RCMP ROYAL CANADIAN MOUNTED POLICE

Guide de sécurité des contrats

M7594224467

Sécurité ministérielle – Direction générale Ottawa

LVERS M7594224467

Table des matières

1. Introduction

1.1. Préambule

1.1.1. Les énoncés de contrat et les annexes du présent guide de sécurité de la Liste de vérification des exigences relatives à la sécurité (LVERS) ne s'appliquent qu'au présent contrat.

1.1.2. Tous les entrepreneurs employés dans le cadre du présent contrat doivent soutenir et maintenir l'environnement de sécurité de la Gendarmerie royale du Canada (GRC) en se conformant aux exigences décrites dans le présent document. Des obligations de sécurité plus complètes seront fournies lors de la phase de Demande de propositions (DP), le cas échéant. Le présent guide de sécurité ne couvre que les services ou le personnel qui stockent ou traitent des renseignements non classifiés.

1.2. Définitions

Compromission	Brèche de sécurité au gouvernement qui comprend, entre autres : • Un accès non autorisé à des renseignements ou des biens de nature délicate, ou la communication, la modification, l'utilisation, l'élimination ou la destruction de renseignements ou de biens de nature délicate, qui pourraient occasionner une perte de confidentialité, d'intégrité, de disponibilité ou de valeur; • Tout agissement, comportement, menace ou geste d'une personne à l'égard d'un employé à son lieu de travail ou d'une personne dans les installations fédérales qui a créé un dommage ou un préjudice à cet employé ou à cette personne; • Les événements entraînant une perte de l'intégrité ou de la disponibilité des services ou des activités du gouvernement.
Entrepreneur	Entité (peut comprendre une ou plusieurs personnes physiques, des sociétés, des partenariats, des sociétés à responsabilité limitée, des fournisseurs de services, des vendeurs, etc.) qui fournit les services à la GRC et à ses partenaires. Il s'agit de l'entité approuvée et désignée comme « entrepreneur » dans le contrat éventuel.
Utilisateur final	Personne qui utilise une application ou un système aux fins prévues, p. ex. l'utilisateur final, contrairement aux ingénieurs de système, aux développeurs et aux administrateurs.
Fuite d'information	Incident lors duquel une ressource d'information est déposée par inadvertance dans un dispositif ou dans un système qui n'est pas autorisé à traiter ces renseignements (p. ex. ITSG-33, IR-9).
Métadonnées	Information décrivant les caractéristiques des données, y compris, par exemple, les métadonnées structurelles décrivant les structures de données (comme le

	format des données, la syntaxe et la sémantique) et les métadonnées descriptives décrivant le contenu des données (comme les étiquettes de sécurité de l'information).
Données organisationnelles	Données ou renseignements créés pour la GRC, recueillis par celle-ci ou dont elle est propriétaire dans quelque format que ce soit, y compris, sans s'y limiter, le texte, l'audio, la vidéo ou l'image, les logiciels et les métadonnées connexes.
Renseignements personnels	Information qui a trait à une personne identifiable et qui est consignée, dans quelque format que ce soit, conformément à l'*article 3 de la Loi sur la protection des renseignements personnels*. Il s'agit, par exemple, des renseignements relatifs à la race, à l'origine nationale ou ethnique, à la religion, à l'âge, à la situation de famille, à l'adresse, à l'éducation ainsi que les renseignements relatifs au dossier médical, au casier judiciaire, aux opérations financières et aux antécédents professionnels. Les renseignements personnels englobent également tout numéro ou symbole d'identification, comme le numéro d'assurance sociale, attribué à une personne.
Chargé de projet	Entité responsable de la gestion du contrat. Toute modification au contrat doit être autorisée par écrit par le chargé de projet, et l'entrepreneur ne doit pas exécuter de travaux en sus ou en dehors du cadre ou de la portée du contrat à la suite de demandes ou d'instructions verbales ou écrites d'une personne autre que le chargé de projet.
Renseignements ou biens protégés	Renseignements dont la divulgation, la destruction, l'interruption, la suppression, la modification sans autorisation, pourraient vraisemblablement porter préjudice à un intérêt autre que national.
Dossier	Tout document sur papier ou tout groupement de données lisible par machine qui contient des renseignements personnels.
Responsable de la sécurité de la GRC	Entité au sein d'une organisation qui est autorisée à approuver la sécurité du contrat et qui détient le pouvoir de signature de la LVERS.
Autorisation de sécurité	Cote de sécurité nécessaire, comme la cote de niveau Secret ou Très secret, désignée par la Sécurité ministérielle de la GRC, qui peut inclure certaines des étapes ou toutes les étapes de vérification de sécurité énumérées dans la clause de sécurité appropriée.
Événement de sécurité	Tout événement, acte, omission ou situation pouvant nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité.
Incident de sécurité	Tout événement (ou série d'événements), tout acte, toute omission ou toute situation qui a entraîné une compromission. Exemples d'incidents de cybersécurité : exploitation active d'une ou de plusieurs vulnérabilités connues, exfiltration de données, défaillance d'un contrôle de sécurité, atteinte d'un service du gouvernement du Canada (GC) géré ou hébergé dans le nuage, etc.

