Considérations relatives à la sécurité matérielle dans les espaces partagés

GSMGC-023 (2025)

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

Date de publication : 2025-10-20
Date de mise à jour : YYYY-MM-DD

Avant-propos

Considérations relatives à la sécurité matérielle dans les espaces partagés 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).

Il s'agit d'une publication du gouvernement du Canada (GC) qui sert de guide pour les lieux de travail partagés du GC. Elle traite des facteurs de sécurité matérielle à prendre en compte dans ces espaces et peut être utilisée par les fournisseurs d'espaces partagés, les gestionnaires d'installations et tous les utilisateurs de ces espaces de travail du GC.

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-023 (2025) – Considérations relatives à la sécurité matérielle dans les espaces partagés est 2025-10-20

Remerciements

La POSM de la GRC tient à exprimer sa gratitude à la National Protective Security Authority (NPSA) du Royaume-Uni, dont les recherches ont grandement contribué à l'élaboration du présent document. Les ouvrages SHARED WORKSPACES-Security Guidance for Users (en anglais seulement) et SHARED WORKSPACES-Security Guidance for Providers (en anglais seulement) ont fourni une base précieuse pour comprendre la complexité et la dynamique des espaces de travail partagés. Leur expertise et leurs conclusions publiées ont joué un rôle déterminant dans l'élaboration de l'analyse et des conclusions présentées dans le présent document.

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.

Contenu

1. Introduction

La GRC, en tant qu'organisme responsable de la sécurité matérielle du gouvernement du Canada (GC), est chargée de fournir des conseils et des orientations sur toutes les questions liées à la sécurité matérielle.

1.1. But

Le présent guide a pour objectif d'informer les ministères et organismes qui commencent à utiliser des espaces partagés des problèmes liés à la sécurité matérielle et des solutions qui s'y rapportent. Il traite de l'application et de l'efficacité de ces solutions du point de vue des fournisseurs et des utilisateurs. Le respect de ces mesures de base contribuera à protéger les espaces partagés et à réduire au minimum les risques pour le personnel, l'information et les biens du GC.

1.2. Applicabilité

Ce guide s'applique aux fournisseurs d'espaces partagés du GC, aux spécialistes de la sécurité chargées de la sécurité matérielle dans les espaces partagés, aux gestionnaires d'installations ou de biens immobiliers du GC et à tous les utilisateurs d'espaces partagés. Cela inclut le personnel chargé de la gestion immobilière et les décideurs ayant une autorité en matière de gestion ou d'acceptation des risques au sein du ministère ou de l'organisme utilisant les options d'espaces partagés.

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

Tous les employés du 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 matérielle 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
CCTV	Systèmes de surveillance vidéo. Interchangeable avec CCVE
CST	Centre de la sécurité des télécommunications Canada
DPS	Dirigeant principal de la sécurité
DGS	Directive sur la gestion de la sécurité
EDI	Équité, diversité et inclusion
DEI	Dispositifs électroniques d'intrusion
GC	Gouvernement du Canada
GRC	Gendarmerie royale du Canada
GRC POSM	Gendarmerie royale du Canada Principal organisme responsable de la sécurité
PCAM	Prévention du crime par l'aménagement du milieu
PSG	Politique sur la sécurité du gouvernement
SPC	Services partagés Canada
ZA	Zone d'accueil

ZHS	Zone de haute sécurité
ZS	Zone de sécurité
ZT	Zone de travail

4. Glossaire

Terme	Définition
Actif	Actifs corporels ou incorporels du gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public et à la réputation internationale.
Compromission	Divulgation, destruction, suppression, modification, interruption d'accès ou utilisation de renseignements ou de biens non autorisée.
Défense en profondeur	C'est le principe selon lequel les zones de sécurité sont mises en œuvre de manière progressivement restrictive, allant de la zone la moins restrictive à la plus restrictive.
Installation	Une installation peut être un bâtiment (en tout ou en partie) et peut comprendre son site ou son terrain, ou peut-être une zone ou une construction qui n'est pas un bâtiment (par exemple, champs de tir, champs agricoles).
Menace interne	Cas où le personnel autorisé à entrer ou à travailler dans une installation du GC prend délibérément des mesures contre le GC, son employeur ou ses collègues. Les actions peuvent inclure l'activité criminelle, les menaces ou actions physiques, l'espionnage, la subversion et le sabotage.
Atténuation	Mesures prises pour réduire les risques.
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.
Fournisseur	Un fournisseur est un terme général désignant une entité qui possède, opère ou gère une installation pour le compte d'autres parties. Il peut s'agir de Services publics et Approvisionnement Canada (SPAC) ou d'un autre bailleur.
Sauvegarde	Les actifs ou les contrôles externes qui réduisent le risque global pour les employés, les autres actifs ou la prestation de services en

	diminuant la probabilité d'un événement menaçant, réduisant la probabilité de compromission ou en atténuant la gravité du résultat par une interaction directe ou indirecte avec la valeur des actifs, les menaces ou les vulnérabilités.
Utilisateur	Un utilisateur est toute personne, tout groupe, tout service ou toute agence qui utilise un espace à des fins autorisées. Les utilisateurs peuvent être des employés, des visiteurs, des sous-traitants ou toute autre personne autorisée à utiliser l'espace.
Vulnérabilité	Insuffisance liée à la sécurité qui pourrait accroître la susceptibilité à la compromission ou au préjudice

5. Conseils de sécurité pour les fournisseurs d'espaces partagés

Les espaces partagés offrent des environnements innovants et flexibles permettant aux individus et aux organisations de collaborer, d'innover et de se développer. Les espaces partagés s'adressent à un large éventail d'utilisateurs, leur permettant de réaliser des économies grâce au partage des ressources et à la promotion de la collaboration. Ces environnements dynamiques présentent également des défis uniques en matière de sécurité matérielle, les informations sensibles, la propriété intellectuelle et les équipements étant souvent exposés à des risques de vol, d'accès non autorisé ou d'exposition accidentelle.

Les fournisseurs d'espaces de travail jouent un rôle essentiel dans la mise en place des fondements de la sécurité au sein de ces espaces. En mettant en œuvre des mesures de sécurité appropriées, vous protégez non seulement vos utilisateurs, leurs biens et leur vie privée, mais vous préservez également vos installations, vos actifs et votre réputation. Des pratiques de sécurité efficaces renforcent la confiance des utilisateurs, favorisent le respect des exigences en matière de sécurité et créent un environnement propice à l'innovation.

Dans les espaces partagés, il est impératif de prendre en compte la sécurité dès le début. Les stratégies de conception, de modernisation et d'entretien des installations qui répondent aux divers besoins des utilisateurs doivent faire partie intégrante du processus global. En comprenant les risques spécifiques associés aux espaces de travail partagés et en appliquant les contrôles appropriés, les fournisseurs peuvent garantir la sécurité et la collaboration recherchées par les utilisateurs des espaces partagés.

