Guide pour l'établissement des zones de sécurité matérielle

GSMGC-015 (2024)

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

Date de publication : 2023-08-31
Date de mise à jour : 2024-06-01

Avant-propos

Le Guide pour l'établissement des zones de sécurité matérielle est une publication NON CLASSIFIÉE, diffusée avec l'autorisation du principal organisme responsable de la sécurité matérielle, la Gendarmerie royale du Canada (POSM-GRC).

La présente est une publication du gouvernement du Canada pour guider les ministères, les organismes et les employés du gouvernement du Canada dans l'établissement de zones de sécurité matérielle.

Les suggestions de modifications et les autres renseignements peuvent être envoyés par courriel au POSM-GRC à l'adresse : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Entrée en vigueur

La date d'entrée en vigueur de la norme du Guide pour l'établissement des zones de sécurité matérielle GSMGC-015 (2023) était le 2023-08-31; mis à jour 2024-06-01.

Registre des modifications

Nº de la modification	Date	Par	Résumé de la modification
1	2024-09-23	T. Murphy	Ajouter l'EDI, l'annexe A et l'annexe C

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

Table des matières

Avant-propos i
Entrée en vigueur i
Registre des modifications i
1. Introduction 1
1.1. But 1
1.2. Application 1
1.3. Équité, diversité et inclusion dans les systèmes de sécurité matérielle 2
1.4. Technologies de l'information 2
2. Coordonnées 2
3. Abréviations 3
4. Glossaire 3
5. Mise en œuvre de la conception 5
5.1. Besoin de savoir, besoin d'accéder 5
5.2. Sélection des zones 6
5.3. Exigences de base des zones 6
5.3.1. Zone publique (ZP) 7
5.3.2. Zone d'accueil (ZA) 7
5.3.3. Zone de travail (ZT) 7
5.3.4. Zone de sécurité (ZS) 8
5.3.5. Zone de haute sécurité (ZHS) 8
6. Préoccupations et questions relatives à l'établissement de zones 12
6.1. Défense en profondeur (utilisation de toutes les zones de sécurité matérielle) 12
6.2. Stockage des renseignements et des biens dans les zones de sécurité matérielle 13
6.3. Modification de la désignation des zones de sécurité matérielle 13
7. Locaux à usage particulier 14
7.1. Environnement de collaboration pour la recherche scientifique 14
7.2. Local de détention 14
7.3. Salles des serveurs informatiques 15
8. Références et documents connexes 15
Annexe A – Environnement de collaboration pour la recherche scientifique 16
1. But 16
2. Définition: Environnement de collaboration pour la recherche scientifique 16

3. Applicabilité....16
4. Introduction....17
5. Considérations relatives à la conception : 18
6. Sélection des zones de sécurité matérielle....19
7. Exemples de conception....20
7.1. Complètement séparé 20
7.2. Partiellement intégré....21
7.3. Entièrement intégré....22
Annexe B – Local de détention 16
1. Définition :....25
2. Applicabilité : 25
3. Considérations relatives à la conception d'un local de détention....25
3.1. Zone de transfert....25
3.2. Zone de soutien 26
3.3. Zone de traitement....26
3.4. Zone d'attente 26
Annex C – Protection physique des salles de serveurs informatiques....27
1. But....27
1.1. Emplacement de la salle des serveurs....27
1.2. Salles de serveurs partagés....27
2. Sauvegardes....28
2.1. Protection des serveurs dans une salle de serveurs partagée....28
2.2. Salle des serveurs sécurisée....28
2.3. Centre de données sécurisé....29
9. Promulgation....30

1. Introduction

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

1.1. But

Les environnements physiques des installations peuvent être conçus et gérés de façon à réduire le risque d'événements ou d'incidents indésirables. Ainsi, établir des zones correctement peut réduire le risque d'événements liés à la sécurité et contribuer à préserver la confidentialité, la disponibilité et l'intégrité des informations, des biens et des employés du GC. Bien que les zones de sécurité matérielle soient des éléments de sécurité importants, on ne doit pas les voir comme un moyen d'éliminer complètement les risques ni comme la seule méthode de gestion des risques; ils font plutôt partie intégrante de la stratégie globale des ministères et organismes du GC.

1.2. Application

Le présent guide s'applique aux installations contrôlées par le GC et ne doit pas être utilisé pour déterminer une zone de télétravail ou de travail à distance. Il ne détaille pas les exigences de sécurité pour un environnement de télétravail ou de travail à distance. Pour ces lignes directrices, plutôt se référer au guide GSMGC-008 – Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance.

Tous les ministères et organismes sont responsables de la protection des employés, des biens et de la prestation des services qui relèvent d'eux. En ce qui concerne les zones de sécurité matérielle, l'annexe C, section C.2.3.2 de la Directive sur la gestion de la sécurité (DGS) dit : « Mettre en œuvre des mesures afin de veiller à ce que l'accès à l'information (données électroniques) et aux systèmes d'information soit limité aux utilisateurs autorisés qui ont fait l'objet d'un filtrage de sécurité de niveau approprié et qui doivent y avoir accès ». De même, le Guide opérationnel de la sécurité matérielle (GSMGC-010) (section 6.2 – Hiérarchie des zones) précise que « 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 ».

L'orientation fournie dans le présent document doit être considérée comme les exigences de base pour l'établissement de zones de sécurité matérielle. Il incombe aux ministères et organismes du GC de valider ces exigences par rapport à leurs besoins en matière de sécurité. Le présent guide doit être utilisé conjointement avec une évaluation de la menace et des risques (EMR) afin d'élaborer une stratégie efficace pour l'établissement de zones de sécurité matérielle pour chaque installation, et pour soutenir le processus décisionnel concernant la sélection des zones. Les ministères et organismes du GC sont chargés de mettre en œuvre ces lignes directrices et peuvent communiquer avec le POSM-GRC pour en discuter le contenu, pour examiner d'autres guides sur la sécurité matérielle à l'appui des documents dont il est question dans le présent guide, ou pour obtenir des suggestions de mesures de protection

supérieures aux menaces de base en fonction des résultats de l'EMR. D'autres guides du POSM-GRC peuvent être nécessaires pour évaluer des situations de sécurité particulières et sont disponibles auprès du principal organisme responsable de la sécurité matérielle, la Gendarmerie royale du Canada (rcmp-grc.gc.ca).

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. Technologies 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

Sigle ou abréviation	Signification
DPS	Dirigeant principal de la sécurité
ECRS	Environnement de collaboration pour la recherche scientifique
EMR	Évaluation de la menace et des risques
GC	Gouvernement du Canada
LUP	Locaux à usage particulier
MOVS	Ministères et organismes à vocation scientifique
PNE	Procédures normales d'exploitation
POS	Principal organisme responsable de la sécurité
SCT	Secrétariat du Conseil du Trésor
SPAC	Services publics et Approvisionnement Canada
USB	Bus série universel
ZA	Zone d'accueil
ZAR	Zone d'accès restreint
ZHS	Zone de haute sécurité
ZP	Zone publique
ZS	Zone de sécurité
ZT	Zone de travail

4. Glossaire

Terme	Définition
Accompagnateur	Personne possédant une cote de sécurité appropriée qui est responsable de la surveillance continue de personnes n'ayant pas cette même cote dans les secteurs où elle serait normalement exigée.
Besoin d'accéder	Principe selon lequel il est nécessaire qu'une personne autorisée, bénéficiant d'une attestation de sécurité équivalente du GC, accède à une installation ou à une zone donnée afin de s'acquitter de ses fonctions. Il ne faut pas confondre ce terme avec le « besoin de savoir », soit celui de connaître les renseignements contenus ou traités dans ce secteur ou cette zone.
Besoin de savoir	Principe selon lequel il est nécessaire pour une personne d'avoir accès à des renseignements et de les connaître afin de s'acquitter de ses fonctions.
Biens	Éléments d'actif corporels ou incorporels du gouvernement

	du Canada. Ce terme s'applique entre autres 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.
Biens classifiés	Biens dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national.
Biens protégés ou désignés	Biens dont la compromission risquerait vraisemblablement de porter préjudice à un intérêt non national.
Contrôle de l'accès	Processus visant à restreindre l'accès aux biens d'une installation ou à des zones d'accès restreint. Cela peut se faire de différentes manières, notamment en contrôlant les visiteurs et le matériel aux points d'entrée par du personnel, des gardiens ou des moyens automatisés et, le cas échéant, en surveillant les mouvements à l'intérieur de l'installation ou des zones d'accès restreint au moyen de systèmes de contrôle d'accès.
Défense en profondeur	Principe selon lequel les zones de sécurité sont mises en œuvre de manière progressivement restrictive, de la zone la moins restrictive à la plus restrictive.
Exigences de sécurité de base	Dispositions obligatoires en matière de sécurité de la *Politique sur la sécurité du gouvernement* et des instruments politiques s'y rapportant.
Installation	Quelque chose qui est construit, installé ou mis en place pour servir un but particulier. Une installation peut comprendre un édifice spécifique (une partie ou la totalité) ou le site ou le terrain sur lequel il est situé.
Intégrité	Exactitude et intégralité des biens, et authenticité des transactions.
Locataire	Organisation qui occupe un immeuble du gouvernement fédéral administré par un autre ministère, organisme ou société d'État.
Renseignements classifiés	Renseignements dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national.
Renseignements protégés ou désignés	Renseignements dont la compromission risquerait vraisemblablement de porter préjudice à un intérêt non national.
Risque interne	Risque qu'une personne qui possède une connaissance de l'infrastructure d'une organisation (tant l'infrastructure matérielle que les réseaux informatiques) ou qui y a accès en profite pour causer du tort aux employés, aux clients, aux biens, à la réputation ou aux intérêts de l'organisation, par malveillance ou par inadvertance.
Surveillance continue	Surveillance ininterrompue (24 heures par jour, 7 jours sur 7).
Surveillance périodique	Exercice d'une supervision périodique, mais régulière. En

	matière de sécurité matérielle, la fréquence et la sévérité de la surveillance périodique sont déterminées par une organisation ministérielle en fonction d'une EMR.
Zone d'accès restreint (ZAR)	Aire de travail (site ou édifice) au sein d'un ministère où l'accès est restreint aux personnes autorisées. 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.

