Guide de gestion de l’accès
GSMGC-006 (2024)

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

Publication publiée : 2024-01-15
Mise à jour :

Avant-propos

Le Guide de gestion de l'accès est une publication NON CLASSIFIÉE, publiée sous du principal organisme responsable de la sécurité matérielle de la GRC (PORS) de la GRC.

Il s'agit d'une publication du gouvernement du Canada qui sert de guide pour la conception et la gestion des systèmes de gestion de l'accès pour les ministères, les organismes et les employés du gouvernement du Canada.

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

Date d'entrée en vigueur

La date d'entrée en vigueur du Guide de gestion de l'accès GCGMGC-006 est 2024-01-15

Registre des modifications

Amendement no.	Date	Entrée par	Résumé de la modification

Remarque : Le pouvoir de modification ou de dérogation est au principal organisme responsable de la sécurité de la GRC (ASL de la GRC).

Contenu

1. Introduction

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

1.1. But

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

Le guide contient à la fois les mesures de contrôle de sécurité requises, indiquées par l'utilisation du mot « doit », et les mesures de contrôle de sécurité ou les lignes directrices recommandées, indiquées par l'utilisation du mot « devrait ». L'utilisation du mot « doit » indique une référence à une politique ou à une norme établie du GC, tandis que l'utilisation du mot « devrait » renvoie à des conseils ou à une pratique exemplaire.

Les mesures de sécurité matérielle de base sont conçues pour assurer une protection contre les types courants de menaces auxquelles les ministères et organismes du GC seraient confrontés. Certains ministères et organismes ou activités opérationnelles peuvent faire face à des menaces différentes en raison de la nature de leurs activités, de leur emplacement ou de l'attrait de leurs actifs. Il peut s'agir, par exemple, d'établissements policiers ou militaires, de services de santé, de laboratoires, d'installations de recherche de nature délicate, de musées, de comptoirs de services, de bureaux situés dans des zones à criminalité élevée et d'installations situées à l'extérieur du Canada.

1.2. Applicabilité, rôles et responsabilités

Tous les ministères et organismes sont responsables de la protection des employés, de l'information, des biens et de la prestation des services dans leur secteur de responsabilité. Les directives sur la gestion de l'accès fournies dans le présent document doivent constituer la base de référence minimale pour les ministères et organismes du GC.

Les organisations de locataires sont responsables d'informer les ministères et organismes gardiens de leurs exigences en matière de sécurité pour le choix du site et l'aménagement des locataires.

Les ministères et organismes gardiens sont responsables de fournir et de financer les mesures de protection jugées nécessaires par le gardien pour protéger les installations en fonction d'une évaluation de la menace et des risques (EMR) effectuée par le gardien ou pour lui. Cette

responsabilité comprend la mise en œuvre et l'intégration de mesures pour la sécurité de l'immeuble de base (p. ex., portes extérieures et éclairage), les systèmes de l'immeuble (p. ex., ascenseurs, systèmes mécaniques et électriques) et la sécurité des personnes (p. ex., escaliers de sortie, alarmes d'incendie et gicleurs). Les gardiens sont également responsables d'intégrer les exigences financées par les locataires à l'infrastructure de leur immeuble.

Ce guide devrait être utilisé pour appuyer la prise de décisions pour les installations du GC et ne concerne pas spécifiquement les emplacements de télétravail ou de télétravail. D'autres guides peuvent être nécessaires pour évaluer pleinement la sécurité à distance ou en télétravail et sont disponibles auprès de l'organisme responsable de la sécurité physique matérielle - 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. Considérations aux technologies 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 plus d'informations, contacter :

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. Acronymes

Acronyme	Signifiant
CATV	Distribution de télévision par câble
CCCBPI	Commission canadienne des codes du bâtiment et de prévention des incendies
DGS	Directive sur la gestion de la sécurité
EMR	Évaluation de la menace et des risques
GSMGC	Guide de sécurité matérielle du gouvernement du Canada
IT	Technologie de l'information
LSA	Organisme responsable de la sécurité (pour la sécurité matérielle)
NIP	Numéro d'identification personnel
NFC	Code national de prévention des incendies du Canada 2020
PCCE	Prévention du crime par la conception environnementale
PDRR	Protection, détection, réponse et récupération
PSG	Politique sur la sécurité du gouvernement
SA&A	Évaluation et autorisation de sécurité
SCT	Secrétariat du Conseil du Trésor
SOP	Procédures opérationnelles normalisées
TRA	Évaluation des menaces et des risques
ZA	Zone d'accueil
ZHS	Zone de haute sécurité
ZP	Zone d'accès publique
ZS	Zone de sécurité
ZT	Zone de travail

4. Glossaire

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

Actif	Actifs matériels ou immatériels du gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale.
Actifs classifiés	Actifs dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national.
Besoin d'accéder à	Critère utilisé par le ou les dépositaires de renseignements, de biens ou d'installations de nature délicate pour établir, avant de fournir un accès physique ou une entrée, que le destinataire visé doit avoir accès à l'espace pour s'acquitter de ses fonctions officielles.
Besoin de connaître	Le principe selon lequel il est nécessaire pour une personne d'avoir accès à des renseignements et de les connaître afin de pouvoir exécuter ses tâches.
Biens protégés	Biens dont la compromission risquerait vraisemblablement de porter préjudice à un intérêt non national.
Biométrie	Identification d'une personne à partir d'une caractéristique physique : empreintes digitales, iris, traits du visage, géométrie de la main, etc..
Carte Accès	Document délivré par un ministère ou un organisme pour permettre aux personnes autorisées d'accéder à une zone ou à une zone particulière d'une installation ou d'un complexe. Il ne doit pas être confondu avec une carte d'identité qui fournit des données d'identification sur une personne, comme son nom complet, son adresse, son âge, les caractéristiques d'identification, etc., d'un employé du GC.
Cartes d'identité (employé)	Document délivré par un ministère ou un organisme qui fournit des données d'identification sur une personne, comme son nom complet, son adresse, son âge, les caractéristiques d'identification, etc., en tant qu'employé du GC. Il ne faut pas le confondre avec une carte d'accès qui est un dispositif émis pour permettre aux employés d'accéder à des espaces/zones dans une installation du GC en fonction de leur niveau d'accès.
Carte de proximité	Dispositif, souvent combiné à une carte d'accès, contenant une puce lisible qui communique avec un lecteur de contrôle d'accès, un clavier ou un lecteur biométrique. L'utilisation de cette carte fait partie du système d'authentification multiple pour permettre aux employés d'accéder aux espaces et aux zones d'un ministère ou d'un organisme en fonction de leur niveau d'accès.
Contrôle de l'accès	Assurer l'accès autorisé aux biens à l'intérieur d'une installation ou de zones d'accès restreint, en effectuant le triage des visiteurs et du matériel aux points d'entrée par les membres du personnel, les gardes ou de façon informatisée et, lorsque requis, en surveillant leur déplacement à l'intérieur de l'installation ou des zones d'accès restreint en les escortant.

Compromission	Divulgation, destruction, suppression, modification, interruption d'accès ou utilisation de renseignements ou de biens non autorisée.
Cote de fiabilité	Indique que l'évaluation de fiabilité a été complétée avec succès et donne à la personne visée un accès régulier aux biens gouvernementaux et un accès à des renseignements PROTÉGÉS en fonction du besoin de connaître.
Cote de sécurité	Indique que l'évaluation de sécurité a été complétée avec succès; avec un besoin de connaître, permet d'avoir accès à des renseignements classifiés. Il y a trois niveaux : confidentiel, secret et très secret.
Démarcation	Identifier la limite entre les zones et fournir un avis de toute exigence spécifique à la zone pour l'entrée et la sortie en utilisant des panneaux affichés.
Dépositaire	Ministère ou organisme responsable de l'administration des biens immobiliers fédéraux.
Disponibilité	Se dit de l'information utilisable sur demande au soutien des opérations, des programmes et des services.
Escorte	Personne possédant une cote de sécurité appropriée qui est responsable de la surveillance continue de personnes n'ayant pas une cote de sécurité dans les secteurs où une cote de sécurité ou un statut seraient normalement exigés.
Évaluation de la menace et des risques	Processus d'évaluation des biens d'une installation, des menaces qui pèsent sur eux et du rendement des mesures de protection contre ces menaces, visant à définir les risques.
Exigences sécuritaires de base	Dispositions obligatoires de la Politique sur la sécurité du gouvernement et des normes opérationnelles et de la documentation technique connexes.
Installation	Une installation peut être un bâtiment (en tout ou en partie) et peut comprendre son site ou son terrain, ou peut-être une zone ou une construction qui n'est pas un bâtiment (par exemple, champs de tir, champs agricoles).
Intégrité	L'exactitude et l'intégralité des biens, et l'authenticité des transactions.
Intérêt national	Concerne la défense et le maintien de la stabilité sociale, politique et économique du Canada.
Locataire	Un ministère qui occupe un immeuble du gouvernement fédéral administré par un autre ministère ou une société d'État.
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.
Ministères et organismes	Tout ministère, organisme, installation scientifique ou installation connexe du GC qui est responsable de la gestion des biens immobiliers, de l'information, des biens et/ou du personnel fédéraux.