Filtrage de sécurité	Voir la définition à l'annexe A – Définitions, dans la Norme sur le filtrage de sécurité du Conseil du Trésor.
De nature délicate	Dans le domaine de la sécurité en matière de gestion de l'information, catégorie désignant des renseignements ou autres biens qui, s'ils étaient compromis, pourraient vraisemblablement causer un préjudice à l'intérêt national (classifié) ou non national (protégé). Reportez-vous également aux définitions de « classifié » et « protégé ».
Sous-traitant	Toute personne à qui l'entrepreneur confie en sous-traitance la prestation des services de l'entrepreneur, en tout ou en partie.
Sous-traitant ultérieur	Personne physique ou morale, autorité publique, organisme ou autre organisation effectuant le traitement des données personnelles au nom d'un contrôleur des données ou d'un entrepreneur.
Télétravail	Entente entre l'employé d'un entrepreneur et le chargé de projet permettant d'effectuer certaines ou l'ensemble de ses tâches à partir d'un emplacement éloigné. Le télétravail nécessite la conclusion d'une entente de télétravail entre l'entrepreneur et le chargé de projet.
Informations non classifiées	Renseignements n'étant pas de nature délicate qui sont créés et détenus par l'organisation et auxquels toutes les personnes autorisées peuvent avoir accès. La divulgation non autorisée ne causerait aucun préjudice à l'intérêt national ou non national.

2. Exigences générales en matière de sécurité

2.1. Toutes les données organisationnelles, y compris les documents papier et tout autre bien dont la GRC a la responsabilité, doivent être communiquées à l'entrepreneur conformément aux processus déjà approuvés.

2.2. Les renseignements divulgués par la GRC seront gérés, mis à jour et éliminés conformément à l'ensemble du contrat.

2.3. L'entrepreneur avisera rapidement le responsable de la sécurité de la GRC de tout incident de sécurité lié aux données organisationnelles ou au personnel qu'il emploie.

2.4. La présence de biens et d'appareils de TI externes est restreinte dans les installations de la GRC. Les visiteurs qui se rendent dans les locaux de la GRC avec du matériel de TI n'appartenant pas à la GRC doivent remettre tout le matériel électronique à leur arrivée au bureau d'accueil et de sécurité et les reprendre à leur départ.
Remarque : Une exception peut être accordée en cas de cote de fiabilité approfondie valide, avec l'autorisation du chargé de projet. Vous devrez peut-être remplir un formulaire que l'équipe de la Protection des biens examinera.

2.5. Il n'est pas permis de prendre de photos dans les installations de la GRC. Si des photos sont requises, il faut communiquer avec le chargé de projet et la Sécurité ministérielle.

2.6. L'entrepreneur n'est pas autorisé à divulguer des données organisationnelles ou des renseignements secondaires fournis par la GRC à des sous-traitants sans une évaluation de sécurité et une autorisation (ESA) de la GRC.

2.7. La Sécurité ministérielle de la GRC se réserve le droit de mener des inspections et/ou des examens de la sécurité dans les installations de l'entrepreneur et/ou dans les lieux de travail du personnel et de fournir des instructions sur les mesures de protection obligatoires (mesures précisées dans le présent document et possiblement d'autres mesures propres au lieu). Ces inspections peuvent être réalisées avant que des renseignements de nature délicate ne soient communiqués et/ou selon les besoins (si l'entrepreneur déménage ses bureaux). L'objectif de l'inspection est de conserver la robustesse des mesures de sécurité requises.

2.8. Toutes les données organisationnelles doivent être protégées par des moyens cryptographiques. Il faut utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui sont conformes aux Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111 ou versions subséquentes de ce document, disponibles sur le site du Centre canadien pour la cybersécurité). Les exigences en matière d'habilitation de sécurité du personnel des entrepreneurs seront fondées sur les rôles prévus et l'accès aux données et aux systèmes du GC. Au besoin, un guide de classification de sécurité sera ajouté au présent guide de sécurité pour indiquer clairement les exigences en matière d'autorisation de sécurité du personnel.

2.9. Les lieux de travail de tout le personnel de l'entrepreneur doivent être clairement indiqués à l'annexe B – Guide de classification de sécurité et énoncé des travaux (EDT). L'entrepreneur doit faire régulièrement un rapport sur les lieux de travail, ce qui comprend les lieux de télétravail des employés et le nombre de jours travaillés. Si l'on s'attend à ce que le lieu de travail change pendant la durée du contrat, il faut également l'indiquer de manière explicite. Les lieux de travail peuvent comprendre : i) les installations de la GRC, dans le cas du travail sur place; ii) les lieux d'où s'effectue le télétravail; ou iii) un hybride des deux. La GRC doit être avisée de tout changement de lieu de travail qui n'est pas indiqué dans le guide de classification et l'EDT, car cela nécessitera un examen et une approbation du contrat. Le télétravail doit être conforme aux directives de la section sur la gestion du télétravail. Toutes les exigences énoncées à l'annexe C – Lignes directrices de la GRC sur le lieu de télétravail doivent être respectées pendant le télétravail.

2.10. Avant l'autorisation d'un lieu de télétravail donné, toutes les mesures de sécurité ou d'atténuation déterminées dans le cadre d'une évaluation de sécurité de la GRC doivent être respectées.

2.11. Le télétravail doit être effectué au Canada. Des exceptions pour le télétravail à l'extérieur du Canada peuvent être permises dans les pays du Groupe des cinq moyennant une évaluation de sécurité de la GRC et l'approbation écrite du dirigeant principal de la sécurité (DPS) ou de son délégué. Les contrôles et les exigences de sécurité seront déterminés au cours de l'évaluation de sécurité pour chaque lieu de travail.