5.1. Comprendre les menaces et les risques auxquels sont exposés les utilisateurs

Les espaces partagés peuvent constituer des cibles attrayantes pour ceux qui cherchent à obtenir un accès non autorisé à des informations, des actifs ou des systèmes sensibles. Les mêmes environnements ouverts et collaboratifs qui les rendent attrayants pour les utilisateurs peuvent également permettre à des personnes mal intentionnées d'obtenir, ou

de sembler avoir, un accès légitime aux informations et aux actifs de vos utilisateurs. En tant que fournisseur d'espaces partagés, il est essentiel de comprendre les menaces, les risques et les vulnérabilités, ainsi que la manière dont les adversaires peuvent les exploiter, afin de protéger le GC.

- **Acteurs étatiques :** Les acteurs étatiques peuvent cibler les utilisateurs travaillant sur des projets ou des recherches sensibles. Ils exploitent les vulnérabilités pour accéder aux données des utilisateurs, ce qui nuit à la réputation et à l'intégrité des informations et des actifs de GC;
- **Concurrents** : Les concurrents peuvent utiliser les espaces partagés pour recueillir des informations sur les utilisateurs ou les opérations. Ils pourraient se faire passer pour des utilisateurs légitimes, sapant ainsi la confiance des utilisateurs et la réputation du ministère ou de l'organisme;
- **Cybercriminels :** Bien que cela ne soit pas l'objet principal de ces recommandations, les cybercriminels exploitent les systèmes numériques tels que le Wi-Fi ou les contrôles d'accès. Les violations perturbent les services, exposent les données et endommagent les infrastructures, entraînant des temps d'arrêt et nuisant à la réputation;
- **Criminels opportunistes :** Les criminels opportunistes exploitent les opportunités qui se présentent dans les espaces partagés, en ciblant notamment les appareils, les informations, les biens ou les personnes laissés sans surveillance. Ils peuvent chercher à y accéder par des moyens légitimes et, une fois à l'intérieur, profiter des environnements ouverts pour identifier les cibles vulnérables;
- **Risque interne :** Une personne disposant d'un accès autorisé ou d'une connaissance approfondie d'une organisation qui cause un préjudice à cette dernière, de manière intentionnelle ou non, porte atteinte à l'intégrité, à la confidentialité et à la disponibilité de l'organisation, de ses données, de son personnel ou de ses installations par le biais d'espionnage, de terrorisme, de divulgation non autorisée d'informations, de crimes, de sabotage ou de violence ; et
- **Manifestants :** Les manifestants peuvent cibler les espaces partagés en les perturbant ou en les vandalisant. Cela peut être motivé par des problèmes liés aux activités commerciales ou aux chaînes d'approvisionnement des utilisateurs. Leurs actions nuisent à la réputation et ont un impact sur la productivité.

Remarque : N'importe lequel de ces acteurs malveillants pourrait se présenter comme un utilisateur légitime de l'espace de travail partagé, un visiteur ou un sous-traitant.

5.2. Mesures de sécurité matérielle appropriées

Il est entendu que les espaces partagés visent à être des environnements qui maximisent la collaboration et l'économie d'espace. Cela n'est toutefois possible que si les risques liés à la sécurité sont gérés de manière appropriée. La situation se complique lorsque l'on tient compte des besoins variés des ministères et des organismes qui utilisent l'espace à des fins diverses et qui travaillent avec différents niveaux de sensibilité.

Même dans les espaces partagés, les besoins en matière d'espace varient. Le zonage reste nécessaire en fonction de la catégorisation des informations traitées ou stockées, mais la plupart des espaces partagés seront considérés comme des environnements de zone opérationnelle.

Il peut également être nécessaire d'offrir des « quartiers » aux ministères et organismes qui doivent être proches les uns des autres dans un espace partagé. Le recours au modèle des « quartiers » peut également être avantageux pour les ministères et organismes afin de respecter les principes de protection des informations et des actifs selon lesquels seuls ceux qui ont besoin de savoir ou d'accéder à ces informations peuvent le faire. Cela peut être utile à des fins de collaboration ou de sécurité de l'information. Dans certains cas, il peut également être nécessaire de créer des zones de sécurité pour travailler sur des informations classées à des niveaux plus élevés. Des espaces privés peuvent également être nécessaires pour mener des conversations plus sensibles, afin d'éviter qu'elles ne soient entendues par des personnes non autorisées ou simplement pour le confort des personnes qui travaillent dans cet espace.

Les mesures de sécurité matérielle et autres recommandées pour les zones opérationnelles dans les espaces partagés se concentrent principal fermement sur la sensibilisation et les dispositions de base, tandis que celles qui concernent les zones de sécurité ou les espaces privés couvrent des contrôles de sécurité et des pratiques de gestion plus avancées. Il est important de rappeler qu'un fournisseur d'espace doit offrir les exigences minimales de sécurité en fonction des zones requises dans l'espace partagé.

5.3. Filtrage de sécurité

Comme pour toute installation ou propriété du GC, il est obligatoire de s'assurer que l'accès n'est accordé qu'aux personnes disposant du cote ou d'autorisation de sécurité approprié. Il incombera conjointement au fournisseur et à l'utilisateur ou aux utilisateurs de s'assurer que toutes les personnes autorisées à accéder à l'espace partagé ont fait l'objet d'un contrôle de sécurité approprié et disposent du cote ou d'autorisation de sécurité requis.

5.4. Types d'espaces

Les exigences en matière de sécurité matérielle pour les zones de travail et les zones de sécurité sont détaillées dans le document GSMGC-015 – Guide pour l'établissement des zones de sécurité matérielle. Les zones de sécurité matérielle dans les espaces partagés doivent être créées et gérées selon les mêmes directives que celles applicables aux espaces réservés à un seul service et, en réalité, elles nécessitent un contrôle et une gestion accrus afin de garantir la sécurité des informations, des actifs et des personnes du GC. Outre les directives ci-dessus, les zones de sécurité matérielle dans les espaces partagés peuvent inclure :

- **Zone de travail :** Les zones de travail (ZT) sont conçues pour la collaboration, le partage d'équipements et les espaces communs. Les fournisseurs doivent donner la priorité à l'accessibilité et à la sécurité de base pour divers utilisateurs tout en

respectant les exigences physiques et autres exigences de sécurité des ZT;

- **Zone de sécurité :** Les zones de sécurité (ZS) sont destinées aux utilisateurs qui traitent des informations sensibles, pour lesquelles la sécurité est une priorité. Ces espaces exigent des fournisseurs qu'ils mettent en œuvre des mesures de sécurité renforcées, conformes aux directives et aux meilleures pratiques de la GRC;
- **Zone de haute sécurité :** Les zones de haute sécurité (ZHS) font partie des espaces les plus sécurisés et doivent être traitées comme telles, malgré la nécessité de disposer d'espaces diversifiés et partagés. Elles seront rares, mais toutes les mesures de sécurité matérielle et autres doivent être prises en compte avant de mettre en service un tel espace dans une installation partagée;
    - **Espaces privés :** Les espaces privés tels que les bureaux privés, les salles de conférence ou les salles de repos aménagés dans l'une des zones susmentionnées offrent aux utilisateurs un meilleur contrôle sur leur environnement, leur permettant ainsi de bénéficier d'une sécurité et d'une confidentialité plus personnalisées. Ces espaces sont généralement utilisés par des personnes ou de petites équipes qui ont besoin d'un espace de travail dédié, à l'écart des autres utilisateurs, pour se concentrer ou mener des discussions sensibles, où la nécessité de respecter la confidentialité au sein de l'espace partagé doit être prise en compte.