Personne autorisée	Une personne qui travaille avec le gouvernement du Canada, y compris des employés du gouvernement fédéral ainsi que des employés occasionnels, des entrepreneurs, des étudiants et d'autres personnes qui ont obtenu une autorisation de sécurité pour accéder aux renseignements, aux biens, aux installations, aux réseaux et aux appareils électroniques du gouvernement.
Prévention du crime par la conception environnementale	Principe qui encourage l'utilisation de la conception paysagère et/ou architecturale pour réduire ou éliminer les comportements criminels.
Renseignements classifiés	Information dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national.
Renseignements protégés	Renseignements dont la compromission risquerait vraisemblablement de porter préjudice à un intérêt non national.
Serrure Magnétique	Système de verrouillage magnétique fonctionnant sur une alimentation électrique continue. Activé ou déverrouillé lorsque l'alimentation électrique est interrompue par un interrupteur désigné ou un relais d'alarme incendie.
Sortie	Moyens de sortie, y compris les portes, qui mènent de la surface de plancher qu'ils desservent à un bâtiment distinct, à une voie publique ouverte ou à un espace extérieur ouvert protégé de l'exposition au feu du bâtiment et ayant accès à une voie publique ouverte.
Surveillance	Pour surveiller ou détecter une faille de sécurité.
Surveillance continue	Surveillance sur une base continue pour confirmer qu'il n'y a pas eu infraction à la sécurité.
Surveillance périodique	Surveillance périodique, mais régulière pour confirmer qu'il n'y a pas eu d'infraction à la sécurité. La fréquence et la diligence de la surveillance périodique sont fondées sur les recommandations d'une évaluation des risques.
Zone à accès restreint (ZAR)	Aire de travail (site ou édifice) au sein d'un ministère où l'accès est restreint aux personnes autorisées. Comprend la zone d'opérations, la zone de sécurité et la zone de haute sécurité, conformément aux définitions énoncées dans la référence GSMGC-015 – Guide pour l'établissement des zones de sécurité matérielle.
Zone d'accueil	Zone où la transition d'une zone publique à une zone à accès restreint est contrôlée. Exemple–Hall d'accueil ou poste de gardien de sécurité.
Zone de haute sécurité	Zone où l'accès est limité au personnel autorisé détenant la cote de sécurité du GC correspondante et aux visiteurs préapprouvés/contrôlés et escortés de façon appropriée. Exemple – zone où les renseignements et les biens classifiés plus haut que secret sont traités ou stockés.
Zone de sécurité	Zone où l'accès est limité au personnel autorisé détenant la cote de sécurité du GC correspondante et aux visiteurs dûment escortés. Exemple – zone où les renseignements classifiés jusqu'au niveau Secret inclusivement sont traités ou stockés.

Zone de travail	Zone où l'accès est limité au personnel qui travaille à l'intérieur et aux visiteurs dûment escortés. Exemple – Espace de bureau du gouvernement ou entrepôt réservé au personnel
Zone publique	Zone où le public a un accès sans entrave et qui entoure ou forme généralement une partie d'une installation gouvernementale. Exemple : terrain entourant un immeuble.

5. Exigences/privilèges d'accès fondés sur le niveau de filtrage de sécurité

Une exigence fondamentale de la PSG est de limiter l'accès aux renseignements et aux zones sensibles. La PSG restreint également l'accès à ceux qui ont le besoin de savoir, ou un besoin d'accès, afin d'exercer leurs fonctions. Bien que les niveaux de filtrage de sécurité permettent l'accès à certains renseignements ou à certaines zones, l'application des principes du besoin de savoir et du besoin d'accès restreint cet accès à ceux qui sont tenus de lire ou de connaître des renseignements précis ou d'accéder à des zones précises. Le personnel n'a pas le droit d'y accéder simplement parce que c'est pratique ou parce que cela est proportionnel à son niveau d'autorisation de sécurité, à son statut, à son grade ou à son bureau. Les ministères et organismes sont responsables d'examiner activement les privilèges d'accès et devraient révoquer l'accès lorsqu'il n'est plus nécessaire. (Exemple : un employé n'a plus besoin d'avoir accès à un secteur, accepte un poste au sein d'un autre ministère ou organisme, ou lorsqu'il cesse d'être employé au sein du GC).

Une façon efficace de mettre en œuvre et de maintenir le principe du besoin de savoir ou du besoin d'accès consiste à séparer et à contrôler l'accès aux renseignements et aux biens de nature délicate du GC grâce à l'utilisation efficace des zones de sécurité matérielle. Étant donné que les personnes au sein du GC peuvent constituer une menace à la disponibilité, à la confidentialité ou à l'intégrité des renseignements ou des biens du GC (souvent appelés risques internes), limitant l'accès uniquement aux personnes ayant le besoin approprié. . .le fait de savoir / le besoin d'accéder peut réduire le risque de menace interne et aider à protéger l'information et les biens du GC.

La gestion de l'accès est un processus qui utilise une combinaison de matériel de sécurité matérielle et de procédures opérationnelles normalisées (PON) pour réglementer l'accès aux installations, à l'information et aux biens du GC. L'accès devrait être limité uniquement aux personnes qui détiennent une cote de fiabilité ou de sécurité du GC valide au niveau de sécurité approprié, dont les fonctions les obligent à avoir un tel accès, et qui ont été approuvées par l'autorité compétente. Ces exigences sont nécessaires pour que l'autorisation soit accordée et que la gestion de l'accès soit efficace.

Ce tableau indique les privilèges d'accès de base en fonction des niveaux de filtrage de sécurité. Il est important de noter que tous les ministères et organismes ne sont pas structurés de la même façon, par conséquent, certains des niveaux d'examen préalable pourraient ne pas s'appliquer.

Tableau 1 - Privilèges d'accès

		Visiteur (aucune vérification de sécurité)	**Niveaux de filtrage de sécurité**		
			Cote de fiabilité (CF)	Secret	Très Secret (TS)
Accès à la zone	Publique	✓	✓	✓	✓
	Accueil	✓	✓	✓	✓
	Travail	X	✓	✓	✓
	Sécurité	X[1]	✓[1]	✓	✓
	Haute Sécurité	X[1]	X[1]	✓[2]	✓ TS avec endoctrinement peut être nécessaire dans certains ZHS.

légende

✓	Accès à la zone autorisée (à condition que la personne ait besoin de savoir ou d'avoir accès)
✓[1]	L'accès à la zone nécessite une escorte avec une cote de sécurité de niveau Secret minimum.
✓[2]	L'accès à la zone peut nécessiter une escorte en fonction de l'espace. Par exemple, un employé ayant une cote de sécurité de niveau secret peut entrer dans une pièce sans escorte (qui est une zone de haute sécurité), mais un employé ayant une cote de sécurité de niveau secret ne peut pas entrer dans une salle d'environnement classifié (qui est une zone de haute sécurité) sans escorte. (une autorisation de niveau très secret est requise).
X	Accès à la zone autorisé avec une escorte appropriée. Escorté par un employé autorisé: • qui occupe l'espace de façon permanente avec un Cote de fiabilité valide; or • personnel de sécurité ayant un Cote de fiabilité valide.
X[1]	Accès à la zone autorisé avec une escorte appropriée. Escorté par un employé autorisé: • qui occupe l'espace de façon permanente avec une cote de sécurité de niveau Secret ou Très Secret valide; or • le personnel de sécurité détenant une cote de sécurité de niveau Secret ou Très Secret valide.

Pendant les périodes de risque accru, les ministères et organismes peuvent être encouragés à mettre en œuvre des mesures supplémentaires de contrôle de l'accès afin de protéger leur personnel, leurs renseignements ou leurs installations. Veuillez consulter l'annexe A – Réponse aux niveaux de menace plus élevés pour les options de gestion de l'accès offertes aux ministères et organismes.

6. Aménagement de l'installation/Zones

La gestion de l'accès est fondamentalement liée au concept de zonage de sécurité matérielle, et aux mesures de contrôle entre les zones, pour gérer la circulation du personnel et des marchandises dans leur organisation. Le fait de bien connaître le GSMGC-015 – Guide pour l'établissement des zones de sécurité matérielle aidera les ministères et organismes à appliquer les zones de sécurité matérielle appropriées dans leurs installations. Les cinq zones de sécurité matérielle sont les suivantes :

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

Consultez le document GSMGC-015 – Guide pour l'établissement des zones de sécurité matérielle pour obtenir des renseignements supplémentaires sur les zones de sécurité matérielle et les mesures supplémentaires qui peuvent être requises pour les zones de sécurité spécialisées et les zones d'accès contrôlé.

Remarque: Zones temporaires - Tout établissement d'une zone d'accès restreint temporaire (ZT, SZ ou HSZ), à l'intérieur ou à l'extérieur d'une zone contrôlée, doit respecter ou dépasser les mêmes normes utilisées pour répondre aux spécifications minimales d'une zone de sécurité matérielle permanente pendant la durée d'utilisation de la zone temporaire. Ces zones temporaires pourraient être aménagées pour abriter ou traiter des informations sensibles classifiées au-dessus du niveau normalement stocké dans la zone, à condition :

- les mesures de sécurité matérielle nécessaires sont en place;
- le risque accru est documenté au moyen d'une EMR officielle;
- le risque est accepté par l'autorité de sécurité ministérielle de l'organisation (ASE ou son délégué).

Par exemple, un ZS temporaire pourrait être établi autour d'un navire ou d'un camion saisi sous surveillance continue; pourvu de personnel, traitant des informations sensibles, contrôlant positivement l'accès et l'entreposage du bien conformément aux directives pertinentes, voir GSMGC-007 - Transport, transmission et entreposage de matériel protégé ou classifié.

La conception des installations permettant l'observation naturelle, le contrôle de l'accès et le renforcement territorial (zones et signalisation) – composantes clés de la prévention du crime par la conception environnementale (PCCE) – permet aux ministères et organismes de gérer le flux de personnes dans une installation. Ces modèles visent à influencer positivement le comportement et les activités tout en décourageant les actions indésirables du personnel, des visiteurs et des adversaires potentiels. La PCCE dispose d'un ensemble de principes situationnels de prévention du crime à respecter lors de la désignation, de la définition et de la conception de la sécurité d'un environnement. Les principes suivants sont également discutés dans G1-005 Guide pour la préparation d'un énoncé de sécurité matérielle.

