Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Security Classification / Classification de sécurité

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Royal Canadian Mounted Police	2. Branch or Directorate / Direction générale ou Direction: D Division Training Branch
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

The contractor will facilitate child forensic interviewing workshops during the fiscal training year on an "As and When Required" basis. The contractor will provide up-to-date training on interviewing children in Manitoba.

L'entrepreneur animera des ateliers sur les entrevues judiciaires avec les enfants au cours de l'année financière de formation, en fonction des besoins. L'entrepreneur fournira une formation actualisée sur les entrevues avec les enfants au Manitoba.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non: x	Yes / Oui:
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	No / Non: x	Yes / Oui:
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non: x	Yes / Oui:
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	No / Non:	Yes / Oui: x
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	No / Non: x	Yes / Oui:

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada: x	NATO / OTAN:	Foreign / Étranger:

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion: x	All NATO countries / Tous les pays de l'OTAN:	No release restrictions / Aucune restriction relative à la diffusion:
Not releasable / À ne pas diffuser:		
Restricted to: / Limité à :	Restricted to: / Limité à :	Restricted to: / Limité à :
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A: x	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ:	PROTECTED A / PROTÉGÉ A:
PROTECTED B / PROTÉGÉ B:	NATO RESTRICTED / NATO DIFFUSION RESTREINTE:	PROTECTED B / PROTÉGÉ B:
PROTECTED C / PROTÉGÉ C:	NATO CONFIDENTIAL / NATO CONFIDENTIEL:	PROTECTED C / PROTÉGÉ C:
CONFIDENTIAL / CONFIDENTIEL:	NATO SECRET / NATO SECRET:	CONFIDENTIAL / CONFIDENTIEL:
SECRET / SECRET:	COSMIC TOP SECRET / COSMIC TRÈS SECRET:	SECRET / SECRET:
TOP SECRET / TRÈS SECRET:		TOP SECRET / TRÈS SECRET:
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT):		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT):

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Security Classification / Classification de sécurité

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — [X] No / Non [ ] Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — [X] No / Non [ ] Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

[ ] RELIABILITY STATUS / COTE DE FIABILITÉ	[ ] CONFIDENTIAL / CONFIDENTIEL	[ ] SECRET / SECRET	[ ] TOP SECRET / TRÈS SECRET
[ ] TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	[ ] NATO CONFIDENTIAL / NATO CONFIDENTIEL	[ ] NATO SECRET / NATO SECRET	[ ] COSMIC TOP SECRET / COSMIC TRÈS SECRET
[X] SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : Daytime access to instruct course; RCMP FA-2 with Escort
Accès de jour au cours d'instruction; Accès aux installations de la Gendarmerie royale du Canada (GRC) de niveau 2 (AI-2) avec escorte

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — [X] No / Non [ ] Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted? — [ ] No / Non [ ] Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — [X] No / Non [ ] Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — [X] No / Non [ ] Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — [X] No / Non [ ] Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — [X] No / Non [ ] Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — [X] No / Non [ ] Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Security Classification / Classification de sécurité

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ A	 B	 C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRES SECRET
Information / Assets Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

[X] No / Non [ ] Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

[X] No / Non [ ] Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Guide de sécurité des listes de vérification des exigences relatives à la sécurité (LVERS)

Formation de facilitateur d'entrevues judiciaires avec des enfants LVERS nº :2023-111681

Préparé par :
Section de la sécurité ministérielle
de la région du Nord-Ouest
Gendarmerie royale du Canada

Signature manuscrite de la SSM : _____

Exigences générales en matière de sécurité

Description de travail : Division « D »

L'entrepreneur animera les ateliers sur les entrevues judiciaires avec des enfants au fur et à mesure des besoins au cours de l'exercice financier où aura lieu la formation. L'entrepreneur offrira une formation d'actualité sur les entrevues avec les enfants au Manitoba.

Autorisation de sécurité : Accès de niveau 2 aux installations de la GRC (AI2)

*****À l'usage interne de la SSM de la région du Nord-Ouest exclusivement *****
Date de la LVERS (expiration) : 2027/09/13

Tous les entrepreneurs visés par le présent contrat doivent respecter le contexte en matière de sécurité de la GRC en se conformant aux directives précisées dans le présent document.

1. La communication à l'entrepreneur de tous les renseignements protégés (documentation papier) et de tout autre bien de nature délicate dont la GRC a la responsabilité se fera conformément aux processus déjà approuvés.

