Gendarmerie royale du Canada | Royal Canadian Mounted Police

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À :

Bid Receiving/Réception des soumissions

angelo.kaldis@rcmp-grc.gc.ca

REQUEST FOR PROPOSAL

DEMANDE DE PROPOSITION

Proposal to: Royal Canadian Mounted Police

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition à : Gendarmerie royale du Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux appendices ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments: **–** Commentaires :

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT

LE PRÉSENT DOCUMENT COMPORTE UNE EXIGENCE EN MATIÈRE DE SÉCURITÉ

Title – Sujet **Formation annuelle obligatoire en ligne pour les membres d'équipage**		**Date** **2023/04/24**
Solicitation No. – Nº de l'invitation **202105319**		
Client Reference No. - Nº De Référence du Client **202105319**		
Solicitation Closes – L'invitation prend fin		
At/à :	**14 : 00**	EDT (Eastern Daylight Time) HAE (heure avancée de l'Est)
On/le :	**2023/06/13**	

Delivery – Livraison See herein — Voir aux présentes	**Taxes – Taxes** See herein — Voir aux présentes	**Duty – Droits** See herein — Voir aux présentes

Destination of Goods and Services – Destinations des biens et services
See herein — Voir aux présentes

Instructions
See herein — Voir aux présentes

Address Inquiries to –
Adresser toute demande de renseignements à
Angelo Kaldis
Procurement Specialist, HQ Procurement and Contracting
angelo.kaldis@rcmp-grc.gc.ca

Telephone No. – Nº de téléphone
519-318-3897

Delivery Required – **Livraison exigée** See herein — Voir aux présentes	**Delivery Offered** – **Livraison proposée**
Vendor/Firm Name, Address and Representative – Raison sociale, adresse et représentant du fournisseur/de l'entrepreneur :	
Telephone No. – Nº de téléphone	**Facsimile No. – Nº de télécopieur**
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) – Nom et titre de la personne autorisée à signer au nom du fournisseur/de l'entrepreneur (taper ou écrire en caractères d'imprimerie)	
Signature	**Date**

Canada

TABLE DES MATIÈRES

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1. Présentation
1.2. Sommaire
1.3. Comptes rendus
1.4. Mécanisme de recours

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1. Instructions, clauses et conditions uniformisées
2.2. Présentation des soumissions
2.3. Demandes de renseignements en période de soumission
2.4. Lois applicables
2.5. Promotion de l'initiative de dépôt direct
2.6. Améliorations apportées au besoin pendant la demande de soumissions
2.7. Données volumétriques

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1. Procédures d'évaluation
4.2. Méthode de sélection

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

5.1. Attestations préalables à l'attribution du contrat et renseignements supplémentaires
Pièce jointe 1 de la partie 5 : Attestation d'absence de collusion dans l'établissement de la soumission
Pièce jointe 2 de la partie 5 : Formulaire d'attestation de l'éditeur de logiciels-services

PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ

6.1. Exigences en matière de sécurité

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

7.1. Énoncé des travaux
7.2. Clauses et conditions générales
7.3. Exigences en matière de sécurité
7.4. Durée du contrat
7.5. Autorités
7.6. Divulgation proactive des contrats conclus avec d'anciens fonctionnaires
7.7. Paiement

7.8. Instructions relatives à la facturation
7.9. Attestations et renseignements supplémentaires
7.10. Lois applicables
7.11. Priorité des documents
7.12. Ombudsman de l'approvisionnement
7.13. Assurances

Liste des annexes :

Annexe A Énoncé des travaux
Annexe B Base de paiement
Annexe C Liste de vérification des exigences relatives à la sécurité (LVERS) et guide de sécurité
Annexe D Critères d'évaluation

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Présentation

La demande de soumissions contient sept parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

Partie 1 Renseignements généraux : renferme une description générale du besoin;

Partie 2 Instructions à l'intention des soumissionnaires : renferme les instructions, clauses et conditions relatives à la demande de soumissions;

Partie 3 Instructions pour la préparation des soumissions : donne aux soumissionnaires des instructions sur la façon de préparer leur soumission;

Partie 4 Procédures d'évaluation et méthode de sélection : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, ainsi que la méthode de sélection;

Partie 5 Attestations et renseignements supplémentaires : comprend les attestations et les renseignements supplémentaires à fournir;

Partie 6 Exigences en matière de sécurité : comprend les exigences particulières que doivent satisfaire les soumissionnaires;

Partie 7 Clauses du contrat subséquent : contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent.

Les annexes comprennent l'énoncé des travaux, la base de paiement, la Liste de vérification des exigences relatives à la sécurité (LVERS) et le Guide de sécurité, ainsi que les critères d'évaluation.

1.2 Sommaire

1.2.1 La Gendarmerie royale du Canada (GRC) a besoin d'une formation annuelle en ligne sur l'aviation. La formation vise à s'assurer qu'environ 165 membres du personnel du Service de l'air de la GRC, y compris des pilotes, des techniciens d'entretien d'aéronefs (T.E.A.), des agents tactiques d'aviation et des coordonnateurs de vols, satisfont aux exigences de Transports Canada et de la GRC pour maintenir un niveau de compétence sécuritaire. Le Service de l'air de la GRC est autorisé à exploiter des aéronefs à titre d'exploitant privé, à condition que ses pilotes d'aéronefs à voilure fixe et à voilure tournante, ses T.E.A. et ses membres d'équipage suivent des cours obligatoires, dont bon nombre peuvent être administrés au moyen d'une solution Web qui respecte ou dépasse les exigences du *Règlement de l'aviation canadien* (RAC). L'entrepreneur doit exécuter les travaux conformément à l'Annexe « A » – Énoncé des travaux.

Tout contrat subséquent (un contrat seulement) sera valide à partir de la date d'attribution du contrat pour une durée d'un (1) an, avec l'option irrévocable permettant de prolonger le contrat de quatre (4) périodes supplémentaires d'un (1) an selon les mêmes modalités.

Cette exigence est assujettie aux dispositions de l'Accord de libre-échange canadien (ALEC), de l'Accord de libre-échange Canada-Chili, de l'Accord de

libre-échange Canada-Colombie, de l'Accord de libre-échange Canada-Honduras, de l'Accord de libre-échange Canada-Panama, l'Accord de libre-échange Canada-Pérou et de l'Accord de libre-échange Canada-Ukraine.

1.2.2 Ce besoin comporte des exigences relatives à la sécurité. Pour de plus amples renseignements, consulter la Partie 6 – Exigences relatives à la sécurité, exigences financières et autres exigences, et la Partie 7 – Clauses du contrat subséquent. Pour en savoir plus sur le filtrage de sécurité du personnel et de l'organisation ainsi que sur les clauses de sécurité, les soumissionnaires devraient consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html). Prière de noter que le site Web ci-dessus est propre à TPSGC; les exigences et les processus peuvent différer de ceux de la GRC.

1.3 Comptes rendus

Les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Ils doivent en faire la demande à l'autorité contractante dans les 15 jours ouvrables suivant la réception des résultats du processus de demande de soumissions. Le compte rendu peut être fourni par écrit, par téléphone ou en personne.

1.4 Mécanisme de recours

Si vous avez des préoccupations concernant le processus d'approvisionnement, veuillez consulter la page Mécanismes de recours sur le site Achatsetventes.gc.ca. Veuillez noter qu'il existe des délais stricts pour déposer une plainte auprès du Tribunal canadien du commerce extérieur (TCCE) ou du Bureau de l'ombudsman de l'approvisionnement (BOA).

https://achatsetventes.gc.ca/pour-les-entreprises/vendre-au-gouvernement-du-canada/suivi-des-soumissions/processus-de-contestation-des-offres-et-mecanismes-de-recours

http://opo-boa.gc.ca/plaintesurvol-complaintoverview-fra.html

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions par un numéro, une date et un titre sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Travaux publics et Services gouvernementaux Canada.

Modification touchant le nom du ministère : Puisque la présente demande de propositions émane de la Gendarmerie royale du Canada (GRC), il faut interpréter toute mention de Travaux publics et Services gouvernementaux Canada (TPSGC) ou de sa ministre dans les clauses et conditions, y compris celles tirées des CCUA, comme désignant en fait la GRC ou son ministre.

Les soumissionnaires qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions, et acceptent les clauses et les conditions du contrat subséquent.

Le document 2003 (2022-03-29) Instructions uniformisées – biens ou services – besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

Le paragraphe 5.4 du document 2003, Instructions uniformisées – biens ou services – besoins concurrentiels, est modifié comme suit :

Supprimer : 60 jours;

Insérer : Cent quatre-vingts (180) jours.

2.2 Présentation des soumissions

Les soumissions doivent être présentées uniquement à l'Unité de réception des soumissions de la GRC au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions.

REMARQUE : La GRC n'a pas été approuvée pour la soumission au moyen du service Connexion de la Société canadienne des postes (SCP).

Les soumissions transmises à la GRC par télécopieur ne seront pas acceptées.

2.3 Demandes de renseignements en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins sept (7) jours civils avant la date de clôture des soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

Les soumissionnaires doivent citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question. Ils doivent prendre soin d'expliquer chaque question en donnant suffisamment de détails pour permettre au gouvernement du Canada d'y apporter des réponses exactes. Les demandes de renseignements techniques qui

ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » seront traités comme tels, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas de caractère exclusif. Dans ce cas, le Canada peut réviser les questions, ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif et permettre la communication des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permettrait pas de les diffuser à tous les soumissionnaires.

2.4 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur en Ontario, et les relations entre les parties seront déterminées par ces lois.

À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées.

2.5 Promotion de l'initiative de dépôt direct

Les renseignements ci-après ne sont pas liés au processus d'invitation à soumissionner.

Le gouvernement du Canada a lancé le projet de normalisation des chèques, qui vise à mettre fin à l'impression de relevés de paiement et à procéder par dépôt direct dans presque tous les cas. Pour l'instant, cette solution n'est offerte que lorsqu'un paiement en dollars canadiens est déposé dans un compte bancaire canadien. Afin d'être proactive, la Comptabilité générale de la GRC encourage l'inscription des fournisseurs de l'organisme en vue des changements qui seront apportés au processus de paiement.