6.1. Observation naturelle/contrôle d'accès

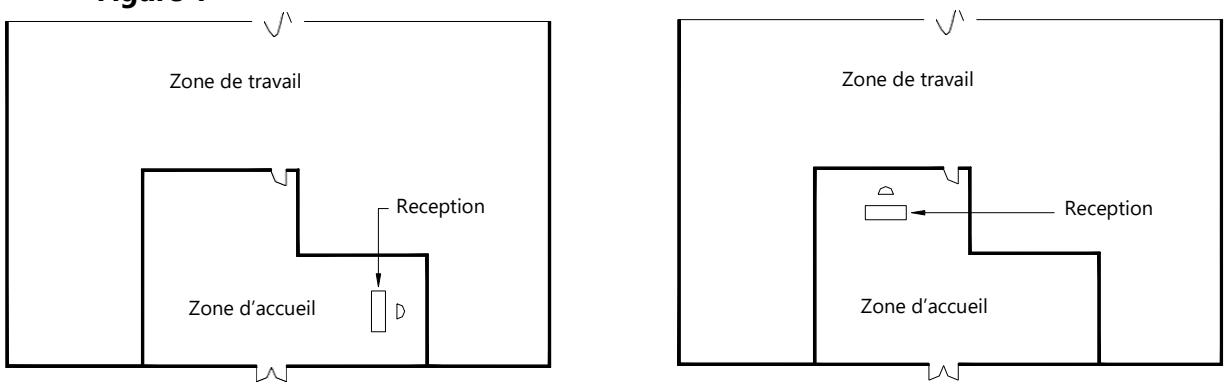
Le principe d'observation naturelle et de contrôle d'accès naturel de la PCCE est un concept de conception efficace qui vise à améliorer la gestion de l'accès des ministères et organismes. L'observation naturelle peut être réalisée en établissant et en maintenant des lignes de visibilité claires et dégagées qui favorisent l'identification facile des personnes et des véhicules en approche ou en transit. Les méthodes d'établissement de cet objectif visuel peuvent comprendre un aménagement paysager bien entretenu, des voies claires, un éclairage de

sécurité, etc. Le contrôle d'accès naturel repose sur le concept de limites clairement définies qui influencent ou contrôlent le flux de mouvement. Quelques exemples de contrôle d'accès naturel sont les clôtures périmétriques, les sentiers pédestres de la rue à la porte du bâtiment, l'aménagement paysager (arbustes, parterres de fleurs, arbres, étangs, etc.) pour agir comme une barrière, les routes sinueuses pour ralentir la vitesse des véhicules, les parterres de fleurs en béton encastrés pour agir comme barrière anti-bélier pour véhicule, etc.).

Les principaux objectifs de l'observation naturelle et du contrôle d'accès naturel sont d'encourager les personnes à entrer et sortir des lieux d'une manière prévisible, facilement surveillée, et dissuader les personnes non autorisées de tenter d'entrer par crainte d'être facilement identifiées et appréhendées.

Par exemple, considérez l'emplacement de la réception dans les deux exemples suivants :

Figure 1



Exemple No. 1 Exemple No. 2

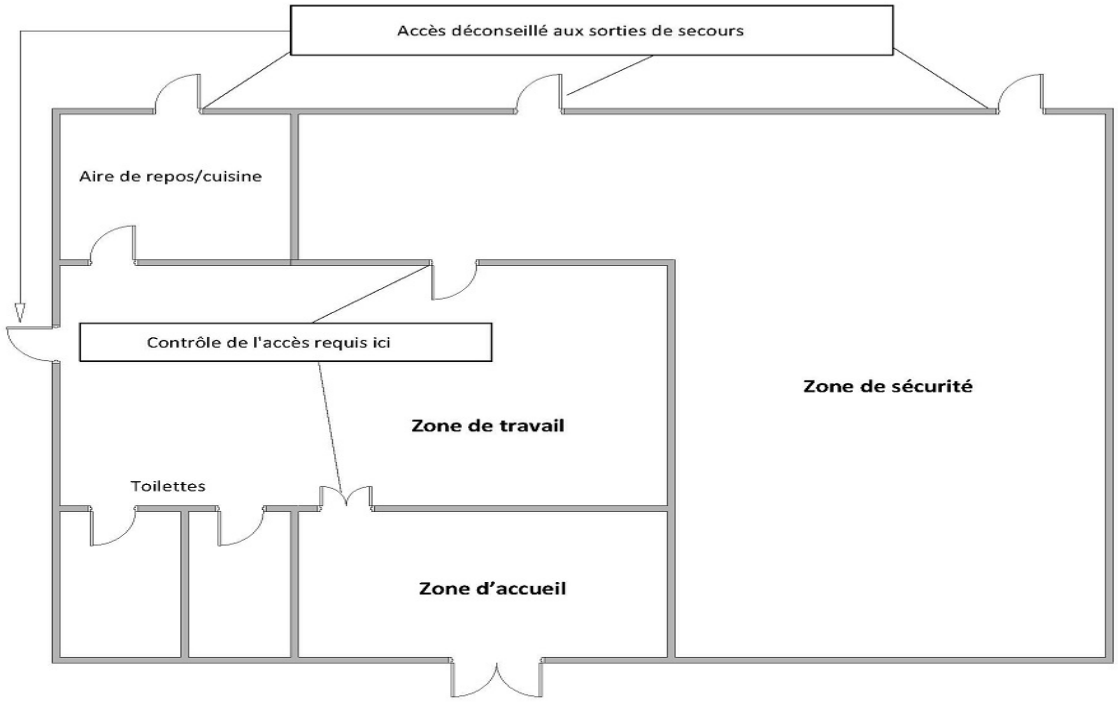
Texte Alt Figure 1 représente un emplacement privilégié pour une réception afin de permettre l'observation d'un hall

Dans l'exemple numéro 1, la réception ne peut pas voir la porte entre la ZA et la ZT. Une personne pourrait attendre un moment opportun pour entrer et passer inaperçue à la réception. Dans l'exemple numéro 2, la réception a été déplacée pour permettre l'observation de la zone d'entrée. Un individu non autorisé se sentirait plus visible s'il essayait d'attendre un moment opportun pour entrer, et serait plus probablement remarqué du comptoir de réception.

6.2. Compartimentation (Zones)

La compartimentation peut être définie comme la séparation physique d'une zone(s) au sein d'une structure afin de promouvoir un sentiment d'appartenance ou de renforcement territorial, fournir des possibilités de surveillance naturelle du point d'accès, et établir une séquence clairement définie de limites par lesquelles un visiteur ou un employé du ministère peut ou non passer. Les personnes qui se déplacent entre ces espaces doivent percevoir les limites et comprendre les règles et les limites associées au franchissement de l'espace fonctionnel. Pour les ministères et organismes, l'emploi de GCPSG-015 – Guide pour l'établissement des zones de sécurité matérielle active la disposition souhaitée.

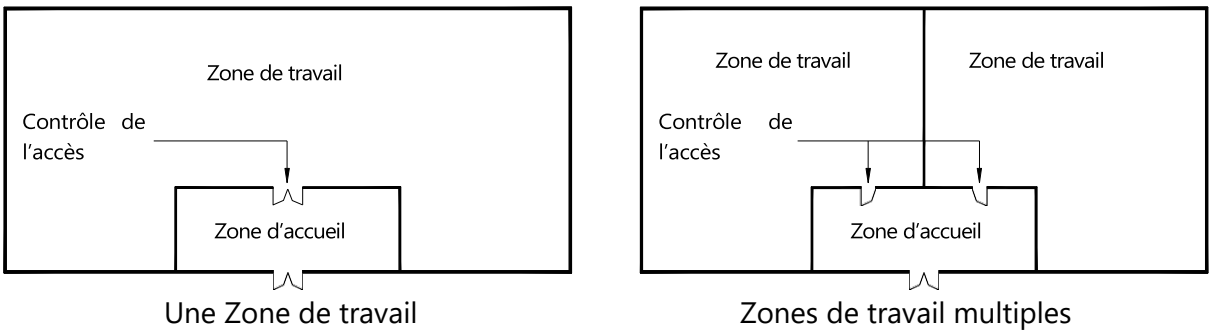
Figure 2 Zones



Texte Alt Figure 2 représente un plan d'étage d'un bâtiment avec différentes zones où l'accès est contrôlé à chaque espace.

Compartimenter un bureau peut réduire le nombre d'employés qui ont accès à des actifs individuels. Dans les grands ministères et organismes, il est habituellement possible de s'organiser en groupes qui ont rarement besoin d'interagir entre eux pour s'acquitter de leurs fonctions. Par exemple, une direction générale de la recherche et du développement d'un ministère peut ne pas avoir besoin d'interagir régulièrement avec une direction générale des communications. Prenons l'exemple suivant :

Figure 3 Séparation interne des zones



Texte Alt Figure 3 représente la division des zones d'opérations pour limiter l'accès entre les sections.

Dans la figure 3, les deux sections partagent la totalité de la ZT, ce qui pourrait mener à un accès non autorisé aux renseignements et aux biens de l'une ou l'autre des sections occupant l'espace. Cela peut entraîner des mesures d'atténuation et des coûts supplémentaires pour protéger leurs renseignements et leurs biens respectifs. Dans la ZT multiple, la ZT a été divisée en deux espaces de travail autonomes, ce qui réduit le risque d'accès non autorisé détenu par l'une ou l'autre des sections.

6.3. Démarcation/Signe

La démarcation consiste à délimiter la frontière entre les zones et à fournir un avis (signalisation) de toute exigence propre à la zone pour l'entrée et la sortie. Bien que cela puisse être réalisé au moyen d'une ligne de ruban adhésif sur le sol, d'un mur temporaire comme un séparateur de pièce, un bureau, etc., la meilleure pratique consiste à installer des barrières physiques (portes, murs, etc.) autour de chaque zone séparée à laquelle l'accès est contrôlé. En soi, cela pourrait ne pas suffire à dissuader les gens de tenter d'entrer. Sans signalisation, par exemple, une personne peut considérer une porte verrouillée comme un inconvénient lorsqu'elle doit entrer, plutôt que comme un identificateur d'une zone d'accès restreint. L'objectif de la signalisation doit être clair pour qu'elle soit respectée. Voir la figure 4.