2. L'information divulguée par la GRC sera administrée, conservée et éliminée conformément au contrat. L'entrepreneur doit à tout le moins respecter la *Politique sur la sécurité du gouvernement*.

3. L'entrepreneur signalera rapidement à la GRC toute utilisation ou divulgation non autorisée des renseignements communiqués aux termes du présent contrat et lui fournira des précisions sur l'utilisation ou la divulgation non autorisée . (c.-à-d. perte accidentelle ou délibérée de renseignements de nature délicate).

4. Il est interdit de prendre des photographies. Si des photos sont requises, prière de communiquer avec le chargé de projet de l'organisation et la Section de la sécurité ministérielle (SSM).

5. L'utilisation de biens personnels, comme des périphériques de bureau, des dispositifs de communication et des supports de stockage amovibles (p. ex., clés USB) est interdite sur l'équipement de la GRC.

6. Il est interdit à l'entrepreneur de 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.

7. La 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 avoir lieu préalablement à la communication de renseignements de nature délicate ou selon les besoins (c.-à-d. en cas de changement du lieu de travail de l'entrepreneur). L'inspection vise à vérifier la qualité des mesures de protection mises en place.
    - demander une vérification des mesures de protection au moyen de photographies. On peut demander de telles photographies préalablement à la communication de renseignements de nature délicate ou selon les besoins (c.-à-d. en cas de changement du lieu de travail de l'entrepreneur). Les photographies visent à vérifier la qualité des mesures de sécurité mises en place.

- fournir des conseils sur les mesures de protection obligatoires (mesures précisées dans le présent document et possiblement d'autres mesures adaptées au site).

8. 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 convenablement chiffrées pendant leur transfert.

Sécurité matérielle

1. **Stockage** : Tous les biens et les renseignements protégés doivent être conservés dans un classeur acceptable pour la SSM de la GRC. Le classeur doit se trouver à tout le moins dans une zone dite « zone des opérations ». Par conséquent, les installations de l'entrepreneur doivent comprendre une zone ou pièce respectant les critères suivants :

	Zone des opérations
Définition	Une zone dont l'accès est réservé aux personnes qui y travaillent et aux visiteurs dûment accompagnés. Remarque : Tout employé travaillant dans la zone des Opérations doit : • Soit détenir une cote de fiabilité de la GRC (CFG) valide, • Soit être accompagné d'une personne détenant une CFG valide.
Périmètre	Délimitée par un périmètre visible ou par un périmètre de sécurité, selon les besoins du projet. Par exemple, les commandes peuvent se trouver dans une pièce ou un bureau fermé à clé.
Surveillance	Contrôlée périodiquement par des employés autorisés. Par exemple, les utilisateurs de l'espace travaillant au site peuvent voir s'il y a eu atteinte à la sécurité.

Remarque : Consulter l'annexe A pour de plus amples renseignements à propos du concept de zone de sécurité.

2. **Discussions**: Si on prévoit des conversations de nature délicate, les zones des opérations doivent être séparées des espaces publics ou conçues de manière à posséder des propriétés acoustiques garantissant de manière raisonnable aux utilisateurs que leurs échanges ne pourront pas être entendus par des tiers. Par exemple, une pièce privée, un bureau fermé ou une salle de conférence.

3. **Production**: La production (création ou modification) de renseignements ou de biens protégés doit s'effectuer dans une zone répondant aux critères d'une zone des opérations.

4. **Destruction**: L'entrepreneur doit détruire toutes les ébauches et les impressions erronées (copies endommagées ou excédentaires). Il faut détruire les renseignements protégés conformément aux dispositions du *Manuel de la sécurité de la GRC*. L'équipement ou le système servant à détruire les documents de nature délicate doit correspondre au degré de destruction requis. On doit se servir d'un équipement de destruction approuvé par la GRC.

   Degrés de destruction approuvés pour les renseignements « Protégé B » :

   - La taille des résidus doit être inférieure à 1 x 14,3 mm (découpage en particules).

Remarque :

- Si l'entrepreneur n'est pas en mesure de respecter les exigences de la GRC en matière de destruction, il faut retourner à la GRC tous les renseignements et biens de nature délicate en vue de leur destruction adéquate.
- On doit protéger toute ébauche ou impression erronée de nature délicate en attente de destruction de la façon convenue jusqu'à sa destruction.

5. **Transport/Transmission :** L'échange physique de renseignements de nature délicate doit respecter les modalités du contrat. Si on fait appel à un service de livraison, celui-ci doit fournir une preuve d'expédition, un suivi pendant l'exécution et une attestation de livraison.

