Considérations relatives à la sécurité matérielle dans la conception des installations

GSMGC-014 (2024)

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

Date de publication : 2024-07-01
Mise à jour: YYYY-MM-DD

Avant-propos

Le guide Considérations relatives à la sécurité matérielle dans la conception des installations est une publication NON CLASSIFIÉE, publiée avec l'autorisation du principal organisme responsable de la sécurité matérielle de la Gendarmerie royale du Canada (POSM-GRC).

Cette publication du gouvernement du Canada sert de guide pour les inspections de sécurité des ministères, organismes et employés du gouvernement du Canada.

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

Reproduction

Date d'entrée en vigueur

La date d'entrée en vigueur de GSMGC-014 (2024) – Considérations relatives à la sécurité matérielle dans la conception des installations est 2024-07-01.

Registre des modifications

No de modification	Date	Par	Résumé de la modification

Remarque : C'est le POSM-GRC qui est autorisé à apporter des modifications.

Contents

1. Introduction

La GRC, Principal Organisme Responsable de la Sécurité Matérielle pour le gouvernement du Canada, est chargée de fournir des conseils et des directives sur toutes les questions liées à la sécurité matérielle.

1.1. But

Le présent document a pour but de fournir au personnel de sécurité du gouvernement du Canada (GC) des conseils sur la préparation des mémoires de conception de la sécurité matérielle et des éléments connexes et des considérations pour les installations du GC, qu'il s'agisse de nouvelles constructions ou de la modernisation des espaces existants. Ce guide devrait être utilisé conjointement avec une évaluation des menaces et des risques (EMR) et/ou une conception axée sur les menaces pour déterminer les besoins particuliers. Les détails techniques spécifiques concernant l'équipement de sécurité ne sont pas abordés dans ce guide (tels que les types de matériel de porte ou les alarmes d'intrusion).

Ce guide est destiné à être utilisé conjointement avec d'autres guides du Principal Organisme Responsable de la Sécurité Matérielle publiés qui sont disponibles à Principal organisme responsable de la sécurité matérielle - Gendarmerie royale du Canada (rcmp-grc.gc.ca)

1.2. Applicabilité

Le présent guide s'applique aux employés du GC qui ont la responsabilité de concevoir la construction ou la rénovation d'un immeuble ou d'une installation du GC. De plus, le présent guide s'applique au personnel de sécurité affecté à l'élaboration des exposés sur la conception de la sécurité matérielle afin de s'assurer que les considérations et les normes pertinentes en matière de sécurité matérielle sont communiquées au gestionnaire de projet et intégrées au projet le plus tôt possible.

1.3. Équité, diversité et inclusion dans les systèmes de sécurité matérielle

Tous les employés du gouvernement du Canada (GC) ont la responsabilité de protéger les personnes, les renseignements et les biens du GC. Il est important que les politiques et les pratiques en matière de sécurité ne servent pas d'obstacles à l'inclusion, mais soutiennent et respectent plutôt tout le personnel du GC tout en veillant à ce que les mesures de sécurité appropriées soient maintenues pour protéger le personnel, les biens et l'information du GC.

Les initiatives visant à promouvoir l'égalité et l'inclusion entre les diverses communautés et patrimoines au sein du GC devraient être respectées dans le développement et la maintenance des systèmes de sécurité matérielle. Les ministères et organismes devraient respecter toutes les lois, politiques et directives du GC sur l'équité, la diversité et l'inclusion (EDI) dans la promotion d'un milieu de travail juste et équitable pour toutes les personnes,

tout en s'assurant qu'elles s'acquittent de leurs responsabilités en matière de sécurité.

Les ministères et organismes devraient mener un exercice de gestion des risques pour veiller à ce que, même si la dignité de tous est respectée, la protection des renseignements, des biens et du personnel du GC soit maintenue. Toutes les questions sur les politiques et les directives de l'EDI doivent d'abord être adressées à l'autorité ministérielle responsable.

1.4. Considérations relatives à la technologie de l'information

Suite aux menaces qui évoluent constamment et l'intégration de la sécurité physique et de la technologie de l'information (TI), il est essentiel d'évaluer le risque de toute application et/ou de tout logiciel connecté à un réseau pour faire fonctionner et soutenir l'équipement dans les bâtiments contrôlés par le gouvernement du Canada.

Avant de mettre en œuvre des applications et/ou des logiciels qui contrôleront et/ou automatiseront certaines fonctions de l'immeuble, votre service de sécurité ministériel exige la réalisation d'une évaluation et d'une autorisation de sécurité (SA&A). Cela permettra de s'assurer que l'intégrité et la disponibilité des composants que les applications et/ou logiciels contrôlent sont maintenues et que tout risque mis en évidence sera atténué. Il est fortement recommandé de commencer le processus SA&A tôt afin de s'assurer que les calendriers de livraison des projets ne sont pas affectés. Pour plus d'informations sur le processus SA&A, veuillez consulter votre service de sécurité ministériel.

2. Coordonnées

Pour de plus amples renseignements, veuillez communiquer avec :
Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
73, promenade Leikin, arrêt postal 165
Ottawa (Ontario)
K1A 0R2
Courriel: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Abréviations

Acronyme	Signifiant
CCTV	Systèmes de surveillance vidéo. Interchangeable avec CCVE
COS	Centre des opérations de sécurité
EASI	Évaluation et autorisation de la sécurité des installations
EMR	Évaluation des menaces et des risques
GC	Gouvernement du Canada
PSG	Politique sur la sécurité du gouvernement
RCMP LSA	RCMP Lead Security Agency for Physical Security

SA&A	Évaluation et autorisation de sécurité
SCT	Secrétariat du Conseil du Trésor du Canada
PCAM	Prévention du crime par l'aménagement du milieu
ZA	Zone d'accueil
ZAR	Zone à accès restreint
ZHS	Zone de haute sécurité
ZS	Zone de sécurité
ZT	Zone de travail
ZP	Zone publique