Si votre soumission est retenue dans le cadre du présent processus ou de toute autre invitation à soumissionner de la GRC, nous vous encourageons à vous inscrire au dépôt direct. Veuillez communiquer avec la Comptabilité générale de la GRC par courriel pour recevoir le formulaire *Demande d'adhésion du bénéficiaire au paiement électronique* ainsi que les directives pour le remplir.

Si vous avez des questions sur le projet de normalisation des chèques ou si vous souhaitez vous inscrire, veuillez écrire à corporate_accounting@rcmp-grc.gc.ca.

2.6 Améliorations apportées au besoin pendant la demande de soumissions

Les soumissionnaires qui estiment qu'ils peuvent améliorer, techniquement ou technologiquement, le devis descriptif ou l'énoncé des travaux contenu dans la demande de soumissions, sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la demande de soumissions. Les soumissionnaires doivent indiquer clairement les améliorations suggérées et les motifs qui les justifient. Les suggestions qui ne restreignent pas la concurrence ou qui ne favorisent pas un soumissionnaire en particulier seront examinées à la

condition qu'elles parviennent à l'autorité contractante au plus tard sept (7) jours avant la date de clôture de la demande de soumissions. Le Canada aura le droit d'accepter ou de rejeter n'importe laquelle ou la totalité des suggestions proposées.

2.7 Données volumétriques

Les données volumétriques du nombre estimatif d'apprenants ont été fournies aux soumissionnaires pour les aider à préparer leurs soumissions. L'inclusion de ces données dans la présente demande de soumissions ne représente pas un engagement de la part du Canada que son utilisation future des services précisés dans la présente demande de soumissions correspondra à ces données. Elles sont fournies strictement à titre informatif.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

Le Canada demande que le soumissionnaire présente sa soumission complète par courriel dans des sections distinctes, sauvegardées et jointes comme suit :

Section I : Soumission technique (1 copie électronique en format PDF)

Section II : Soumission financière (1 copie électronique en format PDF)

Section III : Attestations (1 copie électronique en format PDF)

Remarque importante :

Pour les soumissions présentées par courriel, le Canada ne sera responsable d'aucune défaillance attribuable à l'utilisation de ce mode de transmission ou de réception. Entre autres, il n'assumera aucune responsabilité pour ce qui suit :

a) la réception d'une soumission brouillée ou incomplète;

b) un retard dans la transmission ou la réception de la soumission dans la boîte de courriels de l'autorité contractante (la date et l'heure indiquées sur le courriel reçu par l'autorité contractante sont considérées comme l'heure et la date de la réception de la soumission);

c) la disponibilité ou l'état du matériel utilisé pour la réception;

d) une incompatibilité entre le matériel utilisé pour l'envoi et celui utilisé pour la réception;

e) un défaut de la part du soumissionnaire de bien identifier la soumission;

f) l'illisibilité de la soumission;

g) la sécurité des données incluses dans la soumission.

Une soumission transmise par voie électronique constitue l'offre officielle du soumissionnaire et doit être soumise conformément à l'article 05 du document 2003 (2022-03-29), Instructions uniformisées – biens ou services – besoins concurrentiels.

La GRC impose des restrictions à l'égard des courriels entrants. La taille maximale d'un courriel, y compris ses pièces jointes, est de 5 Mo. Les fichiers ZIP ou les liens vers des documents de la soumission ne seront pas acceptés. Les courriels dépassant la taille maximale ou contenant des fichiers ZIP en guise de pièces jointes seront bloqués et ne pourront pas entrer dans le système de courriel de la GRC. Une soumission transmise par courriel bloquée par le système de courriel de la GRC sera considérée comme n'ayant pas été reçue. Il incombe au soumissionnaire de veiller à ce que sa soumission ait bien été reçue.

Les prix doivent figurer dans la soumission financière seulement. Aucun prix ne doit être indiqué ailleurs dans la soumission.

Le Canada demande que les soumissionnaires suivent les instructions de présentation décrites ci-après pour préparer leur soumission :

a) utiliser un système de numérotation correspondant à celui de la demande de soumissions.

En avril 2006, le Canada a adopté une politique exigeant que les ministères et organismes fédéraux prennent les mesures nécessaires pour tenir compte des facteurs environnementaux dans le processus d'approvisionnement : la Politique d'achats écologiques (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32573). Pour aider le Canada à atteindre ses objectifs, les soumissionnaires devraient :

1. inclure toutes les certifications environnementales pertinentes pour votre organisation (p. ex. ISO 14001, Leadership in Energy and Environmental Design [LEED], Carbon Disclosure Project, etc.).

2. inclure toutes les certifications environnementales ou déclarations environnementales de produit (DEP) propres à votre produit ou service (p. ex. Forest Stewardship Council [FSC], ENERGYSTAR, etc.).

3. À moins d'indication contraire, les soumissionnaires sont encouragés à soumettre leurs soumissions par voie électronique. Si des copies papier sont requises, les soumissionnaires doivent :

   a) utiliser du papier de 8,5 po x 11 po (216 mm × 279 mm) contenant des fibres certifiées provenant d'un aménagement forestier durable et contenant au moins 30 % de matières recyclées;

   b) utiliser un format qui respecte l'environnement, soit une impression noir et blanc, recto-verso/à double face et des agrafes ou des trombones plutôt qu'une reliure Cerlox, à attaches ou à anneaux.

Section I : Soumission technique

Dans leur soumission technique, les soumissionnaires devraient démontrer leur compréhension des exigences contenues dans la demande de soumissions et expliquer comment ils répondront à ces exigences. Ils doivent démontrer leur capacité d'effectuer les travaux de façon complète, concise et claire.

La soumission technique devrait traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

Section II : Soumission financière

3.1.1 Les soumissionnaires doivent présenter leur soumission financière conformément à la base de paiement qui figure à l'annexe B.

3.1.2 Fluctuation du taux de change

C3011T (2013-11-06), Fluctuation du taux de change

Section III : Attestations

Les soumissionnaires doivent présenter les attestations et les renseignements supplémentaires exigés à la Partie 5.

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

a) Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les critères d'évaluation « techniques » et « financiers ».

b) Une équipe d'évaluation composée de représentants du Canada évaluera les soumissions.

4.1.1 Évaluation technique

Les critères techniques obligatoires et les critères techniques cotés sont inclus dans l'annexe D.

4.1.2 Évaluation financière

4.1.2.1 Critères financiers obligatoires

Guide des CCUA, clause A0220T (2014-06-26), Évaluation du prix – soumission

4.2 Méthode de sélection – Note combinée la plus haute sur le plan du mérite technique et du prix

1. Pour être déclarée recevable, une soumission doit :
   a) répondre à toutes les exigences de la demande de soumissions;
   b) respecter tous les critères obligatoires;
2. Les soumissions qui ne répondent pas aux exigences a) ou b) seront déclarées non recevables.
3. La sélection sera faite en fonction du meilleur résultat global sur le plan du mérite technique et du prix. Le ratio sera de 20 % pour le mérite technique et de 80 % pour le prix.
4. Afin de déterminer la note pour le mérite technique, la note technique globale de chaque soumission recevable sera calculée comme suit : le nombre total de points obtenus divisé par le nombre total de points pouvant être accordés, multiplié par 20 %.
5. Afin de déterminer la note pour le prix, chaque soumission recevable sera évaluée proportionnellement par rapport au prix évalué le plus bas et selon le ratio de 80 %.
6. Pour chaque soumission recevable, la cotation du mérite technique et la cotation du prix seront ajoutées pour déterminer la note combinée.
7. La soumission recevable ayant obtenu le plus de points ou celle ayant le prix évalué le plus bas ne sera pas nécessairement choisie. La soumission recevable qui obtiendra la note combinée la plus élevée pour le mérite technique et le prix sera recommandée pour l'attribution du contrat.

Le tableau ci-dessous présente un exemple où les trois soumissions sont recevables et où la sélection de l'entrepreneur se fait en fonction d'un ratio de 20/80 à l'égard du mérite technique et du prix, respectivement. Le nombre total de points pouvant être accordé est de 20, et le prix évalué le plus bas est de 45 000,00 $ (45).

Méthode de sélection - Note combinée la plus haute sur le plan du mérite technique (20 %) et du prix (80 %)

		Soumissionnaire 1	**Soumissionnaire 2**	**Soumissionnaire 3**
Note technique globale		10/20	20/20	10/20
Prix évalué de la soumission		55 000,00 $	50 000,00 $	45 000,00 $
Calculs	**Note pour le mérite technique**	10/20 × 20 = 10	20/20 × 20 = 20	10/20 × 20 = 10
	Cote pour le prix	45/55 × 80 = 65,45	45/50 × 80 = 72,00	45/45 × 80 = 80,00
Cote combinée		75,45	92,00	90
Note globale		3e	1er	2e

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

Les soumissionnaires doivent fournir les attestations et les renseignements supplémentaires exigés pour qu'un contrat leur soit attribué.

Les attestations que les soumissionnaires remettent au gouvernement du Canada peuvent être vérifiées à tout moment par ce dernier. À moins d'indication contraire, le gouvernement du Canada déclarera une soumission non recevable, ou un entrepreneur en situation de manquement, s'il est déterminé que le soumissionnaire a fait, sciemment ou non, de fausses déclarations concernant les attestations, que ce soit pendant la période d'évaluation des soumissions ou pendant la durée du marché.

L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. À défaut de répondre et de coopérer à toute demande ou exigence imposée par l'autorité contractante, la soumission sera déclarée non recevable, ou constituera un manquement aux termes du contrat.

5.1 Attestations préalables à l'attribution d'un contrat renseignements supplémentaires

Les attestations et renseignements supplémentaires énoncés ci-dessous devraient être joints à la soumission, mais peuvent aussi être présentés par la suite. Si l'une des attestations exigées ou l'un des renseignements supplémentaires requis n'est pas fourni conformément aux exigences, l'autorité contractante informera le soumissionnaire du délai dont il dispose pour le faire. À défaut de fournir les attestations ou les renseignements supplémentaires énoncés ci-dessous dans le délai prévu, la soumission sera déclarée non recevable.

5.1.1 Dispositions relatives à l'intégrité

Conformément à la section de la *Politique d'inadmissibilité et de suspension* intitulée « Renseignements à fournir lors d'une soumission, de la passation d'un contrat ou de la conclusion d'un accord immobilier » (https://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html), le soumissionnaire doit fournir les documents requis, selon le cas, pour que son offre passe à l'étape suivante du processus :

- Déclaration de condamnation à une infraction – Formulaire de déclaration d'intégrité (s'il y a lieu);
- documentation requise (liste de noms pour le formulaire de vérification de l'intégrité).