3. Contrôles de sécurité matérielle

3.1.1 L'expédition des armes à feu est régie par le *Règlement* pris en vertu de la *Loi sur les armes à feu.* Le Règlement régissant la réception des armes à feu des fabricants est le ***Règlement sur l'entreposage, l'exposition et le transport des armes à feu et autres armes par des entreprises***. Dans le cadre de ce programme, les armes à feu seront classées comme des **armes de poing prohibées**, de sorte que nous devrons respecter l'article 12 du *Règlement* :

Transport des armes à feu à autorisation restreinte et des armes de poing prohibées

12 (1) L'entreprise ne peut transporter une arme à feu à autorisation restreinte ou une arme de poing prohibée que si les conditions suivantes sont respectées :

a) elle est non chargée;

b) elle se trouve dans un contenant :

(i) qui est fait d'un matériau opaque et dont la résistance, la construction et les caractéristiques sont telles qu'on ne peut le forcer facilement et qu'il ne peut s'ouvrir accidentellement pendant le transport;

(ii) qui, sous réserve du paragraphe (2), ne porte aucune marque extérieure pouvant indiquer qu'il contient une arme, un dispositif prohibé ou des munitions;

c) dans le cas où le contenant visé à l'alinéa b) se trouve dans un véhicule non surveillé :

(i) si le véhicule est muni d'un coffre ou d'un compartiment similaire pouvant être bien verrouillés, le contenant se trouve dans le coffre ou le compartiment, lequel est bien verrouillé;

(ii) si le véhicule n'est pas muni d'un coffre ou d'un compartiment similaire pouvant être bien verrouillés, le véhicule — ou la partie de celui-ci renfermant le contenant — est bien verrouillé et le contenant n'est pas visible de l'extérieur du véhicule.

(2) Le sous-alinéa (1)b)(ii) ne s'applique pas dans les cas suivants :

a) la seule marque apposée sur l'extérieur du contenant pouvant indiquer que celui-ci contient une arme, un dispositif prohibé ou des munitions représente un nom ou une adresse;

b) le contenant et son contenu sont importés au Canada ou en sont exportés.

4. Contrôles de sécurité des technologies de l'information (TI)

4.1. Transfert des obligations en matière de sécurité

4.1.1. Les obligations de sécurité s'appliquent à l'entrepreneur et à tout sous-traitant ultérieur dans la mesure où elles sont applicables. L'entrepreneur doit s'assurer que ses sous-traitants respectent ces obligations en matière de sécurité, le cas échéant.

4.2. Recours à des sous-traitants et/ou à des sous-sous-traitants

4.2.1. L'entrepreneur doit fournir une liste des sous-traitants et des sous-sous-traitants qui pourraient être utilisés pour exécuter toute partie du travail visant à fournir le service à la GRC ou qui sont liés à une enquête sur un événement ou un incident de sécurité qui pourrait avoir une incidence sur les données organisationnelles de la GRC. La liste doit comprendre l'information suivante :

a) Le nom des sous-traitants et/ou des sous-sous-traitants;
b) L'identification du travail qui serait effectué ou du service qui serait fourni par les sous-traitants et/ou les sous-sous-traitants;
c) L'endroit où les sous-traitants et/ou les sous-sous-traitants effectueraient le travail.

4.2.2. L'entrepreneur doit fournir une liste des sous-traitants et/ou des sous-sous-traitants dans les dix jours suivant la date d'entrée en vigueur du contrat.

4.2.3. L'entrepreneur doit aviser la GRC du recours à tout nouveau sous-traitant et/ou sous-sous-traitant au moins 14 jours avant de lui donner accès aux données organisationnelles.

4.3. Rôles et responsabilités liés à la sécurité

4.3.1. L'entrepreneur doit clairement définir les rôles et responsabilités relatifs aux contrôles et aux fonctions de sécurité de la solution prévue pour lui-même et pour la GRC. Ces rôles et responsabilités touchent, au minimum, ce qui suit :

a) Gestion des comptes;
b) Protection des frontières;
c) Sauvegarde des biens et des systèmes d'information;
d) Gestion des incidents;
e) Surveillance de système;
f) Gestion des vulnérabilités.

4.4. Gestion du télétravail

4.4.1. Les lieux de travail de tout le personnel de l'entrepreneur doivent être clairement indiqués dans le Guide de classification de sécurité et dans l'énoncé des travaux (EDT). L'entrepreneur doit faire régulièrement un rapport sur les lieux de travail, ce qui comprend les lieux de télétravail des employés et le nombre de jours travaillés. Si l'on s'attend à ce que le lieu de travail change pendant la durée du contrat, il faut également l'indiquer de manière explicite. La GRC doit être avisée de tout changement de lieu de travail qui n'est pas indiqué dans le Guide de classification et l'EDT, car cela nécessitera un examen du contrat et une approbation de sécurité.

4.4.2. Les lieux de travail peuvent comprendre : i) les installations de la GRC, dans le cas du travail sur place; ii) les lieux d'où s'effectue le télétravail; ou iii) un hybride des deux. Lorsque le lieu de travail est hybride, le chargé de projet doit fournir un calendrier détaillé indiquant les dates auxquelles le personnel travaillera dans quelle catégorie. Le télétravail comprend tout travail effectué dans un emplacement se trouvant à l'extérieur d'une installation de la GRC. Le télétravail doit être effectué au Canada, mais des exceptions pour le télétravail à l'extérieur du

Canada peuvent être permises dans les pays du Groupe des cinq moyennant une évaluation de sécurité de la GRC et l'approbation écrite du dirigeant principal de la sécurité (DPS) ou de son délégué. Peu importe le lieu de travail à distance, toutes les directives de sécurité énoncées dans le présent document s'appliquent. Cela comprend les travaux dans les installations de l'entrepreneur, dans la résidence d'un employé de l'entrepreneur ou dans tout autre lieu de travail à distance.