- Aux contrôles de l'accès, où le personnel doit entrer et sortir, identifier chaque zone avec des panneaux détaillant les restrictions et/ou les exigences d'entrée, comme le personnel autorisé seulement;
- Les visiteurs doivent être escortés;
- Aucun appareil électronique; et
- Zone de travail.

Fait tout aussi important, l'affichage pour rappeler au personnel qu'il sort d'une zone à sécurité élevée est un outil utile pour rappeler à tous de verrouiller les armoires de sécurité, de ne pas discuter de renseignements classifiés ou d'autres contre-mesures de sécurité propres au site utilisées par les ministères et organismes.

Figure 4

Texte alt Figure 4 représente un exemple de signalisation située à un contrôle de l'accès.

À noter: Les panneaux doivent être conformes au Manuel du Programme de coordination de l'image de marque, être fixés en place pour qu'ils puissent être facilement observés à l'approche et, dans la mesure du possible, comporter des illustrations.

6.4. Sécurité-incendie et code du bâtiment

Les systèmes et les procédures de gestion de l'accès ne doivent jamais mettre en danger la sécurité du personnel dans les propriétés du GC. Les ministères et organismes doivent faire tous les efforts possibles pour respecter la législation applicable en matière de conception, de composition, de sécurité-incendie, d'accessibilité à la mobilité, de santé et sécurité au travail, etc.

La législation canadienne applicable devrait être considérée comme la norme minimale pour les ministères et organismes situés à l'extérieur du Canada; toutefois, si les lois locales sont d'une norme de sécurité ou d'un seuil légal plus élevé, les exigences de sécurité des bâtiments plus élevées/plus normatives seront utilisées. Dans ces cas, le personnel de la sécurité matérielle et de la conception et de l'entretien des immeubles devrait travailler ensemble pour élaborer des solutions qui satisferont à la fois la responsabilité de l'employeur de fournir un milieu de travail sécuritaire et la responsabilité des employés de protéger l'information et les biens du GC conformément à avec la politique.

6.4.1. Sorties d'urgence

En vertu du Code national de prévention des incendies (CNPI) de 2020, la Commission canadienne des codes du bâtiment et de prévention des incendies (CCCBPI) énonce les normes minimales de conception physique pour la sécurité-incendie des installations. Bien que les systèmes de sécurité-incendie, comme les sorties de secours, soient nécessaires pour préserver la vie dans des situations mettant en danger la vie des personnes/d'urgence, ces sorties peuvent également être utilisées pour contourner les méthodes de contrôle d'accès décrites dans le présent guide. Les ministères et organismes devraient élaborer des solutions et/ou des PON pour empêcher l'accès par les sorties de secours en fonction d'une EMR mise à jour. Comme pratique exemplaire, les sorties de secours devraient être:

- Activation intérieure (ouverture) seulement;
- Bien éclairé (GSMGC-004 – Guide sur les considérations liées à l'éclairage de sécurité);
- Connecté à un système d'alarme d'intrusion surveillé et/ou à une alarme sonore locale pour avertir les autres que la porte a été ouverte;
- S'il est appuyé par l'EMR, surveillé par un système de vidéosurveillance en collaboration avec le système d'alarme d'intrusion.

6.4.2. Alimentation d'urgence

Afin de maintenir le contrôle de l'accès pendant une panne de courant, un système de contrôle d'accès doit être connecté à une source d'alimentation de secours. Idéalement, le système devrait être raccordé à un groupe électrogène de secours qui pourrait permettre au système de contrôle d'accès électronique de fonctionner pendant une période plus longue jusqu'à ce que le courant soit rétabli. Comme pratique exemplaire, les systèmes de contrôle d'accès doivent être configurés sur une alimentation de secours pour permettre un accès ininterrompu basé sur une EMR.

À noter: L'alimentation de secours des systèmes de contrôle d'accès est différente de celle des verrous d'agrandissement. Les systèmes de verrouillage magnétique doivent être alimentés par une alimentation électrique (avec batteries), mais doivent également utiliser un relais pour mettre la supervision incendie hors ligne et qui va couper l'alimentation du verrou magnétique en cas d'incendie. Voir 7.5.3 Serrures magnétiques.

7. Méthodes de contrôle de l'accès

Un système de contrôle d'accès permet de déplacer le personnel et le matériel autorisés à l'intérieur et à l'extérieur des installations, tout en détectant et en retardant éventuellement le déplacement du personnel/des visiteurs non autorisés et des objets interdits.

Les objectifs d'un système de contrôle d'accès utilisé pour la protection physique sont les suivants :

- Permettre uniquement aux personnes autorisées d'entrer et de sortir;
- Détecter et empêcher l'entrée ou la sortie de matériel de contrebande (armes, explosifs, outils non autorisés ou biens essentiels);
- Fournir de l'information au personnel de sécurité pour faciliter l'évaluation et l'intervention. (rassembler le rapport en cas d'urgence); et
- Intégrer la flexibilité nécessaire pour tenir compte des changements dans les niveaux de menace (Annexe A) et permettre un retour rapide aux opérations normales.

Lors de l'établissement de la conception et de l'aménagement des zones de sécurité matérielle, les deux premières zones (ZP et ZA) devraient établir les conditions d'accès pour les trois zones réglementées (ZT, ZS, ZHS); avec l'exigence de sécurité de base selon laquelle l'accès est contrôlé pour la ZT et les zones supérieures. Ceci est détaillé en détail dans GCPSG-015 – Guide pour l'établissement des zones de sécurité matérielle.

Étant donné qu'il n'y a pas deux installations identiques, les ministères et organismes devraient s'appuyer sur les principes de base suivants en matière de gestion de l'accès et élaborer leurs propres contre-mesures et PNE qui sont appuyées par une EMR. Certaines méthodes couramment utilisées de gestion des accès peuvent inclure:

- Pièces d'identité, accès ou cartes d'accès combinées;
- Matériel de sécurité matérielle (portes et serrures);
- Les systèmes d'accès par carte électronique (cartes de proximité, claviers de contrôle d'accès codés); et
- Le périmètre de l'installation ou les points d'accès aux limites (portes des véhicules, tourniquets pour piétons).

Une combinaison de ces éléments peut être utilisée pour accroître ou renforcer l'efficacité globale de toute stratégie de gestion de l'accès.

7.1. Protection, détection, réponse et rétablissement (PDRR)

Les ministères et organismes devraient intégrer des éléments de protection, de détection, réponse et de rétablissement (PDRR) dans leur stratégie de gestion de l'accès. Pour en savoir plus, consultez le Guide de la GRC GSMGC-019 Guide de Protection, Détection, Réponse, et Récupération :

- La protection est assurée par l'utilisation d'obstacles physiques, procédurales et psychologiques pour retarder ou dissuader l'accès non autorisé;
- La détection implique l'utilisation de dispositifs, de systèmes et de procédures appropriés pour signaler qu'une tentative ou un accès non autorisé a eu lieu;
- Réponse implique la mise en œuvre de mesures pour s'assurer que les incidents de sécurité sont traités immédiatement. La mesure réponse comprend le signalement aux responsables de la sécurité appropriés et veille à ce que des mesures correctives immédiates et à long terme soient prises en temps opportun
- Le rétablissement fait référence au rétablissement des niveaux complets de prestation de services à la suite d'un incident.

Les PON des ministères et organismes devraient être claires pour s'assurer que les interventions appropriées sont activées en cas d'accès non autorisé détecté. Les incidents de sécurité doivent être signalés au coordonnateur de la sécurité de l'organisation en remplissant et en soumettant un rapport d'incident de sécurité. Quelques exemples de violations du contrôle d'accès comprennent, sans s'y limiter:

- Accès non autorisé;
- Les clés perdues ou volées, la carte d'accès à l'immeuble ou la carte d'identité;
- Toute altération connue ou soupçonnée des systèmes et dispositifs de sécurité mécaniques; et
- Toute altération connue ou soupçonnée des systèmes et dispositifs de sécurité électronique.

7.2. Cartes d'identité et d'accès

Le DSM, Annexe C : Procédures obligatoires pour le contrôle de la sécurité matérielle, oblige les ministères et organismes à mettre en œuvre des mesures pour assurer l'accès à l'information du GC. Les biens et les installations sont réservés aux personnes autorisées par la délivrance de cartes d'identité pour les employés et les cartes d'accès, pour les employés et d'autres personnes autorisées, pour l'accès contrôlé et surveillé aux zones ou installations réglementées.

Les cartes d'identité visent à distinguer les employés d'un ministère ou d'un organisme des personnes appartenant à un autre ministère, à un autre organisme ou au grand public qui nécessiteraient une autorisation et une supervision distinctes sur les lieux. Seules les personnes ayant une cote de sécurité valide du GC et employées par le ministère ou l'organisme sont admissibles à une carte d'identité.

Les cartes d'accès sont destinées à permettre au titulaire d'entrer dans tout espace/zone(s) restreint(s) selon le principe du besoin d'accès. Les cartes d'accès peuvent également être utilisées par les entrepreneurs, personnel de livraison ou les visiteurs d'une installation du GC.

Les ministères et organismes peuvent également utiliser une carte d'identité et une carte d'accès combinées pour le personnel, pourvu que les capacités minimales, décrites à la section 7.4 Systèmes d'accès électroniques, soient respectées.

Les caractéristiques physiques communes et uniques des cartes d'identification et d'accès se trouvent dans Annexe B de ce guide. Les utilisations appropriées et les pratiques exemplaires se trouvent dans Annexe C.

7.3. Systèmes d'accès mécaniques

Les mesures mécaniques pour contrôler l'accès impliquent l'utilisation d'une barrière physique à un point d'entrée. Des exemples de ces barrières comprennent les portes, les tourniquets et les portails. Lorsqu'elles sont utilisées pour le contrôle d'accès, ces barrières doivent être combinées à des moyens supplémentaires pour permettre ou refuser l'accès. Cela peut inclure le personnel de réception ou les agents de sécurité, les systèmes d'accès électroniques ou les moyens mécaniques.