Veuillez consulter le site Web Formulaires concernant le Régime d'intégrité pour obtenir des détails additionnels (http://www.tpsgc-pwgsc.gc.ca/ci-if/formulaires-forms-fra.html).

5.1.2 Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation de soumission

En présentant une soumission, le soumissionnaire atteste que le soumissionnaire, et tout membre de la coentreprise si le soumissionnaire est une coentreprise, n'est pas nommé dans la liste des « soumissionnaires à admissibilité limitée du PCF » du Programme de contrats fédéraux (PCF) pour l'équité en matière d'emploi disponible au bas de la page

du site Web d'Emploi et Développement social Canada (EDSC) – Travail (https://www.canada.ca/fr/emploi-developpement-social/programmes/equite-emploi/programme-contrats-federaux.html).

Le Canada aura le droit de déclarer une soumission non recevable si le nom du soumissionnaire, ou celui de tout membre de la coentreprise si le soumissionnaire est une coentreprise, figure dans la « Liste d'admissibilité limitée à soumissionner du PCF » au moment de l'attribution du contrat.

5.1.3 Attestations additionnelles préalables à l'attribution du contrat

5.1.3.1 Attestation d'absence de collusion dans l'établissement de soumission

L'attestation d'absence de collusion dans l'établissement de soumission ci-jointe (PIÈCE JOINTE 1 de la PARTIE 5 – ATTESTATION D'ABSENCE DE COLLUSION DANS L'ÉTABLISSEMENT DE SOUMISSION) a été élaborée par le Bureau de la concurrence à l'intention de l'autorité contractante lorsque celle-ci demande des soumissions, des offres ou des propositions. Cette attestation sert à dissuader les soumissionnaires de truquer l'appel d'offres en exigeant qu'ils dévoilent à l'autorité contractante tous les faits importants au sujet des échanges et des ententes qu'ils ont eus avec les autres soumissionnaires concernant l'appel d'offres.

5.1.3.2 Anciens fonctionnaires

Les contrats attribués à d'anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen scrupuleux du public et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du Trésor sur les contrats attribués à d'anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée ci-dessous avant l'attribution du contrat. Si la réponse aux questions et, s'il y a lieu les renseignements requis, n'ont pas été fournis par le temps où l'évaluation des soumissions est complétée, le Canada informera le soumissionnaire du délai à l'intérieur duquel l'information doit être fournie. Le défaut de se conformer à la demande du Canada et de satisfaire à l'exigence dans le délai prescrit rendra la soumission non recevable.

Définitions
Aux fins de cette clause, « ancien fonctionnaire » signifie tout ancien employé d'un ministère au sens de la *Loi sur la gestion des finances publiques*, L.R.C., 1985, ch. F-11 ou un ancien membre des Forces armées canadiennes ou de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être :

a) un particulier;
b) une personne morale;
c) une société constituée d'anciens fonctionnaires;
d) une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.

« Période du paiement forfaitaire » signifie la période mesurée en semaines de salaire à l'égard de laquelle un paiement a été fait pour faciliter la transition vers la retraite ou vers un autre emploi par suite de la mise en place des divers programmes visant à réduire la taille de la fonction publique. La période du paiement forfaitaire ne comprend pas la période visée par l'allocation de fin de services, qui se mesure de façon similaire.

Le terme « pension » désigne une pension ou une allocation annuelle versée en vertu de la *Loi sur la pension de la fonction publique* (LPFP), L.R.C., 1985, ch. P-36, et toute augmentation versée en vertu de la *Loi sur les prestations de retraite supplémentaires*, L.R.C., 1985, ch. S-24 dans la mesure où elle a une incidence sur la LPFP. La pension ne comprend pas les pensions payables en vertu de la *Loi sur la pension de retraite des Forces canadiennes*, L.R., 1985, ch. C-17, de la *Loi sur la continuation de la pension des services de défense*, 1970, ch. D-3, de la *Loi sur la continuation des pensions de la Gendarmerie royale du Canada*, 1970, ch. R-10, de la *Loi sur la pension de retraite de la Gendarmerie royale du Canada*, L.R., 1985, ch. R-11, de la *Loi sur les allocations de retraite des parlementaires*, L.R. 1985, ch. M-5, et la partie de la pension payable en vertu de la *Loi sur le Régime de pensions du Canada*, L.R. (1985), ch. C-8.

Ancien fonctionnaire touchant une pension

Selon les définitions ci-dessus, est-ce que le soumissionnaire est un ancien fonctionnaire touchant une pension?

Oui ( ) Non ( )

Si oui, le soumissionnaire doit fournir l'information suivante pour tous les anciens fonctionnaires touchant une pension, le cas échéant :

a) le nom de l'ancien fonctionnaire;

b) la date de cessation d'emploi ou de la retraite de la fonction publique.

En fournissant ces renseignements, les soumissionnaires acceptent que le statut du soumissionnaire retenu, en tant qu'ancien fonctionnaire touchant une pension, figure dans les rapports de divulgation proactive, sur les sites Web des ministères, conformément à l'Avis sur la Politique des marchés : 2019-01 et aux Lignes directrices sur la divulgation des marchés.

Directive sur le réaménagement des effectifs

Le soumissionnaire est-il un ancien fonctionnaire qui a touché un paiement forfaitaire conformément aux modalités de la Directive sur le réaménagement des effectifs? **Oui ( ) Non ( )**

Si oui, le soumissionnaire doit fournir l'information suivante :

a) le nom de l'ancien fonctionnaire;

b) les conditions de l'incitatif versé sous forme de paiement forfaitaire;

c) la date de cessation d'emploi;

d) le montant du paiement forfaitaire;

e) le taux de rémunération qui a servi au calcul du paiement forfaitaire;

f) la période correspondant au paiement forfaitaire, incluant la date de début, la date de fin et le nombre de semaines;

g) le nombre et le montant (honoraires professionnels) des autres contrats assujettis aux conditions d'un programme de réaménagement des effectifs.

5.1.3.3 Formulaire d'attestation de l'éditeur de logiciels-services

Si l'éditeur de logiciels-services (défini comme l'entité ou la personne qui est titulaire du droit d'auteur pour toute solution de logiciel-service incluse dans la soumission et qui détient la licence et peut autoriser d'autres personnes à utiliser sa solution de logiciel-service et ses composants sous-jacents) a l'intention de présenter une soumission et de se qualifier comme fournisseur, il doit soumettre le formulaire d'attestation avec la pièce jointe 2 de la partie 5.

PIÈCE JOINTE 1 de la PARTIE 5 – ATTESTATION D'ABSENCE DE COLLUSION DANS L'ÉTABLISSEMENT DE LA SOUMISSION

Je, soussigné, en présentant la soumission ou l'offre jointe (ci-après « soumission ») à :

_____
(Nom du destinataire de cette soumission)

pour : _____
(Nom et numéro de la soumission et du projet)

à la suite de l'appel d'offres (ci-après l'« appel d'offres ») lancé par :

_____
(Nom de l'autorité adjudicative)

déclare ce qui suit et atteste que ces déclarations sont vraies et complètes à tous les égards.

Je déclare au nom de : _____ que :
(Dénomination sociale du soumissionnaire ou de l'offrant [ci-après le « soumissionnaire »])

1. j'ai lu et que je comprends le contenu de la présente attestation;

2. je comprends que la soumission ci-jointe sera déclarée inadmissible si les déclarations contenues dans la présente attestation ne sont pas vraies ou complètes à tous les égards;

3. je suis autorisé par le soumissionnaire à signer la présente attestation et à présenter, en son nom, la soumission qui y est jointe;

4. toutes les personnes dont le nom apparaît sur la soumission ci-jointe ont été autorisées par le soumissionnaire à fixer les modalités qui y sont prévues et à signer la soumission en son nom;

5. aux fins de la présente attestation et de la soumission ci-jointe, je comprends que le mot « concurrent » s'entend de tout organisme ou personne, autre que le soumissionnaire, affilié ou non au soumissionnaire :
   (a) a été invité par l'appel d'offres à présenter une soumission;
   (b) pourrait éventuellement présenter une soumission à la suite de l'appel d'offres compte tenu de ses qualifications, de ses habiletés ou de son expérience;

6. le soumissionnaire déclare (cocher l'une ou l'autre des déclarations suivantes) :
   a) qu'il a établi la présente soumission sans consultation et sans avoir communiqué ou établi d'entente ou d'arrangement avec un concurrent;

   b) qu'il a établi la présente soumission après avoir consulté un ou plusieurs concurrents, communiqué ou établi une entente ou un arrangement avec ces derniers et qu'il divulgue, dans le document ci-joint, tous les détails s'y rapportant, y compris le nom des concurrents et les raisons de ces consultations, communications, ententes ou arrangements;

7. sans limiter la généralité de ce qui précède aux alinéas (6)(a) ou (b), le soumissionnaire déclare qu'il n'y a pas eu de communication, d'entente ou d'arrangement avec un concurrent relativement :
   a) aux prix;
   b) aux méthodes, aux facteurs ou aux formules pour établir les prix;
   c) à la décision de présenter ou de ne pas présenter une soumission;
   d) à la présentation d'une soumission qui ne satisfait pas aux spécifications de l'appel d'offres; à l'exception de ce qui est spécifiquement divulgué conformément à l'alinéa (6)(b) ci-dessus;

8. en plus, il n'y a pas eu de communication, d'entente ou d'arrangement avec un concurrent en ce qui concerne les détails liés à la qualité, à la quantité, aux spécifications ou à la livraison des biens ou des services visés par le présent appel d'offres, sauf ceux qui ont été spécifiquement autorisés par l'autorité adjudicative ou spécifiquement divulgués conformément à l'alinéa (6)(b) ci-dessus;

9. les modalités de la soumission ci-jointe n'ont pas été et ne seront pas intentionnellement divulguées par le soumissionnaire, directement ou indirectement, à un concurrent avant la première des dates suivantes, soit l'heure de l'ouverture officielle des soumissions, soit l'attribution du marché, à moins d'être requis de le faire par la loi ou d'être requis de le divulguer conformément à l'alinéa (6)(b).