5. Mise en œuvre de la conception

Lorsqu'elles sont convenablement intégrées, les zones de sécurité matérielle devraient contribuer à l'environnement de sécurité global d'une installation. L'établissement de zones de sécurité matérielle devrait promouvoir un sentiment d'appartenance ou un renforcement du sentiment territorial, fournir des occasions de surveillance naturelle et établir un ensemble clairement défini de frontières par lesquelles un visiteur ou un employé peut passer.

Avant qu'une personne passe d'une zone à une autre, elle devrait percevoir la délimitation des zones (implicite ou explicite) et comprendre les règles et les restrictions associées au fait de la franchir. On doit également tenir compte des besoins d'espace fonctionnel du ministère lorsqu'on établit la délimitation des zones.

L'établissement des zones de sécurité matérielle ne devrait pas se limiter à respecter les exigences techniques prescrites pour les zones (voir la section 5.3) ni à satisfaire les besoins d'espace fonctionnel. Inversement, des mesures de sécurité excessives, inappropriées ou ne tenant pas compte des besoins d'espace fonctionnel seront ignorées et finiront par devenir inefficaces. On devrait éviter ou éliminer tout ce qui pourrait inciter le personnel non autorisé à traverser les délimitations des zones (à savoir, les toilettes, la cafétéria, etc.).

5.1. Besoin de savoir, besoin d'accéder

L'une des exigences fondamentales de la Politique sur la sécurité du gouvernement (PSG) est de limiter l'accès aux renseignements et aux zones de nature délicate. La PSG limite en outre l'accès aux personnes qui ont besoin de savoir ou d'accéder aux renseignements pour s'acquitter de leurs fonctions. Alors que les cotes de sécurité permettent l'accès général à certains renseignements ou zones, l'application des principes du besoin de savoir et du besoin d'accéder limite cet accès à ceux qui ont besoin de consulter des renseignements précis ou d'accéder à des zones particulières. Les membres du personnel n'ont pas le droit d'accéder uniquement parce que cela leur conviendrait ou en raison de leur statut, de leur grade, de leur poste ou de leur niveau d'autorisation. Les ministères et organismes du gouvernement fédéral sont chargés d'examiner les privilèges d'accès et doivent révoquer l'accès lorsqu'il n'est plus nécessaire (p. ex. si un employé n'a plus besoin d'accéder à une zone, s'il accepte un poste dans un autre ministère ou un autre organisme ou s'il prend sa retraite).

Une bonne façon de mettre en œuvre ou de maintenir les principes du besoin de savoir et du

besoin d'accéder consiste à isoler et à contrôler l'accès aux renseignements et aux biens de nature délicate en établissant efficacement des zones de sécurité matérielle. Étant donné que des personnes au sein d'un ministère ou d'un organisme du GC peuvent constituer une menace pour la disponibilité, la confidentialité ou l'intégrité des renseignements ou des biens du GC (ce qu'on appelle « risque interne »), le fait de limiter l'accès aux seules personnes ayant besoin de savoir ou besoin d'accéder peut réduire le risque interne et contribuer à la protection des renseignements et des biens du GC.

5.2. Sélection des zones

Afin que l'on puisse déterminer la ou les zones appropriées en vue du traitement, du stockage ou de la destruction de biens de nature délicate, il est d'abord nécessaire d'établir les exigences de base. Le Guide opérationnel de la sécurité matérielle GSMGC-010 du POSM-GRC désigne les zones de sécurité matérielle en fonction de la catégorie de sécurité et du préjudice correspondant qui résulterait de la divulgation, de la destruction, du retrait, de la modification, de l'interruption ou de l'utilisation abusive non autorisée des renseignements ou des biens qu'elles contiennent. Ces catégories et niveaux de préjudice se trouvent également dans l'annexe J de la DGS.

SÉLECTION DES ZONES			
Catégorie *(voir la remarque 1)*	**Degré de préjudice** *(voir les remarques 1 et 2)*	**Zone de base** *(voir la remarque 3)*	**Menace accrue**
Protégé A	Préjudice limité ou modéré	Zone de travail	Zone de travail
Protégé B	Préjudice grave	Zone de travail	Une EMR doit être effectuée afin de déterminer les mesures de protection
Protégé C	Préjudice extrêmement grave	Zone de sécurité	
Confidentiel	Préjudice limité ou modéré	Zone de travail	
Secret	Préjudice grave	Zone de sécurité	
Très secret	Préjudice d'une gravité exceptionnelle	Zone de haute sécurité	

REMARQUES :

1. Conformément à l'annexe J de la DGS.
2. Consulter le POSM-GRC pour savoir comment stocker les biens, autres que des renseignements, qui ont des exigences élevées d'intégrité et de disponibilité.
3. Pour déterminer les biens, il faut attribuer des niveaux d'évaluation du préjudice pour l'intégrité, la disponibilité et la valeur du bien. Passer à une zone de niveau supérieur pourrait être nécessaire si le niveau établi pour le préjudice dépasse celui établi pour la confidentialité.

5.3. Exigences de base des zones

Les tableaux suivants résument les cinq zones fondamentales et leurs exigences de base. En

plus de ces zones, il est devenu nécessaire d'élargir les options afin de mieux tenir compte des besoins actuels du GC. On parle ici des « locaux à usage particulier », mentionnés dans les annexes du présent guide. L'annexe A traite de l'environnement de collaboration pour la recherche scientifique (ECRS) et l'annexe B, de l'établissement de zones pour les locaux de détention.

5.3.1. Zone publique (ZP)

ZONE D'ACCÈS PUBLIC	
Définition	Zone où l'accès est libre pour le public et qui entoure habituellement un immeuble gouvernemental ou en fait partie.
Exemples	Les terrains entourant un immeuble, comme les trottoirs et les corridors publics, ainsi que les vestibules d'ascenseur dans des immeubles à plusieurs occupants.
Périmètre	Il n'y a pas d'exigences de périmètre pour une ZP, mais elle peut comporter des panneaux indiquant l'entrée ou l'emplacement de la ZA.
Surveillance	S.O.

5.3.2. Zone d'accueil (ZA)

ZONE D'ACCUEIL	
Définition	Où la transition d'une ZP à un ZAR est délimitée et contrôlée.
Exemples	Elle est située généralement à l'entrée de l'immeuble où survient le premier contact entre le public et le ministère ou l'organisme, y compris des endroits où des services sont fournis et où des renseignements sont échangés. L'accès au public peut être restreint pendant certaines heures de la journée ou pour des motifs particuliers.
Périmètre	Elle peut être délimitée par des panneaux de signalisation. Le périmètre peut varier en fonction de l'heure du jour.
Surveillance	L'étendue de la surveillance variera en fonction de l'heure du jour ou de la façon précisée par l'EMR.
Remarques : Il faut tenir compte du fait qu'après les heures de fermeture ou de verrouillage, une ZA peut devenir une ZT, car elle pourrait faire partie de l'installation du GC qui nécessite une protection (p. ex. la nécessité de contrôler l'accès en cas d'inoccupation).	

5.3.3. Zone de travail (ZT)

ZONE DE TRAVAIL	
Définition	Secteur dont l'accès est limité au personnel ayant une cote de sécurité adéquate qui y travaille et aux visiteurs escortés.
Exemples	Espace à bureaux à aires ouvertes typique.
Périmètre	Elle doit être indiquée par un périmètre reconnaissable ou un périmètre de sécurité tel qu'il est précisé dans l'EMR
Surveillance	*** Périodique.**
*** Surveillance périodique =** faisant l'objet de confirmation sur une base régulière qu'il n'y a pas eu d'atteinte à la sécurité. La fréquence et la diligence de la surveillance sont fondées sur les recommandations d'une EMR. Par exemple, une patrouille de surveillance, des registres de détection électronique des intrusions, ou des employés qui travaillent sur les lieux.	

5.3.4. Zone de sécurité (ZS)

ZONE DE SÉCURITÉ	
Définition	Zone dont l'accès est limité au personnel autorisé ayant une cote de sécurité adéquate et aux visiteurs autorisés et visiteurs escortés.
Exemples	Une zone où des renseignements ou des biens Secret sont traités ou conservés.
Périmètre	Elle doit être indiquée par un périmètre reconnaissable ou un périmètre de sécurité tel qu'il est précisé dans l'EMR
Surveillance	Surveillée continuellement, c'est-à-dire jour et nuit, sept jours par semaine.
****Surveillance continue** = avec confirmation sur une base continuelle qu'il n'y a pas eu d'atteinte à la sécurité. Exemples : système de détection électronique des intrusions ou personne qui garde un point particulier de façon constante.	

