ANNEXE D

Guide de sécurité de la GRC

Sous-direction de la sécurité ministérielle de la GRC – Sécurité matérielle
Exigences en matière de sécurité matérielle – Programme national de recrutement de la GRC – Services d'évaluation médicale / psychologique nº 202006332/333
2020-11-16

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

Programme national de recrutement de la GRC
Services d'évaluation médicale / psychologique

Programme national de recrutement de la GRC
Services d'évaluation médicale / psychologique

Préparé par :
Sous-direction de la sécurité ministérielle
Gendarmerie royale du Canada

Date : 16 novembre 2020

CONTEXTE / APPLICATION

Les exigences de sécurité énoncées dans le présent guide visent principalement l'entreprise sous contrat qui coordonnera l'ensemble du projet conjointement avec la GRC et les professionnels médicaux/psychologiques. Les exigences en matière de sécurité de l'information auxquelles doivent satisfaire les professionnels de la santé (médicaux et psychologiques) qui traiteront directement avec les postulants sont régies par leur code de déontologie et leurs règlements professionnels respectifs, à moins d'indications contraires précisées dans le présent document.

Des cotes de sécurité de la GRC ne seront requises que pour les employés de l'entreprise principale sous contrat qui coordonnera l'ensemble du projet. Des cotes de sécurité de la GRC ne seront pas requises pour les professionnels de la santé (médicaux et psychologiques) régis par leur code de déontologie et leurs règlements professionnels respectifs.

EXIGENCES GÉNÉRALES DE SÉCURITÉ

Tous les entrepreneurs engagés dans le cadre du présent contrat sont tenus de collaborer au maintien de l'environnement de sécurité de la GRC en se conformant aux directives énoncées ci-après.

1. Tous les renseignements protégés (documents papier) et autres biens de nature délicate dont la GRC est responsable doivent être transmis à l'entrepreneur suivant des processus approuvés préalablement.

2. Les renseignements communiqués par la GRC doivent être gérés, tenus à jour et éliminés conformément aux clauses du contrat. À tout le moins, l'entrepreneur est tenu de respecter la Politique sur la sécurité du gouvernement.

3. L'entrepreneur doit aviser promptement la GRC de toute utilisation ou divulgation non autorisée de renseignements communiqués en vertu du présent contrat et il doit transmettre à la GRC les détails de l'utilisation ou de la divulgation non autorisée (p. ex. en cas de perte, accidentelle ou délibérée, de renseignements de nature délicate).

4. La prise de photos est interdite. Si des photos sont requises, il faut communiquer avec l'autorité contractante et la Section de la sécurité ministérielle.

5. Il est interdit d'utiliser des biens personnels, p. ex. périphériques, dispositifs de communication ou dispositifs de stockage portatifs (clés USB), conjointement avec la technologie de la GRC.

6. L'entrepreneur n'est pas autorisé à divulguer des renseignements de nature délicate reçus de la GRC à des sous-traitants qui n'ont pas la cote de sécurité de la GRC leur permettant de consulter les renseignements en question ou sans autorisation préalable par la GRC.

7. La Section de la sécurité ministérielle (SSM) de la GRC se réserve le droit :
    - d'effectuer des inspections des installations et des systèmes de l'entrepreneur (y compris de ses serveurs) et de formuler des recommandations sur les mesures de sécurité (mesures de sécurité précisées dans le présent document et autres mesures possibles propres aux installations). Des inspections peuvent être réalisées avant que des renseignements de nature délicate soient communiqués ou au besoin (p. ex. si le lieu de travail de l'entrepreneur change). L'inspection vise à s'assurer de la qualité des mesures de sécurité.
    - de demander des vérifications, effectuées à l'aide de photos et de documents écrits, des mesures de sécurité. Des photos peuvent être demandées avant que des renseignements de nature délicate soient communiqués ou au besoin (p. ex. si le lieu de travail de l'entrepreneur

change). La vérification à l'aide de photos vise à s'assurer de la qualité des mesures de sécurité.
- de formuler des conseils sur les mesures de sécurité obligatoires (mesures de sécurité précisées dans le présent document et autres mesures possibles propres aux installations).

8. Afin d'assurer le contrôle souverain du Canada sur ses données, toutes les données protégées ou classifiées (renseignements protégés et classifiés) qui sont sous le contrôle du gouvernement doivent être stockées sur des serveurs qui se trouvent au Canada. Toutes les données en transit doivent être chiffrées de façon appropriée.