5.5. Culture de sécurité dans un espace partagé

Pour les fournisseurs d'espaces partagés, favoriser une culture de sécurité forte fait non seulement partie de leur devoir de diligence envers les utilisateurs, mais constitue également un facteur clé pour attirer et fidéliser les clients. En promouvant une culture proactive et soucieuse de la sécurité, les fournisseurs peuvent instaurer la confiance, renforcer leur réputation et mieux accompagner leurs utilisateurs à mesure que leurs besoins en matière de sécurité évoluent.

La nomination d'un comité de sécurité des espaces partagés est une étape importante dans la mise en place d'une culture de sécurité solide. Parmi les autres facteurs favorisant une culture de sécurité solide, on peut citer :

- **Sensibilisation à la sécurité et signalement :** Mettre l'accent sur la sensibilisation à la sécurité encourage les utilisateurs à signaler les comportements suspects. Cela peut se faire grâce à un personnel accessible, à des messages et à une signalisation. Cela favorise l'adoption de politiques de sécurité et de procédures de signalement et permet de recueillir en permanence les commentaires des utilisateurs afin d'améliorer la sécurité des espaces communs;
- **Collaboration et responsabilité :** La collaboration lors de la mise en œuvre des politiques et procédures de sécurité garantit que les besoins du GC et des utilisateurs sont satisfaits. Organisez régulièrement des séances avec les utilisateurs afin d'examiner et de traiter les problèmes de sécurité actuels ou émergents. Offrez aux utilisateurs une formation sur l'utilisation et la sécurité de tous les espaces communs et sur la manière de gérer efficacement les visiteurs; et

- **Conformité et confiance :** Encouragez la communication entre tous les utilisateurs des espaces partagés afin de garantir le respect des exigences en matière de sécurité. Affectez du personnel dédié aux espaces partagés afin d'assurer une communication rapide et efficace sur les besoins liés à la sécurité. Instaurez un climat de confiance en démontrant une application cohérente des politiques et pratiques de sécurité, telles que les procédures de contrôle d'accès et de gestion des visiteurs.

5.6. Conception et aménagement des espaces partagés

Lors de la conception d'espaces partagés, les fournisseurs doivent prendre en compte les mesures de sécurité dès le départ et utiliser à cette fin le processus SA&A. Une approche intégrée et holistique de la sécurité à ce stade du processus favorise la flexibilité des opérations et l'évolutivité des contrôles de sécurité.

Tenez compte des besoins des utilisateurs et des directives de la GRC pour déterminer les mesures de contrôle de sécurité les plus appropriées lors de la conception d'un espace partagé. Définissez les exigences en matière de zonage de l'espace, mettez en œuvre toutes les exigences de sécurité matérielle de ces zones et déterminez les points de contrôle d'accès nécessaires entre les zones. Il peut également être utile d'examiner si la séparation des quartiers est nécessaire et quels contrôles de sécurité pourraient être requis dans ces cas.

Déterminez les systèmes de sécurité requis par chaque utilisateur et essayez de trouver des points communs dans l'application de ces systèmes. À ce stade, il serait également utile de déterminer si des utilisateurs auront accès à ces systèmes, lesquels et quel sera leur niveau d'accès (observateur ou administrateur). Veillez à concevoir et à installer des systèmes de sécurité appropriés en tenant compte des besoins de tous les utilisateurs en matière de performance et d'adaptabilité/évolutivité. Installez des systèmes de surveillance vidéo (CCTV), de contrôle d'accès et de détection d'intrusion qui peuvent être mis à niveau ou adaptés pour répondre à l'évolution des besoins des utilisateurs. Assurez-vous que tous les systèmes de sécurité répondent aux exigences de sécurité du GC et aux directives de la GRC.

Si vous concevez des bâtiments autonomes comme espaces partagés, pensez à mettre en place une surveillance naturelle. Les principes de prévention du crime par l'aménagement du milieu (PCAM) favorisent la sécurité en offrant une bonne visibilité, en délimitant clairement les zones publiques et les zones contrôlées, en utilisant l'éclairage pour créer des conditions propices à la sûreté et à la sécurité, et en mettant en place des routines de nettoyage et d'entretien pour montrer que l'espace est bien entretenu.

5.7. Problèmes de confidentialité dans les espaces partagés

Garantir la confidentialité des utilisateurs est une attente fondamentale pour les fournisseurs d'espaces partagés. En adaptant les mesures de confidentialité au zonage de sécurité et à d'autres exigences, les fournisseurs peuvent trouver un équilibre entre la sécurité et la collaboration souhaitée par les utilisateurs.

Zones de travail : Dans les ZT, prévoyez des salles de réunion ou des salles calmes pouvant être réservées afin de préserver la vie privée des utilisateurs. Installez des écrans dans les espaces communs tels que les cuisines ou les espaces de pause afin d'offrir un minimum d'intimité aux utilisateurs. Rappelez régulièrement aux utilisateurs d'utiliser les espaces privés pour les discussions sensibles ou bruyantes et de mettre leurs effets personnels en sécurité lorsqu'ils se trouvent dans les espaces communs. Veillez à mettre en place des canaux de communication clairs permettant aux utilisateurs de signaler tout problème lié à la vie privée et prenez des mesures pour y remédier rapidement.

Espaces privés : Permettez aux utilisateurs de personnaliser leurs espaces grâce à des mesures de confidentialité telles que des stores ou des conteneurs de sécurité départementaux. Installez des stores ou des films de confidentialité sur les cloisons vitrées et les fenêtres, proposez des espaces de rangement sécurisés et verrouillables pour les effets personnels des utilisateurs et fournissez des déchiqueteuses ou des services de destruction. Accompagnez les tiers et les sous-traitants qui effectuent des travaux pour votre compte lorsqu'ils ont besoin d'accéder à l'espace privé d'un utilisateur. Discutez avec les utilisateurs afin d'identifier leurs besoins en matière de confidentialité lors de leur intégration et répondez à leurs demandes de personnalisation dans la mesure du possible. Intégrez les exigences des utilisateurs en matière de confidentialité, telles que des cloisons en verre plein ou dépoli ou des protections acoustiques, dans les contrats de service, et revoyez-les et mettez-les à jour régulièrement.