5.3.5. Zone de haute sécurité (ZHS)

ZONE DE HAUTE SÉCURITÉ	
Définition	Zone dont l'accès est limité au personnel autorisé qui détient une attestation de sécurité valide et de niveau approprié et aux visiteurs autorisés et visiteurs escortés.
Exemples	Une zone où des renseignements ou des biens Très secret ou supérieurs sont traités ou conservés.
Périmètre	Il doit être délimité au moyen d'un périmètre construit selon les caractéristiques techniques recommandées dans l'EMR.
Surveillance	Surveillance continue, c'est-à-dire jour et nuit sept jours par semaine, avec consignation détaillée des données sur les accès, qui seront vérifiées par la suite.

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

- d'entreposer des biens dont les niveaux de menace diffèrent dans une même installation;
- d'établir divers degrés de contrôle de l'accès afin de protéger des biens de différents niveaux;
- de réduire les coûts en traitant et en détruisant des renseignements et des biens de différents niveaux dans une même installation;
- avec une planification appropriée, de modifier les zones d'une période à l'autre (p. ex., une ZT pendant les heures de travail peut devenir une ZS pendant les heures où elle est inoccupée, ou une ZA peut devenir une ZT pendant une période similaire).

Le nombre approprié de zones à l'intérieur d'une installation est établi en fonction du nombre de locataires (un ou plusieurs) et du propriétaire/gardien de l'installation (gouvernement fédéral ou provincial, administration municipale, secteur privé). Dans le cas d'un immeuble gouvernemental ayant plusieurs locataires, le comité de sécurité de l'immeuble doit établir la hiérarchie des zones dans les aires communes. Le locataire est chargé de délimiter des zones appropriées dans ses locaux.

Il convient de prendre note que les définitions précédentes n'empêchent pas d'établir un ZAR temporaire à l'intérieur ou à l'extérieur d'une zone contrôlée. Ces zones temporaires peuvent être créées pour héberger ou traiter des documents dont le niveau de classification est

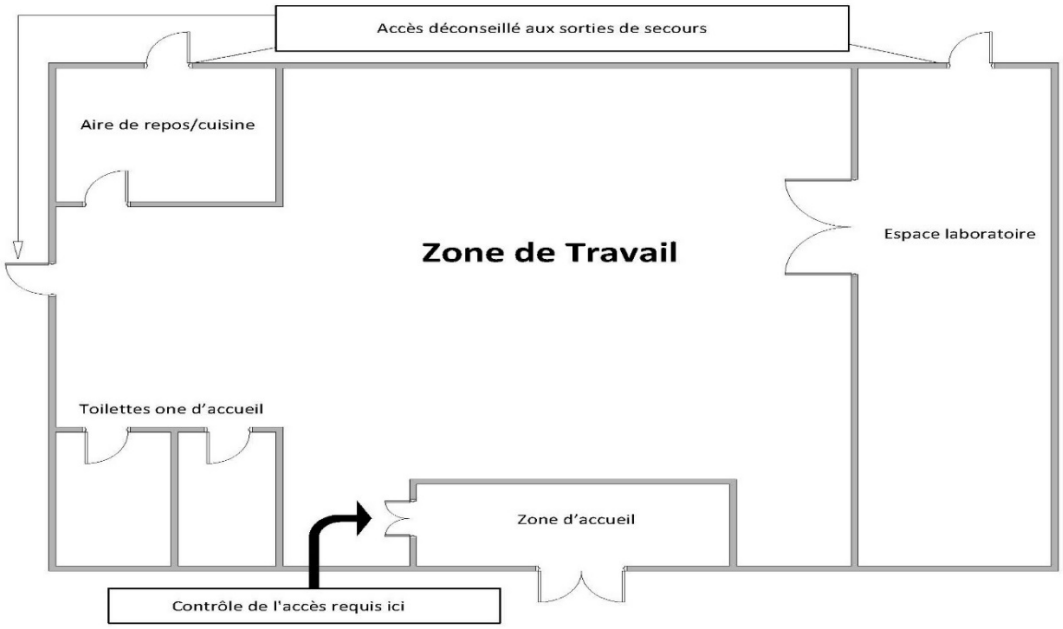
supérieur à celui des documents normalement stockés dans la zone, à condition que les mesures de sécurité matérielle nécessaires soient en place, que le risque accru fasse l'objet d'une EMR formelle et que le risque soit accepté par le DPS (ou son délégué). Par exemple, une ZS temporaire pourrait être établie autour d'un navire ou d'un camion saisi placé sous surveillance continue. Un autre exemple pourrait être un bureau à aires ouvertes qui fonctionne normalement comme une ZT, mais qui pourrait servir de ZS à condition que la personne qui manipule les documents en ait le contrôle total à tout moment et qu'elle empêche toute divulgation non autorisée.

Lors de la conception et de l'aménagement des zones de sécurité matérielle, les deux premières zones (ZP, ZA) doivent préparer le terrain pour l'accès aux ZAR. Selon l'exigence de sécurité de base, l'accès doit être contrôlé à partir d'une ZT. Comme il n'y a pas deux installations identiques, les endroits où commencent les ZT seront également différents d'une installation à l'autre. Les exemples suivants (figures 1 à 5) illustrent ces considérations dans quelques types d'installations génériques.

Figure 1

Texte de remplacement – La figure 1 représente le plan d'une installation type.

Figure 2

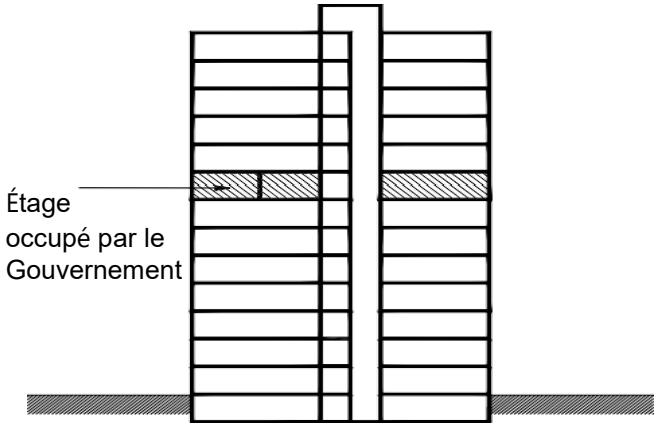


Texte de remplacement – La figure 2 représente un plan d'étage type.

Les figures 1 et 2 illustrent des exemples d'installations gouvernementales spécialisées sur des terrains appartenant à l'État. La ZP est constituée des terrains entourant l'édifice et, bien que les ministères et organismes puissent vouloir surveiller cette zone, il n'est pas nécessaire d'en contrôler l'accès. Un ZA est située à l'entrée principale.

Dans cette zone, le public dispose d'un moyen d'établir un premier contact et d'échanger des renseignements. Cela peut se produire à la réception, où du personnel est présent pour contrôler l'entrée dans l'espace. L'accès au-delà du ZA est limité aux personnes qui ont besoin d'y accéder. Il doit y avoir un périmètre reconnaissable, p. ex. une porte ou une disposition de mobilier, qui délimitent clairement l'entrée de la ZAR et dont l'accès est contrôlé à partir de ce point. L'accès doit également être contrôlé à chaque point où le ZT permet l'accès à un ZS.

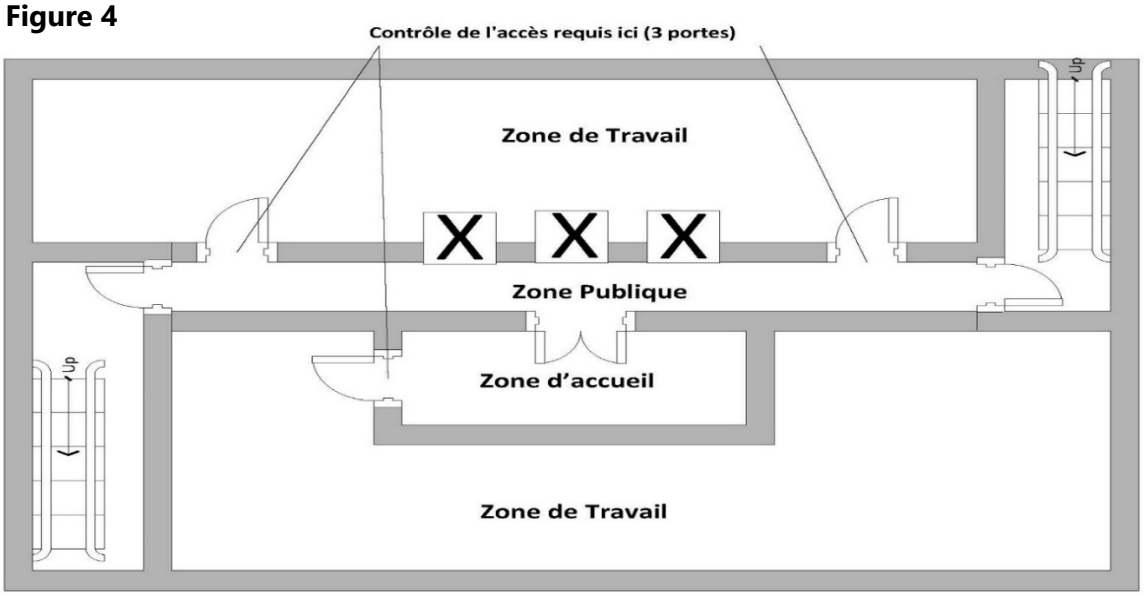
Figure 3



Section de l'édifice

Texte de remplacement – La figure 3 représente, comme section d'un édifice à plusieurs étages, l'espace occupé par un locataire du GC.