Gestion de l'information et responsabilités :

- Gérer tous les renseignements reçus de façon confidentielle et prendre toutes les mesures nécessaires pour en préserver la confidentialité, l'intégrité et la disponibilité et les protéger contre tout accès, utilisation ou 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 sécurité de la GRC et qui ont « besoin de savoir ». Il faut prendre les mesures nécessaires pour empêcher l'accès physique ou visuel à ces renseignements et à ces biens par des personnes qui pourraient se trouver à proximité, mais qui ne détiennent pas la cote de sécurité requise ou qui n'ont pas « besoin de savoir »;

- 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 de toute autre disposition législative applicable concernant des renseignements liés au présent contrat. Si on lui en fait la demande, l'entrepreneur doit prendre 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 d'effectuer une évaluation de sécurité (lorsque la Section de la sécurité ministérielle de la GRC l'exige) pour tous les lieux où des renseignements seront traités et/ou stockés (version papier/électronique) dans le cadre du présent contrat. Cette évaluation est nécessaire pour déterminer si les mesures de sécurité administratives, techniques et matérielles nécessaires pour assurer la protection de la vie privée de même que la confidentialité, l'intégrité et la disponibilité des renseignements peuvent être mises en œuvre et si des modifications aux exigences sont identifiées et apportées en fonction des conditions des installations. Les deux parties doivent approuver et signer l'évaluation avant que des travaux soient exécutés dans le cadre du présent contrat.

Marquage de sécurité des renseignements :

Les organisations sont tenues de mettre en œuvre les procédures suivantes pour le marquage de sécurité des renseignements :

- Pour les renseignements de niveau PROTÉGÉ, inscrire la mention « PROTÉGÉ » dans le coin supérieur droit de la première page du document et la lettre « A » ou « B », selon le cas, pour préciser le niveau de protection;

- Marquer les lettres ou formulaires d'accompagnement ou de transmission ou les bordereaux de circulation en fonction du plus haut niveau de classification ou de protection des pièces qui y sont jointes;
- Marquer tous les documents utilisés pour préparer des renseignements de niveau PROTÉGÉ. Cela comprend les notes, les ébauches, les copies conformes et les 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 et transmission :

Nota : Cette section s'applique aux professionnels de la santé (médicaux et psychologiques) et à l'entrepreneur principal.

L'échange physique de renseignements de nature délicate doit se faire selon les clauses du contrat. Si on a recours à un service de livraison, il doit fournir une preuve d'expédition, un suivi en transit et une attestation de livraison.

Transport	Transport : Transfert de renseignements et de biens de nature délicate d'une personne ou d'un endroit à un autre par une personne qui a besoin de connaître les renseignements ou d'accéder au bien.
Transmission	Transmission : Transfert de renseignements et de biens de nature délicate d'une personne ou d'un endroit à un autre par 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 doivent être communiqués en fonction du besoin de savoir et uniquement à des titulaires d'une cote de sécurité.

La sécurité des renseignements et des biens de niveau PROTÉGÉ durant la transmission 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.
- Pour le transport de renseignements « Protégé B » (déplacement vers/de lieux neutres aux fins de réunions et/ou d'entrevues) : On peut utiliser, à la place d'une seule enveloppe, une mallette ou un autre contenant de résistance équivalente ou supérieure. Un emballage/une enveloppe double doit être utilisé pour protéger les articles fragiles ou pour garder intacts des colis encombrants, lourds ou aux formes irrégulières.
- Pour la transmission de renseignements « Protégé B » (Postes Canada ou messagerie recommandée) : L'adresse doit rester vague. Ajouter « À ouvrir uniquement par le destinataire » si le principe du besoin de savoir ou d'accéder le justifie.

Reproduction :

Nota : Cette section s'applique aux professionnels de la santé (médicaux et psychologiques) et à l'entrepreneur principal.

Les reproductions de renseignements de niveau PROTÉGÉ doivent porter la même mention de sécurité que les 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 :

Nota : Cette section s'applique aux professionnels de la santé (médicaux et psychologiques) et à l'entrepreneur principal.

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 PROTÉGÉ 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 :
    - Ils ne doivent être détruits qu'à l'aide de l'équipement de destruction approuvé, ou dans une installation autorisée par la GRC;
    - 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;
    - Les renseignements et les biens de niveau PROTÉGÉ en attente d'être détruits doivent être séparés des autres renseignements et biens à détruire;
    - Un employé détenant une cote de fiabilité de la GRC doit être présent pour surveiller la destruction des renseignements de niveau PROTÉGÉ;
    - 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

Nota : Cette section s'applique aux professionnels de la santé (médicaux et psychologiques) et à l'entrepreneur principal.

