



RETURN BIDS TO:

RETOURNER LES SOUMISSIONS À:

**Bid Receiving - PWGSC / Réception des soumissions -
TPSGC**

11 Laurier St./11, rue Laurier

Place du Portage, Phase III

Core 0B2 / Noyau 0B2

Gatineau

Québec

K1A 0S5

Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT

MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

**THIS DOCUMENT CONTAINS A SECURITY
REQUIREMENT**

Vendor/Firm Name and Address

**Raison sociale et adresse du
fournisseur/de l'entrepreneur**

Issuing Office - Bureau de distribution

Special Projects/Projets Spéciaux

Terrasses de la Chaudière 4th Floor

10 Wellington Street

Gatineau

Québec

K1A 0S5

Title - Sujet RCMP Group Life Insurance	
Solicitation No. - N° de l'invitation M7594-192673/A	Amendment No. - N° modif. 004
Client Reference No. - N° de référence du client M7594-192673	Date 2019-11-25
GETS Reference No. - N° de référence de SEAG PW-\$\$ZL-103-36918	
File No. - N° de dossier 103zl.M7594-192673	CCC No./N° CCC - FMS No./N° VME
Solicitation Closes - L'invitation prend fin at - à 02:00 PM on - le 2019-12-02	
Time Zone Fuseau horaire Eastern Standard Time EST	
F.O.B. - F.A.B. Plant-Usine: <input type="checkbox"/> Destination: <input type="checkbox"/> Other-Autre: <input type="checkbox"/>	
Address Enquiries to: - Adresser toutes questions à: Paré, Lindsay	Buyer Id - Id de l'acheteur 103zl
Telephone No. - N° de téléphone (613) 314-8028 ()	FAX No. - N° de FAX () -
Destination - of Goods, Services, and Construction: Destination - des biens, services et construction:	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	Delivery Offered - Livraison proposée
Vendor/Firm Name and Address Raison sociale et adresse du fournisseur/de l'entrepreneur	
Telephone No. - N° de téléphone Facsimile No. - N° de télécopieur	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)	
Signature	Date

Modification 004
Invitation M7594-192673/A

Cette modification vise à:

- 1) répondre aux questions des fournisseurs concernant cette invitation, comme cela indiqué à la section A.

SECTION A

Questions et réponses

Question 10

L'entrepreneur doit fournir une installation de secours pour les serveurs où tous les dossiers du Programme d'administration des assurances de la GRC seront stockés et pourront être récupérés dans les délais de rétablissement établis. Cette installation devrait être située à au moins 500 km du site principal visé par le contrat. Les serveurs de fichiers conservés dans les installations de l'entrepreneur doivent être situés dans une salle (zone) des serveurs réservée à cette fin dont l'accès est restreint aux personnes possédant les cotes de fiabilité appropriées et ayant besoin de savoir. Les serveurs qui contiennent les données de la GRC doivent être confinés dans une armoire de serveur verrouillée munie d'une alarme anti-sabotage surveillée.

La GRC pourrait-elle envisager de remplacer la phrase surlignée ci-dessus par la suivante: «Cette installation devrait être située à au moins 400 km du site principal visé par le contrat»?

Réponse 10

La distance requise entre l'installation de secours pour les serveurs et le site principal visé par le contrat sera changé à 400 km, voir document attaché Guide de Sécurité LVERS.

Question 11 & 12

Les enregistrements confidentiels des centres d'appels de la GRC doivent-ils être conservés et, le cas échéant, doivent-ils être entreposés sur place?

Le cas échéant, doivent-ils être entreposés séparément du registre des appels entreposés pour le compte d'autres clients?

Réponse 11 & 12

Tel que défini à l'article 10.3 les Services continus d'administration des régimes d'assurance incluent documenter toutes les activités liées aux assurances, dont les registres de l'administration du centre d'appels et de la gestion des cas, puis entreposer les dossiers physiques et stocker les fichiers électroniques.

L'article 7.2.16 Technologie de l'information définit que l'entrepreneur doit s'assurer que toutes les données de la GRC sont logiquement séparées des autres données.

Le Guide de sécurité – LVERS décrit les exigences en matière de de stockage de l'information (versions papier et électroniques), notamment:

- L'accès aux dossiers du programme doit être restreint aux employés du Programme d'administration des assurances de la GRC qui possèdent la cote de fiabilité appropriée et qui ont besoin de savoir;
- Le stockage des dossiers sur papier doit être effectué dans une salle des dossiers clairement définie et réservée à cet effet (sur rayons ouverts) ou dans des contenants approuvés par la Section de la sécurité ministérielle (SSM) de la GRC. L'accès à la salle des dossiers et aux contenants devrait se faire à partir de la zone de traitement de l'information du Programme d'administration des assurances

de la GRC (bureau général). La salle des dossiers ne doit pas être située sur un mur extérieur et ne doit pas comporter de fenêtres (intérieures ou extérieures);

- Lorsque les serveurs de fichiers sont situés dans les bureaux du Programme d'administration des assurances de la GRC, ils devraient être situés dans une salle de serveurs réservée à cet effet et conçue pour répondre aux exigences de la salle d'entreposage des fichiers;
- Lorsque les serveurs de fichiers sont conservés dans les installations de l'entrepreneur, celles-ci doivent être situées dans une salle des serveurs réservée à cette fin dont l'accès est restreint aux personnes possédant les cotes de fiabilité appropriées et ayant besoin de savoir. Les serveurs qui contiennent les données de la GRC doivent être confinés dans une armoire de serveur verrouillée munie d'une alarme anti-sabotage surveillée.