Figure 4



Texte de remplacement – La figure 4 représente une section d'immeuble à plusieurs étages et d'un espace occupé par un locataire du GC.

Les figures 3 et 4 illustrent un exemple d'édifice à plusieurs étages dans lequel le gouvernement loue plusieurs étages. La ZP comprend le hall d'entrée du rez-de-chaussée, ainsi que l'ascenseur et les couloirs de chaque étage. Un ZA est adjacent à la ZP sur un côté de l'étage. Les autres zones de bureaux sont des ZT.

L'accès au ZT depuis la ZA doit être contrôlé. Dans cet exemple, il est possible d'entrer dans le ZT depuis le ZA ou la ZP (le couloir). Dans la mesure du possible, l'accès aux ZT doit se faire en passant par un ZA.

Des zones de sécurité matérielle devraient être mises en œuvre d'une manière progressivement restrictive, de la zone la moins restrictive (ZP) à la plus restrictive (ZT, ZS ou ZHS), de façon à ce qu'il soit nécessaire de franchir des points d'entrée séquentiels. Un point d'entrée est une caractéristique technique qui permet de canaliser la circulation de manière à contrôler efficacement l'accès à cet endroit-là. Les points d'entrée des différentes zones devraient être faciles à reconnaître. Le périmètre d'une zone ne doit permettre aucun accès, à moins qu'il y ait des exigences fonctionnelles, p. ex. un comptoir de service qui gère ou traite les demandes des clients. Il doit être clair que l'entrée dans un ZT est limitée au personnel autorisé et aux visiteurs accompagnés comme il se doit. En règle générale, cela se fait au moyen d'une signalisation dans le ZA ou indiquant comment s'y rendre. Le plan d'étage ci-dessous (figure 5) illustre certains des critères proposés.

En plus du respect des exigences de base, les ministères et les organismes peuvent vouloir mettre en place des mesures supplémentaires pour limiter davantage l'accès à l'intérieur d'une installation. La nécessité d'un ZS ou d'une ZHS à l'intérieur d'une installation dépend de la catégorie des documents manipulés, ainsi que des menaces spécifiques à l'égard du ministère. Différents moyens de contrôle d'accès peuvent être appropriés en fonction de la zone à laquelle le point d'entrée donne accès. Il peut s'agir d'un membre du personnel ou d'un agent de sécurité qui vérifie les laissez-passer pour entrer dans un ZT ou d'un système de contrôle d'accès biométrique perfectionné pour entrer dans une ZHS. La sélection de la mesure de contrôle d'accès peut être déterminée à l'aide d'une EMR. Il faudrait également établir des procédures de filtrage du personnel et des barrières matérielles de niveau correspondant pour appuyer les mesures de contrôle d'accès.

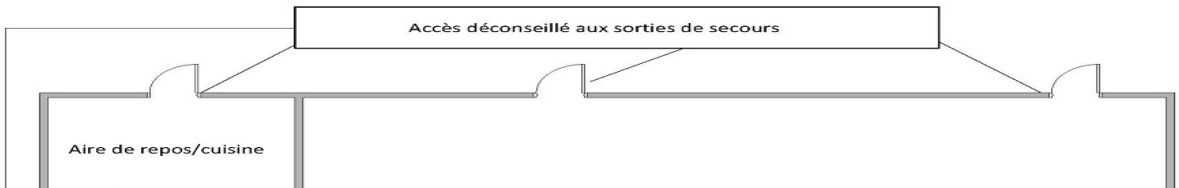


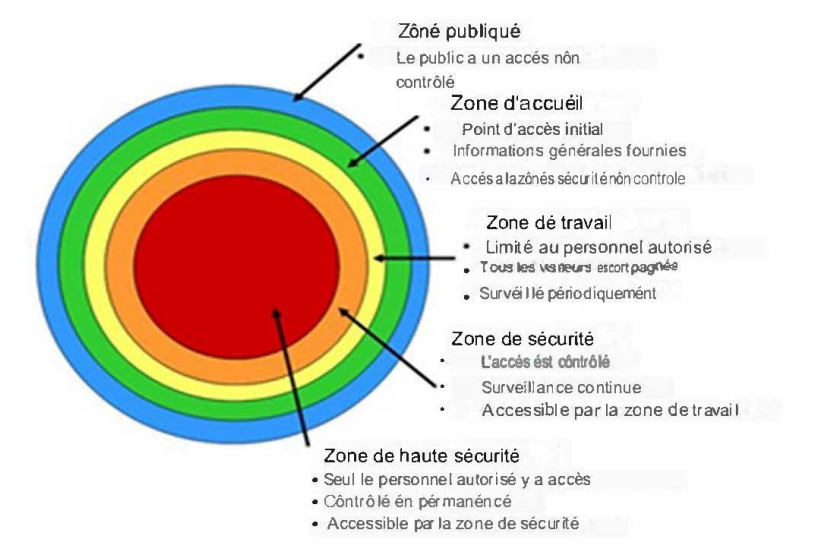
Figure 5

Texte de remplacement – La figure 5 est le plan d'un édifice comportant différentes zones de sécurité matérielle dont l'accès est contrôlé.

6. Préoccupations et questions relatives à l'établissement de zones

6.1. Défense en profondeur (utilisation de toutes les zones de sécurité matérielle)

Il ne faut pas omettre ou contourner les zones de sécurité, car il faut toutes les zones nécessaires pour créer une « défense en profondeur ». Il s'agit du principe selon lequel les zones de sécurité sont mises en œuvre de manière progressivement restrictive, de la zone la moins restrictive à la plus restrictive. Dans certains cas, cependant, les exigences opérationnelles de certains ministères ou de certaines installations peuvent rendre inefficace la mise en place de toutes les zones de sécurité matérielle, et il existe également des situations limitées où il peut être difficile ou peu pratique de le faire. Dans de tels cas, une seule zone peut être contournée ou exclue du modèle d'établissement de zones, à condition que les mesures de sécurité de cette zone soient compensées dans la zone subséquente. Tout écart en matière d'établissement de zones doit être soigneusement et minutieusement consigné dans une EMR, et les risques qui en découlent doivent être acceptés par l'autorité de sécurité, soit le DPS ou son délégué.



6.2. Stockage des renseignements et des biens dans les zones de sécurité matérielle

La norme GSMGC-007 – Transport, transmission et entreposage de matériel protégé ou classifié décrit les exigences minimales en matière de stockage de documents de nature délicate par zone de sécurité matérielle et par catégorie de sécurité. Dans des circonstances limitées et dans le cadre d'une solution de gestion des risques au niveau du ministère, il est possible d'envisager le stockage de petites quantités de documents de catégorie supérieure dans des zones de sécurité matérielle inférieure. Avant de stocker des renseignements à ce titre, il convient d'effectuer une EMR afin d'analyser tout risque résiduel et d'envisager des mesures de contrôle de sécurité supplémentaires pour garantir la protection des documents. Le DPS ou son délégué doit alors autoriser l'acceptation du risque résiduel. Les ministères et les organismes peuvent communiquer avec le POSM de la GRC pour poser des questions spécifiques concernant ces écarts et demander des conseils sur les étapes subséquentes.

6.3. Modification de la désignation des zones de sécurité matérielle

Il est possible que la désignation de la zone de sécurité matérielle change au cours d'une journée ouvrable (p. ex., le ZA est fermé à clé et n'est pas accessible au personnel ou aux clients pendant les heures de fermeture du bureau ou pendant les heures d'accès limité, notamment à l'heure de la pause-repas). La nouvelle désignation des zones pendant ces périodes dépendra des activités qui y sont menées pendant les heures normales, du type de mesures de sécurité utilisées en dehors des heures normales, des moments où la zone est fermée, et des personnes qui y ont accès. Il convient d'examiner attentivement toute mesure de sécurité matérielle supplémentaire qui pourrait être nécessaire dans ce cas. La mise en œuvre d'une telle solution peut exiger une EMR et être approuvée par le DPS ou son délégué après un examen approfondi et l'acceptation de tout risque résiduel en cause.

7. Locaux à usage particulier

Les locaux à usage particulier (LUP) sont des locaux non normalisés additionnels dont un ministère ou un organisme a besoin pour mener des activités fonctionnelles ou de secteur d'activité spécifique. Ces espaces ne doivent être mis en place qu'en cas de besoin, en fonction d'exigences particulières ou essentielles du point de vue opérationnel du ministère ou de l'organisme. Le POSM-GRC recommande qu'un LUP ne soit utilisé que dans des circonstances limitées, p. ex. :

- lorsqu'il s'agit de répondre à des exigences opérationnelles pour des groupes non gouvernementaux;
- pour accueillir temporairement des personnes en attente d'un interrogatoire dans le cadre d'une enquête ou d'un transfert vers un autre établissement du GC ou un établissement gouvernemental national ou étranger;
- uniquement pour des travaux non classifiés ou de nature non délicate, à moins qu'ils ne soient spécifiquement désignés et approuvés par le DPS ou son délégué.