Transport	Transport : La transmission de renseignements ou de biens de nature délicate d'une personne à une autre ou d'un lieu à un autre par l'entremise de quelqu'un ayant besoin de connaître les renseignements ou d'avoir accès au bien.
Transmettre	Transmettre : La transmission de renseignements ou de biens de nature délicate d'une personne à une autre ou d'un lieu à un autre par l'entremise de quelqu'un n'ayant pas besoin de connaître les renseignements ou d'avoir accès au bien.

Note:

- Dans le cas du transport de renseignements « Protégé B » (à destination ou en provenance d'endroits tiers en vue d'une rencontre ou d'une entrevue, on peut utiliser à la place d'une simple enveloppe, une mallette ou un autre contenant d'une solidité égale ou supérieure. On utilisera une enveloppe ou un emballage double pour protéger les articles fragiles ou garder intacts les articles encombrants, lourds ou surdimensionnés.
- Dans le cas de la transmission de renseignements « Protégé B », (par Postes Canada ou messagerie recommandée, l'adresse doit demeurer vague et s'accompagner de la mention « À n'être ouvert que par » si le principe du besoin de savoir ou d'avoir accès le justifie.

Sécurité de la TI

Contrôle approprié des renseignements Protégé A et Protégé B

Transport et transmission

1. S'il est nécessaire d'envoyer des renseignements Protégé A ou Protégé B de la GRC par voie électronique, il faut les envoyer au moyen d'un dispositif de stockage portatif respectant la norme FIPS140 2, fourni par la GRC, avec un accès restreint au personnel de l'entrepreneur ayant obtenu l'autorisation de sécurité de la GRC et au client de la GRC. Le dispositif de stockage portatif respectant la norme FIPS 140-2 doit être remis en personne ou expédié au lieu de travail de l'entrepreneur par l'entremise d'un service de messagerie approuvé. On ne peut pas transmettre de renseignements de nature délicate de la GRC à destination ou en provenance d'une adresse courriel externe.

2. Le mot de passe du dispositif de stockage portatif doit être fourni verbalement, en personne ou au téléphone, uniquement aux membres du personnel de l'entrepreneur ayant obtenu la cote de sécurité de la GRC.

    - Si le traitement électronique de renseignements Protégé A ou Protégé B de la GRC est nécessaire, l'entrepreneur doit veiller à ce que les renseignements soient chiffrés lorsqu'ils ne sont pas utilisés et à ce que les mécanismes de contrôle de l'accès soient activés.

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

Utilisateurs mobiles

1. Pour les appareils mobiles, n'utiliser que l'équipement approuvé fourni par la GRC.

2. Pour les ordinateurs portables, utiliser une méthode approuvée de chiffrement complet du disque dur et chiffrer les renseignements de nature délicate lorsqu'ils ne sont pas utilisés.

3. Retirer les justificatifs ou le jeton d'authentification et gardez-les sur vous lorsque les outils technologiques associés sont laissés sans surveillance.

4. S'assurer que l'ordinateur portable ou les médias de stockage contenant des renseignements de nature délicate sont rangés dans un classeur de sécurité approuvé lorsque les renseignements ne sont pas chiffrés. Consulter le MA, ch. XI.3., partie H.

Téléphonie

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

6. L'utilisation de téléphones intelligents/cellulaires fournis par la GRC est réservée aux employés de la GRC, aux organisations autorisées et à leurs mandataires travaillant pour le compte de la GRC ainsi qu'aux organisations autorisées et à leurs mandataires.

7. Les téléphones intelligents/cellulaires fournis par la GRC ne peuvent traiter que les renseignements allant jusqu'à « Protégé A » dans l'espace de travail ministériel ,pour les fins des activités de la GRC.

8. Seuls les périphériques externes fournis par la GRC peuvent être utilisés à l'externe avec un téléphone intelligent fourni par la GRC.

Impression, numérisation et photocopie

9. S'il faut imprimer ou numériser des renseignements protégés de la GRC, l'entrepreneur doit disposer d'au moins un ordinateur, une imprimante et un numériseur additionnels réservés à cet usage. L'équipement ne doit pas être relié au réseau local ou à Internet. L'ordinateur doit être muni d'une méthode de chiffrement du lecteur de disque approuvée par la GRC.