TOUS LES AUTRES TERMES ET CONDITIONS DEMEURENT INCHANGÉS



Guide de sécurité – LVERS

Régimes d'assurance de
la GRC no de LVERS : 201902673

Préparé par : Glenna Burke, Kevin Therrien
Section de la sécurité ministérielle centrale
Gendarmerie royale du Canada

Initiales de l'examineur et date : _____

Initiales de l'examineur et date : _____

Date du modèle : 8 août 2017



Royal Canadian
Mounted Police

Gendarmerie royale
du Canada

Canada

Préambule

Tous les entrepreneurs visés par le présent contrat doivent respecter l'environnement de sécurité de la Gendarmerie royale du Canada (GRC) en se conformant aux directives énoncées dans le présent document.

Exigences générales en matière de sécurité

La sécurité des documents, des dossiers et toute autre information qui sont en possession de l'entrepreneur pour les besoins établis est d'une importance cruciale pour la GRC.

1. Il est interdit à l'entrepreneur de retirer des lieux de travail déterminés des biens ou des renseignements protégés, ou d'en faire des copies.
2. L'entrepreneur doit exécuter tout le travail et offrir tous les services au Canada, et toutes les données recueillies, conservées ou gérées ne doivent pas être échangées, transmises ou fournies sous forme électronique ou autre à toute entité à l'extérieur des frontières canadiennes, assurant ainsi la conformité avec la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels* (<http://laws.justice.gc.ca>).
3. L'entrepreneur doit respecter toutes les normes de sécurité du gouvernement du Canada (GC) avant de traiter ou de stocker toute information dans ses installations.
4. L'entrepreneur doit également collaborer avec la GRC ou sa partie désignée pour l'examen de sécurité conformément à la Liste de vérification des exigences relatives à la sécurité (LVERS).
5. L'entrepreneur doit coopérer avec la GRC, pour toute la durée du contrat, pour les vérifications de sécurité de ses installations et de l'infrastructure. Remarque : La GRC se réserve le droit d'exécuter un balayage du système ou une vérification pour valider la conformité avec les exigences de sécurité ministérielles.
6. L'entrepreneur doit s'assurer que toute connexion réseau est sécurisée et répond aux exigences et aux normes de sécurité de la GRC (p. ex. solution VPN répondant à la norme FIPS 140-1 au niveau 2); la GRC exige que tous les flux d'information soient unidirectionnels.
7. L'entrepreneur doit s'assurer que tous les accès sont protégés au moyen d'un accès fondé sur les rôles nécessitant l'utilisation d'une identification et d'une authentification. Les rôles doivent être définis et associés à des accès spécifiques. Un rôle unique doit être établi pour la création et la modification d'autres rôles. Le même nom d'utilisateur ou mot de passe ne doit pas être attribué à deux utilisateurs différents, même si les deux individus assument des fonctions communes.
8. L'entrepreneur doit, pour la GRC, se doter d'un réseau encodé de bout en bout, ce qui comprend les sous-traitants, et leur point de connexion. L'entrepreneur et tous les sous-traitants doivent respecter les normes du gouvernement du Canada en matière de niveau de chiffrement.
9. L'entrepreneur doit faire en sorte que l'ensemble des systèmes de données, des méthodes de connexion et de télécommunications, des transferts de données, des rapports, des locaux et des personnes qui ont accès aux données et aux systèmes, et qui traitent toute information protégée respectent les lois et politiques sur la protection des renseignements personnels et la sécurité du Gouvernement du Canada, y compris les définitions et documents applicables.
10. L'entrepreneur doit s'assurer que toutes les informations protégées de type « B » sont conservées cryptées sur les serveurs de l'emplacement de l'entrepreneur.
11. L'entrepreneur doit s'assurer que tout échange d'information avec la GRC se fasse selon la « méthode tirer » plutôt que selon la « méthode pousser » et soit fondé sur les transactions.