Il convient de prendre note que ce ne sont pas tous les ministères et organismes du GC qui auront besoin de LUP dans leurs installations, et que les LUP ne doivent pas être utilisés comme un moyen de contourner les exigences du GC sur les attestations de sécurité.

7.1. Environnement de collaboration pour la recherche scientifique

Un ECRS est un LUP facultatif qui permet aux membres de la communauté scientifique extérieurs au GC (ressortissants étrangers, chercheurs ou scientifiques des universités et du secteur privé) de travailler en collaboration avec le GC pour mener des recherches et des essais scientifiques dans un environnement contrôlé et sécurisé, séparé des autres renseignements ou biens du GC.

Un environnement de collaboration en recherche scientifique ne peut être mis en œuvre que par les ministères et organismes du GC spécifiquement désigné comme ministères ou organismes à vocation scientifique (MOVS). Les ECRS doivent être nettement distingués des espaces de cotravail du GC; ils ne peuvent pas les remplacer ni ne doivent servir à contourner la procédure d'attestation de sécurité. Les MOVS qui ont besoin d'un ECRS doivent toujours effectuer une vérification complète et approfondie des références de tout chercheur ne disposant pas d'une attestation de sécurité du GC et désignée pour travailler dans ces espaces. Voir l'annexe A.

7.2. Local de détention

Un local de détention est un LUP utilisé pour détenir des personnes dans le cadre d'une enquête ou d'une procédure d'exécution de la loi. Les ministères et organismes du GC qui comptent l'exécution de la loi parmi leurs responsabilités (p. ex. la GRC, l'Agence des services frontaliers du Canada [ASFC] ou le ministère des Pêches et des Océans [MPO]) peuvent avoir besoin de ce type de LUP. Voir l'annexe B.

7.3. Salles des serveurs informatiques

Contrairement aux ECRS et aux espaces de détention, presque tous les ministères et organismes du GC ont besoin d'une ou de plusieurs salles de serveurs informatiques pour héberger la technologie de l'information (IT) du GC qui appuie tous les processus du GC. La conception et la gestion de ces systèmes de TI sont guidées par le Centre de la sécurité des télécommunications du Canada. Pour en savoir plus sur l'emplacement et la protection physique des salles de serveurs d'ordinateurs, consultez l'annexe C.

8. Références et documents connexes

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité
- Centre de la sécurité des télécommunications du Canada.
- Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion dans la fonction publique fédérale
- Directive sur l'obligation de prendre des mesures d'adaptation
- Guide à l'intention des employés deux esprits, transgenres, non-binaires et de la pluralité des genres dans la fonction publique fédérale
- Guide d'équipement de sécurité
- GSMGC-007 – Transport, transmission et entreposage de matériel protégé ou classifié
- GSMGC-008 – Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance
- GSMGC-010 – Guide opérationnel de la sécurité matérielle
- GSMGC-011 – Guide des systèmes de surveillance vidéo (CCTV)
- GSMGC-013 – Principes fondamentaux du vitrage en sécurité matérielle
- G13-01 Pièces d'entreposage sécuritaire
- G13-02 Mur mitoyen sécuritaire

Annexe A – Environnement de collaboration pour la recherche scientifique

1. But

La présente annexe donne des conseils de sécurité matérielle complémentaires au guide proprement dit, concernant la conception et la mise en place d'environnements de collaboration pour la recherche scientifique (ECRS). Dans les présentes lignes directrices, la recherche scientifique est définie comme une investigation ou une étude systématique de théories et/ou d'hypothèses scientifiques. Elle est de nature quantitative et repose fortement sur la collecte de données. La recherche scientifique est souvent utilisée dans les domaines de la biologie, de la physique et de la chimie.

2. Définition: Environnement de collaboration pour la recherche scientifique

Un ECRS est un environnement conçu pour permettre aux membres de la communauté scientifique extérieurs au gouvernement du Canada (GC), c.-à-d. les ressortissants étrangers, les chercheurs ou les scientifiques des universités et du secteur privé, de travailler en collaboration avec les ministères et organismes du GC pour mener des recherches et des essais scientifiques dans un environnement contrôlé et sécurisé.

3. Applicabilité

L'application, l'utilisation et le fonctionnement d'un ECRS ainsi que les directives contenues dans cette annexe ne s'appliquent qu'aux ministères et organismes du GC spécifiquement identifiés comme ministères et organismes à vocation scientifique (MOVS) et ne doivent pas être confondus avec les sites/installations de travail collaboratif du GC. Les MOVS collaborent avec des partenaires scientifiques d'organisations extérieures au GC, comme le milieu universitaire et l'industrie, y compris des ressortissants étrangers, dans le cadre de recherches scientifiques collaboratives en laboratoire. Agriculture et Agroalimentaire Canada, Santé Canada et l'Agence de la santé publique du Canada sont des exemples (non exhaustifs) de MOVS. Il est important de prendre note que l'acceptation des risques liés à l'utilisation des ECRS relève du DPS du ministère ou de l'organisme ou de son délégué qui exploite le ECRS.

L'utilisation d'un ECRS est applicable lorsque :

- Il n'est pas possible ou pratique d'obtenir les autorisations de sécurité applicables pour les partenaires collaborateurs en raison de :
    - Des chercheurs ayant une nationalité étrangère ; et
    - Des chercheurs ou des collaborateurs du milieu universitaire ou de l'industrie et lorsque la nature de ces collaborations est de très courte durée.

Si la nature de la recherche collaborative est considérée comme sensible, protégée ou classifiée selon les directives du GC, reportez-vous à la sélection des zones pour plus d'informations sur la sélection des zones de sécurité matérielle qui pourraient être nécessaires pour assurer la protection des informations recherchées ou collaborées.

Il convient de noter que les collaborateurs ne doivent être autorisés à accéder qu'aux informations spécifiques à leur travail et non à la totalité des informations.

L'utilisation d'un ECRS n'est PAS applicable :

- Lorsque la recherche est menée en collaboration/menée entre des ministères et des organismes du GC (même ceux identifiés comme des SBDA) où tous les utilisateurs détiennent une habilitation ou un statut de sécurité du GC ; et
- Comme moyen de contourner ou de contourner le processus d'habilitation de sécurité.

Les MOVS responsables des opérations d'un ECRS doivent toujours procéder à un contrôle approfondi de tous les chercheurs collaborateurs pour vérifier leurs titres universitaires ou industriels et effectuer toutes les procédures de contrôle d'accès au site requises.

Les directives décrites dans cette annexe se limitent aux principes généraux (sécurité physique, « besoin de savoir », « besoin d'accès », sécurité du personnel, etc.). Les exigences de sécurité globales pour le SRCE doivent être conçues en fonction des exigences de sécurité globales du projet entrepris dans l'environnement. L'acceptation du risque lié à l'utilisation d'un ECRS incombe au CSO ou à son délégué du ministère ou de l'agence qui héberge l'espace.

L'orientation donnée dans la présente annexe se limite à des principes généraux (sécurité matérielle, « besoin de connaître », « besoin d'accéder », sécurité du personnel, etc.). Les exigences de sécurité globales pour l'ECRS doivent être conçues en fonction des exigences de sécurité globales du projet réalisé dans l'environnement. L'acceptation des risques liés à l'utilisation d'un ECRS incombe au DPS ou à son délégué du ministère ou de l'organisme dans lequel se trouve l'espace en question.

4. Introduction

Comme il n'y a pas deux installations identiques, l'emplacement des laboratoires ou des zones de recherche diffère d'une installation à l'autre. Les mesures de sécurité matérielle pour l'ECRS doivent être conformes aux exigences relatives à l'établissement des zones de sécurité matérielle du GC pour la catégorie des travaux de recherche, et être intégrées à la sécurité globale de l'installation. Conformément au présent guide, le modèle d'établissement des zones de la sécurité matérielle du GC comprend cinq zones :

- zone publique (ZP);
- zone d'accueil (ZA);
- zone de travail (ZT);
- zone de sécurité (ZS);
- zone de haute sécurité (ZHS).

Bien que l'option privilégiée soit d'avoir un ECRS complètement séparé de toutes les autres zones du GC, un ECRS peut aussi être intégré dans n'importe laquelle des zones existantes, moyennant une planification adéquate et des contrôles de sécurité supplémentaires, il convient de réaliser une EMR qui identifie tous les risques et les mesures supplémentaires de contrôle de la sécurité matérielle nécessaire avant de mettre en place un ECRS, en particulier dans un ZS ou une ZHS.

ENVIRONNEMENT DE COLLABORATION POUR LA RECHERCHE SCIENTIFIQUE (ECRS)	
Définition	Espace conçu pour permettre aux membres de la communauté scientifique extérieurs au GC de travailler en collaboration avec les ministères du GC sur des projets de recherche dans un environnement contrôlé/sécurisé.
Exemples	Une zone où des personnes externes du GC, p. ex. représentant des gouvernements étrangers, des universités ou le secteur privé, peuvent mener des recherches et des essais scientifiques.
Établissement de la zone	Le zonage pour l'espace de collaboration doit respecter les exigences fondamentales d'un accès progressivement restrictif et être intégré à la sécurité globale de l'installation.
Périmètre	Il doit être délimité au moyen d'un périmètre construit selon les caractéristiques techniques recommandées dans l'EMR.
Surveillance	Surveillance continue**, c'est-à-dire jour et nuit, sept jours par semaine, avec consignation détaillée des données d'accès, qui seront vérifiées par la suite.

