais être accessibles à partir des zones de travail ou des zones de sécurité.

7.5.5. Aires de service communes

Il convient de tenir compte de la sécurité des employés dès l'étape de la conception et de la mise en place des aires de service communes (comme les gymnases, les zones de restauration, les salles de réunion ou de conférence). Le personnel ne devrait pas être obligé de franchir des zones d'accès restreint pour accéder aux aires communes.

7.5.6. Télécommunications et liaison des données dans un immeuble

Une EMR devrait être employée pour déterminer les mesures de sécurité matérielle adaptées au réseau de câblage des télécommunications dans une installation. Vous trouverez de plus amples renseignements dans la Politique sur les services et le numérique.

7.6. Contrôle des zones à accès restreint

Plusieurs choix s'offrent aux ministères et aux organismes pour contrôler l'accès aux zones d'accès restreint. Parmi ceux-ci figurent la reconnaissance des personnes, les insignes d'accès, les mesures mécaniques (par exemple, les clés), le contrôle électronique des accès, etc. Le choix approprié dépendra de l'emplacement de l'immeuble, du nombre d'employés, de l'EMR, etc. Veuillez consulter le guide de la GRC G1-024 Contrôle de l'accès pour de plus amples renseignements sur les méthodes de contrôle de l'accès.

7.6.1. Cartes d'identité/insignes d'accès

« Tous les employés du gouvernement doivent obtenir une carte d'identité qui présente au moins le nom du ministère ou de l'organisme pour lequel l'employé travaille, le nom et la photo de l'employé, un numéro de carte unique et une date d'expiration. » Les insignes d'accès identifient les employés et les visiteurs autorisés. Un insigne d'accès temporaire identifiant clairement le porteur comme un non-salarié doit être délivré à tous les visiteurs (y compris les employés non autorisés, les entrepreneurs et le personnel d'entretien) qui ne peuvent être accompagnés par une escorte lors de leurs déplacements. Les cartes d'identité et les insignes d'accès peuvent être combinés en une seule carte. Veuillez vous référer au guide de la GRC G1 – 006, Cartes d'identité/Insignes d'accès pour obtenir des renseignements supplémentaires.

7.6.2. Contrôle électronique d'accès

Le contrôle électronique d'accès est une protection supplémentaire pour contrôler l'accès à une installation. Une EMR permettra d'établir si le recours à un tel système est pertinent et rentable.

7.6.3. Système de télévision/équipement vidéo en circuit fermé (TVCF/EVCF)

L'équipement du TVCF/EVCF peut aider un ministère à surveiller l'accès à ses installations. Une EMR aidera à déterminer le besoin d'un système de TVCF/EVCF. Tout détail concernant la conservation, le stockage, l'utilisation ou la diffusion de vidéos devrait faire partie du processus d'EMR et peut nécessiter des recherches sur les lois et règlements locaux.

7.6.4. Centre des opérations de sécurité (COS)

Un centre des opérations de sécurité (COS), qu'il soit interne au ministère ou externe, constitue le point central de surveillance des divers systèmes, comme le système électronique de contrôle de l'accès, le système électronique de détection des

intrusions et le système de TVCF/EVCF. Le COS comprend habituellement d'autres dispositifs de sécurité des personnes ou de protection personnelle tels qu'un panneau d'alarme incendie. Les grands ministères ou les installations complexes peuvent exiger un COS complet. Toutefois, une version réduite d'un COS peut être nécessaire dans toutes les installations du GC. Consultez le document Guide des considérations relatives à la conception d'un centre des opérations de sécurité – GSMGC-003.

7.6.5. Aires insonorisées

Une aire insonorisée est un endroit spécialement conçu et géré de manière à empêcher au moyen de l'atténuation des bruits que des renseignements protégés et classifiés soient ébruités. En raison du coût de construction et d'opération d'une aire insonorisée, les ministères et les organismes devraient évaluer attentivement la nécessité, le risque et le rapport coût-efficacité des options. Lorsque la construction et l'utilisation d'une aire insonorisée sont envisagées, consultez le Guide de construction des aires insonorisées – GSMGC-017 Guide de construction des zones de discussion sécurisées ou le POSM de la GRC.