12. L'entrepreneur doit aviser sans délai le responsable du projet avant d'apporter des modifications à son effectif, ses lieux de travail, y compris les déplacements dans l'immeuble, ses systèmes informatiques ou tout autre élément susceptible d'avoir une incidence sur la sécurité de l'information de la GRC, afin que l'examen de sécurité soit mis à jour.
13. L'information divulguée par la GRC sera administrée, conservée et éliminée conformément au contrat. À tout le moins, l'entrepreneur doit respecter la Politique sur la sécurité du gouvernement.
14. L'entrepreneur avisera promptement la GRC de tout incident de sécurité lié à l'information fournie par la GRC (c.-à-d. perte accidentelle ou délibérée de renseignements de nature délicate).
15. Il est interdit de prendre des photos. Si des photos sont requises, il faut communiquer avec l'autorité contractante et la Section de la sécurité ministérielle.
16. L'utilisation de biens personnels, comme des périphériques de bureau, des dispositifs de communication et des supports de stockage amovibles (p. ex. clés USB), sur l'équipement de la GRC est interdite.
17. L'entrepreneur n'est pas autorisé à divulguer de l'information de nature délicate reçue de la GRC à un sous-traitant n'ayant pas la cote de sécurité de la GRC requise pour accéder à l'information en question.
18. **La Section de la sécurité ministérielle (SSM) de la GRC se réserve le droit de :**
 - Mener des inspections dans le site ou les installations de l'entrepreneur. De telles inspections peuvent être réalisées avant que des renseignements de nature délicate ne soient échangés ou au besoin (p. ex. si le bureau de l'entrepreneur devait déménager). Le but de l'inspection est d'assurer la qualité des mesures de protection mises en place.
 - Demander la vérification, au moyen de photos, des mesures de protection. De telles photos peuvent être demandées avant que des renseignements de nature délicate ne soient échangés ou au besoin (p. ex. si le bureau de l'entrepreneur devait déménager). Le but des photographies est d'assurer la qualité des mesures de protection mises en place.
 - Fournir des directives sur les mesures de protection obligatoires (mesures précisées dans le présent document et, le cas échéant, mesures de protection supplémentaires propres au site).
19. Afin d'assurer le contrôle souverain du Canada sur ses données, toutes les données sensibles ou protégées contrôlées par le gouvernement seront stockées sur des serveurs situés au Canada. Les données seront chiffrées de façon appropriée pendant le transfert.

Remarque : si, au cours de la période du contrat, l'entrepreneur est jugé en violation d'une exigence de sécurité imposée par la GRC (dans l'énoncé des travaux, le contrat ou autrement), le chargé de projet peut, à sa discrétion :

Ordonner que l'entrepreneur prenne les mesures jugées nécessaires pour se conformer aux exigences de sécurité, dans le délai fixé par le chargé de projet.

Sécurité matérielle

Gestion de l'information et responsabilités :

- Gérer tous les renseignements reçus de façon confidentielle et prendre toutes les mesures nécessaires pour préserver leur confidentialité, leur intégrité ainsi que leur disponibilité et les protéger contre l'accès, l'utilisation ou la divulgation accidentels ou non autorisés.
- L'accès à des renseignements et à des biens de niveau PROTÉGÉ doit être limité aux personnes qui détiennent une cote de fiabilité valide de la GRC et qui ont un « besoin de savoir ». Il faut prendre les mesures nécessaires pour empêcher l'accès physique ou visuel à ces renseignements et ces biens par des personnes non habilitées et qui n'ont pas un « besoin de savoir » qui pourraient se trouver à proximité de ceux-ci.
- Ne pas diffuser les renseignements reçus ou générés dans le cadre du présent contrat à un quelconque tiers sans l'autorisation préalable écrite de la GRC, sauf si la loi l'exige.
- Informer immédiatement la GRC advenant qu'une demande soit reçue en vertu de la *Loi sur la protection des renseignements personnels*, de la *Loi sur l'accès à l'information*, ou émanant d'une autre autorité légitime, concernant des renseignements liés au présent contrat. Si on lui en fait la demande, l'entrepreneur prend les mesures nécessaires pour empêcher la communication des renseignements dans les limites prévues par la loi.
- Retourner à la GRC tout renseignement qui n'aurait pas dû être transmis.

Évaluation de sécurité

- Les participants sont conjointement responsables de la réalisation d'une évaluation de sécurité pour tous les lieux où des renseignements seront traités et/ou stockés (version papier/électronique) dans le cadre du présent contrat. Cette démarche est nécessaire pour évaluer si les mesures de protection techniques et matérielles, nécessaires pour assurer la protection de la vie privée de même que la confidentialité et l'intégrité des renseignements ainsi que leur disponibilité, peuvent être mises en œuvre et si des modifications aux exigences sont ciblées et apportées en fonction des conditions du site. Les deux parties doivent approuver et signer l'évaluation avant que des travaux soient exécutés dans le cadre du présent contrat.

Contrôle des insignes d'accès et des clés

- Les privilèges d'accès aux zones du Programme d'administration des assurances de la GRC et aux locaux associés au Programme qui s'y trouvent doivent être examinés périodiquement pour s'assurer que seuls les employés qui en ont besoin ont accès aux zones du Programme.
- Lorsqu'un employé part ou n'a plus besoin d'accéder aux zones du Programme, l'accès doit être supprimé immédiatement et le registre d'accès doit être mis à jour par le bureau de la sécurité.
- Les clés (et les dispositifs comme les instruments, les cartes, les combinaisons et les numéros de code utilisés pour ouvrir ou fermer les armoires ou les pièces de projet) doivent être protégées selon le niveau de confidentialité le plus élevé des renseignements ou des biens auxquels elles donnent accès. Cette disposition s'applique également aux renseignements enregistrés qui permettraient la production d'une clé.