5. Considérations relatives à la conception :

- Il appartient au MOVS de déterminer la catégorie de l'ECRS en fonction de son interprétation de la nature délicate, de la catégorie réelle au GC ou des risques/dangers liés à la recherche. En cas de catégories multiples, les exigences de la catégorie la plus élevée sera nécessaire.
- Idéalement, l'ECRS devrait être conçu comme une zone séparée et distincte, avec un accès limité ou inexistant aux autres zones de laboratoire de l'installation. Il doit respecter les exigences fondamentales de la défense en profondeur, l'établissement de zones de sécurité matérielle progressivement restrictives et les exigences d'accès, les principes du besoin de connaître/besoin d'accéder, et être intégré à la sécurité globale de l'installation.
- L'ECRS doit être autonome et disposer de postes de travail, de matériel scientifique, de salle à manger, de toilettes et de contrôles de TI ne permettant pas l'accès aux réseaux informatiques du GC. Les possibilités pour le personnel non autorisé de franchir les limites des zones (p. ex. les toilettes, la cafétéria, etc.) doivent être éliminées, sauf si des contraintes de conception de l'édifice ne le permettent pas – dans ce cas, il faut réaliser une EMR et obtenir d'une autorité compétente l'acceptation des risques.
- L'ECRS doit répondre aux exigences de contrôle de la sécurité matérielle nécessaires à la catégorie de la recherche menée (p. ex. ZT, ZS, etc.). S'il n'est pas possible de construire la zone requise, il convient de réaménager les espaces existants. Il est recommandé de réaliser une EMR et de déterminer tous les risques.
- L'ECRS doit être intégré à la structure fonctionnelle globale du laboratoire où il est aménagé, y compris en ce qui concerne l'accès aux espaces communs et au matériel de

laboratoire partagé.

- Le ministère doit planifier correctement l'ECRS avant le début de tout projet de recherche scientifique et tenir compte de la protection des renseignements et des biens du GC qui ne font pas partie de la recherche, ainsi que du degré de préjudice lié aux renseignements, aux biens et aux droits de propriété de grande valeur.
- Le ministère qui héberge l'ECRS doit élaborer des procédures normales d'exploitation (PNE) destinées à fournir aux employés des instructions et des procédures claires, étape par étape, lorsqu'ils travaillent dans l'ECRS. Les PNE doivent notamment aborder les points suivants:
    - l'assainissement de l'espace de travail;
    - les accompagnateurs des employés;
    - les contrôles de TI (pas de connexion intranet/ réseau du GC);
    - les exigences de surveillance (surveillance périodique ou continue);
    - les systèmes de contrôle de l'accès.

  Remarque: Une liste de vérification utilisée avant l'entrée et la sortie peut également renforcer les mesures de sécurité.
- Au fur et à mesure de l'évolution de la recherche, des changements dans la nature délicate des renseignements et/ou des biens peuvent nécessiter l'adaptation ou la modification des dispositions de sécurité de l'ECRS afin d'atténuer l'évolution des risques en matière de sécurité.
- Lorsqu'elles sont convenablement intégrées, les zones de sécurité matérielle devraient améliorer l'environnement de sécurité global d'un établissement.

Remarques: Des zones de sécurité matérielle établies uniquement en se fondant sur les exigences techniques prescrites ou intégrées seulement en tenant compte des exigences fonctionnelles de l'espace peuvent se révéler insuffisantes ou inefficaces. Les mesures de sécurité qui sont excessives ou qui ne répondent pas aux exigences fonctionnelles seront contournées et deviendront inefficaces. Voir la section 5.3 du présent guide.

Il est également important de prendre note qu'au fur et à mesure de l'évolution de la recherche au sein d'une installation du GC, la nature délicate des renseignements et des biens peut changer. Il peut alors être nécessaire d'adapter ou de modifier les dispositions de sécurité de l'ECRS afin d'atténuer l'évolution des risques de sécurité. Ces considérations doivent être prises en compte dans l'EMR initiale pour la conception de l'espace, et dans les paramètres du projet de recherche scientifique mené dans l'installation. Ces considérations doivent faire l'objet d'une gestion prudente et continue des risques par le DPS ou son délégué.

6. Sélection des zones de sécurité matérielle

Pour déterminer la ou les zones de sécurité matérielle appropriées pour l'ECRS, il faut d'abord déterminer la catégorie du travail effectué. Il faut ensuite établir les exigences minimales de sécurité de base pour protéger ce travail. Le Guide opérationnel de la sécurité matérielle (GSMGC-010) de la GRC désigne les zones de sécurité matérielle en fonction de la catégorie des renseignements et des biens et du préjudice correspondant qui découlerait de leur divulgation, destruction, retrait, modification, interruption ou utilisation abusive non autorisée. Ces zones sont

définies dans le tableau ci-dessous et dans la section 5.2 en fonction de leur niveau de préjudice, avec des exemples spécifiques pour mettre en évidence la délimitation des zones pour un ECRS.

SÉLECTION DES ZONES			
Catégorie *(voir la remarque 1)*	**Degré de préjudice** *(voir les remarques 1 et 2)*	**Zone de base** *(voir la remarque 3)*	**Menace accrue**
Protégé A	Préjudice limité ou modéré	Zone de travail	Zone de travail
Protégé B	Préjudice grave	Zone de travail	Une EMR doit être effectuée afin de déterminer les mesures de protection
Protégé C	Préjudice extrêmement grave	Zone de sécurité	
Confidentiel	Préjudice limité ou modéré	Zone de travail	
Secret	Préjudice grave	Zone de sécurité	
Très secret	Préjudice d'une gravité exceptionnelle	Zone de haute sécurité	

REMARQUES :

1. Conformément à l'annexe J de la DGS.
2. Consulter le POSM-GRC pour savoir comment stocker les biens, autres que des renseignements, qui ont des exigences élevées d'intégrité et de disponibilité.
3. Pour déterminer les biens, il faut attribuer des niveaux d'évaluation du préjudice pour l'intégrité, la disponibilité et la valeur du bien. Passer à une zone de niveau supérieur pourrait être nécessaire si le niveau établi pour le préjudice dépasse celui établi pour la confidentialité.

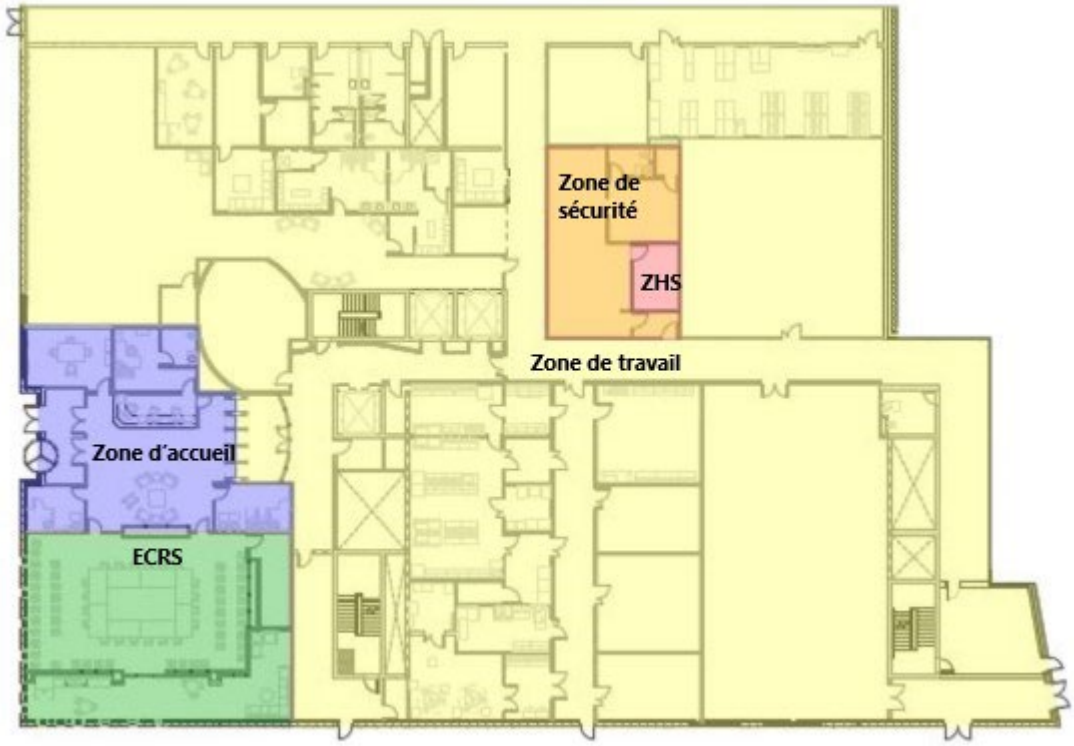
Si un espace de laboratoire défini ou un ECRS n'est pas disponible, il peut être nécessaire d'établir un ZAR temporaire à l'intérieur ou à l'extérieur d'une zone contrôlée. Par exemple, un ZS temporaire peut être établi autour d'un projet de recherche scientifique. La nécessité de limiter l'accès non autorisé à cette zone doit être évaluée, mais il faut au moins envisager la signalisation et la délimitation de l'espace de travail. Il faut recourir à des gardiens, des cloisons, des systèmes de vidéosurveillance ou d'autres mesures de contrôle. Il peut également être nécessaire de mettre en place une surveillance continue, par le biais d'agents de sécurité contractuels ou d'autres outils de surveillance.