_____

(Nom en caractères d'imprimerie et signature de la personne autorisée par le soumissionnaire)

_____ _____

(Titre) (Date)

PIÈCE JOINTE 2 de la PARTIE 5– Formulaire d'attestation de l'éditeur de logiciels-services

Formulaire 1 – Formulaire d'attestation de l'éditeur de logiciels-services

(à remplir lorsque l'entrepreneur est l'éditeur de logiciels-services)

L'entrepreneur atteste qu'il est l'éditeur de logiciels-services de toutes les solutions de logiciel-service suivantes et qu'il a les droits requis pour accorder les licences conformément aux modalités du contrat avec le Canada.

_____

_____

_____

_____

_____

(L'entrepreneur doit ajouter ou supprimer des lignes au besoin.)

Nom de l'éditeur de logiciels-services (ELS) _____

Signature du signataire autorisé de l'ELS _____

Nom en caractères d'imprimerie du signataire autorisé de l'ELS _____

Titre en caractères d'imprimerie du signataire autorisé de l'ELS _____

Adresse du signataire autorisé de l'ELS _____

Téléphone du signataire autorisé de l'ELS _____

Courriel du signataire autorisé de l'ELS _____

Date de signature _____

PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ

6.1 Exigences en matière de sécurité

1. Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées :

   a) Les services infonuagiques proposés par le soumissionnaire doivent satisfaire aux exigences en matière de sécurité énoncées à la partie 7 – Clauses du contrat subséquent.

   b) Le soumissionnaire doit participer à tout processus d'évaluation de la sécurité et d'autorisation (ESA) jugé nécessaire par le chargé de projet ou la Sécurité ministérielle. Avant que des solutions élaborées en tout ou en partie par des soumissionnaires ne soient transférées dans un environnement de production, une autorisation d'exploitation complète doit être accordée. L'obtention d'une autorisation d'exploitation nécessite une évaluation de sécurité dans le cadre du processus d'ESA, qui peut être lancé en communiquant avec la Sécurité ministérielle. Référence, section 6.3 – Processus d'évaluation et d'autorisation de la sécurité des TI dans le Guide de sécurité à l'annexe C.

2. On rappelle aux soumissionnaires qu'ils doivent obtenir rapidement l'autorisation de sécurité requise. La décision de retarder l'attribution du contrat, pour permettre au soumissionnaire retenu d'obtenir l'attestation de sécurité requise, demeure à l'entière discrétion de l'autorité contractante.

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

Les clauses et conditions suivantes s'appliquent à tout contrat découlant de la demande de soumissions et en font partie intégrante.

7.1 Énoncé des travaux

L'entrepreneur doit exécuter les travaux conformément à l'Énoncé des travaux qui se trouve à l'annexe A.

7.2 Clauses et conditions générales

Toutes les clauses et conditions identifiées dans le contrat par un numéro, une date et un titre, sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Services publics et Approvisionnement Canada (SPAC).

Modification touchant le nom du ministère : Puisque le présent contrat est lancé par la Gendarmerie royale du Canada (GRC), il faut interpréter toute mention de Services publics et Approvisionnement Canada (SPAC) ou de sa ministre dans les clauses et conditions, y compris celles tirées des CCUA, comme désignant en fait la GRC ou son ministre.

7.2.1 Conditions générales

Le document 2035 (2014-09-25) Conditions générales — besoins plus complexes de services, s'applique au contrat et en fait partie intégrante.

7.3 Exigences en matière de sécurité

7.3.1 Les exigences suivantes relatives à la sécurité, soit la Liste de vérification des exigences relatives à la sécurité (LVERS) s'appliquent au contrat et en font partie intégrante.

7.3.2 Processus d'évaluation et d'autorisation de la sécurité des TI

7.3.2.1 Le soumissionnaire doit confirmer auprès de la Section de la sécurité des technologies de l'information et des communications de la GRC qu'il détient une autorisation d'exploitation valide.

7.4 Durée du contrat

7.4.1 Période du contrat

La période du contrat va de la date du contrat au _____ inclusivement **(dates à indiquer à l'attribution du contrat)**.

7.4.2 Option de prolongation du contrat

L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat d'au plus quatre (4) périodes d'une (1) année chacune, selon les mêmes conditions. L'entrepreneur accepte que pendant les périodes de prolongation du contrat, il sera payé conformément aux dispositions applicables prévues à la base de paiement.

Le Canada peut exercer cette option à n'importe quel moment, en envoyant un avis écrit à l'entrepreneur avant la date d'expiration du contrat. L'option, qui ne pourra être exercée que par l'autorité contractante, sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

7.5 Autorités

7.5.1 Autorité contractante

L'autorité contractante pour le contrat est :

Nom : Angelo Kaldis
Titre : Spécialiste en approvisionnement, Sous-direction des acquisitions et des marchés de la Direction générale
Gendarmerie royale du Canada
Téléphone : 519-318-3897
Courriel : angelo.kaldis@rcmp-grc.gc.ca

L'autorité contractante est responsable de la gestion du contrat, et toute modification doit être autorisée, par écrit, par l'autorité contractante. L'entrepreneur ne doit pas effectuer de travaux dépassant la portée du contrat ou des travaux qui n'y sont pas prévus suite à des demandes ou des instructions verbales ou écrites de toute personne autre que l'autorité contractante.

7.5.2 Chargé de projet (sera nommé au moment de l'attribution du contrat)

Le chargé de projet pour le contrat est :

Nom : _____
Titre : _____
Gendarmerie royale du Canada
Direction : _____
Adresse : _____

Téléphone : ___-___-_____
Courriel : _____

Le chargé de projet représente le ministère ou organisme pour lequel les travaux sont exécutés dans le cadre du contrat. Il est responsable de toutes les questions liées au contenu technique des travaux prévus dans le contrat. On peut discuter des questions techniques avec le chargé de projet; cependant, celui-ci ne peut pas autoriser les changements à apporter à l'énoncé des travaux. Ces changements peuvent être effectués uniquement au moyen d'une modification au contrat émise par l'autorité contractante.

7.5.3 Représentant de l'entrepreneur (information à fournir au moment de l'attribution du contrat)

Le représentant de l'entrepreneur pour le contrat est :

Nom : _____
Titre : _____
Adresse : _____

Téléphone : ___-___-_____
Courriel : _____

7.6 Divulgation proactive des contrats conclus avec d'anciens fonctionnaires

En fournissant de l'information sur son statut en tant qu'ancien fonctionnaire touchant une pension en vertu de la *Loi sur la pension de la fonction publique* (LPFP), l'entrepreneur a accepté que cette information soit publiée sur les sites Web des ministères, dans le cadre des rapports de divulgation proactive des marchés, et ce, conformément à l'Avis sur la Politique des marchés : 2019-01 du Secrétariat du Conseil du Trésor du Canada.

7.7 Paiement

7.7.1 Base de paiement – prix unitaires fermes

À condition de remplir de façon satisfaisante toutes ses obligations en vertu du contrat, l'entrepreneur sera payé des prix unitaires fermes précisés dans l'annexe « B », selon un montant total de _____ $ **(à insérer au moment de l'attribution du contrat)**. Les droits de douane sont compris, et les taxes applicables sont en sus.

Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.

7.7.2 Limite des dépenses

1. La responsabilité totale du Canada envers l'entrepreneur aux termes du contrat ne doit pas dépasser la somme de _____ $ **(à insérer au moment de l'attribution du contrat)**. Les droits de douane sont compris, et les taxes applicables sont en sus.
2. Aucune augmentation de la responsabilité totale du Canada ou du prix des travaux découlant de tout changement de conception ou de toute modification ou interprétation des travaux, ne sera autorisée ou payée à l'entrepreneur, à moins que ces changements de conception, modifications ou interprétations n'aient été approuvés, par écrit, par l'autorité contractante avant d'être intégrés aux travaux. L'entrepreneur ne doit pas exécuter des travaux ou fournir des services qui entraîneraient une augmentation de la responsabilité totale du Canada avant d'avoir obtenu l'approbation écrite de l'autorité contractante. L'entrepreneur doit informer, par écrit, l'autorité contractante concernant la suffisance de cette somme :
   a) lorsque 75 % de la somme est engagée;
   b) quatre mois avant la date d'expiration du contrat, ou
   c) dès que l'entrepreneur juge que les fonds du contrat sont insuffisants pour l'achèvement des travaux,

   selon la première de ces conditions à se présenter.
3. Lorsqu'il informe l'autorité contractante que les fonds du contrat sont insuffisants, l'entrepreneur doit lui fournir par écrit une estimation des fonds additionnels requis. La présentation de cette information par l'entrepreneur n'augmente pas la responsabilité du Canada à son égard.

7.7.3 Méthode de paiement – Paiements multiples

Guide des CCUA, clause H1001C (2008-05-12), Paiements multiples

7.7.4 Taxes – entrepreneur établi à l'étranger

Guide des CCUA, clause C2000C (2007-11-30) Taxes – Fournisseurs étrangers

7.8 Instructions relatives à la facturation

1. L'entrepreneur doit soumettre ses factures conformément à l'article intitulé « Présentation des factures » des conditions générales. Les factures ne doivent pas être soumises avant que les travaux identifiés dans la facture soient exécutés.
2. Les factures doivent être distribuées comme suit :
   a) Une (1) copie doit être envoyée au chargé de projet identifié dans la section « Responsables » du contrat aux fins d'attestation et de paiement.
   b) Une (1) copie doit être envoyée à l'autorité contractante identifiée sous l'article intitulé « Responsables » du contrat.

7.9 Attestations et renseignements supplémentaires

7.9.1 Conformité

À moins d'indications contraires, le respect continu des attestations fournies par l'entrepreneur avec sa soumission ou préalablement à l'attribution du contrat, ainsi que la coopération constante quant aux renseignements supplémentaires, sont des conditions du contrat et leur non-respect constituera un manquement de la part de l'entrepreneur. Les attestations pourront faire l'objet de vérifications par le Canada pendant toute la durée du contrat.

7.10 Lois applicables

Le marché doit être interprété et régi selon les lois en vigueur de _____ **(à insérer lors de l'attribution du marché)**, et les relations entre les parties seront déterminées par ces lois.

7.11 Priorité des documents

En cas d'incompatibilité entre le libellé des textes énumérés dans la liste, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte sur celui de tout autre document qui figure plus bas sur la liste :

a) les articles de la convention;
b) les conditions générales 2035 (2008-05-12), Conditions générales - besoins plus complexes de services;
c) l'annexe A, Énoncé des travaux;
d) l'annexe B, Base de paiement;
e) l'annexe C – Liste de vérification des exigences relatives à la sécurité;
f) la soumission de l'entrepreneur en date du ____ **(à insérer au moment de l'attribution du contrat)**.