- Lorsqu'on remet une clé, on doit demander à la personne qui la reçoit d'apposer sa signature dans un registre. On doit noter dans ce registre, que l'agent de sécurité de l'entreprise doit conserver, le numéro des clés, les coordonnées des armoires qu'elles permettent d'ouvrir et les noms des destinataires de ces clés.
- Le bureau de la sécurité de l'organisation doit tenir un registre des dates et des motifs de chaque changement de clé.
- Les combinaisons assignées devraient être changées :
 - o Au moins tous les douze (12) mois;
 - o Lorsque les personnes ayant accès à l'armoire sont mutées, renvoyées ou n'ont plus besoin d'accéder à l'armoire;
 - o Lorsqu'une armoire a été ou est susceptible d'avoir été ouverte par effraction, la clé doit être changée immédiatement.

Marquage des renseignements

Les organisations sont tenues de mettre en œuvre les procédures suivantes en matière de marquage de l'information :

- Pour les renseignements protégés, inscrire le mot « PROTÉGÉ » dans le coin supérieur droit de la première page du document et, au besoin, la lettre « A » ou « B » pour préciser le niveau de protection;
- Marquer les lettres d'accompagnement ou d'envoi ou les formulaires ou bordereaux de circulation en fonction du plus haut niveau de classification ou d'information que les pièces jointes contiennent;
- Marquer tous les documents utilisés pour préparer les renseignements de niveau PROTÉGÉ. Il peut s'agir de notes, d'ébauches de documents, de copies conformes ou de photocopies;
- Effectuer le marquage à l'aide de caractères plus grands que ceux utilisés dans le corps du document;
- Marquer de façon parfaitement visible les graphiques, les cartes, les dessins, etc., à proximité de la marge ou du titre de manière à ce que la mention soit bien en évidence lorsque le document est plié.

Transport/transmission

La communication matérielle d'information de nature délicate doit respecter les dispositions du contrat. Le service de livraison utilisé, le cas échéant, doit fournir une preuve d'expédition, un suivi pendant l'expédition et une attestation de livraison.

Transport	Transport : la transmission de renseignements et de biens de nature délicate d'une personne ou d'un lieu à un autre par l'entremise d'une personne qui a besoin de connaître les renseignements ou besoin d'accéder au bien.
Transmission	Transmission : la transmission de renseignements et de biens de nature délicate d'une personne ou d'un lieu à un autre par l'entremise d'une personne qui n'a pas besoin de connaître les renseignements ou d'accéder au bien.

Il est essentiel de sécuriser les renseignements de nature délicate avant de les transmettre à qui que ce soit. Ces renseignements sont communiqués en fonction du besoin de savoir et uniquement à des titulaires d'une autorisation de sécurité.

La sécurité des renseignements et des biens de niveau PROTÉGÉ durant la transmission et le transport dépend des facteurs suivants :

- Un emballage adéquat;
- Le suivi durant le transport;
- Une attestation de livraison;
- La transmission par un service postal approuvé ou par un service de messagerie ayant une attestation de sécurité;
- Au sujet du transport d'information « Protégé B » (à destination ou en provenance d'un lieu neutre de réunion ou d'entrevue) : on peut utiliser à la place d'une seule enveloppe ou d'une enveloppe extérieure une mallette ou un autre contenant de résistance équivalente ou supérieure. Une enveloppe ou un emballage double doit être utilisé pour protéger les articles fragiles ou pour garder intacts des colis encombrants, lourds ou aux formes irrégulières;
- Au sujet de la transmission d'informations « Protégé B » (Postes Canada ou messagerie recommandée) : l'adresse doit rester vague. Ajouter au besoin « À ouvrir uniquement par le destinataire » si le principe du besoin de savoir ou d'accéder le justifie.

Reproduction

La cote de sécurité des reproductions de documents de niveau PROTÉGÉ doit être apposée de la même façon que les documents originaux.

Des précautions particulières doivent être prises lors de l'utilisation de photocopieurs, et des photocopieurs réservés au contrat doivent être fournis. Des avis portant sur la marche à suivre pour reproduire des documents doivent être placés bien en vue, près de chaque appareil. Il faut veiller à ne pas laisser de documents originaux dans les appareils et à enlever toutes les copies, y compris les documents à jeter. À la fin du contrat ou lors du remplacement des photocopieurs ou des disques durs, tous les dispositifs doivent être remis à la GRC.

Destruction

La méthode choisie pour détruire les renseignements de nature délicate dépend du niveau de sensibilité. Lorsqu'un document ou un fichier numérique a plus d'une classification ou d'un niveau de protection, il faut choisir la méthode de destruction pour le plus haut niveau de sensibilité.