Le moyen mécanique le plus courant pour contrôler l'accès est la serrure à clé. Lorsque des serrures à clé sont utilisées pour le contrôle d'accès, le contrôle de qui a accès aux clés devient critique. Si les clés peuvent être facilement copiées, le contrôle de l'accès ne peut pas être garanti. De même, si une clé est perdue, prêtée ou volée, il y a un risque d'accès non autorisé et la serrure doit être remplacée. Si la clé perdue est une clé principale, un plus grand nombre de points d'accès seront affectés. Néanmoins, si le bon contrôle des clés est assuré par un système centralisé, les serrures mécaniques à clé peuvent être une méthode efficace et peu coûteuse pour contribuer à la gestion de l'accès.

Les serrures à combinaison, souvent sous la forme d'un clavier à combinaison à bouton-poussoir, sont une alternative aux serrures à clé. Ceux-ci sont vulnérables en ce sens que les personnes non autorisées peuvent apprendre les combinaisons, ce qui limite leur efficacité en fonction de la sensibilisation à la sécurité des utilisateurs. Les combinaisons ne doivent pas être consignées à l'endroit où elles peuvent être trouvées par d'autres personnes. Les serrures doivent être placées de façon à réduire au minimum le risque d'être épier. Pour une protection supplémentaire, les combinaisons doivent être fréquemment modifiées.

De plus amples informations sur le matériel de verrouillage et les exigences de contrôle des clés sont décrites dans GSMGC 010 – Guide opérationnel de la sécurité matérielle.

7.4. Systèmes d'accès électronique

Les systèmes de contrôle d'accès électronique comprennent souvent un certain nombre de caractéristiques qui ne se trouvent pas dans les systèmes mécaniques. Certaines de ces caractéristiques comprennent:

- La capacité d'identifier et d'enregistrer où la saisie a été effectuée et avec quelle clé ou dispositif ;
- La capacité de permettre ou de refuser l'accès selon l'heure de la journée;

- La possibilité de modifier l'autorisation d'accès sans modifier le matériel;
- La capacité de surveiller l'état d'une porte pour indiquer si elle est ouverte, fermée, verrouillée;
- La capacité d'indiquer les tentatives non autorisées d'accès (porte ouverte trop longtemps, entrée forcée);
- La capacité de lier la clé, la carte d'accès ou l'appareil à des renseignements sur la personne à qui il est attribué (par exemple, photographie, statut de l'employé, niveau d'accès accordé); et
- La possibilité d'etre integré à d'autres dispositifs de sécurité électroniques tels que la vidéosurveillance. Cela peut également restreindre l'accès aux différentes zones accessibles uniquement pour l'utilisateur spécifique.

Dans certaines situations, il peut être moins coûteux et plus efficace d'utiliser des systèmes électroniques pour contrôler l'accès. L'exigence la plus importante pour que les systèmes électroniques soient efficaces est une conception physique appropriée, facile à utiliser, combinée à la conformité appropriée par des utilisateurs formés.

En règle générale, avec un système de gestion électronique de l'accès, l'utilisateur doit présenter une carte d'accès, un code ou un autre élément - appelé clé - à un point d'entrée, que le système peut identifier. Les composants qui peuvent être inclus dans ces systèmes sont:

7.4.1. Claviers

En règle générale, un clavier est monté près d'un point d'entrée, mais certaines installations peuvent avoir des claviers autonomes. Les utilisateurs autorisés entrent leur code d'entrée pour obtenir l'accès. Le système est relativement peu coûteux, mais vulnérable si les codes d'entrée sont génériques parmi tout le personnel, partagés par l'utilisateur, devinés ou épiés. La meilleure pratique consiste à utiliser un système de gestion des codes NIP (numéro d'identification personnel) qui fournit des codes NIP individuels à chaque membre du personnel.

7.4.2. Cartes d'accès électroniques/lecteur de carte de proximité

Les cartes d'accès électroniques, ou cartes de proximité, sont présentées à un lecteur de carte à un point d'entrée. Une base de données connectée au lecteur identifie les informations sur le titulaire de la carte, y compris le droit d'accès à ce point d'entrée particulier. Si une carte est perdue ou volée, les privilèges de cette carte peuvent être facilement modifiés dans la base de données sans modification du point d'entrée ou du lecteur. Actuellement, la forme la plus courante de contrôle d'accès électronique, les cartes d'accès sont souvent utilisées en combinaison avec des codes NIP individuels et / ou une carte d'identification / d'accès combinée.

7.4.3. Biométrie

Les dispositifs biométriques peuvent garantir que la personne qui demande l'entrée n'utilise pas la carte d'accès ou le code d'une autre personne. Il le fait en exigeant que la personne présente une caractéristique physique à un lecteur. Il peut s'agir d'un balayage oculaire, d'une empreinte digitale, d'une empreinte de main ou d'un visage

qui peut être reconnu et authentifié par le système. Les systèmes biométriques sont parfois lents ou peu pratiques et souvent plus coûteux que les autres systèmes. Ils peuvent ne pas bien fonctionner pour tous les utilisateurs, car certaines personnes ont des caractéristiques physiques qui rendent difficile leur inscription dans le système. Les systèmes biométriques sont généralement moins appropriés pour les zones à fort trafic, et plus appropriés lorsqu'il y a un nombre limité d'utilisateurs et des exigences de sécurité relativement élevées pour contrôler l'accès. Les ministères et organismes du GC devraient effectuer une évaluation des facteurs relatifs à la vie privée (ÉFVP) lorsqu'ils envisagent l'introduction de systèmes biométriques.

7.5. Matériel de verrouillage du contrôle d'accès

En plus de la capacité d'identifier qui a le droit d'entrer dans une zone, un système de gestion électronique de l'accès comportera également des éléments mécaniques pour accorder cet accès. Ceux-ci peuvent inclure:

7.5.1. Serrures électriques

Les serrures électriques permettent à une poignée de porte de rétracter le loquet uniquement lorsqu'elle est autorisée par une carte d'accès (carte de proximité/puce), un code NIP, une lecture biométrique ou une combinaison de ceux-ci. Normalement, le loquet de la porte est immobile.

7.5.2. Gâches électriques

La grève est la partie de la quincaillerie de porte dans laquelle le loquet de porte s'adapte. Un système de gâche électrique peut permettre d'ouvrir la porte, dans laquelle le loquet de porte est immobile, en libérant la gâche sans exiger que le loquet soit rétracté. Semblable à une serrure électrique, cette activation nécessiterait l'utilisation d'une carte d'accès (proximité/puce), d'un code NIP, d'une lecture biométrique ou d'une combinaison de ces éléments.

7.5.3. Serrures électromagnétiques

Certaines portes sont maintenues fermées par des aimants électroniques. L'aimant est libéré lorsque le courant électrique est retiré de l'aimant. Bien qu'elles soient très strictes, les restrictions du code du bâtiment et des règlements sur les incendies peuvent limiter l'utilisation et la sécurité offertes par ce type de serrure si elles nuisent à l'évacuation lors d'un incident d'urgence (c.-à-d. évacuations en cas d'incendie), comme indiqué dans 6.4.2. D'alimentation d'urgencer.

7.5.4. Tourniquets/sas

Similaires aux caractéristiques mécaniques pleine hauteur pour ralentir physiquement ou empêcher l'accès, les tourniquets et les sas à commande électronique ont l'avantage supplémentaire de la surveillance à distance (via CCTV ou une salle de contrôle), de la désactivation à distance en cas d'alarme ou d'urgence, et l'identification de l'utilisateur.

L'avantage de l'utilisation de tourniquets est la réduction de la possibilité de talonnage. Le talonnage se produit lorsqu'un utilisateur autorisé entre par une porte et, pendant que la porte est en position ouverte, une autre personne passe sans être traitée par le système. Les tourniquets de contrôle d'accès sont conçus pour permettre à une seule personne d'entrer à la fois.

Les sas sont composés de deux portes séparées par un court couloir ou une passerelle. Généralement contrôlée par une carte d'accès (de proximité / puce), un code NIP, une lecture biométrique ou une combinaison de celles-ci, une seule porte peut être activée / ouverte à la fois pour entrer dans la zone. Les sas permettent à plusieurs utilisateurs d'entrer dans l'espace entre les portes en même temps, ce qui permet d'entrer un plus grand volume de personnel, mais augmente le risque d'incidents de talonnage. De même, si la porte intérieure est ouverte, pour que le personnel puisse sortir, le personnel non autorisé pourrait entrer dans une zone de sécurité matérielle. Les ministères et organismes devraient inclure des campagnes de sensibilisation et de formation régulières pour s'assurer que le personnel ne contrevient pas à ses propres procédures de gestion de l'accès.

7.6. Personnel de réception/Services de gardiens

L'utilisation de mécanismes et de systèmes de gestion de l'accès permet de gérer 24/7, de façon rentable le flux de personnel à l'intérieur d'une installation; toutefois, l'efficacité de ces systèmes se détériorera s'ils ne sont pas surveillés ou gérés par le personnel. Les ministères et organismes sont encouragés à élaborer des PON qui délèguent des rôles et des responsabilités au personnel chargé de surveiller et de gérer la gestion de l'accès de leurs installations.

7.6.1. Personnel de la réception

Le personnel de la réception, qui joue principalement un rôle d'interaction avec le public, doit bien connaître les PON de gestion de l'accès de l'établissement. Cette information devrait comprendre les mesures à prendre pour:

- Visiteurs préautorisés;
- Les visiteurs non annoncés et les demandes du grand public;
- Le personnel contractuel et de livraison;
- Le personnel des services d'application de la loi et des services d'urgence; et
- Le personnel ne détient pas/ne présente pas sa carte d'identité et/ou sa carte d'accès.