7.12 Ombudsman de l'approvisionnement

7.12.1 Règlement des différends

Les parties conviennent de faire tous les efforts raisonnables, de bonne foi, pour régler à l'amiable tout différend ou toute revendication relatifs au contrat en favorisant la tenue de négociations entre leurs représentants ayant autorité pour régler les différends. Si les parties ne parviennent pas à un accord dans les 25 jours ouvrables après le signalement initial du litige, par écrit, auprès de l'autre partie, l'une ou l'autre partie peut communiquer avec le Bureau de l'ombudsman de l'approvisionnement (BOA) pour demander des services de règlement des différends et de médiation. Le BOA peut être joint par courriel, à l'adresse boa.opo@boa-opo.gc.ca, par téléphone au 1-866-734-5169, ou par l'intermédiaire de son site Web, à l'adresse www.opo-boa.gc.ca. Pour de plus amples renseignements sur les services du BOA, veuillez consulter le *Règlement concernant l'ombudsman de l'approvisionnement* ou le site Web du BOA.

7.12.2 Administration des marchés

Les parties reconnaissent que l'ombudsman de l'approvisionnement nommé en vertu du paragraphe 22 (1) de la *Loi sur le ministère des Travaux publics et des Services gouvernementaux* examinera une plainte déposée par le plaignant concernant l'administration du contrat si les exigences du paragraphe 22.2 (1) de la *Loi sur le ministère des Travaux publics et des Services gouvernementaux* et les articles 15 et 16 du *Règlement concernant l'ombudsman de l'approvisionnement* ont été respectés.

Pour déposer une plainte, on peut joindre le Bureau de l'ombudsman de l'approvisionnement par courriel à l'adresse boa.opo@boa-opo.gc.ca, par téléphone au 1-866-734-5169 ou par l'entremise de son site Web à l'adresse www.opo-boa.gc.ca.

7.13 Assurances

Guide des CCUA, clause G1005C (2016-01-28), Assurance – aucune exigence particulière

ANNEXE A – ÉNONCÉ DES TRAVAUX

1. TITRE

Formation annuelle obligatoire en ligne pour les membres d'équipage de la GRC

2. CONTEXTE

La formation annuelle sur l'aviation est une exigence de Transports Canada visant à s'assurer que les pilotes, les techniciens d'entretien d'aéronefs et les membres d'équipage (agents tactiques d'aviation/coordonnateurs de vols) maintiennent un niveau de compétence sécuritaire. Ces exigences figurent à la sous-partie 4 de la partie VI *du Règlement de l'aviation canadien* (RAC). En vertu de ce règlement, le Service de l'air de la GRC est autorisé à exploiter des aéronefs à titre d'exploitant privé, à condition que ses pilotes et techniciens d'entretien d'aéronefs suivent des cours de formation obligatoires, dont bon nombre peuvent être administrés au moyen d'une solution Web. Le présent énoncé des travaux est conforme à la section 6, portant sur les exigences d'instruction et de maintien de la compétence, du manuel d'exploitation des aéronefs à voilure fixe et du manuel des opérations des aéronefs à voilure tournante de la GRC, et au manuel de contrôle de la maintenance de la GRC. Ces manuels assurent la conformité aux exigences en matière de formation énoncées à la sous-partie 604 du RAC.

3. ACRONYMES

AT	Autorité technique
EDT	Énoncé des travaux
GRC	Gendarmerie royale du Canada
CFIT	Impact sans perte de contrôle
FWOM	Manuel d'exploitation des aéronefs à voilure fixe
MCM	Manuel de contrôle de la maintenance
MOAVT	Manuel des opérations des aéronefs à voilure tournante
NASA	National Aeronautics and Space Administration
OAT	Opérations aériennes tactiques
RAC	*Règlement de l'aviation canadien*
ACAS	Système anticollision embarqué
TCAS	Système avertisseur de proximité
SIMDUT	Système d'information sur les matières dangereuses utilisées au travail
T.E.A.	Technicien d'entretien d'aéronef
FW	Voilure fixe (aéronef)
RW	Voilure tournante (hélicoptère)

4. DOCUMENTS ET RÉFÉRENCES APPLICABLES

1. Manuel d'exploitation des aéronefs à voilure fixe de la GRC
   - Section 6.6 – Programmes de formation
2. Manuel des opérations des aéronefs à voilure tournante de la GRC
   - Section 6.6 – Programmes de formation
3. Manuel de contrôle de la maintenance de la GRC
   - Section 4.1.1
4. *Règlement de l'aviation canadien*
   - Article 604 – Opérateurs privés

5. TÂCHES

L'entrepreneur doit offrir une formation en ligne à rythme libre sur les sujets suivants liés à l'aviation. Les sujets visent des groupes d'apprenants spécifiques, et l'entrepreneur doit s'assurer que le contenu de chaque sujet est pertinent pour le secteur de l'aviation canadien. Les sujets énumérés ci-dessous sont le minimum requis.

5.1 Pilotes d'aéronef à voilure fixe (maximum de 50 apprenants) :

a) ACAS/TCAS
b) Avion remorqueur
c) Conditions météorologiques
d) Contamination des surfaces critiques d'un aéronef
e) Différences entre le Canada et les États-Unis
f) Espace aérien pour la navigation fondée sur les performances
g) Examen des opérations – propre à la sous-partie 604
h) Examen radar
i) Facteurs humains pour les pilotes
j) Gestion de la fatigue
k) Gestion de la menace et des erreurs
l) Gestion des ressources à bord d'un aéronef monopilote
m) Gestion des ressources de l'équipage
n) Givrage en vol
o) Haute altitude – physiologie et effets
p) Impact sans perte de contrôle (CFIT)
q) Instruction relative aux procédures d'urgence
r) Minimum de séparation verticale réduit
s) Principes de survie
t) Sensibilisation à l'incursion sur piste
u) Systèmes de gestion de la sécurité
v) Transport de marchandises dangereuses

5.2 Pilotes d'aéronef à voilure rotative (maximum de 20 apprenants) :

a) Avion remorqueur
b) Conditions météorologiques
c) Contamination des surfaces critiques d'un aéronef
d) Examen des opérations – propre à la sous-partie 604
e) Facteurs humains pour les pilotes
f) Gestion de la fatigue
g) Gestion de la menace et des erreurs
h) Gestion des ressources à bord d'un aéronef monopilote
i) Gestion des ressources de l'équipage
j) Givrage en vol
k) Haute altitude – physiologie et effets
l) Impact sans perte de contrôle (CFIT)
m) Instruction relative aux procédures d'urgence
n) Principes de survie
o) Sensibilisation à l'incursion sur piste
p) Systèmes de gestion de la sécurité
q) Transport de marchandises dangereuses

5.3 Techniciens d'entretien d'aéronefs (maximum de 45 apprenants) :

a) Avion remorqueur
b) Examen de la maintenance – opérations, règlements et normes
c) Facteurs humains pour les techniciens
d) Gestion de la fatigue
e) Gestion des ressources d'entretien
f) Instruction relative aux procédures d'urgence
g) Minimum de séparation verticale réduit pour la maintenance
h) Sensibilisation à l'incursion sur piste
i) Transport de marchandises dangereuses

5.4 Membres d'équipage (agents tactiques d'aviation et coordonnateurs de vols) [maximum de 50 apprenants] :

a) Contamination des surfaces critiques d'un aéronef
b) Gestion des ressources de l'équipage
c) Givrage en vol
d) Haute altitude – physiologie et effets
e) Impact sans perte de contrôle (CFIT)
f) Instruction relative aux procédures d'urgence
g) Sensibilisation au transport de marchandises dangereuses

5.5 Sujets liés à la santé et à la sécurité au travail faisant partie de la formation de tous les groupes d'apprenants :

a) Équipement de protection individuelle
b) Ergonomie
c) Prévention des blessures au dos
d) Prévention des incendies
e) Prévention des maladies transmissibles
f) Protection contre les chutes
g) Sécurité en matière d'électricité
h) Sensibilisation au sujet des espaces clos
i) Sensibilisation au sujet du carburant et des matières inflammables
j) SIMDUT

5.6 Tâches administratives

L'entrepreneur doit effectuer les tâches administratives suivantes en plus d'offrir la formation en ligne à rythme libre requise :

a) Tenir à jour des dossiers de formation des apprenants consultables en ligne.
b) Par l'intermédiaire d'un lien Web, fournir à 10 administrateurs du Service de l'air de la GRC un accès aux dossiers de formation en ligne des employés de la GRC. Les administrateurs doivent être en mesure de consulter, au minimum, les renseignements suivants sur la formation d'une personne :
    i. nom;
    ii. liste des sujets assignés;
    iii. date à laquelle la formation sur le sujet a été achevée;
    iv. date d'expiration du sujet.
c) Les rôles d'administrateur doivent être distincts des rôles d'apprenant, puisque les administrateurs peuvent également être des apprenants.
d) Faire appel à des spécialistes pour tenir les sujets de formation à jour. Voici des exemples de spécialistes : la Fondation pour la sécurité aérienne en ce qui concerne l'impact sans perte de contrôle, ainsi que la NASA et le Conseil national de recherches Canada en ce qui concerne le givrage.
e) Un examen en ligne doit être fourni pour chaque module de chaque sujet de formation.
f) Envoyer par courriel un rapport annuel sur les sujets offerts pour s'assurer que la GRC respecte la sous-partie 604 du *Règlement de l'aviation canadien*.
g) Envoyer des notifications par courriel aux apprenants et aux administrateurs :
    i. pour assigner un sujet lorsqu'il est accessible à l'apprenant;
    ii. dans les deux (2) semaines suivant la date d'échéance du sujet de formation assigné à une personne. Les sujets de formation sont considérés comme en retard si la formation sur ce sujet n'a pas été achevée dans les deux semaines suivant l'assignation.