- À moins d'indications contraires, les renseignements et les biens de niveau PROTÉGÉ A et B, d'origine canadienne, peuvent être détruits par l'organisation, avec l'approbation de la GRC.
- Les renseignements et les biens de niveau PROTÉGÉ dont la destruction a été autorisée doivent être éliminés conformément aux dispositions suivantes :
 - o Ils ne doivent être détruits qu'à l'aide de l'équipement de destruction approuvé, ou dans une installation autorisée par la GRC;
 - o Les renseignements en attente d'être détruits ou acheminés à l'endroit où ils seront détruits doivent être protégés de la manière prescrite pour les renseignements et les biens de niveau PROTÉGÉ du plus haut niveau;
 - o Les renseignements et les biens de niveau PROTÉGÉ en attente d'être détruits doivent être séparés des autres renseignements et biens à détruire;

- o Un employé ayant une cote de fiabilité de la GRC doit être présent pour surveiller la destruction des renseignements de niveau PROTÉGÉ;
- o Les copies excédentaires et les déchets qui pourraient révéler des renseignements de niveau PROTÉGÉ doivent être protégés au niveau approprié et doivent être détruits rapidement.

Communication verbale et par message

Si les renseignements doivent être transmis par voie électronique (c.-à-d. par courriel), veuillez aussi consulter la section sur les systèmes de sécurité des TI.

- Les renseignements de niveau PROTÉGÉ ne peuvent être transmis sans le cryptage approuvé par la GRC.
- Les téléphones et les télécopieurs non protégés ne doivent pas être utilisés pour communiquer des renseignements de niveau PROTÉGÉ B ou PROTÉGÉ C.
- Lorsque vous discutez de renseignements de niveau PROTÉGÉ, soyez conscient de votre environnement, car il pourrait y avoir quelqu'un qui n'a pas « besoin de savoir » à proximité.

Incidents de sécurité

L'entrepreneur doit immédiatement signaler tout incident de sécurité à la GRC et mener une enquête préliminaire sur l'incident afin de déterminer toutes les circonstances, y compris :

- Quelle est la nature de l'incident et quand et où s'est-il produit?
- Qui l'a signalé et à qui et quand l'a-t-on fait?
- Quels sont les renseignements ou les biens visés (en détail)?
- Quel était le marquage de sécurité et quelle est la description du renseignement ou du bien en cause?
- De qui provenaient ces renseignements ou ces biens?
- Quand, pendant combien de temps et dans quelles circonstances le renseignement ou le bien était-il vulnérable à une divulgation non autorisée, et à qui?
- Quelles mesures a-t-on prises pour protéger les renseignements ou les biens et limiter les dommages?
- Y a-t-il des renseignements ou des biens qui ont été perdus ou égarés?

EXIGENCES EN MATIÈRE DE SÉCURITÉ MATÉRIELLE

Zonage :

- Le Programme d'administration des assurances de la GRC doit être situé dans une aire de bureaux clairement définie et réservée au Programme (voir les sections Zone de traitement de l'information et Zone de stockage de l'information) dont l'accès est restreint aux employés du Programme d'administration des assurances de la GRC qui possèdent la cote de fiabilité appropriée et qui ont besoin de savoir;
- La zone réservée au traitement de l'information (bureau général) du Programme d'administration des assurances de la GRC ne doit pas se trouver dans un endroit où un code du bâtiment demanderait d'y entrer pour accéder à une voie de sortie ou qui donne accès à une autre zone de programme dans l'établissement qui n'est pas liée au Programme d'administration;
- Le stockage des dossiers sur papier doit être effectué dans la zone de traitement de l'information (bureau général) du Programme d'administration des assurances de la GRC et être accessible à partir de cette zone;
- Le stockage électronique des dossiers doit se faire soit sur des serveurs situés dans la zone réservée au Programme d'administration des assurances de la GRC, soit dans la salle des serveurs de l'entrepreneur réservée à cet effet;

- L'accès à la zone de traitement de l'information (bureau général) doit se faire à partir d'une zone sécurisée à accès restreint.

Zone de traitement de l'information (bureau général) :

Il faut prendre des mesures particulières pour protéger les renseignements et les biens de niveau PROTÉGÉ contre la divulgation et l'accès non autorisé lorsqu'on les sort des contenants ou des locaux d'entreposage des dossiers approuvés.

- Généralités :
 - o Vous devez éviter de laisser les renseignements ou les biens de niveau PROTÉGÉ sans surveillance;
 - o Vous devez vous assurer que l'information et les biens ne peuvent pas être vus et que la discussion à leur sujet ne peut pas être entendue par des personnes qui n'ont pas la cote de fiabilité appropriée ou qui n'ont pas besoin de savoir.
- Murs et portes du périmètre :
 - o La principale zone de traitement de l'information (y compris le centre d'appels) doit être située dans une aire de travail réservée à cet effet possédant des murs séparateurs périphériques (panneaux de gypse à structure métallique) à pleine hauteur (d'un étage à l'autre).
 - o Les portes menant à la zone de traitement de l'information doivent être en bois à âme massive avec cadre métallique creux, scellant acoustique et seuil en aluminium.
 - o Les murs séparateurs périphériques et les portes d'accès (vestibule à double porte) doivent être conçus de façon à atteindre un indice de transmission du son (ITS) de 55.
- Contrôle de l'accès, détection des intrusions et surveillance :
 - o La zone de traitement de l'information (bureau général) doit être équipée d'un système d'alarme assurant une surveillance en tout temps, muni de détecteurs de mouvements offrant une couverture complète dans l'aire de bureaux et de contacts de porte (pour toutes les portes du périmètre) et pouvant être activé et désactivé par les employés du Programme d'administration des assurances de la GRC.
 - o L'accès au bureau du Programme d'administration des assurances de la GRC doit se faire par l'intermédiaire d'un vestibule réservé, avec des portes munies d'un contrôle d'accès électronique.
 - o La GRC doit pouvoir consulter les registres de contrôle d'accès.