7.6.2. Services de gardes de sécurité

Si une EMR indique une exigence en matière de sécurité pour le recours à des agents de sécurité, les questions liées au type de garde (employé par le GC ou contractuel), aux tâches, à la formation, à l'équipement et à la sécurité doivent être abordées. Comme pour le personnel de la réception, les agents de sécurité offrent de la flexibilité et une couche supplémentaire à une stratégie de gestion de l'accès en agissant comme première ligne de défense dans la conception PDRR d'un ministère ou d'organismes.

Des PON pour la gestion de l'accès doivent être élaborées, en plus de celles énumérées à l'article 7.6.1, si les rôles et responsabilités énoncés ci-dessous sont inclus:

- Utilisation d'équipement de détection de métaux et/ou appareil de radiographie;
- L'utilisation d'une unité de manutention et de confinement du courrier;
- Fouille des personnes;
- Fouiller les véhicules;
- L'utilisation et la surveillance des systèmes de vidéosurveillance; et
- Intervention d'urgence (incendie, activités criminelles, incidents violents, urgences médicales).

Ces PON devraient également refléter les impacts des niveaux de menace plus élevés, comme indiqué à l'annexe A du présent guide.

7.7. Principes d'escorte de sécurité

Le personnel est autorisé à entrer dans un local du GC et/ou une zone de sécurité matérielle s'il détient les éléments suivants:

- Une autorisation de sécurité valide du GC et/ou un privilège d'accès décrits ci-dessus au point 5. Exigence d'accès (voir le tableau 1);
- Ils ont un besoin de savoir ou d'accès valide; et
- Ils ont l'autorisation d'entrer.

Important: Les personnes qui ne répondent pas à tous ces critères doivent être escortées par du personnel du GC qui respecte les trois (3) critères.

7.7.1. Techniques d'escorte

Les escortes de sécurité sont efficaces tant que les membres du personnel d'escorte utilisent les techniques appropriées. Les pratiques exemplaires comprennent les suivantes:

- Donner une séance d'information préalable pour informer le visiteur, l'entrepreneur ou l'invité des restrictions et des autres conditions d'accès;
- S'assurer que l'escorte possède les connaissances techniques ou propres au secteur pour reconnaître les activités non autorisées et les risques pour le personnel, les biens et l'information du GC (comme les salles de serveurs);
- S'assurer que les appareils électroniques et autres articles interdits sont remis, Le cas échéant, à l'installation ou à la zone;
- Maintenez le contact visuel du personnel escorté en tout temps et évitez les situations où il pourrait être inapproprié d'accompagner la personne (par exemple, les toilettes). La meilleure pratique consiste à employer des escortes de même sexe si possible dans ces circonstances;
- Tenir un registre des visiteurs de l'installation. Cela permet de comptabiliser correctement les personnes qui obtiennent l'accès et peut servir d'outil de référence rapide pour comptabiliser le personnel en cas d'urgence (évacuations en cas d'incendie); et

- Maintenir un moyen de communiquer avec d'autres membres du personnel ou du personnel de sécurité, si la zone le permet.

Important: Il est communément admis d'escorter les visiteurs dans une zone de sécurité matérielle pour rencontrer le personnel du GC. Après avoir remis le visiteur à l'hôte de la réunion, celui-ci est maintenant responsable de l'escorte continue du visiteur. Les ministères et organismes doivent inclure des directives sur ces situations dans leur PON sur la gestion de l'accès.

7.7.2. Violations d'escorte

Tout défaut d'escorter correctement un visiteur, un entrepreneur ou un invité à l'intérieur d'une installation du GC augmentera le risque de compromission de l'information ou des biens du GC. Les actions et comportements suivants ne doivent pas être autorisés:

- **Aucune escorte** - Ne jamais laisser une personne escortée sans surveillance ni lui permettre de dicter où elle se rendra à l'intérieur de l'installation;
- **Distractions** – Une escorte doit rester attentive à son environnement et à la personne sous escorte. Il faut éviter les distractions (lire un livre, utiliser un appareil sans fil, converser avec d'autres membres du personnel, etc.);
- **Nombre inférieur d'accompagnateurs** – de grands groupes de visiteurs ou d'entrepreneurs qui doivent travailler dans des endroits différents ne peuvent pas être escortés correctement par une seule personne. La meilleure pratique consiste à fournir des escortes supplémentaires pour surveiller à partir de points de vue distincts et/ou à diviser le groupe en petits groupes qui restent ensemble tout au long de l'escorte;
- **Discuter de l'information du GC** – toute information du GC discutée qui n'est pas liée au but de la visite doit être évitée. Cela peut constituer une atteinte à la sécurité de l'information; et
- **Entrepreneurs escortant des entrepreneurs** – Sauf si le personnel contractuel ou le personnel de sécurité détient une cote de sécurité valide du GC (Secret/Très Secret), l'escorte doit être limitée à la ZP et à la ZA seulement. Le personnel contractuel et les agents de sécurité devraient avoir les tâches détaillées dans le contrat de service et PON.

8. Programmes de sensibilisation à la sécurité pour la gestion de l'accès

Les ministères et organismes devraient avoir un programme de sensibilisation à la sécurité, conformément à leur EMR, qui garantit que tous les employés savent qu'ils font partie du programme de gestion de l'accès. Les PON et les campagnes de sensibilisation à la sécurité, élaborées par le coordonnateur de la sécurité, devraient mettre l'accent sur la connaissance de la situation, ce qui comprend, sans s'y limiter, les éléments suivants:

- Les mesures que le personnel doit prendre lorsqu'il prend connaissance de personnes sans autorisation dans ses installations;

- Que les cartes d'identité, les cartes d'accès et les clés mécaniques ne sont pas partagées avec d'autres personnes;
- Veiller à ce que les personnes non autorisées ne se glissent pas dans une zone réglementée.
- Ne pas oublier qui se trouve à proximité lorsque vous discutez de renseignements de nature délicate;
- Remettre en question les personnes qui ne portent pas ou n'affiche pas de carte d'accès approuvée;
- S'assurer que les portes, qui sont normalement verrouillées, ne sont pas maintenues ouvertes ou autrement désactivées;
- S'assurer que les alarmes sont activées lorsqu'un espace est inoccupé, le cas échéant;
- S'assurer que les portes et les contenants de sécurité sont bien verrouillés;
- Signaler les incidents de sécurité, y compris les accès non autorisés, le vol ou la perte de cartes d'identité, de cartes d'accès à l'immeuble, de clés mécaniques, etc. à leur équipe de sécurité; et
- Effectuer les tâches d'escorte nécessaires.

9. Références et documents connexes

- Politique sur la sécurité du gouvernement – https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578.
- Directive sur la gestion de la sécurité - https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32611
- Directive sur la gestion de l'identité - https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=16577
- Directive sur l'évaluation des facteurs relatifs à la vie privée - https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=18308
- Directive sur l'obligation de prendre des mesures d'adaptation - https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32634
- Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion dans la fonction publique fédérale - https://www.canada.ca/fr/conseil-prive/organisation/greffier/appel-action-faveur-lutte-contre-racisme-equite-inclusion-fonction-publique-federale.html
- Guide à l'intention des employés deux esprits, transgenres, non-binaires et de la pluralité des genres dans la fonction publique fédérale - https://publicservicepride.ca/fr/guide/
- Manuel du Programme de coordination de l'image de marque - https://www.canada.ca/fr/secretariat-conseil-tresor/services/communications-gouvernementales/programme-federal-image-marque/manuel.html
- Identification du personnel - Norme graphique du Programme fédéral de l'image de marque - https://www.canada.ca/fr/secretariat-conseil-tresor/services/communications-gouvernementales/norme-graphique/identification-personnel-norme-graphique-pfim.html
- Norme sur le filtrage de sécurité – https://intranet.canada.ca/pol/doc-fra.aspx?id=28115&section=glossary
- Code national de prévention des incendies - Canada 2020-

https://www.publications.gc.ca/site/fra/9.897550/publication.html

- Niveaux nationaux de la menace terroriste pour le Canada - https://www.canada.ca/fr/services/defense/securitenationale/niveau-menace-terroriste.html
- GSMGC-004 Guide sur les considérations liées à l'éclairage de sécurité (rcmp-gfc.gc.ca)
- GSMGC-007 Transport, transmission et entreposage (rcmp-grc.gc.ca)
- GSMGC-009 Guide sur les considérations liées aux clôtures de sécurité (rcmp-grc.gc.ca)
- GSMGC-010 Guide opérationnel de la sécurité matérielle (rcmp-grc.gc.ca)
- GSMGC-015 Guide pour l'établissement des zones de sécurité matérielle (rcmp-grc.gc.ca)
- GSMGC-019 Guide de Protection, Détection, Réponse, et Récupération

Annexe A - Réagir à des niveaux de menace plus élevés

En plus de respecter le niveau de sécurité de base établi dans la Politique sur la sécurité du gouvernement les ministères et organismes doivent être en mesure de répondent aux déclarations de niveaux de sécurité accrus. Ces mesures accrues sont décrites dans le GSMGC-010 Guide opérationnel de la sécurité matérielle et Niveaux nationaux de la menace terroriste pour le Canada.

Les ministères et organismes devraient tenir compte des mesures de protection de la gestion de l'accès suivantes pendant les périodes de menace accrue et/ou lorsqu'une augmentation de la disponibilité opérationnelle est prévue. Ces procédures sont des pratiques exemplaires suggérées qui devraient être prises en considération dans le cadre de la réponse au besoin d'une préparation accrue.

1. Niveau de menace très faible/faible

Les opérations quotidiennes sont considérées comme la base de référence des procédures de gestion de l'accès; elles sont appuyées par une EMR. Au cours de cette période, les ministères et organismes sont encouragés à promouvoir la sensibilisation au cours des séances initiales d'intégration, des séances de mise à jour périodiques ou des séances de sensibilisation, et des exercices pratiques pour les employés de tous les niveaux de l'organisation.