Entreposage

10. Le cas échéant, les copies de sauvegarde de l'information de la GRC classée « Protégé A » ou « Protégé B » sont soumises aux mêmes directives de sécurité (chiffrement et contrôles d'accès) que l'information directe.

11. Il faut nettoyer ou détruire les fichiers électroniques et les supports conformément à la norme ITSP.40.006, *Nettoyage des supports de TI*, ou ses versions ultérieures, qu'on peut consulter sur le site Web du Centre canadien pour la cybersécurité. On peut effacer les renseignements protégés au moyen des options suivantes :

    - Un support contenant de l'information gouvernementale « PROTÉGÉ » ne peut être réutilisé qu'une fois que des bits de données « 1 »et « 0 »auront été écrites alternativement au moins trois fois dans toutes les zones de données du support.
    - Un support contenant de l'information gouvernementale « PROTÉGÉ » qui n'a pas été effacée à la satisfaction de la GRC doit être détruit conformément aux méthodes approuvées par la GRC (installation agréée de destruction des métaux, incinération, meule d'ébauchage ou ponceuse à disque, désintégration à sec, pulvérisation ou fusion).

12. À la cessation du contrat, il faut immédiatement retourner à la GRC tous les dispositifs de stockage fournis par la GRC pendant la durée du présent contrat.

Exigences relatives à la sécurité du personnel

Accès aux installations de la GRC, niveaux I, II, III et IV

Dans le cas des entrepreneurs ne devant avoir accès qu'à une installation de la GRC et non pas à des renseignements, systèmes, biens et/ou installations protégés ou classifiés; dans ce contexte, la GRC souhaite ne mener que des vérifications auprès des *autorités locales d'application de la loi.* Il faut l'indiquer dans les documents contractuels pour les fins du processus d'approvisionnement de TPSGC.

Le personnel de l'entrepreneur doit faire l'objet d'une vérification de la GRC auprès des autorités locales d'application de la loi avant son admission dans l'installation ou le site. La GRC se réserve en tout temps le droit de refuser à tout membre du personnel de l'entrepreneur l'accès à la totalité ou à une partie de l'un ou l'autre de ce qui précède.

Si la GRC exige le niveau d'accès 1 ou 2 aux installations, le soumissionnaire retenu, c.-à-d. l'entrepreneur, transmettra à la GRC les éléments suivants :

1. Le formulaire SCT 330-23;
2. Copie d'une pièce d'identité avec photo et signature délivrée par le gouvernement (recto et verso).

Si la GRC exige le niveau d'accès 3 ou 4 aux installations, le soumissionnaire retenu, c.-à-d. l'entrepreneur, transmettra à la GRC les éléments suivants :

1. Le formulaire SCT 330-23;
2. Le formulaire SCT 330-60;
3. Copie d'une pièce d'identité avec photo et signature délivrée par le gouvernement (recto et verso);
4. Deux jeux d'empreintes digitales.

La GRC :

1. Mènera des vérifications auprès des autorités locales d'application de la loi;
2. A la responsabilité de satisfaire aux exigences d'accompagnement dans ses installations ou sites;
3. n'exigera pas de cotes de sécurité organisationnelles ou personnelles pour les fournisseurs ou entrepreneurs fournissant les services;
4. remplira le formulaire de commande 9200 de TPSGC afin de signaler que l'exigence relative à la sécurité n'est pas associée à une LVERS.

Cote de fiabilité de la GRC (CFG), cote « Secret » ou « Très Secret »

Dans le cas des entrepreneurs devant avoir accès à des renseignements, à des biens et/ou à des installations protégés de la GRC; dans ce contexte, la GRC souhaite effectuer toutes les vérifications requises pour l'obtention de la cote de fiabilité de la GRC. Il faut l'indiquer dans les documents contractuels pour les fins du processus d'approvisionnement de TPSGC.

Le personnel de l'entrepreneur doit faire l'objet d'une vérification de la GRC avant d'obtenir l'accès aux renseignements, aux systèmes, aux biens et/ou aux installations protégés ou classifiés de la GRC. La GRC se réserve le droit de refuser en tout temps à tout membre du personnel de l'entrepreneur l'accès à l'un ou l'autre de ce qui précède.

Si la GRC établit une exigence visant une cote de fiabilité de la GRC ou une autorisation de sécurité, le soumissionnaire retenu, c.-à-d. l'entrepreneur, devra présenter à la GRC les éléments suivants :

1. Le formulaire SCT 330-23;
2. Le formulaire SCT 330-60;
3. Le formulaire 1020-1 (entretien de sécurité);
4. Deux pièces d'identité avec photo et signature délivrées par le gouvernement; (Certificat de naissance et permis de conduire);
5. Deux jeux d'empreintes digitales;
6. Un visa de travail (le cas échéant);
7. Deux photos de passeport.