Zone de stockage de l'information (versions papier et électroniques)

- Généralités :
 - o L'accès aux dossiers du programme doit être restreint aux employés du Programme d'administration des assurances de la GRC qui possèdent la cote de fiabilité appropriée et qui ont besoin de savoir;
 - o Le stockage des dossiers sur papier doit être effectué dans une salle des dossiers clairement définie et réservée à cet effet (sur rayons ouverts) ou dans des contenants approuvés par la Section de la sécurité ministérielle (SSM) de la GRC. L'accès à la salle des dossiers et aux contenants devrait se faire à partir de la zone de traitement de l'information du Programme d'administration des assurances de la GRC (bureau général). La salle des dossiers ne doit pas être située sur un mur extérieur et ne doit pas comporter de fenêtres (intérieures ou extérieures);

- o Lorsque les serveurs de fichiers sont situés dans les bureaux du Programme d'administration des assurances de la GRC, ils devraient être situés dans une salle de serveurs réservée à cet effet et conçue pour répondre aux exigences de la salle d'entreposage des fichiers;
- o Lorsque les serveurs de fichiers sont conservés dans les installations de l'entrepreneur, celles-ci doivent être situées dans une salle des serveurs réservée à cette fin dont l'accès est restreint aux personnes possédant les cotes de fiabilité appropriées et ayant besoin de savoir. Les serveurs qui contiennent les données de la GRC doivent être confinés dans une armoire de serveur verrouillée munie d'une alarme anti-sabotage surveillée;
- o L'entrepreneur doit fournir une installation de secours pour les serveurs où tous les dossiers du Programme d'administration des assurances de la GRC seront stockés et pourront être récupérés dans les délais de rétablissement établis. Cette installation devrait être située à au moins 400 km du site principal visé par le contrat. Les serveurs de fichiers conservés dans les installations de l'entrepreneur doivent être situés dans une salle (zone) des serveurs réservée à cette fin dont l'accès est restreint aux personnes possédant les cotes de fiabilité appropriées et ayant besoin de savoir. Les serveurs qui contiennent les données de la GRC doivent être confinés dans une armoire de serveur verrouillée munie d'une alarme anti-sabotage surveillée;
- Murs et portes du périmètre de la salle des fichiers :
 - o La zone de stockage de l'information/salle des serveurs (le cas échéant) doit posséder des murs séparateurs périphériques (des panneaux de gypse à structure métallique avec treillis métallique) à pleine hauteur (d'un étage à l'autre);
 - o La ou les portes de la zone de stockage de l'information/salle des serveurs (le cas échéant) doivent être creuses et métalliques, tout comme leur cadre.
- Contrôle de l'accès, détection des intrusions et surveillance :
 - o La zone de stockage de l'information/salle des serveurs (le cas échéant) doit être équipée d'un système d'alarme (indépendant de la zone de traitement de l'information) assurant une surveillance en tout temps, muni de détecteurs de mouvements offrant une couverture complète et de contacts de porte (pour toutes les portes du périmètre) et pouvant être activé et désactivé par les employés du Programme d'administration des assurances de la GRC.
 - o L'accès à la salle de stockage des dossiers ou à la salle des serveurs (s'il y a lieu) doit se faire par une porte réservée à cet effet équipée d'un contrôle d'accès électronique avec pêne dormant intégré (le pêne dormant ne peut être outrepassé par le contrôle d'accès électronique).
 - o La GRC doit pouvoir consulter les registres de contrôle d'accès.

Sécurité de la TI

Contrôle approprié des renseignements Protégé A et Protégé B

Transport/transmission

Supports amovibles

1. S'il est nécessaire d'envoyer des données Protégé A ou Protégé B de la GRC, celles-ci doivent être envoyées au moyen d'un dispositif de stockage portatif conforme à la norme FIPS 140-2 fourni par la GRC dont l'accès est limité au personnel de l'entrepreneur ayant une cote de sécurité de la GRC et au client de la GRC seulement. Le dispositif de stockage portatif conforme à la norme FIPS 140-2 doit être livré en personne ou par messenger approuvé aux locaux de l'entrepreneur. Les renseignements sensibles de la GRC ne doivent pas être transmis à une adresse de courriel externe ou à partir d'une telle adresse.
2. Le mot de passe pour le dispositif de stockage portatif doit être fourni verbalement, soit en personne ou par téléphone, et uniquement aux membres du personnel de l'entrepreneur ayant obtenu la cote de sécurité de la GRC.
3. Si le traitement électronique de l'information « Protégé A » ou « Protégé B » de la GRC est nécessaire, l'entrepreneur doit veiller à ce que :
 - l'information soit chiffrée lorsqu'elle n'est pas utilisée;
 - l'information soit chiffrée pendant le transfert;
 - des mécanismes de contrôle de l'accès aient été mis en œuvre.