Les rapports de rassemblement doivent également être produits par l'équipe de sécurité du ministère ou de l'organisme et/ou le locataire et/ou le personnel de sécurité (les personnes qui ont accès aux systèmes de contrôle d'accès) pendant les situations d'urgence pour assurer la santé et la sécurité des employés. Cette fonction de rapport devrait être exécutée pendant chaque exercice d'évacuation afin de cerner les lacunes en matière de sensibilisation ou de formation et d'intégrer la comptabilité du personnel en cas d'urgence dans l'état d'esprit du ministère et de l'organisme.

Selon l'urgence, il peut être nécessaire de s'abriter sur place plutôt que de quitter l'installation. Par exemple, des conditions météorologiques extrêmes, des manifestations violentes ou un tireur actif à l'extérieur de l'installation. Chaque installation devrait avoir identifié des endroits où les occupants pourraient se rassembler. Ces zones sont conçues avec des structures de mur isolées pour fournir une protection supplémentaire contre la menace et ont tendance à être à l'intérieur de la structure.

2. Niveau de menace modéré

Pendant le niveau de menace moyen, les ministères et organismes devraient envisager de faire preuve d'une vigilance accrue dans l'application des mesures de protection utilisées pour gérer l'accès aux niveaux inférieurs. Voici quelques exemples de vigilance accrue :

- Accroître le niveau d'observation aux points d'accès où des cartes d'accès ou des contrôles d'accès électroniques sont utilisés;
- Employer des gardes supplémentaires au besoin;
- S'assurer que la carte d'accès de chacun est bien visible;

- Changer les codes d'accès et/ou les combinaisons sur les serrures;
- Vérifier l'emplacement des clés et s'assurer qu'elles n'ont pas été perdues; et
- Assurer une vérification plus approfondie de l'identité des visiteurs.

Les ministères et organismes devraient également faire preuve de plus de vigilance dans le contrôle des colis reçus afin d'identifier les articles suspects. Une formation supplémentaire pourrait être offerte au personnel sur la façon de repérer les colis suspects. Les procédures à suivre une fois qu'un article suspect a été reçu pourraient également être examinées pour s'assurer que le personnel est pleinement conscient de ses responsabilités.

3. Niveaux de menace élevé et critique

Les ministères et organismes devraient préparer des plans d'urgence qu'ils pourraient mettre en œuvre pendant les périodes de niveaux de menace élevés et critiques. En préparant ces plans, les ministères et organismes devraient tenir compte des éléments suivants:

3.1. Restrictions relatives au personnel

Fournir un accès uniquement au personnel essentiel.

Les ministères et organismes devraient envisager de réduire le nombre d'employés sur place pour assurer la sécurité du plus grand nombre possible d'employés. Pour ce faire, les ministères et organismes pourraient identifier les personnes qui doivent être sur place pour maintenir les services essentiels et permettre seulement à ces personnes d'accéder à l'installation. D'autres dispositions pourraient être prises pour tous les autres membres du personnel, se rendre à un autre établissement, le travail à domicile ou, si ces solutions de rechange ne sont pas disponibles, le fait de ne pas se présenter au travail avant d'en avoir été avisé autrement.

3.2. Restrictions de zone

Restreindre l'accès aux zones essentielles seulement.

Afin de fournir des services essentiels, toutes les zones d'une installation peuvent ne pas être nécessaires. Afin d'accroître la sécurité du personnel, les ministères et organismes pourraient vouloir restreindre l'accès d'un étranger à certaines zones. Un quai de chargement, par exemple, pourrait être considéré comme non essentiel en cas d'urgence. Les livraisons pourraient être tenues à l'écart de l'installation et le personnel de livraison pourrait être prié de revenir à une date ultérieure. L'accès à la zone de chargement ne serait pas autorisé, sauf pour le personnel de sécurité.

3.3. Restrictions relatives aux points d'entrée

Réduire le nombre et augmenter le niveau de contrôle aux points d'entrée.

Dans les installations comportant un certain nombre de points d'entrée de périmètre, le contrôle de l'accès peut être amélioré en éliminant certains points d'accès. Par exemple, une installation peut avoir un contrôle d'accès électronique installé à une porte d'entrée ainsi qu'une porte latérale adjacente à un stationnement. L'accès par la porte latérale pourrait être retiré, et tout le monde pourrait être obligé d'entrer par la porte d'entrée. Les contrôles à la porte d'entrée pourraient alors être augmentés pour inclure une présence accrue des gardes et

assurer la vérification des cartes d'accès.

3.4. Contrôle

Enregistrer l'accès et la sortie.

Il faut tenir un registre de tout le personnel entrant et sortant. En plus de fournir des renseignements sur les personnes qui ont eu accès à l'installation et sur le moment où elles y étaient, les dossiers indiquent qui se trouve dans l'installation en cas d'urgence. Cet enregistrement peut produire des rapports de rassemblement en cas d'urgence.

3.5. Codes et combinaisons

Changer les codes NIP / combinaisons sur les serrures qui contrôlent l'accès.

Les serrures à combinaison et les codes NIP sont vulnérables à l'apprentissage par des personnes non autorisées. Cette menace est réduite lorsque la combinaison et / ou le code NIP est modifié et soigneusement communiqué uniquement aux utilisateurs autorisés. Lorsqu'un niveau de menace accru est déclaré, cette procédure doit être répétée pour s'assurer que l'accès est réservé au personnel autorisé.

3.6. Périodes d'accès

Limiter les périodes d'accès.

À des niveaux de menace très faibles et faibles, il se peut que l'accès au personnel en dehors des heures normales de travail soit un risque acceptable. Cela devrait être examiné à des niveaux de menace plus élevés, tandis que les ministères et organismes devraient envisager de réduire le personnel ayant des privilèges d'accès en dehors de la journée de travail normale.

4. Entrée et sortie graduelles

Les ministères et organismes sont encouragés à développer des plans qui intègrent à la fois l'augmentation et la diminution des mesures utilisées pendant les périodes de menace accrue ou réduite. Toute diminution de l'efficacité opérationnelle découlant de l'utilisation de contre-mesures pendant un niveau de menace plus élevé, pour protéger la sécurité du personnel, devrait être limitée dans la durée afin d'éviter la complaisance et d'accroître l'adhésion du personnel. La préparation de plans pour une réduction progressive des contre-mesures, si elles sont appuyées par l'environnement ou l'EMR, aidera les décideurs à atteindre cet équilibre.

Annexe B – Caractéristiques de la carte d'identification et d'Accès

Un outil efficace pour identifier les personnes autorisées à entrer dans une installation, les cartes d'identification et d'accès sont similaires dans la conception et l'utilisation; mais ont des fins très distinctes dans les systèmes de gestion de l'accès. Les ministères et les organismes doivent veiller à ce qu'une application uniforme de la gestion de l'identité soit utilisée dans l'élaboration de leurs programmes d'identification et de cartes d'accès respectifs; à l'appui du Secrétariat du Conseil du Trésor du Canada Directive sur la gestion de l'identité, Directive sur la gestion de la sécurité, Annexe C : Procédures obligatoires pour le contrôle de la sécurité physique, et Norme de conception du Programme de coordination de l'image de marque.

1. Caractéristiques physiques

Au minimum, les cartes d'identité et d'accès pour les employés du GC doivent contenir:

- Le nom de la personne;
- Photographie en couleur ou image numérisée;
- La date d'expiration (de trois à cinq ans à compter de la date de délivrance); et
- Un numéro propre à la carte.

Voir le Tableau 2 pour obtenir des renseignements sur des caractéristiques comparables.

Les champs de renseignements supplémentaires doivent assurer que chaque élément est justifiable en vertu de la législation existante, c.-à-d. la date de naissance ou les descripteurs physiques. La photographie du porteur doit fournir une vue frontale de la tête/du visage et du haut des épaules.

Toutes les informations sur les cartes doivent être écrites à la machine sans effacements ni modifications. Les ministères et organismes peuvent choisir d'omettre une signature sur une carte d'identité en fonction de l'EMR ou des besoins opérationnels du ministère ou de l'organisme. Sur les cartes d'accès, l'emplacement de l'installation peut être identifié, mais la meilleure pratique consiste à omettre l'emplacement.

La taille de la carte pour les deux doit être au moins conforme aux normes de l'industrie (comme CR80, 54 mm x 86 mm, semblable aux cartes de crédit ou de débit); tout en permettant aux cartes d'accès d'être plus grandes en taille et une photographie sensiblement plus grande que les cartes d'identification s'il est nécessaire de pouvoir vérifier visuellement la carte à distance.

Les renseignements requis sur la carte de visiteur/Escorte requise peuvent être limités au nom du ministère ou de l'organisme, aux privilèges d'emplacement, à la date d'expiration et au numéro de carte unique. Ces cartes sont émises et récupérées quotidiennement.

2. Caractéristiques de sécurité

Si une EMR indique que des dispositifs de sécurité supplémentaires sont requis pour les cartes d'identification ou d'accès, les dispositifs de sécurité incorporés ne doivent pas entraîner de défauts, obscurcir les informations imprimées ni entraver l'accès aux informations lisibles par machine. Les caractéristiques de sécurité disponible comprennent:

- Des ratios plus élevés de plastique et de résine utilisés dans le matériau stratifié;
- Filigranes et hologrammes;
- Gravures au laser et images visibles uniquement sous un éclairage spécial; et
- Conceptions optiques difficiles à modifier ou à manipuler.