Zones de sécurité : Répondez aux besoins spécifiques des utilisateurs en matière de confidentialité en fournissant toutes les exigences de sécurité dans un ZS. Fournissez des serrures de haute sécurité conformément aux directives de la GRC et un contrôle d'accès qui permet aux utilisateurs d'avoir un registre vérifiable des personnes qui ont accédé à leurs espaces. Fournissez des espaces acoustiques si nécessaire, en tenant compte des directives de la GRC, et escortez les tiers et les entrepreneurs lorsqu'ils effectuent des travaux pour votre compte, en particulier lorsqu'ils doivent accéder à des ZS. Soutenez les utilisateurs en leur fournissant des directives claires sur les protocoles d'accompagnement et en leur fournissant les ressources nécessaires, telles que des laissez-passer temporaires pour les visiteurs ou des points d'accès surveillés. Procédez à des examens réguliers des mesures de sécurité et veillez au respect des processus et procédures convenus.

5.8. Systèmes de sécurité matérielle dans les espaces partagés

Un environnement sécurisé aide les utilisateurs à travailler en toute confiance, quel que soit l'espace. Les fournisseurs doivent mettre en œuvre des mesures visant à dissuader et à empêcher les accès non autorisés, à surveiller l'activité et à réagir aux incidents.

	Zones de travail	Espaces privés	Zones de sécurité
Critères des systèmes	Veillez à ce que tous les points d'entrée/sortie de l'espace de travail et toutes les autres zones à haut risque soient couverts par CCTV.	Offrez aux utilisateurs la possibilité d'introduire des mesures de sécurité supplémentaires telles que des verrous départementaux ou des conteneurs de sécurité dans les zones privées.	Fournir des technologies améliorées telles que l'accès biométrique et la détection d'intrusion.
Améliorations	Installez des barrières de contrôle d'accès qui empêchent le talonnage. Assurez-vous qu'il existe un contrôle d'accès progressif entre les zones et les quartiers au sein de l'espace.	Installez des systèmes de contrôle d'accès, tels que des serrures et des lecteurs de cartes, dans les bureaux et les pièces privés.	Installez des systèmes de contrôle d'accès améliorés pour les espaces spécifiques, les zones critiques ou les pièces, complétés par une surveillance CCTV supplémentaire. Assurez la séparation lorsque cela est nécessaire.
Comportements	Former le personnel à surveiller les espaces communs et à identifier et signaler toute activité suspecte.	Inspectez régulièrement tous les dispositifs du système de sécurité matérielle et traitez rapidement tout problème signalé par les utilisateurs.	Mettre en place des protocoles de sécurité supplémentaires, tels que l'entrée supervisée pour le personnel tiers.
Gouvernance	Mettre en place et maintenir un processus permettant de réviser et de mettre à jour régulièrement les systèmes de sécurité matérielle en fonction des commentaires des utilisateurs.		Veiller au respect des exigences de sécurité afin d'identifier les modèles d'accès suspects et de garantir que les exigences spécifiques des utilisateurs sont satisfaites.

5.9. Gestion de l'accès et contrôle des visiteurs

Certains espaces partagés ont délibérément assoupli leurs politiques d'accès. Cependant, il est important de trouver le juste équilibre entre l'ouverture et la prévention des accès non autorisés. Il est important que vous fournissiez un espace qui gère bien les accès afin d'atténuer efficacement les risques et d'offrir aux utilisateurs la tranquillité d'esprit qu'ils souhaitent. Pour connaître toutes les exigences en matière de contrôle d'accès, consultez les directives de la POSM sur le contrôle d'accès. Toutefois, certaines considérations sont énumérées dans le tableau ci-dessous.

	Zones de travail	Espaces privés	Zones de sécurité
Critères des systèmes	Choisissez des systèmes de gestion des visiteurs adaptés à vos périodes les plus chargées et formez le personnel d'accueil à leur utilisation.	Fournir aux utilisateurs des systèmes d'accès personnalisables et des protocoles clairs d'enregistrement des visiteurs.	Prise en charge de systèmes avancés de préapprobation des visiteurs et intégration de solutions de vérification d'identité.
Améliorations	Fournir des services d'accueil en plus des systèmes de sécurité matérielle.	Déployez des identifiants de contrôle d'accès pour des espaces spécifiques.	Utilisez des contrôles d'accès appropriés pour les zones critiques afin d'empêcher toute entrée non autorisée.
Pratiques opérationnelles	Former le personnel à surveiller l'activité des visiteurs et à reconnaître et signaler les comportements suspects.	Veiller à ce que les politiques relatives aux visiteurs sur le lieu de travail soient respectées, notamment en accompagnant et en enregistrant les invités.	Veiller à ce que les visiteurs soient soumis à un contrôle préalable et accompagnés à tout moment après leur entrée dans les zones de sécurité.
Gouvernance	Veiller à ce que les registres des visiteurs soient conservés en toute sécurité et pendant une période définie, et résoudre les problèmes liés à l'accès de manière transparente.	Vérifiez régulièrement les journaux d'accès aux espaces utilisateurs et traitez rapidement les cas de non-conformité.	Veiller au respect des conditions d'accès aux ZS, faire respecter les règles par les utilisateurs et traiter rapidement les cas de non-conformité identifiés.

5.10. Sécurité opérationnelle et gestion des incidents

La sécurité opérationnelle et la gestion des incidents concernent le rôle que jouent les personnes, les politiques et les procédures dans le fonctionnement quotidien d'un espace partagé. La manière dont les problèmes de sécurité sont prévenus, traités et résolus lorsqu'ils surviennent est importante. Rassurez les utilisateurs en leur garantissant que les incidents de sécurité sont pris au sérieux et traités rapidement.

La sensibilisation aux menaces et aux risques est importante et permet d'identifier les risques potentiels dans les ZT, tels que le vol ou l'utilisation abusive des ressources partagées, d'aider les utilisateurs à mettre en place des pratiques d'évaluation des risques pour les espaces privés et d'évaluer les ZS pour les menaces ciblées, telles que l'espionnage ou le sabotage.

Les fournisseurs doivent élaborer une série de procédures de base en matière de gestion des urgences que le personnel devra suivre en cas d'incident sur le lieu de travail ou à proximité. La collaboration avec les utilisateurs pour définir des plans d'urgence spécifiques à chaque espace favorise l'alignement sur les besoins de l'ensemble de l'espace. La mise en œuvre de

plans d'urgence sur mesure, comprenant des itinéraires d'évacuation sécurisés et des dispositifs de verrouillage, garantit la protection continue des zones de sécurité qui protègent les informations et les actifs de GC.

Fournir un point de contact centralisé pour signaler les incidents de sécurité ou les activités suspectes et veiller à ce que tous les utilisateurs sachent quand, comment et à qui signaler ces incidents. Veiller à ce que des mesures de confinement rapides soient prises en cas d'incidents impliquant des informations sensibles, en coordination directe avec les utilisateurs concernés et, si nécessaire, avec les forces de l'ordre. Les départements doivent se référer aux procédures obligatoires pour la gestion des incidents de sécurité figurant à l'annexe G de la directive sur la gestion de la sécurité.