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

- Les renseignements de niveau PROTÉGÉ ne peuvent être transmis sans le chiffrement approuvé par la GRC.
- Des téléphones et des télécopieurs non protégés ne doivent pas être utilisés pour communiquer des renseignements de niveau PROTÉGÉ B ou PROTÉGÉ C.

- Lorsqu'on discute de renseignements de niveau PROTÉGÉ, il faut être conscient de son environnement, car quelqu'un qui n'a pas « besoin de savoir » pourrait se trouver à proximité.

Incidents de sécurité :

Nota : Cette section s'applique aux professionnels de la santé (médicaux et psychologiques) et à l'entrepreneur principal.

L'entrepreneur doit immédiatement signaler tout incident de sécurité à la GRC et mener une enquête préliminaire sur l'incident afin d'en 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, à qui et quand?
- Quels sont les renseignements ou les biens visés (en détail)?
- Quel était le marquage de sécurité et quelle est la description des renseignements ou des biens en cause?
- De qui provenaient ces renseignements ou ces biens?
- Quand, pendant combien de temps et dans quelles circonstances les renseignements ou les biens étaient-il vulnérables 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

Zones : Consulter l'annexe A pour en savoir plus sur le concept de la zone de sécurité.

- Le Programme national de recrutement de la GRC (services d'évaluation médicale / psychologique) doit être situé dans une aire de bureau clairement définie (voir les sections Zone de traitement des renseignements et Zone de stockage des renseignements) dont l'accès est contrôlé.
- Le stockage des dossiers papier doit être effectué dans l'aire de bureau assignée par l'entrepreneur au Programme national de recrutement 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 l'aire de bureau assignée par l'entrepreneur au Programme national de recrutement de la GRC, soit dans la salle des serveurs de l'entrepreneur réservée à cet effet.
- L'accès à la zone de traitement des renseignements (bureau général) doit se faire à partir d'une zone sécurisée à accès restreint.

Zone de traitement des renseignements (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 autorisés lorsqu'on les sort des contenants ou des locaux de stockage de dossiers approuvés.

- Généralités :
  - Ne pas laisser de renseignements et de biens de niveau PROTÉGÉ sans surveillance;
  - S'assurer que les renseignements et les biens de niveau PROTÉGÉ ne peuvent pas être vus et que toute discussion à leur sujet ne peut pas être entendue par des personnes qui ne détiennent pas la cote de fiabilité appropriée ou qui n'ont pas « besoin de savoir ».

- Murs et portes du périmètre :
  - L'aire de bureau assignée par l'entrepreneur au Programme national de recrutement de la GRC doit comporter un périmètre clairement défini (murs et portes).
- Contrôle de l'accès, détection des intrusions et surveillance :
  - L'aire de bureau assignée par l'entrepreneur au Programme national de recrutement de la GRC doit être équipée d'un système d'alarme 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).

Zone de stockage des renseignements (versions imprimées et versions électroniques) :

- Généralités :
  - L'accès aux dossiers du programme doit être limité aux employés qui travaillent dans l'aire de bureau assignée par l'entrepreneur au Programme national de recrutement de la GRC et qui détiennent la cote de sécurité appropriée et qui ont « besoin de savoir »;
  - Le stockage des dossiers papier doit respecter les dispositions en matière de « verrouillage » du gouvernement du Canada. Les dossiers doivent être stockés dans l'aire de bureau assignée par l'entrepreneur au Programme national de recrutement de la GRC, et l'accès aux dossiers doit être limité à ceux qui détiennent la cote de sécurité appropriée et qui ont « besoin de savoir ».

AUTRES RÉFÉRENCES EN MATIÈRE DE SÉCURITÉ

Se reporter aux sections sur la sécurité des TI et sur la sécurité du personnel en ce qui concerne d'autres exigences en matière de sécurité.

Exigences en matière de sécurité du personnel

Cote de fiabilité approfondie (CFA) de la GRC

Pour l'entrepreneur ayant besoin d'avoir accès à des renseignements, systèmes, installations ou biens protégés de la GRC. Dans ce scénario, la GRC effectue toutes les vérifications requises pour la délivrance d'une CFA. Aux fins du processus d'approvisionnement de TPSGC, cette exigence doit être indiquée dans les documents contractuels.