4. Glossaire

Terme	Définition
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.
Compartimentation	La séparation physique d'une zone(s) au sein d'une structure
Conception fondée sur les menaces	Appliquer des mesures préventives et des garanties dans la conception d'un bâtiment, d'une installation ou d'un espace. Fondé sur les principes énoncés dans le document de l'Agence internationale de l'énergie atomique intitulé *Menaces de référence*.
Distance de sécurité	Distance entre une menace potentielle et le bien. Exemple – Rue publique (zone publique) à l'entrée d'un immeuble (zone d'accueil)
Énoncé de conception de la sécurité	Document qui décrit la philosophie et les concepts de la protection physique ainsi que les mesures de protection physiques pour une installation.
Évaluation des menaces et des risques (EMR)	Processus d'évaluation des biens d'une installation, des menaces qui pèsent sur eux et du rendement des mesures de protection contre ces menaces, visant à définir les risques.
Évaluation et autorisation de la sécurité des installations (EASI)	Processus utilisé par les organisations pour s'assurer que les installations nouvelles et existantes du gouvernement du Canada et les projets d'aménagement font l'objet d'évaluations de la sécurité. Des contrôles de sécurité appropriés sont déterminés et mis en œuvre avant que l'autorisation d'occuper l'installation soit accordée.
Menace	Événement ou acte délibéré ou accidentel qui pourrait porter préjudice aux personnes, à l'information, aux biens ou aux services.
Vidéosurveillance	Tout composant d'un système de surveillance électronique comprenant des caméras, des moniteurs, du matériel d'enregistrement et d'autres technologies pour surveiller n'importe quel espace. Interchangeable avec CCTV et CCVE
Vitrage	Matériau transparent utilisé pour les fenêtres.

Zone d'accueil (ZA)	Zone où la transition d'une zone publique à une zone à accès restreint est contrôlée. Exemple–Hall d'accueil ou poste de gardien de sécurité.
Zone à accès restreint (ZAR)	Aire de travail (site ou édifice) au sein d'un ministère où l'accès est restreint aux personnes autorisées. Comprend la zone d'opérations, la zone de sécurité et la zone de haute sécurité, conformément aux définitions énoncées dans la référence GSMGC-015 – Guide pour l'établissement des zones de sécurité matérielle
Zone de haute sécurité (ZHS)	Zone où l'accès est limité au personnel autorisé détenant la cote de sécurité du GC correspondante et aux visiteurs préapprouvés/contrôlés et escortés de façon appropriée. Exemple – zone où les renseignements et les biens classifiés plus haut que secret sont traités ou stockés.
Zone de sécurité (ZS)	Zone où l'accès est limité au personnel autorisé détenant la cote de sécurité du GC correspondante et aux visiteurs dûment escortés. Exemple – zone où les renseignements classifiés jusqu'au niveau Secret inclusivement sont traités ou stockés.
Zone de travail (ZT)	Zone où l'accès est limité au personnel qui travaille à l'intérieur et aux visiteurs dûment escortés. Exemple – Espace de bureau du gouvernement ou entrepôt réservé au personnel
Zone publique (ZP)	Zone où le public a un accès sans entrave et qui entoure ou forme généralement une partie d'une installation gouvernementale. Exemple : terrain entourant un immeuble.

5. Évaluation de la sécurité matérielle

Pour qu'un système de sécurité matérielle soit efficace, il doit être élaboré en fonction de la compréhension des menaces et des risques qu'il est conçu pour contrôler. Les détails techniques spécifiques concernant l'équipement de sécurité ne sont pas abordés dans le présent guide (tels que les types de quincaillerie de porte ou les alarmes d'intrusion); toutefois, les méthodes d'intégration des systèmes de sécurité matérielle dans la conception d'un bâtiment ou d'une installation au lieu d'ajouter ces systèmes par la suite, sont mis en évidence. Cette approche peut être réalisée en utilisant les concepts et/ou activités suivants. Les renseignements obtenus ou utilisés dans le processus de conception de l'installation qui sont de nature classifiée peuvent devoir être classifiés conformément aux normes de la Directive sur la gestion de la sécurité et traitées conformément au GSMGC-007 Transport, transmission et entreposage de matériel protégé ou classifié.

5.1. Évaluation des menaces et des risques

L'évaluation des menaces et des risques (EMR) est un processus utilisé pour déterminer, analyser et traiter les vulnérabilités observées par rapport aux menaces connues ou prévues afin d'établir l'environnement de risque et fait partie intégrante de la stratégie globale de gestion des risques d'un ministère ou d'un organisme. La portée et l'application des EMR

varient, mais ce processus peut permettre d'identifier et de résoudre plus efficacement les vulnérabilités tout au long d'un projet de construction. L'ASL de la GRC peut fournir des renseignements supplémentaires sur le processus d'EMR dans le Guide d'évaluation des menaces et des risques GSMGC-022 (2024) ou en communiquant avec RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca

5.2. Conception fondée sur les menaces

La conception fondée sur les menaces est un profil du type, de la composition, des capacités, des méthodes, des dommages projetés et/ou de l'intensité d'une menace délibérée, accidentelle ou naturelle sur laquelle reposent l'ingénierie et les opérations de sécurité d'une installation. Cela est fondé sur les principes énoncés dans le document de l'Agence internationale de l'énergie atomique intitulé Menaces de référence. La conception fondée sur les menaces vise à éliminer ou à réduire l'impact des menaces attribuées aux vulnérabilités dans la conception ou l'emplacement d'une installation; par conséquent, les deux devraient être utilisés en tandem. Les étapes de la conception axée sur les menaces sont les suivantes :

5.2.1. Évaluation des menaces

La phase d'évaluation des menaces de la conception fondée sur les menaces exige la collecte de tous les renseignements pertinents pour une évaluation préliminaire des menaces nécessitant des mesures d'atténuation intégrées à la conception d'un bâtiment, d'une installation ou d'un espace. Les renseignements recueillis au cours d'une EMR peuvent être inclus dans cette phase, car ils appuient le même objectif.