Les enseignements tirés des incidents constituent une partie importante du processus. Tenez un registre des incidents et examinez les tendances afin d'améliorer en permanence les contrôles de sécurité. Examinez régulièrement les commentaires des utilisateurs et analysez en détail tous les incidents afin d'améliorer la sécurité globale. Organisez des réunions après les incidents afin d'identifier les enseignements à en tirer et collaborez avec les utilisateurs pour renforcer la sécurité.

5.11. Cybersécurité

Comme mentionné précédemment, ces directives ne sont pas spécifiques à la cybersécurité et toute préoccupation particulière dans ce domaine doit être traitée par le Centre de la sécurité des télécommunications (CST) ou Services partagés Canada (SPC). La sécurité des systèmes informatiques dans les espaces partagés exige que les fournisseurs jouent un rôle proactif. Les cyberattaques peuvent prendre de nombreuses formes, mais la grande majorité d'entre elles peuvent être atténuées par la mise en œuvre de quelques contrôles essentiels. Il est important de s'assurer que toutes les mesures de cybersécurité sont en place et de mener des audits pour vérifier leur efficacité.

Les fournisseurs jouent un rôle essentiel dans l'aide apportée aux utilisateurs pour protéger l'infrastructure numérique et minimiser l'impact des cyberincidents. Les fournisseurs sont encouragés à partager avec les utilisateurs des conseils pour rester en sécurité en ligne, notamment des recommandations que tous les utilisateurs devraient suivre pour rester en sécurité en ligne et protéger leurs appareils.

6. Consignes de sécurité pour les utilisateurs

Les espaces de travail partagés offrent des solutions flexibles et rentables pour les particuliers et les organisations. Ces environnements sont conçus pour favoriser la créativité, la collaboration et l'évolutivité. Ils s'adressent à un large éventail d'utilisateurs en offrant des ressources partagées et en encourageant les partenariats.

Les espaces de travail partagés posent également des défis uniques en matière de sécurité, que vous partagiez des espaces de travail dans une zone de coworking, traitiez des informations sensibles, utilisiez des équipements sensibles ou essayiez simplement d'avoir une conversation dans la zone partagée. Ces espaces peuvent être vulnérables à des accès non autorisés ou à la divulgation accidentelle d'informations, ce qui présente différents risques pour la sécurité.

Cette section s'adresse aux utilisateurs d'espaces de travail partagés et fournit des conseils pour vous aider à protéger vos informations et vos actifs. En comprenant les espaces et les environnements, vous pouvez identifier les mesures les plus pertinentes pour votre situation. En comprenant les menaces et les risques, puis en appliquant les mesures appropriées, vous pouvez profiter pleinement des avantages des espaces partagés tout en protégeant vos informations, vos actifs et les autres utilisateurs de l'espace.

6.1. Qui vous expose à un risque

Les espaces partagés peuvent constituer des cibles faciles pour les acteurs malveillants qui cherchent à accéder sans autorisation à des informations et des actifs sensibles. L'environnement ouvert et collaboratif qui les rend populaires les rend également faciles d'accès pour toute personne mal intentionnée. En tant qu'utilisateur d'un espace partagé, il est important que vous compreniez les principaux acteurs malveillants qui pourraient chercher à exploiter ces vulnérabilités pour accéder aux informations et aux actifs de GC.

- **Acteurs étatiques :** Les acteurs étatiques peuvent cibler les utilisateurs travaillant sur des projets ou des recherches sensibles. Ils exploitent les vulnérabilités pour accéder aux données des utilisateurs, ce qui nuit à la réputation et à l'intégrité des informations et des actifs de GC;
- **Concurrents :** Les concurrents peuvent utiliser les espaces partagés pour recueillir des informations sur les utilisateurs ou les opérations. Ils pourraient se faire passer pour des utilisateurs légitimes, sapant ainsi la confiance des utilisateurs et la réputation du ministère ou de l'organisme;
- **Cybercriminels :** Bien que cela ne soit pas l'objet principal de ces recommandations, les cybercriminels exploitent les systèmes numériques tels que le Wi-Fi ou les contrôles d'accès. Les violations perturbent les services, exposent les données et endommagent les infrastructures, entraînant des temps d'arrêt et nuisant à la réputation;
- **Criminels opportunistes :** Les criminels opportunistes exploitent les opportunités qui se présentent dans les espaces partagés, en ciblant notamment les appareils, les informations, les biens ou les personnes laissés sans surveillance. Ils peuvent chercher à y accéder par des moyens légitimes et, une fois à l'intérieur, profiter des environnements

ouverts pour identifier les cibles vulnérables;

- **Risque interne :** Une personne disposant d'un accès autorisé ou d'une connaissance approfondie d'une organisation qui cause un préjudice à cette dernière, de manière intentionnelle ou non, porte atteinte à l'intégrité, à la confidentialité et à la disponibilité de l'organisation, de ses données, de son personnel ou de ses installations par le biais d'espionnage, de terrorisme, de divulgation non autorisée d'informations, de crimes, de sabotage ou de violence ; et
- **Manifestants :** Les manifestants peuvent cibler les espaces partagés en les perturbant ou en les vandalisant. Cela peut être motivé par des problèmes liés aux activités commerciales ou aux chaînes d'approvisionnement des utilisateurs. Leurs actions nuisent à la réputation et ont un impact sur la productivité.

  Remarque : N'importe lequel de ces acteurs malveillants pourrait se présenter comme un utilisateur légitime de l'espace de travail partagé, un visiteur ou un sous-traitant.

6.2. Quel type d'utilisateur êtes-vous ?

Identifiez le type d'utilisateur qui correspond le mieux à votre situation particulière afin d'obtenir des conseils personnalisés sur la gestion des risques de sécurité dans les espaces partagés. Bien que ces exemples illustrent des activités et des mesures de sécurité typiques, ils ne couvrent pas toutes les situations. Reportez-vous à la section Types d'espaces pour obtenir des conseils plus détaillés en fonction du type d'espace que vous utilisez.

	Utilisateur occasionnel	**Utilisateur régulier**	**Utilisateur spécialisé**
Profil	Les travailleurs qui n'utilisent les espaces partagés qu'occasionnellement, en recourant au « hot desking » pour des raisons pratiques.	Les travailleurs qui utilisent quotidiennement des espaces partagés et ont besoin de flexibilité dans tous les espaces au sein de l'établissement.	Les travailleurs qui utilisent des ZS pour traiter et stocker en permanence des informations hautement sensibles.
Besoins en espace	Espace de travail avec accès à Internet et accès à des espaces privés pour les travaux sensibles. Accès occasionnel aux ZS.	Des espaces de travail flexibles pour le travail individuel et la collaboration en équipe. Accès à des espaces privés pour garantir la confidentialité et accès à des ressources communes telles que des salles de réunion.	Espace de travail privé avec mesures de sécurité renforcées.

