LVERS **Directive de sécurité**

Offre à commandes

pour

du Programme national d'ADN pour les personnes disparues (PNAPD)

LVERS #: **PSPCM7594-173247**

Preparé par :
Section de la sécurité ministérielle
Gendarmerie royale du Canada

Initiales et date du réviseur : _____
Initiales et date du réviseur : _____

Date du modèle : le 3 août 2017

Préambule

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

Given the nature of this project, the following guidelines only apply to sensitive RCMP information disseminated from the RCMP (by designated contact) to the contractor.

Exigences générales en matière de sécurité

1. Tous les renseignements « Protégé B » (documents papier) et autres biens de nature délicate dont la GRC a la responsabilité seront fournis à l'entrepreneur par l'entremise de processus préapprouvés.

2. 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.

3. 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).

4. 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.

5. La Section de la sécurité ministérielle (SSM) se réserve le droit de mener des inspections de sécurité dans les installations de l'entrepreneur et de donner de l'orientation à l'égard des mesures de protection obligatoires (mesures précisées dans le présent document et possiblement d'autres mesures propres au site). De telles inspections peuvent être réalisées avant que de l'information de nature délicate ne soit échangée et/ou au besoin (p. ex., si le bureau de l'entrepreneur devait déménager.

6. 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.

7. Aucun travail ne doit être commencé concernant cette exigence jusqu'à ce que les mesures de sécurité nécessaires soient approuvées par le responsable du projet de la GRC.

Sécurité matérielle

1. **Entreposage :** Les renseignements/biens protégés doivent être entreposés dans un contenant approuvé par la SSM de la GRC. Le contenant doit être situé (au minimum) dans une « zone de travail ». Par conséquent, les installations de l'entrepreneur doit être dotées d'une aire ou d'une salle répondant aux critères suivants :

Zone de travail	
Définition	Secteur dont l'accès est limité au personnel qui y travaille et aux visiteurs dûment accompagnés. Remarque : Tout employé travaillant avec dans la zone de travail doit : • détenir une cote de fiabilité de la GRC valide, ou • être escorté par une personne qui détient une cote de fiabilité de la GRC valide.
Périmètre	Doit être délimité 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	Surveillance périodique par des employés autorisés. Par exemple, des utilisateurs du local qui travaillent sur les lieux sont en mesure d'observer toute atteinte à la sécurité.

Remarque : Vous trouverez à l'Annexe A plus d'information sur les zones de sécurité.

2. **Discussions :** Dans le cas de conversations de nature potentiellement délicate, les zones de travail doivent être à distance de sécurité des espaces publics ou être dotées de propriétés d'isolement acoustique des entretiens (c'est-à-dire que l'utilisateur peut raisonnablement s'attendre à ne pas être entendu par hasard). Par exemple, pièce, salle de conférence ou bureau privé.

3. **Production :** Les renseignements protégés doivent être produits (fabriqués ou modifiés) dans une aire correspondant aux critères d'une zone de travail.

4. **Destruction :** L'entrepreneur doit détruire toutes les ébauches ou les impressions manquées (copies en surplus ou endommagées. Les renseignements protégés doivent être détruits conformément aux dispositions du Manuel de sécurité de la GRC. L'équipement ou le système (c.-à-d. la déchiqueteuse utilisé pour détruire les documents de nature délicate) est coté selon le degré de destruction. L'équipement de destruction utilisé doit avoir été approuvé par la GRC.

Les niveaux de destruction approuvés pour des renseignements classés « Protégé B » sont notamment les suivants :

- La largeur des résidus (lanières) doit être inférieure à 1 mm x 14,3 mm.

Remarque :

- Si l'entrepreneur n'est pas en mesure de satisfaire aux exigences de la GRC en matière de destruction, il doit retourner tous les renseignements et les biens de nature délicate à la GRC afin qu'ils puissent être détruits selon les règles.

- Toute ébauche ou impression manquée d'information de nature délicate en attente d'élimination doit être protégée de la façon convenue jusqu'à sa destruction.

5. **Transport/Transmission :** L'échange physique de renseignements de nature délicate doit respecter les termes du contrat. Lorsqu'on fait appel à un service de messagerie, celui-ci doit fournir une preuve d'expédition, une façon de faire le suivi de l'envoi et une preuve 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.

Nota :

- Transport de renseignements cotés Protégé « B » (transport à partir d'un endroit neutre pour des réunions ou des entrevues, ou vers cet endroit neutre) : 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.
- Transmission de renseignements cotés Protégé « B » (Postes Canada ou service de messagerie autorisé) : L'adresse soit rester vague. Ajouter au besoin « À ouvrir uniquement par le destinataire » si le principe du besoin de savoir ou d'accéder le justifie.

Sécurité de la TI

1. Si des renseignements de la GRC qui sont cotés Protégé A ou Protégé B doivent être transmis par voie électronique, on peut le faire de l'une des deux façons suivantes :

- Ils peuvent être transmis à l'aide d'un dispositif de stockage portatif conforme à la norme FIPS 140-2 et fourni par la GRC, avec un accès restreint aux membres du personnel de l'entrepreneur ayant obtenu la cote de sécurité de la GRC et au client de la GRC. Le dispositif de stockage portatif conforme à la norme FIPS 140-2 doit être livré en mains propres dans les locaux de l'entrepreneur ou y être expédié par l'intermédiaire d'un messager digne de confiance (Nota : La DSICI de SPAC peut fournir une liste de services de messagerie dignes de confiance).