7. Exemples de conception

7.1. Complètement séparé

Pour un ECRS, nouvellement construit (figure 1), qu'il s'agisse d'une installation autonome ou d'une installation existante qui ne permet l'accès à aucune autre zone opérationnelle d'une installation du GC est une situation idéale. L'environnement est autonome et n'est accessible que par un ZA. Des mécanismes de contrôle de l'accès appropriés sont en place et l'accès à la zone est régulièrement surveillé.

Figure 1 Complètement Séparés



Texte de remplacement – La figure 1 est un exemple de zone de sécurité matérielle. Ici, l'ECRS n'a accès à aucune autre zone opérationnelle d'installation du GC. Il est autonome, accessible uniquement par la zone d'accueil.

7.2. Partiellement intégré

Un réaménagement de l'installation du GC existante, où l'accès à l'ECRS se fasse par un ZT (figure 2), peut être nécessaire, mais ce n'est pas la solution idéale. Si c'est le seul moyen de créer un ECRS, des mécanismes de contrôle de l'accès appropriés doivent être mis en place pour empêcher tout accès non autorisé à d'autres zones de sécurité matérielle. Dans ce secteur, l'accès est régulièrement contrôlé. Le contrôle de l'accès est nécessaire à tous les points d'entrée dans toutes les zones. L'installation d'une signalisation peut indiquer clairement à tout visiteur que l'entrée dans un ZT est réservée aux employés autorisés. La signalisation peut également orienter la personne vers l'emplacement du ZA. L'entrée dans l'espace doit être limitée aux points d'entrée principaux; toutes les sorties de secours doivent être réservées à l'évacuation.

Figure 2 Partiellement Intégré

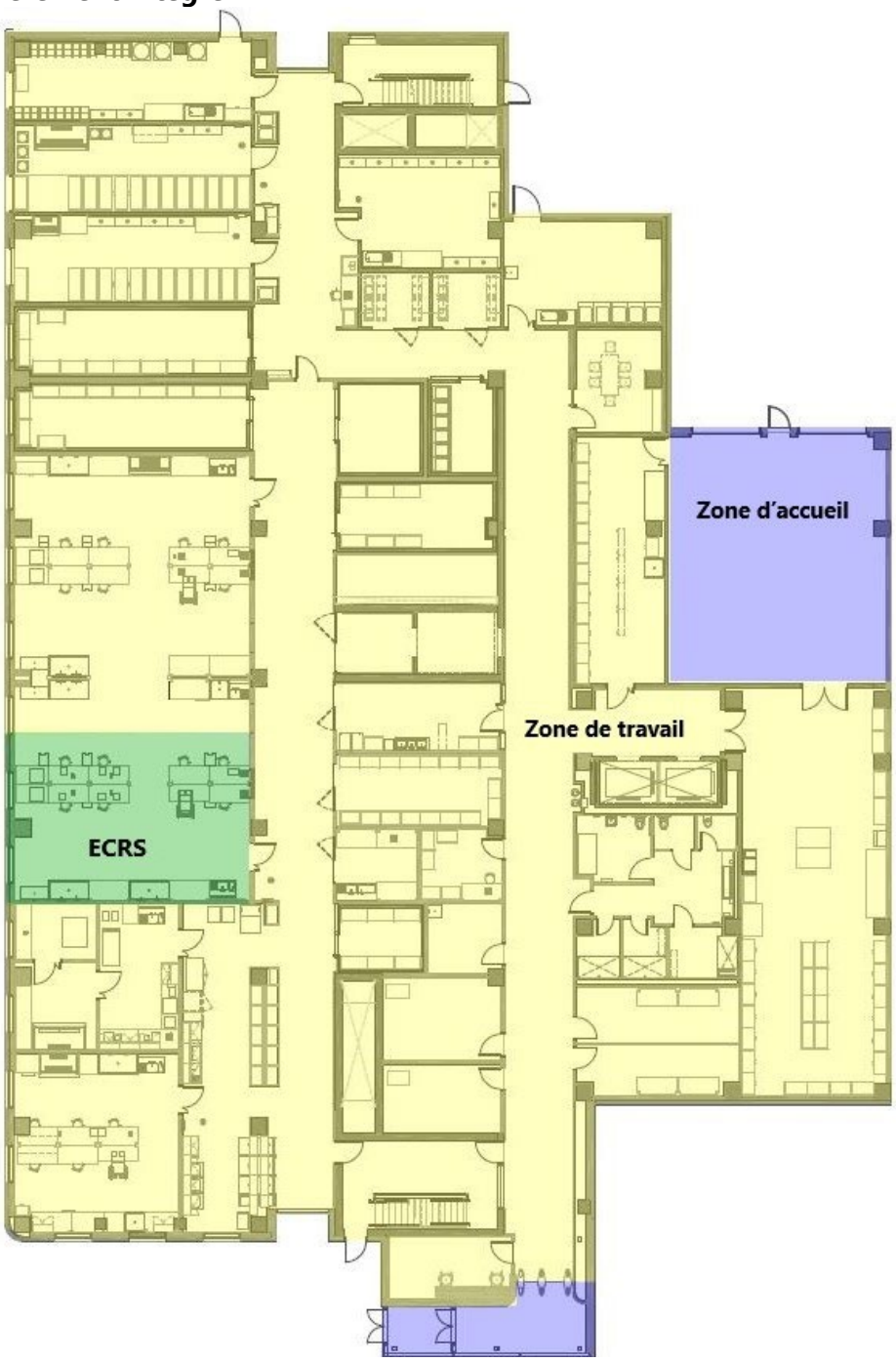
Texte de remplacement – La figure 2 est un exemple de zone de sécurité matérielle. Ici, l'accès à l'ECRS s'effectue par une zone de travail. Tous les points d'entrée dans les zones sont dotés de points d'accès contrôlés.

7.3. Entièrement intégré

Si l'ECRS est situé entièrement à l'intérieur d'une installation du GC, en particulier un ZS ou une ZHS (figure 3), l'accès non autorisé est beaucoup plus difficile à gérer. Ce type d'installation ne doit être utilisé qu'en dernier recours et seulement s'il n'existe pas d'autres options. Les MOVS doivent créer des IPO détaillées qui comprennent des dispositions

relatives à la surveillance constante et à l'accompagnement en direction et en provenance de l'ECRS, ainsi que toute autre mesure de contrôle de la sécurité jugée appropriée dans le cadre du processus d'EMR. Dans ce cas, l'entrée et la sortie de l'espace doivent être limitées à un seul point, toutes les autres sorties étant utilisées uniquement pour les évacuations d'urgence.

Figure 3 Entièrement Intégré



Texte de remplacement – La figure 3 est un exemple de zone de sécurité matérielle. Ici, l'accès à l'ECRS s'effectue par une zone de sécurité.

Annexe B – Local de détention

1. Définition :

La présente annexe donne des instructions de sécurité matérielle complémentaires au guide proprement dit, concernant la conception et la mise en place d'un local de détention. Le local de détention est un LUP défini comme étant un regroupement de zones de sécurité matérielle contrôlées et surveillé dans le but de restreindre l'accès et la sortie pour héberger temporairement et protéger des détenus ou d'autres personnes. La mise en place de ce type de local permet d'éviter que la personne détenue ne s'échappe, ne se blesse ou ne blesse quelqu'un d'autre, de préserver l'intégrité d'une enquête ou d'empêcher la subornation de témoins.

2. Applicabilité :

Un local de détention n'est pas une nouvelle zone de sécurité matérielle ajoutée à la hiérarchie des zones de sécurité. Cette zone doit être utilisée uniquement lors de besoins opérationnels lorsqu'il faut détenir des personnes dans le cadre de responsabilités fonctionnelles; elle n'est pas obligatoire pour tous les ministères et organismes du gouvernement du Canada. Les ministères et organismes susceptibles d'utiliser ces locaux sont notamment la GRC, l'Agence des services frontaliers du Canada (ASFC), le ministère des Pêches et des Océans (MPO) et le Service correctionnel du Canada (SCC).

La présente annexe n'a pas pour but de remplacer une législation formelle pour la création d'une zone de détention; il s'agit simplement d'une orientation sur l'emplacement d'une zone de détention au sein d'une installation. Des procédures normales d'exploitation (PNE) doivent être élaborées pour régir l'utilisation de ce type de local, et il est recommandé de procéder à une EMR avant l'ajout d'un local de détention dans une installation du GC.

LOCAL DE DÉTENTION	
Définition	Espace ou un groupe d'espaces conçut avec des barrières physiques pour contrôler et restreindre l'accès et la sortie et contenant des contrôles supplémentaires pour assurer des fonctions de surveillance et réduire la possibilité d'automutilation et de violence. L'objectif d'un local de détention est d'empêcher les personnes de s'échapper, de se blesser ou de blesser d'autres personnes, ou d'empêcher la subornation de témoins.
Exemples	Zone où les personnes sont détenues jusqu'à leur transfert dans un autre établissement du GC.
Périmètre	Il doit être délimité au moyen d'un périmètre construit selon les caractéristiques techniques recommandées dans l'EMR.
Surveillance	Surveillance continue**, c'est-à-dire jour et nuit, sept jours par semaine, avec consignation détaillée des données d'accès, qui seront vérifiées par la suite.