Considérations	Choisissez un espace de travail qui vous donne accès aux espaces dont vous avez besoin tout en garantissant la protection des appareils et des documents dans les zones communes. Choisissez votre espace de travail en fonction de vos besoins en matière de sécurité.	Maintenir la flexibilité dans le choix du lieu de travail tout en conservant le contrôle sur l'accès à vos informations et à vos actifs. Veiller à ce que les ressources partagées en dehors des espaces privés soient utilisées de manière appropriée. Faites preuve de vigilance lorsque vous utilisez des ressources partagées ou des espaces ouverts.	Choisissez un espace qui répond aux exigences de sécurité. Tenez compte des autres utilisateurs de l'espace et de leur impact sur votre sécurité. Choisissez votre espace de travail SZ en fonction de vos besoins en matière de sécurité.

6.3. Mesures de sécurité matérielle appropriées

Il est entendu que les utilisateurs d'espaces partagés souhaitent tirer le meilleur parti des avantages offerts par ces espaces tout en gérant les risques liés à la sécurité. Il est important de noter que les utilisateurs d'espaces partagés auront besoin d'utiliser différents espaces et différentes fonctions à différents moments. Même dans les espaces partagés, les besoins en matière d'espace varient et un zonage reste nécessaire en fonction de la catégorie d'informations ou d'actifs traités ou stockés. La plupart des installations d'espaces partagés seront considérées comme des environnements ZT, mais il peut être nécessaire de pouvoir traiter ou stocker des informations ou des actifs de catégorie supérieure.

Il peut également être nécessaire de travailler dans des « quartiers » spécifiques à votre département ou agence, l'idée étant que les employés doivent être proches les uns des autres dans un espace partagé. Cela peut être dans un but de collaboration ou de sécurité des informations afin d'éviter les écoutes indiscrètes.

Les mesures de sécurité matérielle et autres recommandées pour les ZT dans les espaces partagés se concentrent principalement sur la sensibilisation et les dispositions de base, tandis que celles pour les ZS ou les espaces privés nécessitent des contrôles de sécurité et des pratiques de gestion plus avancés. Il est important de rappeler que les utilisateurs doivent respecter toutes les exigences de sécurité en fonction de la zone dans laquelle ils travaillent.

Les utilisateurs peuvent être amenés à transporter ou à transmettre des informations ou des biens vers et depuis l'espace partagé de temps à autre. Il est important de garder à l'esprit

que la sécurité des informations et des biens pendant leur transport est essentielle, en particulier dans les espaces partagés. Pour connaître les exigences en matière d'information et de sécurité lors du transport ou de la transmission d'informations et de biens, consultez le guide GSMGC-007 – Transport, transmission et entreposage de matériel protégé ou classifié.

6.4. Filtrage de sécurité

Comme pour toute installation ou propriété du GC, il est obligatoire de s'assurer que l'accès n'est accordé qu'aux personnes détenant du cote ou d'autorisation de sécurité approprié. Il incombe conjointement au fournisseur et à l'utilisateur ou aux utilisateurs de s'assurer que toutes les personnes autorisées à accéder à l'espace partagé ont fait l'objet d'un contrôle de sécurité approprié et possèdent du cote ou d'autorisation de sécurité requis. Il est également important de rappeler qu'il incombe à l'utilisateur de s'assurer que son cote ou son autorisation de sécurité reste valide et qu'il n'accède qu'aux informations et aux actifs correspondant à son niveau de classification de sécurité.

6.5. Types d'espaces

Les exigences en matière de sécurité matérielle pour les zones de travail et les zones de sécurité sont détaillées dans le document GSMGC-015 – Guide pour l'établissement des zones de sécurité matérielle. Les zones de sécurité matérielle dans les espaces partagés doivent être créées et gérées selon les mêmes directives que celles applicables aux espaces réservés à un seul service et, en réalité, elles nécessitent un contrôle et une gestion accrus afin de garantir la sécurité des informations, des actifs et des personnes du GC. Outre les directives ci-dessus, les zones de sécurité matérielle dans les espaces partagés peuvent inclure :

- **Zone de travail :** Les zones de travail (ZT) sont conçues pour la collaboration, le partage d'équipements et les espaces communs. Les fournisseurs doivent donner la priorité à l'accessibilité et à la sécurité de base pour divers utilisateurs tout en respectant les exigences physiques et autres exigences de sécurité des ZT;
- **Zone de sécurité :** Les zones de sécurité (ZS) sont destinées aux utilisateurs qui traitent des informations sensibles, pour lesquelles la sécurité est une priorité. Ces espaces exigent des fournisseurs qu'ils mettent en œuvre des mesures de sécurité renforcées, conformes aux directives et aux meilleures pratiques de la GRC;
- **Zone de haute sécurité :** Les zones de haute sécurité (ZHS) font partie des espaces les plus sécurisés et doivent être traitées comme telles, malgré la nécessité de disposer d'espaces diversifiés et partagés. Elles seront rares, mais toutes les mesures de sécurité matérielle et autres doivent être prises en compte avant de mettre en service un tel espace dans une installation partagée;
    - **Espaces privés :** Les espaces privés tels que les bureaux privés, les salles de conférence ou les salles de repos aménagés dans l'une des zones susmentionnées offrent aux utilisateurs un meilleur contrôle sur leur environnement, leur permettant ainsi de bénéficier d'une sécurité et d'une confidentialité plus personnalisées. Ces espaces sont généralement utilisés par des personnes ou de petites équipes qui ont besoin d'un espace de travail

dédié, à l'écart des autres utilisateurs, pour se concentrer ou mener des discussions sensibles, où la nécessité de respecter la confidentialité au sein de l'espace partagé doit être prise en compte.

6.6. Culture de la sécurité dans les espaces partagés

Pour les utilisateurs d'espaces partagés, le développement d'une culture de la sécurité est un processus qui évolue en fonction de votre espace de travail et de vos besoins. Que vous travailliez dans un ZT, un espace privé ou un ZS, tout commence par une prise de conscience élémentaire, qui se transforme ensuite en pratiques plus solides. La sécurité est une responsabilité partagée entre toutes les parties qui utilisent un espace partagé. Les utilisateurs qui participent à un comité de sécurité des espaces partagés contribuent à rapprocher les fournisseurs et les utilisateurs afin de renforcer la culture de la sécurité. Parmi les autres facteurs favorisant le développement d'une culture de la sécurité solide, on peut citer :

- **Sensibilisation à la sécurité et signalement :** Comprenez les risques liés aux espaces partagés, tels que le talonnage ou les conversations entendues par hasard. Encouragez une culture où signaler les comportements suspects ou les badges égarés est une seconde nature, et adoptez et respectez les bonnes pratiques en matière de sécurité, comme sécuriser les appareils et les documents lorsque vous ne les utilisez pas;
- **Collaboration et responsabilité :** Donnez l'exemple en illustrant et en encourageant les comportements soucieux de la sécurité au sein de votre espace. Veillez à ce que chacun se sente responsable de la surveillance des accès à votre espace et travaillez en étroite collaboration avec votre fournisseur d'espace afin de remédier aux vulnérabilités potentielles dans toutes les zones de l'espace; et
- **Conformité et confiance :** Renforcez la gestion appropriée des informations et des actifs sensibles par le biais de discussions et de formations. Définissez des attentes claires avec les fournisseurs d'espaces de travail afin de répondre aux besoins en matière de sécurité, examinez régulièrement les incidents et adaptez les comportements en matière de sécurité afin de rester en phase avec les meilleures pratiques.