7.6.6. Pièce d'entreposage sécuritaire (PES)

Les pièces d'entreposage sécuritaire (PES) sont des pièces construites selon des normes techniques particulières. Une PES peut être utilisée pour l'entreposage sur étagère ouverte de documents protégés et classifiés, ce qui requiert normalement un coffre de sécurité approuvé. L'utilisation d'une PES pour l'entreposage élimine la nécessité d'utiliser un coffre de sécurité approuvé seulement si le principe du « besoin de connaître » n'est pas un facteur. Consulter le guide de la GRC G13-001 – Pièces d'entreposage sécuritaire pour connaître les instructions de construction. Lorsque la fonction ministérielle ou une EMR l'exige, une PES peut être appropriée pour l'entreposage de documents qui ont une force probante pendant les enquêtes ou en attente de présentation au tribunal.

7.6.7. Gardes de sécurité

Si une EMR établit une exigence en matière de sécurité pour l'embauche de gardiens de sécurité, les questions liées au type de gardien (exclusif ou contractuel), aux tâches, à la formation, à l'équipement et à la sécurité devraient être abordées.

7.7. Gestion des installations

7.7.1. Baux et autres conventions d'occupation

La section C.2.7 de la DGS stipule ce qui suit : Établir des ententes consignées (bail ou accord d'occupation) qui définissent les exigences pertinentes et les responsabilités respectives en matière de sécurité, lorsque le ministère appuie une autre organisation ou y fait appel, y compris, sans toutefois s'y limiter, d'autres ministères fédéraux, d'autres ordres de gouvernements et des fournisseurs et partenaires du secteur privé, pour répondre aux exigences du ministère en matière de sécurité matérielle.

Les baux et autres conventions d'occupation doivent tenir compte des mesures de sécurité matérielle dont les ministères ont besoin dans un immeuble.

Pour d'autres détails, reportez-vous à la DSM :

- C.2.7.1 Pour les installations situées dans des immeubles dont le ministère est le gardien;
- C.2.7.2 Pour les installations où le ministère est locataire;
- C.2.7.3 Pour les installations à locataires multiples occupées ou gérées par le ministère;
- C.2.7.4 Lorsque des personnes d'un autre ministère ou organisme requièrent un accès régulier aux installations occupées ou gérées par le ministère.

7.7.2. Services d'entretien et de nettoyage

Lorsque le nettoyage ou l'entretien d'un immeuble doit se faire pendant les heures d'accès restreint, le ministère gardien devrait faire office d'autorité contractante.

7.7.3. Affichage intérieur

Au moins une affiche bien en vue à l'entrée principale des installations devrait diriger les visiteurs vers les zones d'accueil des locataires fédéraux. Les affiches qui désignent les installations occupées par les ministères et organismes du gouvernement fédéral doivent être conformes au Programme fédéral de l'image de marque.

7.7.4. Serrures et contrôle des clés

Toutes les serrures devraient être de qualité commerciale. De plus, un protocole de verrouillage complet devrait être mis en œuvre pour l'établissement, y compris le contrôle des clés et la responsabilité des clés. Les serrures des portes du périmètre devraient être réglées différemment des autres serrures, et elles ne devraient pas permettre l'accès à l'aide d'une clé maîtresse. Limiter les clés passe-partout aux locaux d'entretien et autres espaces de ce type peut également être souhaitable, notamment dans les grandes installations.

Les clés pour l'immeuble au complet, les clés de rechange et les renseignements nécessaires pour reproduire les clés ne devraient pas tous être conservés dans le même coffre. Les clés passe-partout ne devraient pas quitter l'immeuble et ne devraient pas permettre d'identifier l'immeuble auquel elles donnent accès. Les entrées principales et secondaires de l'immeuble, les ZS et les ZHS ne doivent pas faire partie du système de verrouillage principal.

7.7.5. Travaux de rénovation

Lorsque des travaux de rénovation sont nécessaires dans des zones d'accès restreint, les responsables de la sécurité et des biens immobiliers des ministères gardiens et locataires devraient consulter les ministères à l'avance. Les consultations devraient fournir des détails sur les dispositions de sécurité pour l'accès des contractants qui

sont acceptables pour le locataire afin d'assurer la sécurité du personnel et d'empêcher la compromission des renseignements ou des biens.