3. Considérations relatives à la conception d'un local de détention

3.1. Zone de transfert

Il s'agit d'une zone qui permet de passer d'un ZA à un ZT. Il peut s'agir d'une baie sécurisée

ou d'un couloir de patrouille. Elle est séparée par une barrière physique bien définie qui a été conçue, construite et aménagée conformément aux exigences spécifiques du site approuvées par le ministère. Elle restreint l'accès au seul personnel autorisé et contrôle les mouvements de manière à limiter les risques de violence et de contrebande.

3.2. Zone de soutien

Il s'agit d'une zone séparée par une barrière physique bien définie qui a été conçue, construite et aménagée conformément aux exigences spécifiques du site approuvées par le ministère. Elle contrôle l'accès, le limitant au seul personnel autorisé. Il peut s'agir, par exemple, d'une zone réservée au personnel, d'un local technique ou d'un local de stockage.

3.3. Zone de traitement

Il s'agit d'une zone séparée par une barrière physique bien définie qui a été conçue, construite et aménagée conformément aux exigences spécifiques du site approuvées par le ministère. Elle restreint l'accès au seul personnel autorisé et contrôle les mouvements de manière à limiter les risques de violence et de contrebande. Cette zone pourrait comprendre des salles d'entrevue.

3.4. Zone d'attente

Il s'agit d'une zone séparée par une barrière physique bien définie qui a été conçue, construite et aménagée conformément aux exigences spécifiques du site approuvées par le ministère. Elle est surveillée conformément à la législation en vigueur et en fonction de la nécessité fonctionnelle de restreindre l'accès au seul personnel autorisé et de contrôler les mouvements de manière à limiter les risques d'automutilation, de violence et de contrebande pour les personnes détenues dans la zone. Les cellules des détenus sont un exemple de zone d'attente.

Il n'est pas nécessaire d'utiliser toutes les zones énumérées ci-dessus. Les présentes lignes directrices fournissent au ministère ou à l'organisme du CG des recommandations minimales. Les exigences réelles doivent être établies en fonction des besoins opérationnels spécifiques.

Annex C – Protection physique des salles de serveurs informatiques

1. But

La présente annexe vise à fournir des conseils en matière de sécurité matérielle liés à la protection matérielle des serveurs informatiques et des salles de serveurs. Les directives indiquées dans la présente annexe ne remplacent pas les renseignements précédents contenus dans le guide principal sur les zones de sécurité matérielle; les renseignements contenus dans la présente annexe et le guide principal doivent être utilisés en tandem.

1.1. Emplacement de la salle des serveurs

Accès aux salles de serveurs, quel que soit le niveau de classification des données traitées ou de la technologie logée dans la salle de serveurs, devrait se limiter aux personnes qui font l'objet d'une enquête de sécurité appropriée et qui ont un besoin opérationnel d'accéder à l'espace et/ou aux visiteurs qui sont escortés de façon appropriée. Le personnel de sécurité, les techniciens en TI du gouvernement du Canada (GC) et les personnes escortées qui obtiennent un accès temporaire peuvent être des exemples de personnes qui ont un besoin opérationnel d'accéder à l'espace.

L'emplacement d'une salle de serveurs dépend du niveau de classification le plus élevé des données traitées ou stockées sur le système en réseau du serveur:
- Protégé A et Protégé B – Zone des opérations (ZT);
- Protégé C et classifié jusqu'au secret – Zone de sécurité (ZS);
- Très secret – Zone de haute sécurité (ZHS).

Il est important de noter qu'il s'agit des exigences minimales et qu'une EMR peut déterminer que la salle des serveurs est située dans une zone plus élevée que celle indiquée.

1.2. Salles de serveurs partagés

Bien que les salles de serveurs partagées entre les ministères et organismes du GC puissent être économiques, il y a d'autres considérations liées à la sécurité matérielle. Lorsque le nombre de personnes autorisées à accéder à la salle de séparation augmente, la probabilité de compromis augmente également. Pour limiter les risques, l'accès à la salle des serveurs devrait être limité aux seules personnes qui ont fait l'objet d'une vérification de sécurité appropriée et qui ont un besoin opérationnel d'accéder à l'espace et/ou aux visiteurs qui sont escortés de façon appropriée. Une EMR devrait être effectuée pour déterminer la faisabilité, ainsi que pour déterminer les mesures de protection requises pour faciliter une salle de serveurs partagée. Les ministères et organismes participants devraient coordonner les politiques et les procédures pour s'assurer que l'accès à la salle est contrôlé. Pour de plus amples renseignements, consultez GSMGC-006 (2024) - Guide de gestion de l'accès.

2. Sauvegardes

Les serveurs informatiques du GC doivent être situés dans une pièce séparée avec des mesures de contrôle d'accès comme une serrure mécanique ou un lecteur de carte électronique. L'accès à cette salle devrait être limité aux seules personnes qui ont fait l'objet d'une vérification de sécurité appropriée et qui ont besoin d'y accéder pour des raisons opérationnelles. La pièce doit être construite avec des murs qui s'étendent de la dalle de plancher à la face inférieure de la dalle de plancher / toit au-dessus. Les pièces dont les murs s'étendent sur le dessous d'un plafond suspendu ne répondraient pas aux exigences d'une salle de serveurs. Une gestion et un stockage appropriés des clés sont nécessaires pour toutes les clés physiques ou les cartes d'accès électroniques.

2.1. Protection des serveurs dans une salle de serveurs partagée

Les serveurs peuvent être considérés comme « verrouillés » lorsqu'une protection matérielle est fournie à l'unité serveur elle-même. Cela peut être fait en utilisant un verrou de couvercle sécurisé (pour éviter toute intrusion physique dans le serveur), des verrous de lecteur sécurisés (pour empêcher l'accès à tous les lecteurs), des dispositifs conçus pour verrouiller les sources possibles d'entrée / sortie (tels que les ports USB et série, les interfaces réseau et les ports ps/2), et des coussins d'ancrage ou des câbles pour fixer le serveur au rack/à la table où il se trouve (pour empêcher le retrait du serveur).

Les serveurs peuvent également être considérés comme verrouillés lorsqu'ils sont placés dans une zone fermée à clé dans une salle de serveurs. Les cages verrouillables peuvent intégrer des dispositifs de contrôle d'accès et de détection d'intrusion séparés en plus de ceux installés pour l'accès à la salle des serveurs. D'autres mesures de contrôle d'accès peuvent être utilisées conjointement pour assurer une surveillance suffisante de l'accès, tel que déterminé par une EMR. Les serveurs peuvent également être considérés comme verrouillés lorsqu'ils sont situés dans un conteneur répertorié dans le Guide d'équipement de sécurité.

2.2. Salle des serveurs sécurisée

Aux fins de la présente annexe, une « salle de serveurs sécurisée » désigne une pièce dans laquelle les murs, la porte et la quincaillerie sont construits de façon semblable aux spécifications d'une salle d'entreposage sécurisée, comme indiqué dans le document G13-01 Pièces d'entreposage sécuritaire (SSR) tout en tenant compte des exigences propres à la conception et à la construction de la salle de sectionnement (comme l'électricité supplémentaire, les évents et les conduits, et la climatisation), ainsi que des menaces pour le serveur, tels que déterminés dans une EMR.

L'accès à cette salle devrait être limité au personnel essentiel qui fait l'objet d'une vérification de sécurité appropriée et qui a un besoin opérationnel d'y accéder, et/ou aux visiteurs dûment escortés. La salle des serveurs sécurisée devrait être surveillée en permanence à l'aide d'un système électronique de détection des intrusions pour assurer le contrôle de l'accès. Des mesures supplémentaires de contrôle d'accès peuvent être mises en

œuvre si une EMR le détermine.

2.3. Centre de données sécurisé

Une salle de serveurs peut être considérée comme un centre de données sécurisé lorsqu'elle est surveillée en permanence par le personnel occupant une salle de contrôle avec une fenêtre ou un mur vitré entre ces emplacements. Le vitrage doit permettre l'observation des serveurs. Toute zone considérée hors de vue par le personnel doit être surveillée en permanence par des caméras de vidéosurveillance. La disposition devrait permettre l'observation de toute personne entrant dans la salle, y compris la surveillance de toute zone d'inscription et de présentation d'une pièce d'identité pour le personnel autorisé.

Le périmètre d'un centre de données sécurisé devrait respecter les normes de construction d'un mur de déminage sécurisé (SDW) décrites dans le document G13-02 Mur mitoyen sécuritaire. La salle de surveillance doit être occupée pendant les heures où l'accès aux serveurs est autorisé. Lorsque 24/7 est indiqué, la salle de contrôle doit être occupée en continu. Une EMR déterminera s'il y a un besoin pour un centre de données sécurisé et toute mesure supplémentaire comme l'occupation continue de la salle de contrôle.

9. Promulgation

Examiné et recommandé aux fins d'approbation

J'ai examiné le document GSMGC-015 (2024) – Guide pour l'établissement des zones de sécurité matérielle, et j'en recommande l'approbation.

Whalen,Lucus Dwyer,000356990

Digitally signed by Whalen,Lucus Dwyer,000356990
Date: 2024.09.23 09:46:07 -04'00'

Lucus Whalen — Date
Gestionnaire intérimaire
GRC, Principal organisme responsable de la sécurité

Approuvé

J'approuve le document GSMGC-015 (2024) – Guide pour l'établissement des zones de sécurité matérielle.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.10.07 11:15:55 -04'00'

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