6.7. Confidentialité dans l'espace partagé

Étant donné que la collaboration et le réseautage constituent certains des principaux avantages des espaces partagés, il est normal que la protection de la vie privée puisse représenter un défi. Il est toutefois possible de disposer d'un espace partagé qui vous permette de gérer votre vie privée aussi efficacement que possible et d'agir de manière à rendre plus difficile l'écoute ou la consultation de vos informations sensibles par des tiers. En prenant la protection de la vie privée au sérieux et en utilisant la zone appropriée pour les conversations et autres besoins professionnels, il est possible d'atteindre l'équilibre souhaité par les utilisateurs entre sécurité et fonctionnalité.

Zones de travail : Dans les ZT, les espaces de travail réservables facilitent la collaboration et le réseautage. Cependant, toutes les mesures nécessaires pour garantir la confidentialité et la sécurité ne sont pas mises en place, car ces espaces sont utilisés par de nombreuses personnes travaillant pour divers départements et agences. Les mesures de confidentialité que les utilisateurs peuvent prendre dans les ZT comprennent :

- Utiliser des salles de réunion ou des salles calmes lorsque cela est nécessaire pour préserver l'intimité;
- L'installation d'écrans/de protections de confidentialité sur les ordinateurs offre un niveau de confidentialité de base contre les « espions par-dessus l'épaule »;
- Choisir un bureau éloigné des zones très fréquentées;
- Sécuriser les documents ou les ordinateurs lorsqu'ils sont laissés sans surveillance, même pour de courtes durées;
- Être conscient de votre environnement lorsque vous travaillez avec des informations sensibles, même si elles ne sont pas classifiées;
- Ne pas passer ni recevoir d'appels dans les zones ouvertes; et
- Respecter la politique du bureau rangé, en retirant et en mettant en sécurité tout le matériel lorsque vous vous absentez de votre espace de travail.

Espaces privés : Dans les espaces privés, les utilisateurs doivent s'assurer que toutes les mesures appropriées sont en place pour garantir la confidentialité et la sécurité. N'oubliez pas que toutes les mesures visant à garantir la confidentialité et la sécurité ne sont pas garanties, car l'espace est utilisé par de nombreuses personnes travaillant pour divers départements et agences. Les mesures de confidentialité que les utilisateurs peuvent prendre dans les espaces privés comprennent :

- Veiller à ce que des mesures de protection de la vie privée, telles que l'installation de stores sur les fenêtres des cloisons, soient mises en œuvre;
- Utilisation de conteneurs de sécurité pour sécuriser les informations et les actifs lorsque cela est nécessaire;
- Utilisation de broyeurs ou de services de destruction appropriés pour une destruction sécurisée;
- Installation d'écrans/de protections de confidentialité sur les ordinateurs pour se prémunir contre les « espions par-dessus l'épaule »;
- Sécuriser les documents ou les ordinateurs lorsqu'ils sont laissés sans surveillance, même pour de courtes durées;
- Être conscient de votre environnement lorsque vous travaillez avec des informations sensibles, même si elles ne sont pas classifiées;
- Respecter la politique du bureau rangé, en retirant et en mettant en sécurité tout le matériel lorsque vous vous absentez de votre espace de travail; et
- Veiller à ce que tous les tiers et sous-traitants soient accompagnés ou disposent d'un statut ou d'une habilitation de sécurité approprié lorsqu'ils se trouvent dans des zones privées, et interpeller ceux qui semblent hors de propos ou qui ne portent pas le badge approprié.

Zone de sécurité : Dans les ZS, les utilisateurs doivent s'assurer que toutes les mesures appropriées sont en place pour garantir la confidentialité et la sécurité. Il est toutefois important de garder à l'esprit que, même si les ZS répondent aux besoins spécifiques des utilisateurs en matière de sécurité et de confidentialité pour les projets sensibles et doivent satisfaire à toutes les exigences de sécurité d'une ZS, toutes les mesures ne doivent pas être considérées comme une garantie, car l'espace peut être utilisé par de nombreuses personnes travaillant pour divers départements et agences. Les mesures de confidentialité que les utilisateurs peuvent prendre dans les ZS comprennent :

- S'assurer que les exigences relatives à une SZ sont présentes, suffisantes et soutenues par le dirigeant principal de la sécurité (DPS) ou le groupe de sécurité de votre département ou agence;
- Ne pas divulguer que votre service ou votre organisme occupe les locaux ou l'espace, en particulier sur les listes de locataires situées dans le hall d'entrée du bâtiment;
- Veiller à ce que des dispositifs de protection de l'intimité, tels que des stores ou des vitrages, soient installés sur les fenêtres des cloisons;
- Utiliser des conteneurs spécifiques hautement sécurisés fournis par votre service ou votre agence pour protéger les informations et les actifs lorsque cela est nécessaire;
- Utilisation de broyeurs ou de services de destruction appropriés pour une destruction sécurisée;
- Installation d'écrans/de protections de confidentialité sur les ordinateurs pour se prémunir contre les « espions par-dessus l'épaule »;
- Sécuriser les documents ou les ordinateurs lorsqu'ils sont laissés sans surveillance, même pour de courtes durées;
- Être conscient de votre environnement lorsque vous travaillez avec des informations et des actifs sensibles, en particulier lorsqu'ils sont classés comme protégés ou confidentiels;
- Respecter la politique du bureau rangé, en retirant et en mettant en sécurité tout le matériel lorsque vous vous absentez de votre espace de travail;
- Veiller à ce que tous les tiers et sous-traitants soient accompagnés ou disposent d'une habilitation de sécurité appropriée lorsqu'ils se trouvent dans les ZS, et interpeller ceux qui semblent hors de propos ou ne portent pas le badge approprié.;
- Veiller à l'utilisation de serrures hautement sécurisées conformément aux directives de la GRC afin de sécuriser les locaux;
- Veiller à ce que les exigences en matière de contrôle d'accès soient respectées (c'est-à-dire ne pas laisser les portes ouvertes pour des raisons de commodité);
- Veiller à ce que des restrictions acoustiques appropriées soient mises en place si des conversations nécessitant une isolation acoustique doivent avoir lieu ou demander qu'une zone de discussion spéciale soit prévue; et
- Veiller à ce que les lacunes constatées dans les mesures de sécurité soient comblées rapidement.