5.2.2. Collecte de renseignements

Le processus de collecte de renseignements vise à déterminer et à énumérer les menaces potentielles pour l'installation proposée. Souvent identifier lors d'une EMR, cela peut inclure la motivation de la menace, l'intention, la capacité et les événements historiques. Il faut consulter des sources d'information fiables, notamment les organismes de renseignement et d'application de la loi, les ministères et organismes gouvernementaux, les rapports d'incident, ainsi que les EMR historiques et actuelles et d'autres évaluations des risques pertinentes. La crédibilité de l'information et de sa source devrait être évaluée de la même manière qu'une EMR. La collecte de renseignements devrait être une activité continue tout au long du cycle de vie d'une liste de conception fondée sur les menaces afin de confirmer que l'information demeure pertinente et reflète les données les plus à jour.

5.2.3. Analyse préliminaire

Les renseignements obtenus sont ensuite analysés pour documenter les motifs, les intentions et les capacités crédibles des menaces potentielles. L'analyse devrait porter une attention particulière aux menaces potentielles qui sont pertinentes et réalistes au mandat du ministère ou de l'organisme et à l'emplacement de l'installation. L'objectif de cette phase est de fournir une évaluation crédible des menaces potentielles, y compris la

composition, la motivation, l'intention et les capacités.

Les caractéristiques suivantes de chaque menace doivent être prises en compte dans l'analyse; toutefois, il se peut qu'il n'y ait pas de données disponibles en raison du manque d'information ou du manque d'information crédible pour chaque menace :

- Motivation
- Intentions
- Outils
- Compétences techniques
- Compétences en cybersécurité
- Connaissances
- Financement
- Menace interne
- Tactiques
- Complexité
- Fréquence des événements historiques
- Attractivité de la cible

Le produit de cette phase est un document d'évaluation des menaces qui décrit l'environnement des menaces et toutes les menaces connues à prendre en considération. Comme il a été mentionné précédemment, l'information provenant d'une EMR peut être utilisée dans l'élaboration du document de conception fondée sur la menace.

5.2.4. Analyse secondaire

Le document d'évaluation des menaces est ensuite analysé en fonction des attributs disponibles. La pertinence de chaque menace peut être déterminée en fonction de la motivation, de l'intention et/ou de la capacité de nuire. Les menaces ayant une plus grande pertinence devraient être prises en considération davantage que celles ayant une moindre pertinence. Les menaces avec des attributs similaires peuvent être assignées à des types de menaces définis par des attributs et des caractéristiques spécifiques. Les considérations à inclure dans les types de menaces plus vastes peuvent être des considérations spécifiques au site et à l'activité, telles que les procédures opérationnelles à l'installation, l'emplacement et l'accessibilité de l'installation, ainsi que les modes et les itinéraires de transport à destination et en provenance de l'installation. L'information analysée est ensuite compilée dans un document décrivant un aperçu de la menace, ainsi que ses attributs et caractéristiques liés à l'installation.

Les résultats de ce document et de l'EMR peuvent être utilisés pour élaborer l'énoncé de conception de la sécurité de l'installation.

5.3. Énoncé de conception de la sécurité

Le contenu d'un mémoire de conception de la sécurité variera selon que le ministère ou

l'organisme loue des installations existantes ou construit de nouvelles installations appartenant au GC. Le niveau de détail normalement fourni dans un dossier de conception de sécurité est de nature générale; afin d'offrir une flexibilité maximale dans le processus de conception. Les éléments d'une installation énumérés à la section 6. Considérations relatives à la sécurité matérielle dans la conception des bâtiments et à la section 7. Sauvegardes sont une sélection de facteurs qui devraient être inclus dans tout énoncé de conception de sécurité. De plus, ces éléments peuvent avoir une relation interdépendante qui devrait être soulignée, afin de renforcer la valeur de l'intégration de mesures de protection qui peuvent traiter de multiples vulnérabilités ou menaces.

Il est utile de comparer ou de noter les recommandations de l'EMR ou des documents de conception fondés sur les menaces aux recommandations applicables dans l'énoncé de conception de sécurité; car il s'agit des mesures correctives destinées à minimiser la vulnérabilité et les risques signalés dans ces processus. L'énoncé de conception de la sécurité devrait commencer par une introduction et un but, suivis des considérations de conception et des mesures de protection applicables, et devrait se terminer par toute référence et documentation à l'appui (comme l'EMR et les documents de conception fondés sur les menaces). Une fois terminé, l'énoncé de conception de la sécurité doit être fourni au gestionnaire de projet et aux autres membres du personnel concerné.

Selon l'installation, il peut y avoir d'autres considérations de conception et/ou mesures de protection qui ne sont pas incluses dans les sections susmentionnées du présent guide. Il incombe au ministère ou à l'organisme de déterminer, en fonction de ses conclusions tirées de l'EMR de l'installation et/ou du document de conception fondé sur les menaces, quelles mesures sont nécessaires pour une installation donnée et formuler des recommandations pour éliminer ou réduire au minimum les vulnérabilités dans la conception et la construction de l'installation.

5.4. Évaluation et autorisation de sécurité des installations

L'Évaluation et autorisation de la sécurité des installations (EASI) est un processus par lequel les organisations s'assurent que des évaluations de la sécurité sont effectuées sur les installations nouvelles et existantes du GC et les projets d'aménagement.

Le processus d'EASI comprend cinq (5) phases:

- Lancement;
- Planification;
- Risques et analyse;
- Mise en œuvre, autorisation et évaluations continues de la Sécurité, et;
- Mis hors service.