4.4.3. Lorsque l'utilisation de l'équipement fourni par la GRC est indiquée dans la LVERS, le chargé de projet et l'entrepreneur doivent :

a) Gérer et surveiller l'accès à distance par l'entrepreneur aux systèmes de la GRC et/ou à ses données organisationnelles;
b) Exécuter l'ensemble des tâches prévues pendant toute la durée du contrat en utilisant l'équipement fourni;
c) Fournir de l'équipement standard de la GRC pour le travail à distance, y compris un ordinateur portable imagé de la GRC avec chiffrement complet approuvé du disque;
d) Utiliser l'authentification multifactorielle avec les justificatifs d'identité standard fournis par la GRC pour toutes les exigences d'accès sécurisé (p. ex. accès au RPV);
e) Veiller à ce que l'entrepreneur comprenne et reconnaisse ses responsabilités et se conforme aux Contraintes d'usage des technologies de l'information de la GRC;S'assurer que l'équipement de la GRC demeure en tout temps dans les lieux de travail indiqués.

4.4.4. Lorsque l'utilisation de l'équipement fourni par la GRC n'est pas indiquée dans la LVERS, l'entrepreneur peut utiliser son propre équipement à condition qu'il respecte les exigences de sécurité énoncées dans la section sur la protection des points terminaux.

4.5. Protection des points terminaux

4.5.1. Lorsque des points terminaux sont fournis par l'entrepreneur, ce dernier doit mettre en œuvre, gérer et surveiller les points d'accès sécurisés à l'aide de protections hébergées actives afin de prévenir l'utilisation de maliciels, les attaques et les abus, conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide to General Server Security [guide relatif à la sécurité générale des serveurs]), des points de référence du Center for Internet Security (CIS) ou d'une norme équivalente approuvée par écrit par la GRC.

4.6. Protection cryptographique

4.6.1. Le personnel de l'entrepreneur doit :

a) Configurer toute solution cryptographique qui est adoptée à l'égard des services et qui est utilisée dans le cadre de la mise en œuvre de mesures de protection de la confidentialité ou de l'intégrité ou encore d'un mécanisme d'authentification (p. ex. solutions liées au réseau privé virtuel, protocole TLS, modules logiciels, indicateurs de rendement clés et jetons d'authentification, le cas échéant), conformément aux algorithmes cryptographiques, aux tailles de clés de chiffrement et aux périodes de validité des clés approuvés par le Centre de la sécurité des télécommunications (CST);

b) Utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui sont conformes aux Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111) ou aux versions subséquentes de ce document, disponibles sur le site du Centre canadien pour la cybersécurité.

4.7. Protection des données

4.7.1. Lorsque l'utilisation de l'équipement fourni par la GRC est requise, toutes les tâches assignées à l'entrepreneur doivent être exécutées à l'aide de l'équipement fourni et suivre les directives de la GRC sur la gestion du télétravail. Le personnel de l'entrepreneur n'est pas autorisé à utiliser des logiciels, des services ou de l'équipement non approuvés qui ne sont pas fournis par la GRC, sauf indication contraire écrite. Si l'utilisation de l'équipement fourni par la GRC n'est pas requise, l'entrepreneur peut utiliser son propre équipement à condition qu'il respecte les exigences de sécurité énoncées dans la section sur la protection des points terminaux.

4.7.2. Les données organisationnelles ne doivent pas être stockées dans les services infonuagiques à moins qu'une autorisation d'exploitation (AE) ait été délivrée par la Sécurité ministérielle de la GRC. Le chargé de projet doit s'assurer qu'une AE a été émise et que toutes les conditions sont respectées pendant toute la durée du contrat.

4.7.3. Toute sauvegarde de données organisationnelles est assujettie aux mêmes lignes directrices de sécurité pour le chiffrement et les contrôles d'accès que la principale source de données.

4.7.4. Les dossiers électroniques et les appareils multimédias doivent être nettoyés ou détruits conformément à la norme ITSP.40.006 ou aux versions ultérieures, accessible sur le site Web du Centre canadien pour la cybersécurité.

4.7.5. L'entrepreneur et/ou son personnel ne doivent pas faire de copies des bases de données ou des parties de ces bases de données contenant des données organisationnelles à l'extérieur des capacités de résilience des services réguliers et dans les lieux ou zones régionaux approuvés au sein de la GRC.

4.7.6. L'entrepreneur et/ou son personnel ne doivent pas déplacer ou transmettre les données organisationnelles au repos à l'extérieur des régions de service convenues, sauf lorsque l'approbation est obtenue de la GRC.

4.7.7. L'entrepreneur doit :

a) Mettre en œuvre un chiffrement de bout en bout pour toutes les données protégées en transit. Tout chiffrement des données en transit doit satisfaire aux exigences du document ITSP.40.111 Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B – ITSP.40.111, ou des versions ultérieures, accessibles sur le site Web du Centre canadien pour la cybersécurité;
b) Mettre en œuvre le chiffrement des données au repos pour tous les services qui hébergent des données organisationnelles, y compris toutes les métadonnées ou tous les journaux dérivés ou liés aux données organisationnelles, lorsque le chiffrement des données au repos demeure en vigueur, ininterrompu et actif en tout temps, même en cas de panne d'équipement ou de technologie, conformément au document ITSP.40.111 Algorithmes

cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B, ou des versions ultérieures, accessibles sur le site Web du (Centre canadien pour la cybersécurité);

c) Mettre en place des contrôles de sécurité qui restreignent l'accès administratif aux données organisationnelles, y compris à toutes les métadonnées ou à tous les journaux dérivés des données et des systèmes organisationnels ou connexes par l'entrepreneur et qui permettent d'exiger l'approbation de la GRC avant que l'entrepreneur puisse accéder aux données organisationnelles pour effectuer des activités de soutien, d'entretien ou d'exploitation;

d) Prendre des mesures raisonnables pour s'assurer que le personnel de l'entrepreneur n'a pas de droits d'accès permanents ou continuels aux données organisationnelles, sans un besoin de savoir, y compris les ressources qui fournissent un soutien technique ou à la clientèle, en fonction de l'approbation de la GRC;

e) Empêcher tout membre du personnel de l'entrepreneur de détenir des justificatifs d'identité qui permettent à ce membre de supprimer, de modifier ou de copier des données organisationnelles à moins que cette personne n'ait été autorisée par la GRC au niveau approprié jugé nécessaire par cette dernière.