Les employés de l'entrepreneur doivent se soumettre à des vérifications effectuées par la GRC avant de pouvoir avoir accès à des systèmes, biens, installations ou renseignements protégés ou classifiés. La GRC se réserve le droit d'interdire à tout employé de l'entrepreneur d'accéder à ses systèmes, biens, installations ou renseignements, et ce, en tout temps.

Dans les cas où la GRC juge qu'une cote de fiabilité approfondie (CFA) ou une habilitation sécuritaire est nécessaire, le soumissionnaire retenu/l'entrepreneur doit lui faire parvenir ce qui suit :

1. formulaire SCT 330-23
2. formulaire SCT 330-60
3. formulaire 1020 (entrevue de sécurité)
4. deux pièces d'identité avec photo (certificat de naissance et permis de conduire)
5. deux jeux d'empreintes digitales
6. visa de travail (s'il y a lieu)
7. deux photos de type passeport
8. entrevue de sécurité

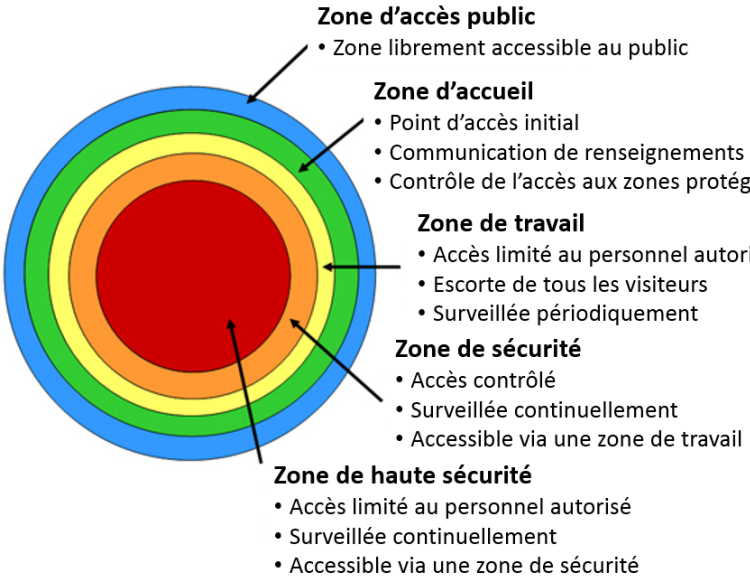
La GRC :

1. effectuera des vérifications de sécurité dont les exigences sont supérieures à celles énoncées dans la Politique sur la sécurité du gouvernement;
2. est responsable des exigences en matière d’escorte dans ses installations ou sur ses sites;
3. effectuera un filtrage de sécurité pour tout haut fonctionnaire clé identifié par la DSIC (en cas de renseignements classifiés).

Annexe A – Zones de sécurité

La *Politique sur la sécurité* du gouvernement (article 10.8 – Limites à l'accès) stipule que « 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. »

Dans la *Norme opérationnelle sur la sécurité matérielle* (article 6.2 – Hiérarchie des zones), on précise que « les ministères doivent assurer l'accès et la protection des biens protégés et classifiés en fonction d'une hiérarchie des zones clairement reconnaissable. »



Zone d'accès public : zone où l'accès est libre pour le public 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 : espace où la transition d'une zone d'accès public à une zone à 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 au public peut être restreint pendant certaines heures de la journée ou pour des motifs particuliers.

Zone de travail : zone 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. Par exemple, des bureaux à aire ouverte ou un local électrique typiques.

Zone de sécurité : zone dont l'accès est limité au personnel autorisé et aux visiteurs autorisés et escortés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée continuellement (24 heures sur 24, 7 jours sur 7). Par 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 escortés comme il se doit; elle doit être indiquée au moyen d'un périmètre bâti selon les caractéristiques techniques recommandées dans l'évaluation de la menace et des risques, surveillée continuellement (24 heures sur 24, 7 jours sur 7) et être un secteur où les détails de l'accès sont enregistrés et vérifiés. Par exemple, une zone où des biens de grande valeur sont manipulés par des employés sélectionnés.

L’accès à ces zones devrait être fondé sur le principe du « besoin de savoir » et être restreint afin de protéger les employés et les biens de valeur. Pour plus de renseignements, consulter le document G1-026 Guide pour l’établissement des zones de sécurité matérielle de la GRC.