Les EMR, la conception fondée sur les menaces, et les énoncés de conception de la sécurité s'inscrivent chacune dans l'une des phases du processus d'EASI. L'EMR et la conception

fondée sur les menaces ont lieu à l'étape de l'analyse des risques, après quoi l'énoncé de conception de la sécurité est élaboré à l'étape de la mise en œuvre, de l'autorisation et des évaluations de sécurité continues. Pour obtenir de plus amples renseignements sur le processus d'EASI, veuillez consulter le document GSMGC-016 - Guide du processus d'évaluation et d'autorisation de sécurité des installations.

5.5. Résumé à l'intention de la direction

En raison de la longueur des mémoires de conception de sécurité, des EMR et des documents de conception fondés sur la menace, il est préférable de créer un résumé ou une note d'information de deux (2) à trois (3) pages, y compris les documents justificatifs, à l'intention des décideurs du projet. Le résumé de gestion ne devrait mettre en évidence que les concepts de conception spécifiques liés à chaque attribut principal énuméré dans le mémoire. L'objectif est d'aider les cadres supérieurs à saisir rapidement les idées de conception importantes nécessaires à la protection de l'installation, ainsi qu'à permettre la décision d'aller de l'avant avec le projet.

6. Considérations relatives à la sécurité matérielle dans la conception des bâtiments

Qu'il s'agisse de construire ou de moderniser une installation, la sécurité matérielle devrait être prise en compte au cours du processus de conception. Les résultats d'une EMR et d'une conception fondée sur les menaces aideront à déterminer les exigences particulières pour une installation donnée, qui devraient ensuite être abordées dans l'énoncé de conception de sécurité. Cette section est destinée à être utilisée conjointement avec les conseils de GSMGC-019 - Guide de protection, détection, réponse, et récupération, GSMGC-015 (2023) - Guide pour l'établissement des zones de sécurité matérielle, et d'autres GSMGC énumérés lors de la compilation d'un énoncé de conception de sécurité pour une installation.

6.1. Protection, détection, réponse et récupération

La protection, la détection, la réponse et la récupération reposent sur le principe que la zone externe et interne des installations gouvernementales peut être conçue et gérée de manière à créer des conditions qui, avec des mesures de contrôle de sécurité physique spécifiques, réduira le risque de préjudice pour les employés, protégera contre et détectera les accès non autorisés ou les tentatives d'accès, et activera des activités de réponse et de récupération efficaces. Pour en savoir plus, consultez le document GSMGC-019 – Guide de protection, détection, réponse et de récupération.

6.2. Zones de sécurité matérielle

Les zones de sécurité matérielle, lorsqu'elles sont bien intégrées, devraient améliorer l'environnement de sécurité global d'une installation. Le zonage de sécurité matérielle devrait favoriser un sentiment d'appartenance ou de renforcement territorial, offrir des possibilités de surveillance naturelle et établir une séquence clairement définie de limites à

travers lesquelles un visiteur ou un employé ayant fait l'objet d'un contrôle approprié peut passer. Les besoins en locaux fonctionnels du Ministère devraient également être pris en considération lors de l'établissement des limites de zonage.

Le zonage de sécurité matérielle ne devrait pas être mis en œuvre simplement en respectant les exigences techniques prescrites pour les zones ni en intégrant les zones dans le plan uniquement en fonction des besoins en espace fonctionnel. Si les mesures de sécurité matérielle qui délimitent les zones sont excessives, inappropriées ou n'ont pas tenu compte des besoins en espace fonctionnel, ces mesures finiront par être contournées et pourraient devenir inefficaces. Il faut éviter ou supprimer les incitatifs qui incitent le personnel non autorisé à franchir les limites du zonage (comme les toilettes ou une cafétéria).

Pour en savoir plus sur le zonage, consultez le guide GSMGC-015 Guide pour l'établissement des zones de sécurité matérielle.

6.3. Périmètre du bâtiment et de la propriété

La distance de sécurité est importante lorsqu'on considère le périmètre du site ou du bâtiment, car elle permet de détecter rapidement une menace, ce qui permet une intervention rapide et limite les effets dommageables sur le personnel et l'infrastructure. La distance exacte peut varier en fonction de divers facteurs et l'EMR peut aider à déterminer une distance appropriée. Il faut en tenir compte dans la construction et/ou le déménagement d'une installation.

Les clôtures peuvent être utilisées pour le périmètre du site. Pour de plus amples renseignements, consultez le guide GSMGC-009 Guide sur les considérations liées aux clôtures de sécurité.

À l'exception des servitudes, l'installation peut devoir être attenante à la limite de la propriété, à une rue ou au mur d'un bâtiment adjacent sur certains sites. Si la séparation de la ligne de propriété ne peut être réalisée, des dispositifs et des procédures de sécurité plus robustes seront nécessaires. Pour en savoir plus, consultez le document GSMGC-019 – Guide de protection, détection, réponse et de récupération..

6.4. Sécurité des personnes et urgences

Bien que des mesures de sécurité matérielle soient nécessaires, elles ne doivent pas remplacer ni annuler les mesures de sécurité vitale ou les exigences légales. Par exemple, les zones de sécurité (ZS) et les zones de haute sécurité (ZHS) nécessitent toujours la possibilité de sortir en cas d'urgence; par conséquent, les portes d'issue de secours doivent toujours être équipées de matériel de barre antipanique pour accélérer l'évacuation d'urgence. Se reporter à tous les codes et politiques applicables, y compris, mais sans s'y limiter, le Code canadien du travail, le Code national de prévention des incendies du Canada, le Code national du bâtiment du Canada, les codes provinciaux, territoriaux et municipaux et les politiques pertinentes du SCT pour assurer la conformité.

6.5. Emplacement des escaliers de sortie

Les escaliers de sortie qui font partie d'un moyen d'évacuation doivent être conformes aux exigences du Code national du bâtiment. Ces escaliers ne doivent pas permettre un accès non contrôlé à la zone de travail (ZT), au ZS ou à la ZHS. La meilleure pratique consiste pour les portes d'un ZS et d'une ZHS à sortir vers une zone moins restrictive avant d'accéder à un espace public sans quincaillerie de porte extérieure capable d'autoriser l'accès à la zone.