4.8. Transport/transmission des données

4.8.1. S'il est nécessaire de transporter des données organisationnelles, elles doivent être transportées au moyen d'un dispositif de stockage portatif conforme à la norme FIPS 140-2 niveau 2 ou supérieur fourni par la GRC. L'accès à cet appareil doit être limité au personnel de l'entrepreneur ayant obtenu une cote de sécurité appropriée, ainsi qu'au client de la GRC. Le dispositif de stockage portatif conforme à la norme FIPS 140-2 de niveau 2 doit être livré en main propre ou expédié conformément à la section Contrôles de sécurité matérielle – Transport/transmission des biens matériels.

4.8.2. 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 appropriée.

4.8.3. Lorsqu'il est nécessaire de transmettre des données organisationnelles, y compris toutes les métadonnées ou tous les journaux dérivés des données organisationnelles ou liés à celles-ci, cela doit être effectué de manière sécurisée, notamment par la mise en œuvre du chiffrement des données en transit, comme indiqué dans la section Protection cryptographique.

4.9. Élimination des données et retour des dossiers

4.9.1. L'entrepreneur doit cryptodéchiqueter les ressources (p. ex. l'équipement, les unités de stockage, les fichiers et la mémoire) qui contiennent des données organisationnelles et s'assurer que les données précédemment stockées ne peuvent pas être consultées par d'autres clients après leur diffusion. Cela comprend toutes les copies des données organisationnelles qui sont créées aux fins de disponibilité accrue et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être harmonisée à l'un des documents suivants :

a) Nettoyage des supports de TI – ITSP.40.006 ou versions ultérieures, accessible sur le site Web du Centre canadien pour la cybersécurité.
b) Lignes directrices pour le nettoyage des supports de TI – NIST SP 800-88; ou
c) À la demande de la GRC, l'entrepreneur doit produire un document qui décrit son processus d'élimination ou de réutilisation des ressources.

4.9.2. L'entrepreneur doit confirmer à la GRC, par la présentation d'une lettre d'attestation ou d'entrées de journal, qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de tout système, de toute capacité (logiciel ou processus), de toute donnée ou de toute information retirés ou détruits une fois que la GRC a cessé d'utiliser les services. La GRC peut exiger une preuve que les clés de chiffrement ont été détruites ou que les données ont été cryptodéchiquetées avec succès pour empêcher la récupération des données.

4.9.3. En cas de résiliation du contrat ou à la demande de la GRC, l'entrepreneur doit :

a) Veiller à ce que tous les contrôles de protection des données et de sécurité demeurent en place, conformément au Guide de sécurité, pendant la période où la GRC récupère les données organisationnelles;
b) Fournir à la GRC l'accès à ses données organisationnelles pendant une période qui permet à la GRC de récupérer toutes les données organisationnelles de l'entrepreneur.

4.10. Intervention en cas d'événement de sécurité

4.10.1. Selon le plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC), voici la définition d'un événement en matière de sécurité : « Tout événement, acte, omission ou situation pouvant nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité ». En conséquence, l'entrepreneur doit avertir et aviser rapidement le responsable de la sécurité de la GRC (par téléphone et/ou par courriel) de toute compromission, de toute violation ou de toute preuve d'un tel événement, notamment ce qui suit :

a) Événement de sécurité;
b) Défaillance de la sécurité d'un bien;
c) Fuite de données;
d) Accès irrégulier ou non autorisé à un bien;
e) Copie à grande échelle d'une ressource d'information;
f) Toute autre activité irrégulière relevée par l'entrepreneur qui l'amène à croire raisonnablement que le risque de compromission ou d'atteinte à la sécurité ou à la vie privée est ou peut être imminent, ou que les mesures de protection existantes ont cessé de fonctionner.

4.10.2. Si l'entrepreneur prend connaissance ou détermine qu'une compromission ou une atteinte à la sécurité s'est produite (par exemple, entraînant la destruction, la perte, la modification, la divulgation ou l'accès accidentels ou illégaux) pendant que l'entrepreneur traite des renseignements personnels ou des données organisationnelles, il doit :

a) Aviser le responsable de la sécurité de la GRC de l'événement de sécurité dans un délai de 24 heures;
b) Enquêter sur l'événement de sécurité et fournir à la GRC des renseignements détaillés sur cet événement;
c) Prendre des mesures raisonnables pour atténuer la cause de l'événement de sécurité et minimiser les dommages qui en découlent.

4.11. Impression, numérisation et photocopie

4.11.1. L'impression, la numérisation et/ou la photocopie de données organisationnelles de nature délicate doivent être autorisées au préalable par la GRC.

4.11.2. Lorsque l'impression, la numérisation ou la photocopie est autorisée, l'entrepreneur doit :

a) Disposer d'imprimantes, de numériseurs ou de photocopieurs réservés supplémentaires qui ne sont pas directement connectés à un réseau, y compris Internet. Les connexions locales réservées de ces appareils aux points terminaux de l'entrepreneur sont acceptables;
b) Respecter les exigences énoncées dans la section Contrôles de sécurité matérielle sur l'entreposage, la production de renseignements sur papier ou d'autres biens et la destruction;
c) Nettoyer et/ou détruire les appareils d'impression, de numérisation et de photocopie (comme les appareils multifonctions, les imprimantes, les photocopieurs) conformément au document ITSP.40.006 Nettoyage des supports de TI
ou versions subséquentes, disponibles sur le site du Centre canadien pour la cybersécurité.