Remarque : L'algorithme AES (norme de chiffrement avancé) utilisant des clés à 128, 192 ou 256 bits est l'algorithme approuvé pour chiffrer de l'information classée « Protégé A » ou « Protégé B ».

Utilisateurs d'appareils mobiles

1. N'utilisez que de l'équipement fourni par la GRC et approuvé en vue de son utilisation mobile.
2. Utilisez une méthode approuvée de chiffrement complet de disque sur les ordinateurs portatifs et chiffrez les renseignements sensibles lorsqu'ils ne sont pas utilisés.
3. Retirez votre jeton d'authentification et gardez-le sur vous lorsque la technologie avec laquelle il est utilisé est laissée sans surveillance.
4. Assurez-vous que l'ordinateur portatif ou le support de stockage contenant des renseignements sensibles est stocké dans un coffre de sécurité autorisé si les renseignements ne sont pas chiffrés. Voir le ch XI. 3., article H du Manuel d'administration.

Téléphonie

5. Toutes les communications vocales par téléphone cellulaire ou mobile doivent s'en tenir à des renseignements de nature non délicate, sauf si le téléphone est spécialement accrédité et émis afin de transmettre des renseignements de nature délicate.

6. L'utilisation des téléphones intelligents et des téléphones cellulaires fournis par la GRC est limitée aux employés de la GRC, aux organisations autorisées et à leurs agents travaillant au nom de la GRC, ainsi qu'aux organisations autorisées et à leurs agents.
7. Les téléphones intelligents et les téléphones cellulaires fournis par la GRC ne sont autorisés à traiter que des renseignements allant jusqu'au niveau « Protégé A » inclusivement, et uniquement dans l'espace de travail de l'entreprise aux fins des activités liées à la GRC.
8. Seuls les périphériques externes fournis par la GRC peuvent être utilisés à l'extérieur avec un téléphone intelligent fourni par la GRC.

Impression, numérisation et photocopies

9. Si de l'information électronique « Protégé » de la GRC doit être imprimée ou scannée, l'entrepreneur doit avoir au moins un ordinateur, une imprimante et un scanneur additionnels réservés à cet usage. L'équipement ne doit pas être branché au réseau local de l'entrepreneur ni à l'Internet. Le disque de cet ordinateur ou de ces ordinateurs devra avoir fait l'objet d'un chiffrement.

Stockage

10. S'il y a lieu, les copies de sauvegarde de l'information classée « Protégé A » ou « Protégé B » de la GRC sont soumises aux mêmes directives de sécurité (chiffrement et contrôle de l'accès) que l'information directe.
11. Les dossiers électroniques doivent être détruits conformément au document ITSG-06, Effacement et déclassification des supports d'information électroniques (consulter le site à l'adresse <https://www.cse-cst.gc.ca/fr/node/270/html/10572f> pour plus de renseignements). L'information « Protégé » doit être effacée selon l'une des options suivantes :
 - a. On peut uniquement réutiliser un support contenant des données gouvernementales « PROTÉGÉ » après que l'information qu'il contient aura été écrasée par un caractère et son complément (p. ex. des bits « 0 » et « 1 ») écrits en alternance au moins trois fois dans toutes les zones de données de ce support.
 - b. Un support contenant de l'information gouvernementale « PROTÉGÉ » qui n'aura pas été réécrit à la satisfaction de la GRC doit être détruit selon les méthodes approuvées par la GRC (dans une installation d'élimination des métaux approuvée, par incinération, au moyen d'une meule d'émeri ou d'une ponceuse à disque, avec de l'acide, par désintégration à sec, par pulvérisation ou par fusion).
12. Tous les dispositifs de stockage fournis par la GRC et utilisés pendant la durée du contrat doivent être remis à la GRC immédiatement lorsque le contrat prendra fin.

Sécurité du personnel

1. Tout le personnel de l'entrepreneur et des sous-traitants doit obtenir et maintenir une attestation de sécurité correspondant au niveau de sensibilité des travaux à réaliser tout au long du cycle de vie du contrat (en conformité avec les dispositions de la LVERS), c'est-à-dire la cote de fiabilité approfondie.
2. L'entrepreneur sera tenu d'informer la GRC de toute modification au personnel en ce qui touche les exigences relatives à la sécurité. Par exemple : Lorsqu'un employé détenant une attestation de sécurité quitte l'entreprise ou ne participe plus à l'exécution du contrat de la GRC, lorsqu'un nouvel employé doit obtenir une attestation de sécurité, ou encore lorsqu'un employé doit renouveler son attestation de sécurité.
3. Puisque le fournisseur et ses employés auront accès à des renseignements protégés ou classifiés, une autorisation de sécurité de la GRC au niveau approprié est requise. Le personnel de l'entrepreneur doit faire l'objet d'une vérification par la GRC avant de se voir accorder l'accès aux systèmes, aux biens, aux installations ou à des renseignements protégés ou classifiés. La GRC se réserve le droit d'interdire l'accès à tout membre du personnel de l'entrepreneur à tout moment.