6.6. Ascenseurs et halls d'ascenseur

Les ascenseurs, y compris les ascenseurs de fret et de cargaison et les monte-plats, ne doivent pas permettre l'accès entre les zones. Les ascenseurs ne doivent permettre l'accès qu'entre les mêmes zones (zone d'accueil à zone d'accueil).

Les halls d'ascenseur, y compris les ascenseurs de fret et de fret à partir du stationnement public et des quais de chargement, devraient s'ouvrir dans une zone publique (ZP) ou une zone d'accueil (ZA), comme un hall d'ascenseur au rez-de-chaussée, afin de s'assurer que seuls les accès sont autorisés. les personnes ayant fait l'objet d'un contrôle approprié ont accès à l'espace d'un établissement. Si les ascenseurs s'ouvrent dans un ZT, il y a une plus grande possibilité que des personnes non autorisées accèdent à l'espace du GC sans être détectées.

6.7. Voies piétonnières

Les voies de circulation piétonnière de ZP à ZT doivent passer par un ZA sous le contrôle de l'établissement pour assurer le contrôle de l'accès, conformément à GSMGC-015 - Guide pour l'établissement des zones de sécurité matérielle. Tous les escaliers requis comme moyen d'évacuation pour ZP doivent être situés dans la ZP.

Les portes de sortie comme moyen d'évacuation des zones d'accès restreint (ZAR) à ZP devraient être équipées de ferme-porte automatiques et fixées du côté de l'escalier ou du couloir, à l'exception des planchers de croisement dans les immeubles de grande hauteur. Les panneaux sur les portes des zones à restriction élevée doivent indiquer un mouvement à sens unique ou une autre signalisation appropriée.

Toutes les mesures de sécurité utilisées pour compenser les lacunes propres au site doivent être incluses dans l'énoncé de conception de sécurité. Le contrôle d'accès électronique peut être utilisé pour réguler le mouvement du personnel autour de l'installation.

6.8. Contrôle des piétons dans un immeuble

Il faut prévoir suffisamment d'espace dans la ZA pour accueillir les visiteurs en attente de service sans perturber les activités normales dans l'installation ou sur les lieux. Un espace de débordement suffisant dans la ZP peut également être utilisé pour assurer que les opérations normales peuvent se poursuivre en cas d'afflux soudain de visiteurs. Au périmètre

de l'espace de l'établissement, il devrait y avoir la possibilité d'ériger une barrière physique ou psychologique comme moyen de contrôle d'accès dans une situation telle qu'une manifestation ou un abri sur place. Pour en savoir plus, consultez le guide GSMGC-006 - Guide de gestion de l'accès.

6.9. Fenêtres

Les fenêtres doivent respecter les exigences architecturales en tenant compte de la sécurité et du vitrage de sécurité inclus dans la phase de conception du projet. Reportez-vous à GSMGC-013 Principes fondamentaux du vitrage en sécurité matérielle pour plus d'informations et de spécifications.

6.10. Espaces communs

Toutes les fonctions communes de l'immeuble devraient être situées dans des zones centralisées. Ces zones devraient faire partie d'un ZT et pourraient comprendre, par exemple, des salles de repas/café, des toilettes et des salles de photocopie générales. Les aires communes pour les visiteurs, comme les toilettes, les salles d'entrevue et les espaces d'orientation, devraient être situées dans le ZA. L'intention est de réduire le mouvement des piétons dans les ZAR et d'éliminer les raisons pour lesquelles les personnes qui ne travaillent pas dans les ZAR entrent légitimement.

6.11. Toilettes

Les toilettes publiques devraient être situées là où il y a une observation visuelle dégagée de l'entrée par un réceptionniste ou un gardien.

Les toilettes du personnel, si elles sont indiquées dans une EMR, peuvent être situées dans un ZT. Les toilettes du personnel devraient être séparées des toilettes publiques pour la sécurité des employés et pour réduire au minimum la possibilité d'accès non autorisé à tout ZAR.

6.12. Espaces utilitaires

Les points d'entrée et de sortie des services publics et des services publics (comme les prises d'air, les conduits mécaniques, les trappes de toit et les approvisionnements en eau) doivent être protégés pour s'assurer que les biens essentiels de l'installation, les mesures de sécurité vitale et les programmes ministériels ne sont pas compromis par un accès non autorisé ou non contrôlé.

Les espaces publics ne doivent pas être adjacents aux entrées des zones plus restrictives. Si possible, ils peuvent être situés près des emplacements prévus pour la gestion de l'accès, comme les zones de contrôle des gardiens.

6.13. Occupants adjacents

L'accès à l'espace d'un établissement devrait être contrôlé et l'incidence des activités

ministérielles sur les occupants adjacents devrait être prise en considération. De même, le mandat et les activités des occupants adjacents devraient également être pris en considération dans le cadre du mandat et des activités du Ministère.

Dans un immeuble à locataires multiples avec des bureaux du GC répartis sur plusieurs étages, les systèmes d'ascenseurs qui séparent l'accès à l'étage dans le hall peuvent aider à empêcher l'accès non autorisé aux espaces du GC, selon la banque d'ascenseurs, les cartes d'accès et la gestion des visiteurs par le personnel de sécurité. Pour de plus amples renseignements, consultez GSMGC-006 - Guide de gestion de l'accès.

6.14. Télécommunications et liaisons de données à l'intérieur de l'installation

Une EMR devrait être utilisée pour déterminer les mesures de sécurité matérielle appropriées pour le câblage de télécommunications dans une installation. Des renseignements supplémentaires se trouvent dans la Politique sur les services et le numérique.

La nécessité de mettre en œuvre des mesures de protection à l'intérieur de l'installation, comme l'alimentation de secours pour l'interphone ou le téléphone interne et l'acheminement des conduits pour transporter les communications, devrait être déterminée par l'EMR et/ou la conception axée sur les menaces. Pour en savoir plus, consultez l'annexe C du GSMGC-015 - Guide pour l'établissement des zones de sécurité matérielle.