5.7 Exigences techniques

a) La solution de formation doit être compatible avec les navigateurs Internet suivants :
   i. Microsoft Edge version 106 et versions subséquentes;
   ii. Google Chrome version 106 et versions subséquentes;
   iii. Safari sur iOS 9.3 et versions subséquentes.

b) La solution de formation doit permettre d'associer les identifiants uniques du Canada (p. ex. adresse de courriel de la GRC) aux comptes d'utilisateur des services infonuagiques correspondants.

c) La solution de formation doit être offerte en anglais, ainsi qu'en français si disponible, en fonction du choix de l'utilisateur.

d) L'entrepreneur doit fournir un numéro de téléphone et une adresse de courriel pour un service de soutien technique disponible pendant les heures normales de travail. Les heures normales de travail sont de 9 h à 17 h, heure de l'Est, du lundi au vendredi. Toute demande présentée en dehors de ces heures doit être traitée le jour ouvrable suivant.

e) Le soutien technique doit être offert en anglais, ainsi qu'en français si disponible, en fonction du choix de l'utilisateur.

f) La solution de formation doit être une solution clé en main, et elle ne doit pas être une version bêta du logiciel ni être en cours de développement.

g) L'entrepreneur doit fournir un environnement de production présentant les caractéristiques suivantes :
   i. Il doit être accessible à un nombre illimité d'utilisateurs, et ce, en tout temps.
   ii. En cas d'inaccessibilité pour maintenance de routine du site, une notification doit être envoyée à l'autorité technique au moins deux (2) jours avant le début de la maintenance.
   iii. Il doit être accessible aux clients 98,5 % du temps, à l'exception des périodes de maintenance.
   iv. L'entrepreneur doit transmettre une notification pour toutes les mises à jour logicielles prévues au moins une (1) semaine avant la distribution de la mise à jour. La notification doit comprendre des notes de version et un calendrier de mise à jour du logiciel.
   v. Une notification doit être fournie pour toutes les mises à jour logicielles au moins une (1) semaine avant la mise à jour. La notification doit comprendre des notes de version et une date de diffusion du logiciel.

h) L'entrepreneur doit être en mesure de désactiver des comptes et de créer de nouveaux comptes individuels pour les apprenants, au besoin. Le nombre maximal de comptes actifs est précisé dans le contrat.

6. Produits livrables

Numéro	Référence des tâches	Description du produit livrable	Quantité et format
6.0	5.0	Prestation d'une solution de formation en ligne dans laquelle le logiciel dans son intégralité, y compris toutes les bases de données, le matériel et les sauvegardes, est fourni par l'entrepreneur à l'extérieur du réseau de la GRC.	Accessible à tous les apprenants désignés aux sections 5.1 à 5.4 et aux administrateurs du Service de l'air de la GRC désignés à la section 5.6. Accessible au moyen de Microsoft Edge, Google Chrome et Safari.
6.1	5.1 à 5.4	Formation en ligne pour les pilotes d'aéronefs à voilure fixe et à voilure tournante, les techniciens d'entretien d'aéronefs (T.E.A.) et les membres d'équipage.	Accès à l'apprentissage en ligne pour un maximum de 165 apprenants.
6.2	5.5	Formation en ligne sur la santé et la sécurité au travail pour tous les apprenants.	Accès à des sujets de formation en ligne pour tous les apprenants désignés aux sections 5.1 à 5.4.
6.3	5.1 à 5.5	Un examen doit être fourni pour chaque module qui se trouve dans chaque sujet de formation.	Un examen par module par sujet de formation pour un maximum de 165 apprenants.
6.4	5.6.b	Accès aux dossiers de formation en ligne des employés de la GRC pour les administrateurs du Service de l'air de la GRC.	Rôle d'administrateur pour 10 administrateurs du Service de l'air de la GRC.
6.5	5.6.f	Rapport d'examen annuel.	Transmission d'un document d'examen par courriel à la fin de chaque période du contrat.
6.6	5.6.g	Notifications par courriel.	Transmission de notifications par courriel lorsqu'un sujet a été assigné à un apprenant, et transmission de notifications par courriel aux apprenants et aux administrateurs lorsqu'un sujet n'est pas achevé dans les délais prévus, comme défini à la section 5.6 g).

7. DATE DE LIVRAISON

Produit livrable	Date de livraison
6.0	Début du contrat.
6.1	Dans les cinq jours ouvrables suivant la réception des renseignements sur l'apprenant.
6.2	Dans les cinq jours ouvrables suivant la réception des renseignements sur l'apprenant.
6.3	Lorsque l'apprenant a achevé un module.
6.4	Début du contrat.
6.5	Douze mois après le début du contrat.
6.6	Notification par courriel dans les deux jours suivant la disponibilité d'un sujet.
	Avis par courriel dans les deux semaines suivant l'échéance d'un sujet.

8. Langue de travail

La langue de tous les travaux et produits livrables doit être l'anglais, et le français si disponible.

9. Lieu de travail

Non requis – en ligne seulement.

10. Déplacements

L'entrepreneur n'a pas à se déplacer dans le cadre de ce contrat.

11. RÉUNIONS

1. Consultation initiale avec l'entrepreneur par téléconférence pour examiner le service. Voici quelques points de discussion :
   - Sélection du sujet pour le groupe d'apprenants pour la période en cours.
   - Calendrier de prestation et période de validité du sujet pour le groupe d'apprenants.
   - Démonstration de la fonctionnalité de l'accès et des outils pour les administrateurs.
   - Contenu du rapport annuel.

2. Réunion annuelle pour discuter des sujets de formation du groupe d'apprenants de la période subséquente.

12. SOUTIEN FOURNI PAR LA GRC

a) La GRC fournira le nom et l'adresse de courriel professionnelle des employés pour l'accès des apprenants et des administrateurs dans la semaine suivant l'attribution du contrat.
b) La GRC fournira une copie des manuels d'exploitation indiqués à la section 4.

ANNEXE B – BASE DE PAIEMENT

À condition de remplir de façon satisfaisante toutes ses obligations en vertu du contrat, l'entrepreneur sera payé selon un prix unitaire ferme comme il est indiqué ci-dessous, selon un montant de _____ $ **(à insérer au moment de l'attribution du contrat)**. Les droits de douane sont compris, et les taxes applicables sont en sus.

AUX FINS D'ÉVALUATION SEULEMENT

Les soumissionnaires doivent inscrire leurs prix unitaires fermes en dollars canadiens dans les colonnes B, C, D, E et F, puis inscrire le prix calculé pour chacun dans la colonne G du tableau ci-dessous pour la période initiale du contrat et chaque période d'option.

Les soumissionnaires doivent remplir toutes les sections du tableau. Si toutes les sections du tableau ne sont pas remplies, la soumission pourrait être rejetée et ne pas être prise en considération.

***Remarque :** L'inclusion de données volumétriques (nombre estimé d'apprenants) dans le présent document ne constitue pas un engagement de la part du gouvernement du Canada que son utilisation future des services précisés dans ce document correspondra à ces données.

Calcul de l'évaluation financière = Somme totale de la colonne G

	Nombre estimatif d'apprenants* (A)	**Période initiale du contrat De : ____ À : _____ (B)**	**Période d'option 1 De : ____ À : _____ (C)**	**Période d'option 2 De : ____ À : _____ (D)**	**Période d'option 3 De : ____ À : _____ (E)**	**Période d'option 4 De : ____ À : _____ (F)**	**Prix estimatif (G = A × B + A × C + A ×D + A × E + A × F)**
Pilotes d'aéronefs à voilure fixe	**50**	$	$	$	$	$	**G1**
Pilotes d'aéronefs à voilure tournante	**20**	$	$	$	$	$	**G2**
Techniciens d'entretien d'aéronefs	**45**	$	$	$	$	$	**G3**
Membres d'équipage	**50**	$	$	$	$	$	**G4**
						TOTAL AUX FINS DE L'ÉVALUATION (G1 + G2 + G3 + G4)	

ANNEXE C – LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS) ET GUIDE DE SÉCURITÉ

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202105319
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: RCMP	2. Branch or Directorate / Direction générale ou Direction: Air Services 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
Aviation On-Line Training for pilots, aircraft maintenance engineers and flight crew members. This will be third party cloud based content accessible by air service employees.
Formation en ligne sur l'aviation pour les pilotes, les techniciens d'entretien d'aéronefs et les membres d'équipage. Il s'agira d'un contenu sur le nuage offert par un tiers et accessible par les employés du Service de l'air.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No Non ☐ 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 ☐ 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 ☐ 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
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 ☐ 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 ☐	NATO / OTAN ☐	Foreign / Étranger ☐

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

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

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

PROTECTED A / PROTÉGÉ A ☐	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) ☐

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
202105319
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?
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 :
☑ No Non ☐ Yes Oui

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

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
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : No security required for persec. IT requirements please see Security Guide / Aucune sécurité n'est requise pour l'outil Persec. Exigences en matière de technologies de l'information : voir le Guide de sécurité.

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?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
☐ No Non ☐ Yes Oui

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

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?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?
☑ No Non ☐ Yes Oui

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

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?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?
☑ No Non ☐ Yes Oui

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?
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?
☑ No Non ☐ Yes Oui

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

Government of Canada | Gouvernement du Canada

Contract Number / Numéro du contrat
202105319
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	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS 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?

☑ 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?

☑ 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 – LVERS

Formation en ligne pour la Sous-direction du service de l'air
Nº LVERS : 202105319

Préparé par :
Sécurité ministérielle
Gendarmerie royale du Canada

1. Préambule

1.1. Tous les énoncés contractuels et les appendices du présent Guide de sécurité de la Liste de vérification des exigences relatives à la sécurité (LVERS) ne s'appliquent qu'à ce contrat.

1.2. Tous les entrepreneurs employés dans le cadre de ce contrat doivent soutenir et tenir à jour l'environnement de sécurité de la Gendarmerie royale du Canada (GRC) en se conformant aux exigences décrites dans le présent document. Des obligations en matière de sécurité plus détaillées seront fournies lors de l'étape de la demande de propositions, le cas échéant. Le présent Guide de sécurité ne concerne que les services ou le personnel qui stockent ou traitent des renseignements de nature délicate jusqu'au niveau non classifié.

2. Définitions

Le **chargé de projet** est l'entité responsable de la gestion du contrat. Toute modification du contrat doit être autorisée par écrit par le chargé de projet et l'entrepreneur ne doit pas effectuer de travaux dépassant ou sortant du cadre du contrat à la suite de demandes ou d'instructions verbales ou écrites provenant d'une personne autre que le chargé de projet.