7.7.6. Comité sur la sécurité de l'immeuble ou des installations

Dans les installations à locataires multiples, un comité de sécurité présidé par le locataire principal ou le ministère gardien devrait être mis sur pied afin de coordonner toutes les exigences du ministère gardien et des ministères locataires en matière de contrôle de l'accès et de planifier des protections supplémentaires pour les situations où la sécurité devrait être accrue. Les représentants des ministères locataires devraient être autorisés par leurs agents de sécurité du ministère à prendre des décisions de planification des mesures de sécurité, comme des services d'agents de sécurité.

8. Stockage

8.1. Généralités

Les renseignements protégés et classifiés devraient être entreposés dans des coffres approuvés et dans les zones d'accès restreint appropriées. Les biens protégés et classifiés (c.-à-d. l'équipement de recherche et de développement classifié, les modèles techniques ou les prototypes) devraient être entreposés dans des coffres approuvés à cette fin. Pour obtenir des directives précises sur l'entreposage, consultez le guide GSMGC-007 – Transport, transmission et entreposage de renseignements protégés ou classifiés. Pour les exigences non respectées par le guide GSMGC-007 Transport, transmission et entreposage de matériel protégé ou classifié , ou par les éléments énumérés dans le document Accueil; GRC : Guide d'équipment de sécurité (rcmp-grc.gc.ca), communiquez avec le POSM de la GRC.

Envisagez des mesures de protection appropriées pour vous assurer que les informations et les biens de valeur classifiés et protégés (ordinateurs portables) sont protégés lorsque les occupants ne se trouvent pas à leur poste de travail pendant une période donnée.

8.2. Coffres de sécurité

Lorsque des matériels protégés ou classifiés de différents niveaux sont entreposés ensemble, la norme d'entreposage doit être respectée pour le bien dont le niveau de classification est le plus élevé. L'entreposage peu fréquent d'une quantité relativement faible d'actifs d'un niveau de classification supérieur avec une quantité plus importante d'actifs d'un niveau de classification inférieur ne justifie pas nécessairement des mesures de protection renforcées. Des renseignements classifiés et des biens de grande valeur comme des instruments monétaires (argent comptant) et des médicaments ne devraient pas être gardés dans le même coffre de sécurité. Les porte-documents ne sont pas des coffres de sécurité et ne devraient pas être utilisés à cette fin. Consultez le document de la GRC G1-001 – Guide d'équipement de sécurité.

Les ministères et les organismes devraient élaborer des procédures pour l'entreposage des biens qui sont partagés avec eux par d'autres ministères et ordres de gouvernement du GC,

des gouvernements étrangers ou des organisations internationales, du secteur de l'éducation et du secteur privé. Ces procédures doivent être conformes aux ententes ou accords internationaux entre les parties concernées et la PSG.

Tous les employés qui travaillent hors site doivent protéger l'information conformément aux exigences minimales énoncées dans le document de la GRC GSMGC-008 – Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance. Les employés devraient aussi consulter la politique sur le télétravail du SCT. En ce qui concerne les travaux contractuels hors site, les ministères et les organismes devraient se fonder sur la Liste de vérification des exigences relatives à la sécurité (LVERS) (Formulaire No. TBS/SCT 350-103) (canada.ca) pour définir les exigences contractuelles et consulter le Programme de sécurité des contrats de Services publics et Approvisionnement Canada (SPAC) pour la protection appropriée des biens protégés ou classifiés dans les installations de l'entrepreneur.

L'accès au contenu des coffres de sécurité doit être limité aux personnes suivantes :

- Les personnes qui possèdent une cote ou une attestation de sécurité correspondant à la classification du matériel entreposé dans le coffre;
- Les personnes qui ont un « besoin de connaître » ou un « besoin d'accéder » au matériel entreposé dans le coffre.

8.3. Biens précieux

Les biens de grande valeur doivent être protégés contre la perte, la destruction ou l'altération. Le degré de protection requis dépend de la valeur du bien lui-même et de l'EMR. Certaines mesures de protection sont contenues dans le G1-001 – Guide d'équipement de sécurité de la GRC. Pour obtenir des renseignements additionnels, veuillez contacter le POSM de la GRC.

8.4. Clés des coffres de sécurité

Dans le contexte de cette section, il est important de comprendre que les « clés » englobent les clés mécaniques, les combinaisons, les cartes d'accès et les numéros d'identification personnels (NIP). Les clés des coffres de sécurité devraient être gardées conformément aux directives de sécurité relatives aux biens ou aux renseignements de nature délicate du niveau le plus élevé auxquels elles donnent accès. Cette exigence s'applique également aux documents qui expliquent les modalités de reproduction des clés.