  NOTA : *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.*

- Il peut aussi être envoyé dans un courriel protégé de la GRC chiffré à l'aide d'Entrust.

2. S'il est nécessaire de traiter/transmettre électroniquement de l'information de la GRC dont la cote est Protégé A ou supérieure, l'entrepreneur doit s'assurer :
   - que l'information est chiffrée lorsqu'elle n'est pas utilisée;
   - que l'information est chiffrée pendant le transfert;
   - que des mécanismes de contrôle de l'accès ont été mis en œuvre.

   NOTA : 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 ».

3. 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.

4. Il est interdit d'utiliser son téléphone intelligent personnel pour l'exécution d'activités opérationnelles de la GRC.

5. 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 :

   - 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.
   - 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).

6. Si de l'information électronique « Protégée » 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.

7. S'il y a lieu, 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 contrôle des accès) que l'information directe.

8. Les dossiers électroniques doivent être détruits conformément à l'ITSG-06, Effacement et déclassification des supports d'information électroniques (voir https://www.cse-cst.gc.ca/fr/node/270/html/10572 https://www.cse-cst.gc.ca/fr/node/270/html/10572 pour obtenir de plus amples renseignements). L'information « Protégé » doit être effacée au moyen de l'une des options suivantes :

   - Un média 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 média.

- Un média 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).

Exigences en matière de sécurité du personnel

1. Tout le personnel de l'entrepreneur 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).

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 faire renouveler son attestation de sécurité.

3. Puisque le fournisseur et ses employés auront accès à de l'information protégée ou classifiée de la GRC, 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 à de l'information protégée ou classifiée, aux systèmes, aux biens et/ou aux installations. La GRC se réserve le droit d'interdire l'accès de tout membre du personnel de l'entrepreneur à l'information, aux systèmes, aux biens et/ou aux installations, quels qu'ils soient, à tout moment.

   Lorsque la GRC signale une exigence visant une cote de fiabilité de la GRC ou une autorisation de sécurité, le soumissionnaire retenu, l'entrepreneur, doit soumettre les éléments suivants à la GRC :

   1. Formulaire SCT 330-23
   2. Tout autre formulaire requis.

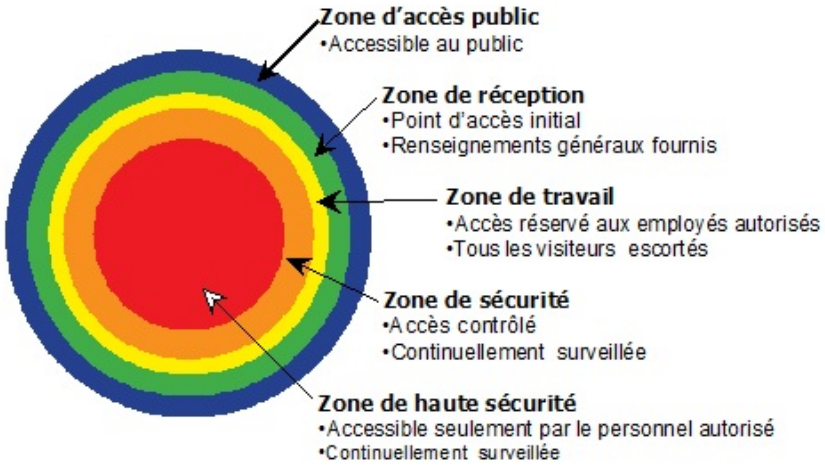
   La GRC:

   1. Réalisera des vérifications de sécurité du personnel qui dépassent les exigences de sécurité identifiées de la Politique sur la sécurité du gouvernement.

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 ».

Selon la *Norme opérationnelle sur la sécurité matérielle (section 6.2, Hiérarchie des zones),* « 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 immeuble et les corridors publics, ainsi que les vestibules d'ascenseur dans des immeubles à plusieurs occupants.

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 située généralement à l'entrée de l'immeuble où survient le premier contact entre le public et le ministère, y compris des endroits où des services sont fournis et où des renseignements sont échangés. 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 dûment accompagnés; Cette zone doit être délimitée par un périmètre reconnaissable et faire l'objet d'une sureillance périodique. Exemples : une aire de bureaux ouverte typique ou un local d'installations électriques typique.

Zone de sécurité – Zone dont l'accès est limité au personnel autorisé ainsi qu'aux visiteurs autorisés et dûment accompagnés. Cette zone doit être délimitée par un périmètre reconnaissable et faire l'objet d'une surveillance continue, soit tous les jours, 24 heures sur 24. Exemple : Une zone où des renseignements secrets sont traités ou conservés.

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. Cette zone doit être délimitée au moyen d'un périmètre construit selon les spécifications recommandées dans l'EMR et faire l'objet d'une surveillance continue, c'est-à-dire tous les jours, 24 heures sur 24. De plus, les renseignements concernant l'accès à cette zone doivent être 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. Pour obtenir de plus amples renseignements, reportez-vous au Guide de la GRC G1-026, Guide pour l'établissement des zones de sécurité matérielle.