6.15. Salles du courrier

Les salles de courrier devraient au moins être gérées comme un ZT. Les salles de courrier doivent être situées à l'intérieur ou à proximité d'une zone d'expédition ou de réception distincte des ZAR ou de l'infrastructure essentielle. Ils devraient être séparés des ZA et avoir la capacité d'être isolés du reste du bâtiment en cas de colis suspects ou d'autres menaces.

6.16. Quais de chargement

Les quais de chargement doivent être situés à l'écart et non directement reliés ou adjacents aux ZAR ou aux éléments d'infrastructure essentiels. Bien que les zones d'expédition et de réception puissent être situées dans le même quai de chargement, il est avantageux de séparer physiquement les zones pour limiter l'impact d'un auteur de menaces s'ils y accèdent.

6.17. Salles de conférence et de réunion

Les salles de conférence et de conférence devraient être situées au moins dans un ZT. Si ces espaces doivent être utilisés pour discuter d'informations sensibles ou classifiées, ils doivent être inclus dans la conception des zones avec une atténuation acoustique supplémentaire et une gestion de l'accès appropriée.

6.18. Salles d'ordinateurs et de serveurs

La sécurité matérielle en ce qui concerne les salles de serveurs informatiques est basée sur la mise en œuvre du contrôle positif. Sous contrôle positif, un espace ou un actif est surveillé activement et protégé en permanence afin que toute modification, ou tentative de modification, de son statut soit immédiatement connue. Les salles d'ordinateurs et de serveurs devraient être gérées comme des ZAR, les pratiques exemplaires limitant l'accès au personnel essentiel seulement. Pour les installations abritant des serveurs classifiés, ces ZAR doivent être situés dans un ZS. Pour en savoir plus, consultez l'annexe C du document GSMGC-015 - Guide pour l'établissement des zones de sécurité matérielle.

6.19. Locaux à usage particulier

Le présent document porte sur les attributs associés aux immeubles de bureaux à usage général. Les espaces tels que les installations médicales, les salles de classe, les laboratoires et les ateliers devraient être énumérés dans le mémoire sur la conception de la sécurité physique, avec les mesures de protection appropriées déterminées par une EMR et/ou une analyse de conception fondée sur les menaces. Vous trouverez plus d'informations et d'exemples dans GSMGC-015 - Guide pour l'établissement des zones de sécurité matérielle.

7. Sauvegardes

Les mesures de protection à prendre en considération peuvent être divisées en deux catégories : les mesures de protection du site et les mesures de protection du bâtiment. Il est recommandé d'utiliser une combinaison de chacune pour assurer l'efficacité de la stratégie de sauvegarde. Le type et le nombre de mesures de protection à utiliser peuvent être déterminés par l'EMR et/ou les documents de conception fondés sur les menaces et notés dans l'énoncé de conception de sécurité pour le gestionnaire de projet, l'équipe d'architectes et les autres parties concernées.

7.1. Mesures de protection du site

Des mesures de protection du site sont mises en œuvre pour le site ou l'emplacement géographique de l'installation. Ces mesures de protection sont à l'extérieur de l'installation et sont axées sur le site lui-même et ses caractéristiques. Cette section est destinée à être utilisée conjointement avec les conseils du GSMGC-019 –Guide de protection, détection, réponse, et récupération, GSMGC-015 – Guide pour l'établissement des zones de sécurité matérielle, GSMGC-006 - Guide de gestion de l'accès, et d'autres GSMGC énumérés lors de la compilation d'un énoncé de conception de la sécurité pour une installation.

7.1.1. Prévention du crime par l'aménagement du milieu

La prévention du crime par l'aménagement du milieu (PCAM) est une approche multidisciplinaire de la prévention du crime au cours de la désignation, de la définition et de la conception de la sécurité d'un environnement qui est complémentaire au GCPSG-019 – Guide de protection, détection, réponse, et récupération. La conception et la gestion des installations dans des environnements naturels et artificiels peuvent

permettre aux ministères et aux organismes de dissuader les actes criminels ou accusatoires tout en gérant de façon sécuritaire la circulation des personnes dans les installations. Ces modèles visent à influencer positivement le comportement et les activités tout en décourageant les actions indésirables du personnel, des visiteurs et des adversaires potentiels.

7.1.1.1. Contrôle du périmètre du site

Pendant les heures d'accès du public, il ne devrait y avoir aucune restriction sur l'accès au site ou à la zone d'accès public du bâtiment, sauf si l'EMR ou l'analyse des menaces fondée sur la conception en décide autrement.

Pendant les heures d'accès limité, le bâtiment doit être verrouillé, mais sans restriction d'accès au site. La signalisation devrait fournir une orientation et une définition claires des zones publiques et restreintes du site.

Les clôtures devraient être utilisées pour le périmètre du site. Pour de plus amples renseignements, consultez le guide GSMGC-009 Guide sur les considérations liées aux clôtures de sécurité. La porte d'accès au toit ou l'écoutille de toit doit être verrouillée avec de la quincaillerie commerciale robuste pour restreindre l'accès non autorisé.

7.1.1.2. Éclairage du site

Fournir un éclairage général du bâtiment, des entrées et des stationnements. Pour de plus amples renseignements et pour connaître les spécifications recommandées, consultez le guide GSMGC-004 Guide sur les considérations liées à l'éclairage de sécurité.

7.1.1.3. Aménagement extérieur

Les buissons ou les branches doivent être évités ou coupés pour maintenir des lignes de vue claires au niveau des yeux vers et depuis le bâtiment. La neige, l'herbe et les arbustes doivent être entretenus pour s'assurer qu'il n'y a pas d'obstacle visuel, que les services d'urgence et le personnel d'intervention ne sont pas retardés et qu'aucun accès non autorisé ne peut être obtenu dans ou au-dessus de l'immeuble. Les objets lâches comme les pierres, les briques de pavage, les bancs et les tables doivent être fixés pour s'assurer qu'ils ne peuvent pas être utilisés comme projectiles.