La **compromission** est une violation de la sécurité du gouvernement. Ceci comprend, sans toutefois s'y limiter :

- 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 au sein d'une installation fédérale qui a causé un dommage ou un préjudice à cet employé ou à cette personne;
- des événements qui engendrent la perte d'intégrité ou de disponibilité des services ou des activités du gouvernement.

Un **compte principal** est un compte doté de privilèges de base permettant de générer des comptes clients ou des sous-comptes qui permettront à l'organisation d'accéder aux services infonuagiques publics commerciaux.

Les **données organisationnelles** sont des renseignements ou des données, y compris tous les fichiers texte, les fichiers audio et vidéo, les fichiers d'image, les données de journal, les noms et les mots de passe des utilisateurs, les logiciels et les métadonnées connexes, peu importe la forme ou le format : A) divulgués par le personnel, les clients, les partenaires, les participants à des coentreprises, les concédants de licence, les fournisseurs de la GRC; B) divulgués par les utilisateurs finaux des services infonuagiques; C) recueillis, utilisés, traités par les services infonuagiques ou stockés dans ceux-ci; qui sont directement ou indirectement divulgués à l'entrepreneur ou aux sous-traitants par la GRC ou au nom de celle-ci ou par le biais de l'utilisation des services infonuagiques, y compris tout renseignement ou donnée (i) auquel l'entrepreneur ou tout sous-traitant obtient l'accès, intentionnellement ou par inadvertance; (ii) se trouvant sur tout réseau, système ou matériel utilisé ou géré pour la GRC par l'entrepreneur pour les services infonuagiques et les services de l'entrepreneur, y compris l'infrastructure de l'entrepreneur.

Un **dossier** est tout document papier ou toute donnée dans un format lisible par machine contenant des renseignements personnels.

Un **entrepreneur** est l'entité (peut inclure une ou plusieurs personnes physiques, sociétés, partenariats, sociétés à responsabilité limitée, fournisseurs de services, fournisseurs, etc.) qui fournit les services à la GRC et à ses partenaires. Il s'agit de l'entité approuvée et désignée comme étant « l'entrepreneur » dans le contrat subséquent.

Un **événement lié à la sécurité** est tout événement, omission ou situation qui pourrait porter atteinte à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité.

Le **fournisseur de services infonuagiques** est une entité (peut inclure une ou plusieurs personnes physiques, sociétés, partenariats, sociétés à responsabilité limitée, etc.) qui est à l'origine du service infonuagique public dans son ensemble.

On entend par **fuite d'information** les incidents au cours desquels des renseignements se retrouvent par inadvertance dans un bien ou un système n'étant pas autorisé à les traiter (p. ex. ITSG-33, IR-9).

L'**habilitation de sécurité** désigne l'habilitation de sécurité nécessaire, comme la cote de fiabilité approfondie ou la cote de niveau Secret, désignée par la Sécurité ministérielle de la GRC, qui peut comprendre une partie ou la totalité des étapes de contrôle de sécurité énumérées dans la clause de sécurité appropriée.

Un **incident de sécurité** est un événement (ou un ensemble d'événements), un acte, une omission ou une situation qui a entraîné une compromission. Exemples d'incidents de cybersécurité : exploitation active d'une ou de plusieurs vulnérabilités relevées, exfiltration de données, défaillance d'un contrôle de sécurité, violation d'un service du gouvernement du Canada hébergé ou géré dans le nuage, etc.

L'**infonuagique** est un modèle qui permet un accès réseau omniprésent, pratique et à la demande à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peuvent être offertes et diffusées rapidement avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de services.

Les **métadonnées** sont des renseignements décrivant les caractéristiques des données et comprennent notamment les métadonnées structurelles décrivant les structures de données (p. ex. le format, la syntaxe et la sémantique des données) et les métadonnées descriptives décrivant le contenu des données (p. ex. les étiquettes de sécurité de l'information).

Les **renseignements personnels** sont les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, tels que définis à l'article 3 de la *Loi sur la protection des renseignements personnels*, notamment les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa religion, à son âge ou à sa situation familiale, à son adresse, à son éducation, à son dossier médical, à son casier judiciaire ou à ses antécédents financiers ou professionnels. Les renseignements personnels comprennent également tout numéro ou symbole identificateur, comme le numéro d'assurance sociale, attribué à une personne.

Les **renseignements Protégé B** sont des renseignements ou des biens qui, s'ils sont compromis, pourraient causer un préjudice grave à une personne, une organisation ou un gouvernement.

Les **renseignements protégés** sont des renseignements ou des biens qui, s'ils sont compromis, risqueraient vraisemblablement de porter atteinte à un intérêt autre que l'intérêt national, c'est-à-dire à l'intérêt d'une personne ou d'une organisation.

Le **responsable de la sécurité** est l'entité qui, au sein d'une organisation, est autorisée à approuver la sécurité du contrat et détient le pouvoir de signature de la Liste de vérification des exigences relatives à la sécurité (LVERS).

Un **sous-traitant** est toute personne à laquelle l'entrepreneur sous-traite l'exécution de ses services, en tout ou en partie.

Un **sous-traitant des données** est une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite des données personnelles pour le compte d'un responsable du traitement des données ou d'un entrepreneur.

Le **télétravail** est une entente entre un employé de l'entrepreneur et le chargé de projet pour effectuer une partie ou la totalité de ses tâches professionnelles à partir d'un emplacement à distance. Le télétravail nécessite la conclusion d'une entente de télétravail entre l'entrepreneur et le chargé de projet.

Un **utilisateur final** est une personne ou un processus de système agissant pour le compte d'une personne autorisée par la GRC à accéder aux services infonuagiques.

3. Exigences générales relatives à la sécurité

3.1. Toutes les données organisationnelles, y compris la documentation papier ou d'autres biens de nature délicate dont la GRC est responsable, seront partagées avec l'entrepreneur par le biais de processus approuvés au préalable.

3.2. Les renseignements divulgués par la GRC seront gérés, conservés et éliminés conformément à l'ensemble des dispositions du contrat.

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

3.4. Il est interdit de prendre des photographies dans les locaux de la GRC. Si des photographies sont nécessaires, il faut communiquer avec le chargé de projet et la Sécurité ministérielle.

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

3.6. La Sécurité ministérielle de la GRC se réserve le droit de procéder à des inspections ou à un examen de sécurité des installations de l'entrepreneur ou des lieux de travail du personnel et de donner des instructions sur les mesures de sécurité obligatoires (mesures de sécurité spécifiées dans le présent document et possiblement des mesures de sécurité supplémentaires particulières au site). Des inspections peuvent être effectuées avant le partage de renseignements de nature délicate ou en fonction des besoins (p. ex. en cas de déménagement des bureaux de l'entrepreneur). L'objectif de l'inspection est de s'assurer du maintien de la robustesse des mesures de sécurité requises.

3.7. Toutes les données organisationnelles doivent être protégées par des moyens cryptographiques. Les algorithmes cryptographiques, la taille des clés cryptographiques et les périodes cryptographiques utilisés doivent être conformes à la norme ITSP.40.111 – Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B, ou à ses versions ultérieures.

3.8. Toutes les communications vocales, y compris les enregistrements, effectuées à l'aide d'un téléphone cellulaire doivent être limitées à des renseignements de nature non délicate, sauf si le téléphone est spécifiquement accrédité et fourni pour des renseignements de nature délicate.

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

4. Sécurité physique

4.1. *Stockage*

4.1.1. Lorsqu'il s'agit d'effectuer des travaux dans les locaux de l'entrepreneur, les données organisationnelles et les biens doivent être conservés dans un contenant approuvé par le responsable de la sécurité de la GRC. Le contenant doit être situé (au minimum) dans une « zone de travail ». À ce titre, les installations de l'entrepreneur doivent disposer d'une zone ou d'une salle répondant aux critères suivants :

Zone de travail	
a) Définition	1) Une zone dont l'accès est limité : i) au personnel qui est autorisé à y travailler; ii) aux visiteurs dûment accompagnés.
b) Périmètre	1) La zone de travail doit être indiquée par un périmètre reconnaissable ou un périmètre de sécurité, selon les besoins du projet. Par exemple, les mesures de contrôle peuvent être un bureau ou un local verrouillé. 2) La zone de travail peut faire l'objet d'un examen par l'unité responsable de la sécurité physique, et peut également nécessiter des mesures de sécurité supplémentaires ou l'acheminement aux échelons supérieurs si l'unité responsable de la sécurité physique de la GRC le juge nécessaire en fonction de l'évaluation de l'espace, des zones environnantes, des conditions particulières au site, etc.
c) Surveillance	1) La zone de travail doit être surveillée périodiquement par le personnel autorisé. Par exemple, les utilisateurs de l'espace qui travaillent sur place sont en mesure d'observer s'il y a eu une atteinte à la sécurité.

Remarque : Consulter l'appendice A pour de plus amples renseignements au sujet du concept de zone de sécurité.

4.1.2. Lorsque les entrepreneurs sont autorisés à travailler à partir d'un lieu de télétravail, les données organisationnelles de nature délicate non chiffrées ou en format papier ne sont pas autorisées. Tous les biens de la GRC doivent être entreposés dans un endroit qui répond aux critères suivants :

Lieu de télétravail	
a) Définition	1) Un espace au Canada* dont l'accès est limité aux membres du personnel travaillant à l'appui du contrat et aux visiteurs accompagnés.
b) Périmètre	1) Lorsque les entrepreneurs travaillent à partir d'un lieu de télétravail, le travail doit être effectué dans un espace réservé à cet effet pouvant être protégé contre la surveillance et l'écoute par les colocataires ou au moyen des fenêtres.
c) Surveillance	1) Les renseignements et les biens de la GRC doivent faire l'objet d'une surveillance régulière par l'entrepreneur. Par exemple, les utilisateurs de l'espace qui travaillent sur place sont en mesure d'observer s'il y a eu une atteinte à la sécurité et de le signaler.

**Le lieu de télétravail doit se situer au Canada. Des exceptions pour le télétravail à l'extérieur du Canada peuvent être autorisées dans les pays du Groupe des cinq avec une évaluation de la sécurité de la GRC et l'approbation écrite de la GRC par le dirigeant principal de la sécurité ou son délégué.*

4.1.3. Pour les lieux de télétravail, l'entrepreneur doit prendre des mesures raisonnables pour protéger les renseignements et les biens de la divulgation non autorisée, de la perte, du vol, du feu, de la destruction, des dommages ou des modifications.