Tableau 2 – Caractéristiques des cartes d'identité et d'accès

Feintes d'information	Carte d'identification	Carte d'accès	Carte combinée (ID et carte d'accès)	Visiteur, entrepreneur ou accompagnateur requis
nom du particulier	Doit	Devrait	Doit	Autorisé
Signature de la personne	Devrait	Autorisé	Devrait	Autorisé
Photographie couleur / Image numérisée	Doit	Devrait	Doit	Autorisé
Nom du ministère ou de l'organisme émetteur	Doit	Autorisé	Doit	Doit
Privilège de localisation - couleurs, forme de badge, codes	Jamais	Autorisé	Autorisé	Autorisé
date d'expiration	Doit	Devrait	Doit	Doit
numéro de carte unique	Doit	Doit	Doit	Doit
date de naissance	Autorisé	Autorisé (mois et année seulement)	Autorisé	S/O

3. Modifications apportées aux cartes Accès

Les ministères et les organismes peuvent choisir de percer une ouverture dans le corps de la carte d'accès pour permettre de la porter sur un cordon. Les ministères et organismes devraient veiller à ce que ces modifications soient étroitement coordonnées avec le fournisseur et/ou le fabricant de la carte afin de s'assurer que l'intégrité du matériel de la carte n'est pas compromise. Il est recommandé aux ministères et organismes de s'assurer que de telles modifications ne:

- Compromettre les exigences et les caractéristiques de durabilité du corps de la carte;
- Invalider les garanties du fabricant de la carte ou d'autres allégations relatives aux produits;
- Modifier ou interférer avec l'information imprimée, y compris la photo; et
- Endommager ou interférer avec la technologie lisible par machine, comme l'antenne ou la puce intégrée.

Les employés ne doivent pas modifier leur carte d'accès ou leur carte d'identité.

Annexe C : Gestion des cartes d'identification et d'Accès

Voici les pratiques exemplaires que les ministères et organismes pourraient utiliser pour accroître l'efficacité de leurs programmes de gestion de l'accès.

1. Programme de sensibilisation

Les ministères et organismes devraient avoir un programme de sensibilisation à la sécurité qui fait en sorte que tous les employés connaissent le système de cartes d'identité et/ou d'accès de l'organisation et leurs responsabilités dans le bon fonctionnement d'un tel système. Ce programme devrait comprendre:

- Familiarisation avec chaque type de carte (p. ex., employé, visiteur, entrepreneur, etc.);
- L'accès accordé par chaque type de carte d'accès;
- Les exigences relatives à l'utilisation et à l'affichage appropriés;
- Les responsabilités du titulaire de la carte;
- La sensibilisation au fait que les cartes d'identité et les clés mécaniques ne sont pas partagées avec d'autres personnes; et
- Les procédures à suivre en cas d'infraction, de perte ou de vol.

2. Gestion des cartes

Chaque ministère et organisme doit établir des procédures pour la bonne administration des cartes d'identité et d'accès. Ces procédures devraient comprendre les éléments suivants:

2.1. Procédures de traitement

- Établir un processus de délivrance et de récupération des cartes d'identité et d'accès; veiller à ce qu'un registre soit tenu sur la date de délivrance, l'identité du titulaire, le numéro de la carte, la date d'expiration/renouvellement et, au besoin, l'autorisation de sécurité du titulaire;
- Vérifier au moment de la délivrance de l'identité de la personne, que le niveau d'autorisation de sécurité approuvé est valide et tenir une séance d'information sur l'utilisation responsable de la carte d'identité ou d'accès par le titulaire;
- Fournir des lignes directrices sur le retrait de cartes pour un motif valable (menace interne);
- Assurez-vous de récupérer les cartes au moment de la cessation d'emploi, du contrat ou lorsque vous n'en avez plus besoin. S'assurer que les cartes sont en bon état de service que jusqu'à la date d'expiration ou de résiliation;
- S'assurer que tout l'équipement nécessaire à l'activation ou à la délivrance des cartes est protégé physiquement à un niveau égal à celui des renseignements et des biens classifiés ou protégés auxquels les cartes activées ou émises pourraient être accessibles, selon une EMR;
- S'assurer qu'un processus est établi pour interdire le retrait des cartes d'accès de l'installation en fonction d'une EMR;
- Établir un processus pour détruire toutes les cartes et cartes périmées ou endommagées;

et

- Veiller à ce qu'aucun responsable du processus ne puisse délivrer une carte d'identité ou d'accès à une personne.

2.2. Éviter les cartes en double

Pour bien contrôler l'accès à une installation du GC, les ministères et organismes doivent limiter la délivrance de cartes d'identité et d'accès à une carte par personne ou à une carte combinée dans le cadre du programme de gestion de l'accès. À moins d'une EMR, l'émission de cartes supplémentaires augmente le risque d'accès non autorisé en raison d'un manque de contrôle positif de ces articles.

2.3. Photographie

Les photographies sur les cartes d'accès doivent être aussi grandes que possible pour faciliter une confirmation visuelle rapide du titulaire de la carte d'accès. Les couvre-chefs, qui ne font pas partie d'une obligation religieuse ou d'une coutume culturelle (par exemple, le hijab, le turban, ou la coiffe autochtone) doivent être retirés pour les photos d'identification et de carte d'accès. Il est acceptable de porter des lunettes; toutefois, les verres teintés ou les lunettes de soleil ne devraient pas être portés à moins que la personne ait une exigence certifiée de porter ce style de verres correcteurs. Les arrière-plans photographiques doivent être de nature neutre et permettre un contraste avec le teint de la personne.

2.4. Cartes expirées

Pour empêcher les employés d'être refuser inutilement l'accès, un programme de renouvellement devrait être intégré au programme de gestion des cartes. Fournir un rappel ou un horaire de renouvellement six mois avant la date d'expiration de la carte d'identité et/ou d'accès devrait empêcher le personnel de le faire. Assurez-vous que les cartes ne sont pas réémises jusqu'à ce que la cote de fiabilité ou de sécurité soit vérifiée et que la personne ait toujours droit à la ou aux cartes. Une fois la nouvelle carte enregistrée et remise au titulaire, la carte expirée doit être identifiée comme non valide dans le système de gestion des cartes et détruite.

2.5. Cartes perdues

Si une pièce d'identité ou une carte d'accès est trouvée, le localisateur doit la retourner au bureau de sécurité ou au point de contact approprié. Si un employé perd sa carte d'identité ou d'accès, il doit en informer immédiatement son gestionnaire/superviseur et l'unité ou le bureau de sécurité du ministère. Dans la mesure du possible, le titulaire de la carte doit indiquer la dernière fois qu'il a utilisé ou était en sa possession. La carte doit être annotée comme perdue/manquante dans le système de gestion des cartes, désactivée (s'il s'agit d'une carte d'accès électronique/de proximité) et remplacée.

3. Utilisation de la carte Accès

3.1. Présenter

Une politique exigeant que les cartes soient portées autour du cou encouragera les employés à participer au contrôle des procédures d'accès. Si des préoccupations en matière de santé et de sécurité sont associées au port de cartes autour du cou (travail autour d'équipement lourd), des mesures de rechange seront nécessaires. Les cordons, les bobines de cartes rétractables, les mousquetons ou les pinces utilisés pour contenir les cartes ne doivent pas comporter de marques ministérielles ou d'agences identifiables.

3.2. Vérification de l'identité visuelle et de la carte

Dans les circonstances où une vérification visuelle de l'identité du titulaire de carte peut être nécessaire pour déterminer si la personne identifiée doit être autorisée à entrer, ces étapes peuvent être appliquées:

- Déterminer si la carte semble authentique, n'a pas été modifiée de quelque façon que ce soit, en analysant un ou plusieurs éléments de données sur la carte (nom, affiliation de l'employé, code d'identification d'emploi, numéro de série de la carte, identification de l'émetteur, nom de l'agence);
- Comparer les traits du visage du titulaire de carte avec la photo sur la carte pour s'assurer qu'ils correspondent;
- Vérifier la date d'expiration de la carte pour s'assurer qu'elle n'a pas expiré.
- Comparer les descriptions des caractéristiques physiques du titulaire de carte à celles du titulaire de carte (facultatif);
- Recueillir la signature du titulaire de carte et la comparer à celle de la carte (facultatif); et
- Vérifier auprès d'une autorité si l'accès doit être accordé au titulaire de carte au besoin (p. ex., le nom ne figure pas sur une liste d'accès).

3.3. Cartes d'accès des visiteurs et des entrepreneurs

Les personnes qui doivent accéder à l'installation ou au complexe doivent faire vérifier leur identité par le personnel de sécurité et déposer une pièce d'identité valide avec photo émise par le gouvernement avant de recevoir une carte d'accès. Les employés doivent être tenus d'enregistrer les visiteurs et les entrepreneurs et d'être responsables de la carte d'accès. Contrairement à une carte d'accès d'employé avec une photo, les cartes d'accès de visiteur/entrepreneur peuvent être utilisées par un certain nombre de personnes. Afin de s'assurer que les cartes représentent une personne dûment autorisée, il faut maintenir un contrôle efficace sur le nombre et l'emplacement des cartes d'accès.

Lorsqu'il est question de l'identité d'un visiteur, il est recommandé de communiquer avec son organisme d'attache pour vérifier son identité. Un visiteur peut demander l'accès, en prétendant qu'ils proviennent d'une organisation spécifique (compagnie de téléphone, compagnie de maintenance ou compagnie de service). Un appel téléphonique à cette organisation, confirmant que la personne travaille effectivement pour elle et qu'elle y a été envoyée, réduirait le risque que cette personne tente d'entrer sans autorisation.

Des cartes peuvent être délivrées aux visiteurs/entrepreneurs indiquant qu'ils ont obtenu une autorisation temporaire pour accéder à une zone. Ils doivent être escortés dans une ZT, une ZS ou une ZHS, à moins d'avoir obtenu la cote de sécurité appropriée et d'avoir obtenu l'accès par l'autorité ministérielle ou l'organisme approprié.

10. Promulgation

Examiné et recommandé aux fins d'approbation.

J'ai examiné et recommande par la présente, GSMGC-006 (2024) Guide de Gestion de l'Accès pour approbation.

Nattress,Shawn Thomas,000302786 Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2024.01.12 13:48:54 -05'00'

Shawn Nattress, Date
Gestionnaire
Principal Organisme Responsible de la Sécurité Materielle, GRC

Approuvé

J'approuve par la présente GSMGC-006 (2024) Guide de Gestion de l'Accès.

St-Pierre,Andre Vincent,000171484 Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.01.19 13:44:17 -05'00'

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