4.12. Gestion de l'identité et de l'accès

4.12.1. Lorsque l'utilisation de l'équipement de la GRC est requise, le personnel de l'entrepreneur se verra attribuer des justificatifs d'identité de la Gestion des biens d'infrastructure (GBI) de la GRC leur permettant d'accéder aux biens protégés de la GRC. Les justificatifs d'identité de la GBI de la GRC ne doivent être utilisés que dans le cadre de l'exécution des tâches décrites dans les documents contractuels et doivent être révoqués à la fin du présent contrat.

4.13. Évaluation de la sécurité et autorisation

4.13.1. Avant que des solutions élaborées en tout ou en partie par des entrepreneurs ne soient transférées dans un environnement de production, une autorisation provisoire d'exploiter ou une autorisation d'exploitation complète doit être accordée. L'obtention d'une autorisation provisoire d'exploiter nécessite une évaluation de sécurité dans le cadre du processus d'ESA, qui peut être lancé en communiquant avec la Sécurité ministérielle.

4.14. Cessation d'emploi

4.14.1. L'entrepreneur doit avoir mis en œuvre une procédure documentée de résiliation ou de changement de statut pour le personnel. Elle doit comprendre au moins ce qui suit :

a) Transmettre un avis de résiliation au chargé de projet le jour même de la résiliation;

b) Retirer l'accès au système d'information le jour même de la résiliation;
c) Résilier et/ou révoquer les authentifiants et/ou les identifiants associés à la personne dans un délai de 24 heures;
d) Mener des entrevues de fin de contrat qui comprennent une discussion sur les éléments énoncés dans la Norme sur le filtrage de sécurité du Secrétariat du Conseil du Trésor (SCT) et toute disposition connexe du Programme de sécurité industrielle;
e) Soumettre le formulaire d'information sur la sécurité 330-47 pour la résiliation de l'autorisation de sécurité de l'entrepreneur;
f) Récupérer tous les biens liés au système d'information de la GRC se rattachant à la sécurité, y compris les cartes d'accès, dans un délai de 24 heures;
g) Conserver l'accès à l'information et aux systèmes d'information de la GRC qui étaient sous le contrôle de la personne faisant l'objet de la résiliation.

4.14.2. Le personnel de l'entrepreneur, à la résiliation du contrat pour quelque raison que ce soit, doit retourner au chargé de projet tous les appareils fournis par la GRC, notamment ce qui suit :

a) Ordinateurs portatifs;
b) Téléphones cellulaires;
c) Clés USB;
d) Cartes à puce.

5. Contrôles de sécurité du personnel

5.1. Tous les entrepreneurs travaillant pour la GRC ou embauchés par celle-ci doivent détenir une autorisation de sécurité valide. Si le personnel de l'entrepreneur a accès à des renseignements de nature délicate de la GRC, l'autorisation requise de la GRC ou l'équivalence approuvée par la GRC* doit être au niveau approprié. Le personnel de l'entrepreneur doit faire l'objet d'une vérification par la GRC avant de se voir accorder l'accès à des renseignements, aux systèmes, aux biens et/ou aux installations. La GRC se réserve le droit d'interdire l'accès à tout membre du personnel de l'entrepreneur à tout moment. En cas d'incident, de sécurité ou autre, la GRC a le droit de refuser ou de suspendre l'accès aux emplacements, aux services ou aux données de la GRC si les situations justifient cette mesure, en attendant l'examen de l'incident.

5.2. Lorsque la GRC détermine qu'une autorisation d'accès à l'installation (FA2) est requise, elle invite les entrepreneurs à visiter son portail en ligne pour y remplir les formulaires d'autorisation. **Il a été déterminé que l'autorisation FA2 correspond au niveau requis pour la formation sur place ou les certifications avec escorte technique.**

5.3. Tout le personnel de l'entrepreneur et des sous-traitants doit maintenir une autorisation de sécurité correspondant au caractère délicat des travaux à réaliser tout au long du cycle de vie du contrat (en conformité avec les dispositions de la LVERS).

5.4. L'autorisation de sécurité du personnel doit être en place avant le début de tout travail lié au besoin.

5.5. Lorsque le recours à du personnel sans cote de sécurité est nécessaire, les rôles doivent être identifiés et approuvés au préalable par la GRC dans la Liste de vérification des exigences relatives à la sécurité (LVERS) une fois le fournisseur retenu choisi.

5.6. Il incombera à l'entrepreneur d'informer la GRC de tout changement concernant les exigences en matière de sécurité relatives au personnel. Par exemple : personnel autorisé qui quitte l'entreprise ou qui ne participe plus au contrat de la GRC, nouveau personnel nécessitant un filtrage de sécurité et personnel nécessitant un renouvellement de son filtrage de sécurité.

5.7. Les vérifications de filtrage de sécurité du personnel effectuées par la GRC dépasseront les exigences de sécurité prescrites par la Politique sur la sécurité du gouvernement.

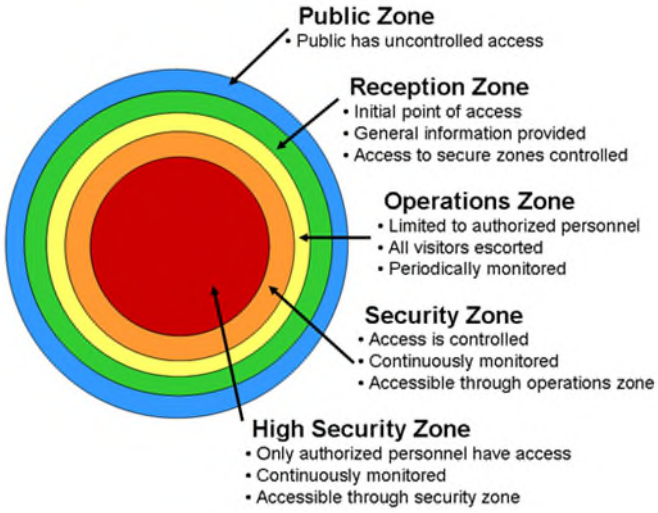
5.8. La GRC se réserve le droit d'augmenter ou de modifier les niveaux de sécurité requis, selon ce qu'elle juge approprié, lorsque les rôles professionnels auront été mieux définis.