7.1.1.4. Observation du site

Le bâtiment et le site devraient être observables à partir de la route par les premiers intervenants et les passants, à moins que cela ne soit jugé indésirable d'après l'EMR et l'analyse de la conception fondée sur les menaces. Dans les bâtiments à plusieurs étages, les ZAR peuvent être situés aux étages supérieurs pour limiter la visibilité des autres bâtiments.

7.1.1.5. Emplacement du bâtiment

Le bâtiment ne doit pas être situé dans une zone susceptible de présenter des risques naturels ou anthropiques récurrents. Le bâtiment doit également être situé à un endroit facilement accessible par les services d'urgence (incendie, police, ambulance) dans toutes les conditions. L'emplacement de l'immeuble devrait avoir suffisamment d'espace pour avoir une distance de sécurité suffisante, comme le détermine une EMR.

Les lignes de communication (téléphone, données, Internet, etc.), les lignes électriques, les lignes d'alimentation en énergie (pétrole, gaz), l'eau et les conduites d'égout doivent être protégées physiquement pour éviter tout dommage accidentel ou intentionnel.

7.1.2. Servitudes traversant le site

Les servitudes sur le site doivent respecter les règlements locaux/provinciaux en matière de construction et/ou les exigences des entreprises de services publics (par exemple, Newfoundland et Labrador Hydro indiquent que les dimensions typiques des servitudes se situent entre 3 et 15 mètres). L'incidence des servitudes sur un site devrait être prise en compte et incluse dans une EMR et/ou une conception fondée sur les menaces.

Les établissements doivent être informés par le gardien de la possibilité d'intrusion sur le site par un propriétaire de servitude, comme des équipes de services publics envoyées pour remplacer ou réparer des lignes aériennes ou des excavations pour réparer ou remplacer des services publics souterrains, sans préavis aux occupants. Si une servitude permet au public d'avoir accès au site, par exemple en cas d'urgence, l'institution doit être informée et accepter l'exigence avant l'occupation.

7.1.3. Télécommunications et liaisons de données à l'extérieur de l'installation

Tous les composants physiques, y compris l'équipement satellitaire, doivent être protégés physiquement pour éviter tout dommage accidentel ou intentionnel. Une EMR devrait être utilisée pour déterminer les mesures de sécurité physique appropriées pour le câblage de télécommunications à l'extérieur d'une installation. Des renseignements supplémentaires se trouvent dans la Politique sur les services et le numérique.

7.1.4. Stationnement du personnel et des visiteurs

Les emplacements de stationnement désignés par des panneaux devraient indiquer les aires de stationnement du personnel et des visiteurs. Pendant les heures d'accès limitées, l'accès du personnel au stationnement intérieur devrait être limité à l'accès aux clés ou à l'accès contrôlé par le gardien.

L'emplacement du stationnement du personnel devrait être envisagé par rapport aux portes de sortie de secours. Si les portes de sortie de secours s'ouvrent dans le stationnement, on peut prévoir une utilisation fréquente, ce qui peut avoir des

répercussions sur une intervention fiable.

Le stationnement des visiteurs devrait faciliter l'orientation vers l'entrée principale de l'installation. Afin d'éviter les obstacles (visuels ou physiques), il ne devrait pas y avoir d'espace aux entrées principales ou latérales pour le stationnement, les arrêts ou les points de dépôt.

7.1.5. Circulation extérieure – Routes

Une définition claire des points d'entrée améliore l'accès légitime et réduit la confusion. Des panneaux devraient être utilisés pour diriger les membres du public vers les points d'entrée appropriés pour les véhicules. Veiller au respect des exigences municipales, provinciales et territoriales applicables.

7.2. Mesures de protection de l'immeuble

Diverses mesures de protection des immeubles peuvent être mises en œuvre pour protéger les biens et les employés du GC. Les EMR et la conception axée sur la menace permettent de déterminer quelles mesures de protection peuvent être requises pour une installation donnée et toute exigence particulière. La meilleure pratique consiste à utiliser une combinaison des garanties suivantes pour un système de sécurité holistique et fiable (par exemple, utiliser le contrôle électronique d'accès et la détection électronique des intrusions avec une salle de stockage sécurisée pour contrôler l'accès et détecter les tentatives d'accès non autorisées potentielles).

Cette section est destinée à être utilisée conjointement avec les conseils du GSMGC-019 – Guide de protection, détection, réponse, et récupération, GSMGC-015 – Guide pour l'établissement des zones de sécurité matérielle, GSMGC-006 - Guide de gestion de l'accès, et d'autres GSMGC énumérés lors de la compilation d'un énoncé de conception de la sécurité pour une installation.

7.2.1. Contrôle électronique de l'accès

Les mesures de contrôle électronique de l'accès fournissent des dossiers précis (vérification) des déplacements des visiteurs et des employés dans l'ensemble d'une installation. Une EMR déterminera la nécessité de mesures de contrôle d'accès électronique et les spécifications de l'équipement. Le contrôle électronique de l'accès peut être utilisé conjointement avec la détection électronique des intrusions et CCTV pour assurer une détection adéquate des tentatives d'accès non autorisé ou réel.

7.2.2. Détection électronique des intrusions

Les systèmes électroniques de détection d'intrusion sont conçus pour assurer une surveillance continue des emplacements vitaux ou de grande valeur, des points de contrôle d'accès, des zones dans lesquelles l'accès est contrôlé (ZT, ZS, ZHS) et de tout autre espace dans lequel la surveillance et le contrôle humains ne sont pas possibles. Une EMR déterminera le besoin de mesures électroniques de détection d'intrusion et les

spécifications de l'équipement. La détection électronique d'intrusion peut être utilisée en conjonction avec le contrôle électronique de l'accès et CCTV pour assurer une détection adéquate des tentatives d'accès non autorisé ou réel. La détection électronique des intrusions doit être surveillée par du personnel capable de coordonner une intervention en cas d'intrusion ou d'urgence. La pratique exemplaire consiste pour les ministères et organismes à établir un Centre des opérations de sécurité (COS) pour diriger cette fonction.