Les clés qui donnent accès aux coffres de sécurité devraient être changées pour toutes les raisons suivantes :

- Annuellement;
- Lorsque des éléments de preuve révèlent que des articles peuvent avoir été compromis;
- Si une EMR indique un changement dans le niveau de risque;
- Un employé n'a plus besoin d'accéder au conteneur de sécurité.

Un dossier de tous les changements apportés aux clés des coffres de sécurité devrait être

conservé et doit inclure la date et le motif du changement, le gardien, l'endroit et, s'il y a lieu, le numéro d'identification de la serrure, le numéro de la combinaison, les doubles, etc. Ce dossier des changements devrait être protégé conformément aux directives se rapportant au niveau de sécurité le plus élevé des biens ou des renseignements qui se trouvent dans le coffre.

8.5. Disposition ou recyclage des coffres de sécurité

La disposition des coffres de sécurité incombe aux ministères et aux organismes. Les coffres de haute sécurité approuvés pour des renseignements protégés de niveau C et classifiés ne doivent pas être disposés ou vendus au secteur privé à des organismes de l'extérieur. Pour obtenir de plus amples renseignements, veuillez consulter le guide de la GRC, G1-001 – Guide d'équipement de sécurité.

Avant la disposition ou le recyclage, il incombe au ministère de veiller à ce que tous les coffres soient entreposés au moins dans une zone de travail, que les coffres soient complètement vidés et que les dossiers soient modifiés en conséquence.

8.6. Réparation et entretien des coffres de sécurité

Les ministères et les organismes doivent s'assurer que les coffres d'entreposage approuvés sont bien entretenus en tout temps. Consultez le document de la GRC G1-001 – Guide d'équipement de sécurité.

9. Transport et transmission

Le maintien d'un accès autorisé au matériel protégé et classifié est primordial lors de son transport. Pendant le transport de biens protégés et classifiés d'une personne à une autre ou d'un lieu à un autre, les mesures de protection à adopter doivent permettre de contrôler l'accès aux renseignements selon le principe du besoin de connaître. Cela s'applique également à l'entretien des contenants. Les ministères et les organismes sont responsables de la protection de l'équipement de sécurité, comme les coffres de sécurité, pendant le transport nécessaire aux activités d'entretien;

Pendant la transmission de biens protégés et classifiés d'une personne à une autre ou d'un lieu à un autre, les mesures de protection à adopter doivent être axées sur l'emballage qui s'impose, ainsi que sur des services postaux et de messagerie fiables (gouvernement ou secteur privé) et sur le degré d'anonymat que ces renseignements peuvent conserver pendant le transport. Pour les biens protégés et classifiés qui sont soumis à un risque plus élevé, des mesures additionnelles de protection devraient être adoptées, tel qu'il est indiqué dans l'EMR.

Les ministères et les organismes doivent transporter ou transmettre des biens protégés et classifiés conformément aux exigences minimales. Des précisions sur les modalités concernant les enveloppes, les adresses et les services de messagerie pour le transport et la transmission de biens protégés et classifiés sont énoncées dans le guide de la GRC GSMGC-007 – Transport, transmission et entreposage de renseignements protégés ou classifiés.

10. Destruction

10.1. Entreposage de rebuts protégés et classifiés

Les biens protégés et classifiés en attente d'être détruits, sur ou hors site, doivent être rangés dans un coffre de sécurité approuvé ou dans une salle sécuritaire. Les ministères et les organismes doivent protéger les renseignements qui sont transportés vers une installation de destruction de la manière prescrite pour les renseignements classifiés ou protégés du plus haut niveau. Consulter le guide de la GRC GSMGC-007 – Transport, transmission et entreposage de renseignements protégés ou classifiés.

10.2. Destruction des biens

Les ministères et les organismes doivent établir des procédures qui permettront d'assurer la sécurité des biens de grande valeur et des biens protégés et classifiés qui doivent être détruits. Ces procédures comprennent les éléments suivants :

- Informer le personnel des niveaux les plus élevés de renseignements protégés et classifiés qui peuvent être détruits au moyen de l'équipement du bureau;
- Veiller à ce que le personnel autorisé soit présent pour surveiller la destruction des biens de grande valeur et des biens protégés et classifiés;
- Séparer les renseignements protégés et classifiés en attente de destruction des renseignements qui ne sont pas de nature délicate.