**Les équivalences de cote/autorisation de sécurité doivent être approuvées par écrit par la GRC par le dirigeant principal de la sécurité (DPS) ou son délégué.*

Annexe A – Concept de zone de sécurité

Selon la *Politique du gouvernement sur la sécurité (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 ».



Public Zone Public has uncontrolled access	Zone d'accès public Zone où l'accès est libre pour le public.
Reception Zone Initial point of access General information provided Access to secure zones controlled	Zone d'accueil Point d'accès initial. Renseignements généraux fournis. L'accès aux zones sécurisées est contrôlé.
Operations Zone Limited to authorized personnel All visitors escorted Periodically monitored	Zone de travail Accès limité aux personnes autorisées. Tous les visiteurs doivent être accompagnés. Fait l'objet d'une surveillance périodique.
Security Zone Access is controlled Continuously monitored Accessible through operations zone	Zone de sécurité L'accès est contrôlé. Fait l'objet d'une surveillance continue. Accessible à partir d'une zone de travail.
High Security Zone Only authorized personnel have access Continuously monitored Accessible through security zone	Zone de haute sécurité Accès strictement restreint au personnel autorisé. Fait l'objet d'une surveillance continue. Accessible à partir d'une zone de sécurité.

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 – Zone 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 des visiteurs peut être limité à certaines heures de la journée ou pour des raisons spécifiques.

Zone de travail – Zone dont l'accès est limité au personnel qui y travaille et aux visiteurs dûment accompagnés; elle doit être balisée par un périmètre reconnaissable et surveillée périodiquement. Exemples : un espace à bureaux à aire ouverte typique ou le 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 elle doit être surveillée continuellement, c'est-à-dire jour et nuit, sept jours par semaine. Exemple : zone où de l'information secrète est traitée ou conservée.

Zone haute sécurité – Zone dont l'accès est limité au personnel autorisé ayant fait l'objet d'un contrôle approprié et aux visiteurs autorisés et dûment escortés; elle doit être indiquée par un périmètre construit conformément aux spécifications recommandées dans l'EMR, être surveillée continuellement, c.-à-d. 24 heures par jour et 7 jours par semaine, et être une zone où les détails d'accès sont consignés et vérifiés. Exemple : une zone où des biens de grande valeur sont traités par le personnel sélectionné.

L'accès aux zones devrait reposer sur les principes du « besoin de savoir » et de la restriction de l'accès pour protéger le personnel et les biens de valeur. Consultez le guide G1-026 Guide pour l'établissement des zones de sécurité matérielle de la GRC pour plus de détails.

Annexe B – Guide de classification de sécurité

Ce tableau doit être rempli par le chargé de projet lorsque la Sécurité ministérielle l'exige. Il est important de fournir le plus de détails possible dans le tableau, car celui-ci constitue une aide à la décision pour l'attribution des niveaux d'autorisation de sécurité (par exemple, il est utile d'inclure des informations telles que le lieu de travail des ressources, les systèmes auxquels ces ressources auront accès et les privilèges d'accès qu'elles peuvent avoir).

Dans certains cas, il est possible de réutiliser l'information contenue dans l'énoncé des travaux associé au contrat.

Au moment de remplir ce tableau, laisser la colonne Niveau d'autorisation de sécurité vide, cette colonne sera remplie par les spécialistes des contrats de la Sécurité du personnel.

Rôle ou fonction	Type de données consulté	Lieu de travail (Inclure la ville si elle se trouve à l'extérieur du Canada)	Description et détails du rôle	Niveau d'autorisation de sécurité
Formateurs	*Aucun accès aux renseignements PROTÉGÉS*	*Sur place, Ottawa/Regina*	- *Formation sur les pistolets* - *Certification et renouvellement de la certification*	FA2 avec escorte

Annexe C – Lignes directrices de la GRC sur le lieu de télétravail

C.1. Les lignes directrices de la GRC sur le lieu de télétravail sont propres au présent contrat seulement.

C.2. Des contrôles d'accès doivent être mis en œuvre pour restreindre l'accès à l'information aux personnes qui ont un « besoin de savoir » véritable.

C.3. Le personnel de l'entrepreneur doit prendre les mesures raisonnables pour protéger les renseignements et les biens fondés sur des données organisationnelles de nature délicate contre la divulgation non autorisée, la perte, le vol, l'incendie, la destruction, les dommages ou les modifications.

C.4. Le ou les lieux de télétravail désignés dans le contrat peuvent faire l'objet d'un examen ou d'une inspection de sécurité en tout temps par un représentant de la GRC pour garantir que tous les contrôles sont conformes aux fins de la protection des biens et des données organisationnelles de nature délicate.

C.5. L'entrepreneur et son personnel doivent signaler rapidement au responsable de la sécurité la GRC toute utilisation ou communication non autorisée des renseignements échangés dans le cadre du présent contrat et lui fournir des précisions sur l'utilisation ou la communication non autorisée.

C.6. Si la nature ou la portée des travaux change, l'entrepreneur doit en aviser rapidement le responsable de la sécurité de la GRC, qui, conjointement avec l'entrepreneur, examinera et déterminera les mesures d'atténuation appropriées en matière de sécurité.