7.2.3. Télévision et vidéo en circuit fermé

CCTV peut aider un ministère ou un organisme à surveiller l'accès à son installation, à évaluer les alarmes valides et nuisibles et à surveiller un emplacement problématique. Une EMR et une analyse de la menace fondée sur la conception détermineront le besoin de vidéosurveillance et les spécifications de l'équipement. La vidéosurveillance peut être combinée avec le contrôle d'accès électronique et la détection électronique de l'intrusion pour assurer une détection adéquate des tentatives d'accès non autorisé ou des accès non autorisés réels, ainsi que pour initier une intervention. Pour de plus amples renseignements, veuillez consulter GSMGC-011 - Guide des systèmes de surveillance vidéo.

7.2.4. Centre des opérations de sécurité

Un COS fournit une installation pour soutenir le personnel de sécurité dans la surveillance, la surveillance, l'affichage, le contrôle, la gestion et la réponse aux événements liés à la sécurité. Un COS fournit généralement des activités de surveillance 24 heures sur 24 au moyen de systèmes de caméras vidéo, de capteurs d'alarme d'intrusion et de systèmes connexes. Le COS permet également de détecter et d'évaluer les notifications d'alarme et de dépêcher le personnel pour résoudre le problème, comme les équipes de sécurité sous contrat, les commissionnaires ou le personnel des services d'urgence. Le COS exerce un certain nombre de fonctions essentielles et la connaissance de la situation est au premier plan de l'objectif opérationnel.

De plus amples renseignements sur les fonctions d'utilisation d'un COS se trouvent dans le guide GCPSG-003 - Guide des considérations relatives à la conception d'un centre des opérations de sécurité.

7.2.5. Pièces d'entreposage sécuritaire

Une Pièce d'entreposage sécuritaire (PES) est conçue pour fonctionner comme un conteneur de stockage approuvé pour le stockage sur étagère ouverte d'une grande quantité d'informations ou de biens classifiés ou protégés. Pour plus d'informations sur les spécifications de construction du PES, reportez-vous à G13-01 Pièces d'entreposage sécuritaire (PES).

7.2.6. Zones de discussion sécurisées

Un Zone de discussion sécurisée (ZDS) est un espace spécialement conçu et géré pour

éviter d'entendre des discussions concernant des informations protégées et classifiées à différents niveaux d'atténuation sonore. Pour obtenir de plus amples renseignements sur les spécifications de construction de la ZDS, veuillez consulter le document GSMGC-017 - Guide de construction des zones de discussion sécurisées.

8. Considérations et garanties supplémentaires

Les ministères et organismes du GC évoluent dans une grande variété d'environnements au Canada et à l'étranger. Ce guide ne peut pas fournir toutes les considérations de conception et les mesures de protection possibles ni inclure des détails techniques spécifiques pour l'équipement de sécurité ou une liste exhaustive des inclusions de l'énoncé de conception de sécurité. L'EMR de l'installation et/ou la conception axée sur les menaces fourniront aux ministères et organismes du GC la plupart des renseignements nécessaires pour atténuer les vulnérabilités dans la conception d'une installation donnée, ainsi que pour aider à la prise de décisions sur l'équipement et les systèmes de sécurité à utiliser.

9. Références et documents connexes

- Politique sur la sécurité du gouvernement- Canada.ca
- Directive sur la gestion de la sécurité- Canada.ca
- Politiques, directives, normes et lignes directrices- Canada.ca
- Code canadien du travail
- Code national du bâtiment : Canada : 2020
- Code national de prévention des incendies : Canada : 2020
- Agence internationale de l'énergie atomique - Menaces de référence
- GSMGC-003 (2021) - Guide des considérations relatives à la conception d'un centre des opérations de sécurité
- GSMGC-004 (2020) - Guide des considérations sur l'éclairage de sécurité
- GSMGC-006 (2024) - Guide de gestion de l'accès
- GSMGC-007 (2022) - Transport, transmission et entreposage de matériel protégé ou classifié
- GSMGC-009 (2022) - Guide sur les considérations liées aux clôtures de sécurité
- GSMGC-011 (2024) - Guide des systèmes de surveillance vidéo
- GSMGC-013 (2024) - Principes fondamentaux du vitrage en sécurité matérielle
- GSMGC-015 (2023) - Guide pour l'établissement des zones de sécurité matérielle
- GSMGC-016 (2022) - Guide du processus d'évaluation et d'autorisation de sécurité des installations
- GSMGC-017 (2024) - Guide de construction des zones de discussion sécurisées
- GSMGC-019 (2023) - Guide de protection, détection, réponse, et récupération
- G13-01 (07/2013) - Pièces d'entreposage sécuritaire

10. Promulgation

Examiné et recommandé aux fins d'approbation.

J'ai examiné et recommande par la présente, GSMGC-014 (2024) Considérations relatives à la sécurité matérielle dans la conception des installations pour approbation.

Murphy,Timothy Robert Brian,000360902
Digitally signed by Murphy,Timothy Robert Brian,000360902
Date: 2024.07.17 14:22:16 -04'00'

Tim R Murphy, CD
Gestionnaire (intérimaire)
Principale Organisme Responsable de la Sécurité Matérielle, GRC

Date

Approuvé

J'approuve par la présente GSMGC-014 (2024) Considérations relatives à la sécurité matérielle dans la conception des installations

St-Pierre,Andre Vincent,000171484
Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.07.18 13:57:55 -04'00'

Andre St-Pierre,
Directeur, Sécurité Matérielle
Gendarmerie royale du Canada

Date