Lorsque la GRC précise une exigence visant une cote de fiabilité approfondie, l'entrepreneur doit lui soumettre les éléments suivants :

1. Formulaire STT 330-23 (vérification des documents sur le respect de la loi);
2. Formulaire SCT 330-60;
3. Formulaire GRC 1020-1 (avant l'entrevue);
4. Exemple du certificat de naissance et du permis de conduire;
5. Deux photos en format passeport.

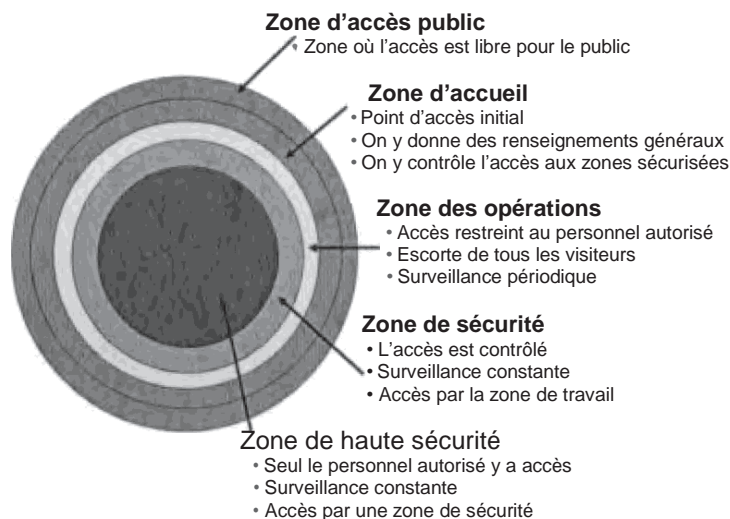
La GRC :

1. réalisera des vérifications de sécurité du personnel qui dépassent les exigences de la *Politique sur la sécurité du gouvernement*;
2. réalisera une entrevue de sécurité;
3. obtiendra un jeu de dactylogrammes.

Annexe A — Concept des zones de sécurité

Selon la *Politique sur la sécurité du gouvernement* (section 10.8, Limites à l'accès), les « ministères doivent limiter l'accès aux renseignements classifiés et protégés et autres biens aux seules personnes qui ont besoin de les connaître et qui ont la cote de fiabilité ou de sécurité appropriée ».

La *Norme opérationnelle sur la sécurité matérielle* (section 6.2, Hiérarchie des zones) stipule que « les ministères doivent assurer l'accès aux biens protégés et classifiés et leur protection en fonction d'une hiérarchie de zones clairement reconnaissables ».



Zone d'accès public – Zone où le public est libre de circuler, et qui entoure habituellement un immeuble gouvernemental ou en fait partie. Exemples : les terrains entourant un bâtiment ou les corridors publics et les vestibules d'ascenseur dans les immeubles à locataires multiples.

Zone d'accueil – Zone où la transition d'une zone d'accès public à une zone d'accès restreint est délimitée et contrôlée. Elle est généralement située à l'entrée de l'immeuble, où se fait le premier contact entre les visiteurs et le Ministère, et comprend les lieux de prestation de services et d'échange de renseignements. L'accès du public peut y être restreint à certaines heures de la journée ou pour des motifs particuliers.

Zone de travail – Secteur dont l'accès est limité au personnel qui y travaille et aux visiteurs accompagnés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée sur une base périodique. Exemples : un espace à bureaux à aire ouverte typique ou un local des installations électriques typique.

Zone de sécurité – Zone dont l'accès est limité au personnel autorisé et aux visiteurs autorisés et accompagnés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée continuellement (jour et nuit, sept jours par semaine). Exemple : une zone où des renseignements secrets sont traités ou conservés.

Zone de haute sécurité – Zone dont l'accès est limité au personnel autorisé qui détient une cote de sécurité valide et de niveau approprié et aux visiteurs autorisés et accompagnés comme il se doit; elle doit être indiquée au moyen d'un périmètre bâti selon les caractéristiques techniques recommandées dans l'EMR, surveillée continuellement (jour et nuit, sept jours par semaine) et être un secteur où les détails de l'accès sont enregistrés et vérifiés. Exemple : une zone où des biens de grande valeur sont manipulés par des employés sélectionnés.

L'accès aux zones doit être fondé sur le principe du besoin de connaître et le fait de restreindre l'accès protège les employés et les ressources de valeur. Se référer au document GI-026 de la GRC, Guide pour l'établissement des zones de sécurité matérielle pour obtenir des renseignements plus détaillés.