C.7. Le responsable de la sécurité de la GRC est le premier point de contact pour la prestation, aux entrepreneurs, de conseils et d'une orientation sur les exigences et les contrôles de la politique de sécurité.

Travail sans papier

C.8. Le chargé de projet doit mettre en œuvre des options de travail sans papier pour le personnel de l'entrepreneur.

C.9. Les données organisationnelles de nature délicate doivent être chiffrées au repos et pendant le transit.

a. Le chiffrement complet du disque est requis pour tous les appareils qui traitent des données organisationnelles de nature délicate.

b. Toutes les données organisationnelles de nature délicate doivent être chiffrées au minimum au moyen de l'algorithme standard de chiffrement avancé (AES) dont la longueur des clés est de 128 (AES-128).

C.10. L'authentification multifactorielle est requise pour l'accès à des données organisationnelles de nature délicate.

C.11. L'utilisation de dispositifs de stockage ou de périphériques personnels (dispositifs USB, téléphones cellulaires, écrans, imprimantes, numériseurs, caméra Web, casque d'écoute, etc.) est interdite pour l'accès aux données organisationnelles et leur traitement.

C.12. Lorsqu'ils sont autorisés, seuls les supports de stockage portatifs approuvés et fournis par la GRC (clé USB, cartes SD, CD/DVD, etc.) sont autorisés.

C.13. Lorsqu'il doit envoyer par courriel ou transmettre des données de nature délicate, l'entrepreneur doit s'assurer que les renseignements sont chiffrés et qu'ils utilisent un service approuvé et autorisé par la GRC.

C.14. Lorsque vous transportez des renseignements et des biens et des renseignements papier de nature délicate sous quelque forme que ce soit à destination et en provenance d'un lieu de télétravail, ne faites aucun arrêt inutile entre des lieux sécurisés. Ne laissez jamais de renseignements et de biens de la GRC sans surveillance, mettez sous clé tous les appareils ou supports papier contenant des données de la GRC et verrouillez les portes lorsque vous vous absentez du lieu de télétravail. Ne laissez jamais de supports papier ou de dispositifs contenant des données organisationnelles de la GRC dans un véhicule.

C.15. Il est interdit de discuter de données organisationnelles de nature délicate ou d'en partager au moyen d'applications d'audioconférence ou de vidéoconférence non approuvées par la GRC.

C.16. Toutes les réunions virtuelles entre la GRC et l'entrepreneur tenues tout au long du contrat utiliseront une solution de vidéoconférence autorisée pour discuter de données organisationnelles de nature délicate. La GRC lancera toutes les séances de vidéoconférence et fournira à l'entrepreneur le lien vers la vidéoconférence.

C.17. L'entrepreneur peut être tenu d'installer le client de vidéoconférence correspondant sur ses points terminaux.

C.18. Lorsqu'il n'est pas utilisé, l'équipement de TI servant au traitement de données organisationnelles de nature délicate doit être entreposé hors de vue et dans une pièce ou un contenant verrouillé (p. ex. tiroir de bureau, boîte, classeur) dont le personnel de l'entrepreneur contrôle l'accès en tout temps.

Contrôle de l'environnement et de l'espace de travail

C.19. Le personnel contractuel doit :

a. Travailler dans un espace réservé aménagé de telle sorte que des personnes partageant le même espace ne puissent pas voir ou entendre ce qui s'y passe, et que l'on ne puisse pas voir non plus, par les fenêtres, ce qui s'y passe;
b. Être conscient de son environnement et veiller à ce qu'aucune donnée organisationnelle de nature délicate en arrière-plan ne soit transmise par vidéo ou audio.

C.20. Toutes les discussions de nature délicate doivent être protégées par les moyens suivants :

a. Utiliser exclusivement de l'équipement et des logiciels approuvés;
b. Utiliser des casques d'écoute pour l'audio ainsi qu'un espace de travail à l'abri des regards, ou une pièce fermée aménagée de telle sorte que des personnes partageant le même espace ne puissent pas voir ou entendre ce qui s'y passe, et que l'on ne puisse pas voir non plus, par les fenêtres, ce qui s'y passe;
c. Activer les caméras Web uniquement lorsqu'elles sont utilisées;
d. Savoir comment désactiver le microphone et fermer la caméra rapidement au besoin;
e. Ne pas discuter de données organisationnelles d'un niveau supérieur à Protégé B;
f. S'assurer que les appareils mobiles sont laissés à l'extérieur des zones où des discussions de nature délicate ont lieu;
g. Éteindre les appareils sans fil permettant la transmission de la voix ou désactiver le microphone de ces appareils pendant les réunions où il est question de données organisationnelles de nature délicate;

C.21. Ne pas discuter de données organisationnelles de nature délicate sur des téléphones personnels ou encore de l'équipement ou des logiciels personnels.

Exigences supplémentaires relatives à l'utilisation du matériel de TI de la GRC

C.22. Lorsqu'il utilise l'équipement de technologies de l'information (TI) de la GRC, le personnel de l'entrepreneur doit :

a. Lire et signer les Contraintes d'usage des technologies de l'information de la GRC;
b. Respecter les politiques et les normes de la GRC en matière de TI et de sécurité.

Résiliation/expiration du contrat

C.23. Au moment d'une résiliation ou d'une expiration visant un membre du personnel de l'entrepreneur, quel qu'il soit, l'entrepreneur doit immédiatement aviser le chargé de projet de la GRC, récupérer tout

l’équipement de TI de la GRC ainsi que toute information connexe, et les soumettre au chargé de projet de la GRC aux fins d’élimination ou de retrait de l’information liée au contrat avec la GRC.