10.3. Destruction de l'information

Les ministères et les organismes doivent établir des procédures qui permettront d'assurer la sécurité pour la protection des renseignements protégés et classifiés qui doivent être détruits. Ces procédures comprennent les éléments suivants :

- Les renseignements protégés et classifiés qui n'ont aucune valeur historique ou archivistique et pour lesquels la période de conservation est expirée doivent être détruits, y compris les copies excédentaires, les brouillons et les rebuts.
- Les ministères et les organismes doivent veiller à ce que les personnes qui procèdent ou assistent au déchiquetage aient fait l'objet d'une enquête de sécurité du personnel convenable au niveau le plus élevé des renseignements qui sont détruits.
- Les ministères et les organismes devraient s'assurer de recevoir un certificat de destruction pour tout matériel détruit par un tiers.
- Les ministères et les organismes doivent s'assurer que les documents déchiquetés sont conformes aux normes de taille énoncées dans le guide de la GRC GSMGC-001 – Guide de sélection de l'équipement de déchiquetage.

10.4. Destruction des supports de stockage électroniques

Pour obtenir des directives sur l'élimination et la destruction des supports de stockage électroniques, consultez le Guide en matière de sécurité des technologies de l'information du Centre de la sécurité des télécommunications Canada (CST) ITSAP.40.006 – Nettoyage et élimination d'appareils électroniques.

10.5. Destruction d’urgence

Au Canada ou à l’étranger, lorsque la probabilité d’une destruction d’urgence est élevée ou lorsque la politique l’exige, comme une zone sécurisée SIGINT (ZSS) ou une installation renfermant des informations sensibles cloisonnées, des ordres locaux doivent être donnés pour la destruction rapide des renseignements très secrets et secrets lorsque leur transport ou leur transmission sécuritaire au Canada ou à un autre endroit n’est pas possible. Ces ordres devraient être revus périodiquement et conservés dans un endroit connu pour autoriser l’accès du personnel en cas d’urgence. Les ordres devraient indiquer ce qui suit :

- Tout l’équipement de destruction est correctement entretenu;
- Un nombre suffisant de membres autorisés du personnel savent se servir de l’équipement;
- Les listes de destruction prioritaire sont disponibles et mises à jour régulièrement.

11. Références ou documents connexes

Directive sur la gestion de la sécurité – Canada.ca

G1-025 Protection, détection et intervention (rcmp-grc.gc.ca)

G1-026 Guide pour l'établissement des zones de sécurité matérielle – Gendarmerie royale du Canada (rcmp-grc.gc.ca)

G1-024 Contrôle de l'accès – Gendarmerie royale du Canada (rcmp-grc.gc.ca)

G1-006 Cartes d'identité/Insignes d'accès – Gendarmerie royale du Canada (rcmp-grc.gc.ca)

GSMGC-003 Guide des considérations relatives à la conception d'un centre des opérations de sécurité

GCPSG-017 Guide de construction des aires insonorisées

G13-01 - Pièces d'entreposage sécuritaire

GSMGC-007 – Transport, transmission et entreposage de renseignements protégés ou classifiés

Guide de sélection de l'équipement de déchiquetage (rcmp-grc.gc.ca)

GSMGC-008 – Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance

ITSAP.40.006 – Nettoyage et élimination d'appareils électroniques

Politique sur les services et le numérique

Code canadien du travail (L.R.C. [1985], ch L-2)

Règlement sur la prévention du harcèlement et de la violence dans le lieu de travail (DORS/2020-130)

12. Promulgation

Examen et recommandation en vue de l'approbation.

J'ai examiné et je recommande l'approbation du Guide opérationnel de la sécurité matérielle GSMGC-010 (2022).

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2022.12.05 10:53:22 -05'00'

Shawn Nattress,
Gestionnaire
Principal organisme responsable de la sécurité de la GRC

Date

Approuvé

J'approuve par la présente le Guide opérationnel de la sécurité matérielle GSMGC-010 (2022).

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2022.12.08 11:29:36 -05'00'

André St-Pierre,
Directeur, Sécurité matérielle
Gendarmerie royale du Canada

Date