6.8. Gestion des accès

Certains espaces partagés sont délibérément peu restrictifs en matière d'accès, ce qui signifie que la plupart ne sont pas conçus pour traiter ou travailler sur des documents hautement sensibles ou classifiés. Il est important que l'accès soit bien géré dans un espace partagé et que le travail ne soit autorisé que jusqu'au niveau de classification pour lequel l'espace a été conçu.

	Zones de travail	Espaces privés	Zones de sécurité
Critères	S'assurer que tous les points d'entrée/sortie des espaces communs sont équipés de systèmes de contrôle d'accès en état de fonctionnement et signaler tout dysfonctionnement.	Si l'espace privé est un espace départemental, assurez-vous que tous les dispositifs de contrôle d'accès fonctionnent correctement.	Veiller à ce que toutes les mesures de contrôle d'accès soient fonctionnelles, y compris les conteneurs de sécurité spécifiques au département ou à l'agence et les systèmes de détection d'intrusion installés.
Améliorations	Le contrôle d'accès dans les espaces partagés est généralement géré par le fournisseur de l'espace de travail, mais des exigences supplémentaires peuvent être nécessaires en fonction des besoins de l'organisation.		Il pourrait être nécessaire de mettre en place des systèmes de contrôle d'accès améliorés (c'est-à-dire une authentification multifactorielle ou biométrique).
Comportements	Les utilisateurs doivent surveiller les espaces communs, identifier et signaler toute activité suspecte, notamment le talonnage ou la présence de personnes non autorisées.	Fermez et verrouillez les portes d'un espace privé chaque fois que vous le quittez. Utilisez les identifiants d'accès qui vous ont été attribués (sans les partager) afin de garantir l'intégrité de l'accès.	Utilisez tout l'équipement de sécurité fourni et suivez toutes les procédures de sécurité pour entrer dans une zone ZS (c'est-à-dire laisser les appareils mobiles à l'extérieur de l'espace).

6.9. Systèmes de sécurité matérielle

Le niveau de sécurité électronique fourni aux espaces partagés peut varier. Bien que tous disposent d'un certain type de contrôle d'accès, il est important de garder à l'esprit que les ressources partagées telles que les salles de réunion, les espaces privés et les ZS peuvent être partagées avec tous les locataires plutôt que d'être réservées à des départements et agences spécifiques. Les départements et agences utilisateurs doivent s'assurer que tous les systèmes de sécurité matérielle requis sont disponibles et fonctionnels avant d'autoriser le personnel à travailler dans un espace partagé.

Les ministères et organismes doivent également s'assurer que toutes les procédures d'urgence sont en place et ont été testées, comme les plans d'évacuation et d'intervention en cas d'intrusion. Si les espaces privés ou les zones de sécurité sont occupés uniquement par le personnel du ministère (c'est-à-dire les quartiers), assurez-vous que tous les équipements de sécurité, conteneurs et systèmes de contrôle d'accès requis sont fonctionnels. Les utilisateurs doivent également s'assurer que les services fournis par les prestataires, tels que la CCTV, n'empiètent pas sur les espaces de travail et ne capturent que des images des zones communes.

Tous les ministères et organismes utilisant ces espaces partagés doivent s'assurer que tous les espaces et équipements appartenant à leur ministère ou sous leur contrôle font l'objet d'inspections régulières afin de détecter toute altération ou tout accès non autorisé. Les ministères et organismes doivent également s'assurer que toutes les procédures, telles que la gestion des visiteurs et leur accompagnement, sont en place et respectées.

6.10. Cybersécurité

Comme mentionné précédemment, ces recommandations ne concernent pas spécifiquement la cybersécurité. Toute préoccupation particulière dans ce domaine doit être adressée au CST ou au SPC. La sécurité des systèmes numériques et des informations exige que chacun joue son rôle. Les cyberattaques peuvent prendre différentes formes, mais la grande majorité d'entre elles peuvent être évitées en mettant en œuvre quelques mesures élémentaires.

Le Wi-Fi disponible doit être protégé par un mot de passe fort, idéalement avec des réseaux séparés pour les visiteurs et les utilisateurs des espaces partagés. Suivez les directives relatives à la gestion des incidents cybernétiques, tels que les violations de données ou les intrusions dans le réseau, et veillez à ce que les utilisateurs respectent toutes les procédures de cybersécurité afin de minimiser les risques, par exemple en verrouillant les appareils et en laissant les appareils mobiles à l'extérieur de la ZS avant d'y entrer, y compris les téléphones portables, les appareils portables personnels et les équipements informatiques non certifiés pour une utilisation dans une ZS.

7. Conclusion

L'essor des espaces partagés représente un changement fondamental dans notre façon de concevoir et d'utiliser les espaces de travail GC. Du point de vue du fournisseur, ces espaces offrent un modèle commercial dynamique qui allie flexibilité, collaboration, espace et économies. Pour les utilisateurs, les espaces partagés sont abordables, adaptables et offrent des possibilités de collaboration qui font souvent défaut dans les bureaux traditionnels.

Le succès de ce modèle dépend de l'alignement des besoins et des attentes des deux parties. Les fournisseurs doivent continuer à innover, en offrant non seulement des espaces physiques, mais aussi des services et des expériences qui apportent une valeur ajoutée tout en protégeant

les informations et les actifs du GC. Les utilisateurs, quant à eux, doivent aborder les espaces de travail partagés avec des objectifs clairs, une volonté de s'engager auprès de la communauté au sens large, tout en veillant à ce que cette nouvelle méthode de travail ne mette pas en péril la sécurité du gouvernement.

En fin de compte, les espaces de travail partagés sont plus qu'une simple solution immobilière : ils reflètent l'évolution des cultures d'entreprise qui privilégient la flexibilité, la connectivité et le bien-être. Lorsqu'ils sont conçus avec soin, ils peuvent constituer une plateforme puissante pour la productivité, la croissance et la collaboration de toutes les parties concernées.

8. Documents de référence et documents sources

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité
- The International Crime Prevention Through Environmental Design Association (en anglais seulement)
- SHARED WORKSPACES - Security Guidance for Users, National Protective Security Authority (NPSA) – United Kingdom (en anglais seulement)
- SHARED WORKSPACES - Security Guidance for Providers, National Protective Security Authority (NPSA) – United Kingdom (en anglais seulement)
- Principal organisme responsable de la sécurité matérielle
- GSMGC-007 – Transport, transmission et entreposage de matériel protégé ou classifié.
- GSMGC-015 – Guide pour l'établissement des zones

9. Promulgation

Examiné et recommandé aux fins d'approbation.

J'ai examiné le document GSMGC-023 (2025) – Considérations relatives à la sécurité matérielle dans les espaces partagés, et j'en recommande l'approbation.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2025.10.20 10:32:47 -04'00'

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

Approuvé

J'approuve par la présente le document GSMGC-023 (2025) – Considérations relatives à la sécurité matérielle dans les espaces partagés.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2025.10.23 12:44:44 -04'00'

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