La GRC :

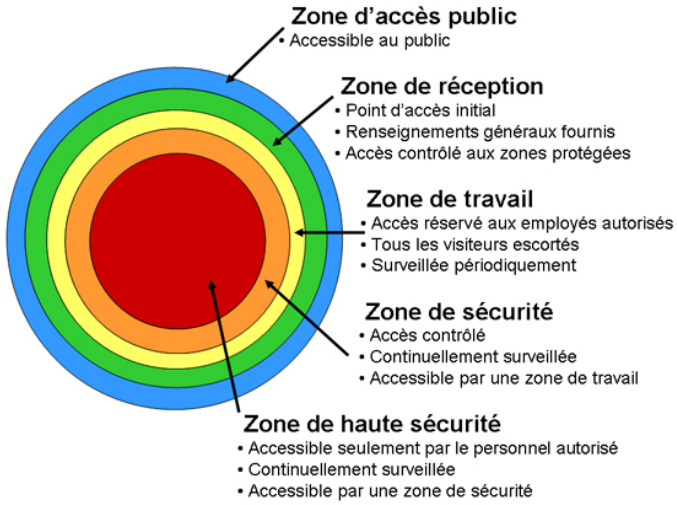
1. Mènera des vérifications de sécurité supérieures aux exigences de la Po*litique sur la sécurité du gouvernement*;

2. A la responsabilité de satisfaire aux exigences d'accompagnement dans ses installations ou sites;
3. Mènera une enquête de sécurité sur les principaux cadres supérieurs désignés par la DSIC (exigence relative à l'information classifiée).

Annexe A – Concept des zones de sécurité

La *Politique sur la sécurité du gouvernement (Partie 10.8 -Restrictions à l'accès)* stipule que « les ministères doivent limiter l'accès aux documents classifiés et protégés et autres biens aux seules personnes qui ont besoin de les connaître et qui détiennent la cote de fiabilité ou de sécurité appropriée ».

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



Zone d'accès public : zone où le public a un libre accès et qui englobe d'ordinaire une installation gouvernementale ou qui en fait partie. Exemples : le terrain entourant un édifice ainsi que les corridors et les halls d'entrée des ascenseurs dans les immeubles à plusieurs occupants.

Zone de réception : zone où la transition d'une zone d'accès public à une zone d'accès restreint est délimitée et contrôlée. Elle se trouve d'ordinaire à l'entrée de l'installation, où a lieu le premier contact entre les visiteurs et le ministère. Il peut s'agir d'endroits où on fournit des services et où on communique des renseignements. L'accès des visiteurs peut être restreint à certaines heures de la journée ou pour des raisons particulières.

Zone des opérations : zone dont l'accès est réservé aux personnes qui y travaillent ainsi qu'à des visiteurs dûment accompagnés; elle doit être signalée par un périmètre visible et faire l'objet d'une surveillance périodique. Exemples : locaux à bureaux ordinaires à plan ouvert ou local électrique ordinaire.

Zone de sécurité : une zone dont l'accès est réservé au personnel autorisé ainsi qu'à des visiteurs autorisés et dûment accompagnés; elle doit être signalée par un périmètre visible et faire l'objet d'une surveillance ininterrompue (jour et nuit, sept jours par semaine). Exemple : une zone au sein de laquelle on traite et stocke des renseignements de niveau secret.

Zone de haute sécurité : zone dont l'accès est limité au personnel autorisé et détenant une cote de sécurité valide et de niveau approprié ainsi qu'aux visiteurs autorisés et dûment accompagnés. Elle doit être signalée par un périmètre établi conformément aux spécifications recommandées dans l'EMR, faire l'objet d'une surveillance ininterrompue (jour et nuit, sept jours par semaine) et être un secteur pour lequel les données relatives à l'accès sont consignées et vérifiées. Exemple : une zone au sein de laquelle du personnel choisi manipule des biens de grande valeur.

L'accès aux zones doit se fonder sur les principes du « besoin de savoir » et de l'accès réservé afin de protéger les employés et les biens de valeur. Pour des précisions, se reporter à G1-026, *Guide de la GRC pour l'établissement des zones de sécurité*.