4.1.4. Les lieux de télétravail ne doivent se trouver que dans des espaces clos et privés, jamais à l'extérieur ou dans un lieu public.

4.1.5. Pendant le travail, l'entrepreneur doit être conscient de son environnement à tout moment et être en mesure de fermer immédiatement tout programme ou application et de verrouiller l'ordinateur si nécessaire.

4.2. *Discussions*

4.2.1. Lorsque des conversations sensibles sont prévues dans les installations de l'entrepreneur, les zones de travail doivent être dotées de barrières acoustiques pleine hauteur continues dont l'indice acoustique correspond au niveau de protection nécessaire selon le degré de sensibilité des discussions.

4.3. *Production de renseignements ou d'autres biens sur support papier*

4.3.1. La production (génération ou modification) de données organisationnelles ou de biens sur support papier doit avoir lieu dans une zone répondant aux critères d'une zone de travail. Pour plus de détails, consulter la section Impression, numérisation et photocopie.

4.4. *Destruction*

4.4.1. Si l'entrepreneur crée de la documentation papier contenant des données organisationnelles pendant la durée du présent contrat, il doit détruire toutes les ébauches ou impressions erronées (copies endommagées ou copies restantes).

4.4.2. Les données organisationnelles stockées de manière éphémère ou temporaire doivent également être détruites lorsqu'elles ne sont plus utilisées.

4.4.3. Les données organisationnelles doivent être détruites par l'entrepreneur conformément aux directives ci-dessous :

a) l'équipement ou le système (c.-à-d. la déchiqueteuse) utilisé pour détruire les documents de nature délicate doit correspondre au degré de destruction requis, conformément au Guide de sélection de l'équipement de déchiquetage (rcmp-grc.gc.ca);

b) toutes les ébauches ou impressions erronées de documents de nature délicate en attente d'élimination doivent être protégées conformément à leur classification de sécurité jusqu'à leur destruction.

4.5. *Transport et transmission de biens matériels*

4.5.1. L'échange physique de renseignements et de biens de nature délicate sur support papier doit être sécurisé avant le transport et la transmission. Lorsqu'un service de livraison est utilisé, ce dernier doit offrir une preuve de l'envoi, ainsi qu'un numéro de repérage pour le suivi du transport et la livraison.

a) Transport	1) Transport : Transfert de renseignements et de biens de nature délicate sur support papier jusqu'au niveau Protégé B inclusivement d'une personne ou d'un lieu à un autre par une personne **ayant besoin de connaître** ces renseignements ou d'accéder à ces biens. 2) Préparation : Enveloppe simple scellée ou mallette verrouillée ou autre contenant offrant la même protection ou une protection supérieure. 3) Méthode de livraison : Personnel autorisé.
b) Transmission	1) Transmission : Transfert de renseignements et de biens de nature délicate jusqu'au niveau Protégé B inclusivement d'une personne ou d'un lieu à un autre par une personne **n'ayant pas besoin de connaître** ces renseignements ou d'accéder à ces biens. 2) Adresse indiquée de manière non spécifique sur l'enveloppe. Ajout de la mention « Ne doit être ouvert que par » en raison du principe du besoin de connaître ou du besoin d'y accéder, lorsque justifié. 3) Préparation : Enveloppe simple scellée. 4) Méthode de livraison : Courrier recommandé, poste prioritaire, service de messagerie commerciale ou courrier de première classe.

5. Contrôles généraux de la sécurité de la technologie de l'information

5.1. *Répartition des obligations en matière de sécurité*

5.1.1. Les obligations en matière de sécurité s'appliquent à l'entrepreneur et à tout sous-traitant ou sous-traitant des données, s'il y a lieu. L'entrepreneur est tenu de s'assurer que ses sous-traitants et sous-traitants des données se conforment à ces obligations en matière de sécurité, le cas échéant.

5.2. *Rôles et responsabilités en matière de sécurité*

5.2.1. L'entrepreneur doit définir clairement les rôles et les responsabilités de l'entrepreneur et de la GRC en ce qui concerne les contrôles de sécurité et les caractéristiques de la solution. Cela comprend, au minimum, les rôles et les responsabilités en ce qui concerne les éléments suivants :

a) la gestion des comptes;
b) la protection des limites;
c) les sauvegardes pour les biens et les systèmes d'information;
d) la gestion des incidents;
e) la surveillance des systèmes;
f) la gestion des vulnérabilités.

5.3. *Recours à des sous-traitants, des sous-traitants des données et des sous-traitants des données secondaires*

5.3.1. L'entrepreneur doit fournir une liste des sous-traitants, des sous-traitants des données et des sous-traitants des données secondaires qui pourraient être utilisés pour effectuer une partie du travail dans le cadre de la prestation du 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 inclure les renseignements suivants :

a) le nom des sous-traitants, des sous-traitants des données et des sous-traitants des données secondaires;
b) la description du travail qui serait effectué ou du service qui serait fourni par les sous-traitants, les sous-traitants des données, les sous-traitants des données secondaires;
c) le ou les lieux où les sous-traitants, les sous-traitants des données et les sous-traitants des données secondaires effectueraient le travail.

5.3.2. L'entrepreneur doit fournir une liste des sous-traitants, des sous-traitants des données et des sous-traitants des données secondaires dans les 10 jours suivant la date d'entrée en vigueur du contrat.

5.3.3. L'entrepreneur doit informer la GRC de tout nouveau sous-traitant, sous-traitant des données et sous-traitant des données secondaires au moins 14 jours avant de lui donner accès aux données de l'organisation.

5.4. *Gestion du télétravail*

5.4.1. Les lieux de travail de l'ensemble du personnel de l'entrepreneur doivent être clairement indiqués dans l'appendice Guide de classification et Énoncé des travaux. L'entrepreneur doit régulièrement rendre compte du lieu de travail, y compris des lieux de télétravail des employés, et du nombre de jours travaillés. Si l'on s'attend à ce que le lieu de travail change pendant la durée du contrat, cela doit également être explicitement indiqué. La GRC doit être informée de tout changement de lieu de travail qui n'est pas indiqué dans l'appendice Guide de classification et Énoncé des travaux, car ce lieu devra faire l'objet d'un examen contractuel et d'une approbation en matière de sécurité.

5.4.2. Lorsqu'il est nécessaire d'utiliser du matériel fourni par la GRC, le chargé de projet et l'entrepreneur doivent effectuer ce qui suit :

a) Gérer et surveiller l'accès à distance de l'entrepreneur aux systèmes et aux données organisationnels de la GRC;

b) Effectuer toutes les tâches tout au long du contrat en utilisant l'équipement fourni;

c) Fournir l'équipement standard de la GRC pour le travail à distance, y compris un ordinateur portatif imagé par la GRC avec chiffrement complet du disque approuvé;

d) Utiliser l'authentification multifactorielle avec des identifiants standard fournis par la GRC pour toutes les exigences d'accès sécurisé (p. ex. accès à un réseau privé virtuel [RPV]);

e) S'assurer que l'entrepreneur a lu et signé la *Politique sur l'utilisation acceptable* de la GRC;

f) Veiller à ce que l'équipement de la GRC demeure en permanence sur les lieux de travail spécifiés.

5.4.3. Si l'utilisation d'équipement fourni par la GRC n'est pas indiquée dans la LVERS, l'entrepreneur peut utiliser son propre équipement à condition que celui-ci respecte les exigences de sécurité énoncées dans la section sur la protection des points d'extrémité.

5.5. *Protection des points d'extrémité*

5.5.1. Lorsque les points d'extrémité sont fournis par l'entrepreneur, celui-ci doit mettre en œuvre, gérer et surveiller des points d'extrémité renforcés sur le plan de la sécurité et dotés de protections actives au niveau de l'hôte afin de prévenir les logiciels malveillants, les attaques et les utilisations abusives, conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles figurant dans le guide NIST 800-123 (Guide to General Server Security), les bases de référence CIS Benchmarks du Center for Internet Security ou une norme équivalente approuvée par écrit par la GRC.

5.6. *Protection cryptographique*

5.6.1. Le personnel de l'entrepreneur doit effectuer ce qui suit :

a) Configurer toute cryptographie utilisée pour mettre en œuvre des mesures de protection de la confidentialité ou de l'intégrité, ou utilisée dans le cadre d'un mécanisme d'authentification (p. ex. solutions de RPV, protocole TLS, modules logiciels, infrastructure à clés publiques et jetons d'authentification, le cas échéant), conformément aux algorithmes cryptographiques, aux tailles de clés cryptographiques et aux périodes cryptographiques approuvées par le Centre de la sécurité des télécommunications (CST).

b) Utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques et des périodes cryptographiques qui ont été validés par le Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/ [en anglais seulement]) et qui sont spécifiés dans la norme ITSP.40.111 – Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B ou dans ses versions ultérieures (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111-algorithms-unclassifiedprotected-and-protected-b-information-itsp40111).

5.7. *Protection des données*

5.7.1. Lorsque l'utilisation de l'équipement fourni par la GRC est requise, toutes les tâches assignées à l'entrepreneur doivent être accomplies à l'aide de l'équipement fourni et conformément aux 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 des équipements non approuvés et non fournis par la GRC, sauf indication contraire par écrit. Si l'utilisation de l'équipement fourni par la GRC n'est pas requise, l'entrepreneur peut utiliser son propre équipement à condition que celui-ci respecte les exigences de sécurité énoncées dans la section sur la protection des points d'extrémité.

5.7.2. Les données organisationnelles ne doivent pas être stockées sur des services infonuagiques à moins qu'une autorisation d'exploitation n'ait été émise par la Sécurité ministérielle de la GRC pour le service infonuagique en cause. Le chargé de projet doit s'assurer qu'une autorisation d'exploitation a été émise et que toutes les conditions sont respectées pendant toute la durée du contrat.

5.7.3. Toutes les données organisationnelles inactives hébergées dans un service infonuagique doivent être chiffrées conformément aux exigences de la GRC, y compris toutes les métadonnées ou tous les journaux dérivés des données organisationnelles ou liés à celles-ci.

5.7.4. Toute sauvegarde de données organisationnelles est soumise aux mêmes directives de sécurité en matière de chiffrement et de contrôle d'accès que la source de données principale.

5.7.5. Les documents et les supports électroniques doivent être nettoyés ou détruits conformément à la norme ITSP.40.006 – Nettoyage des supports de TI (pour plus d'information, consulter la norme à l'adresse suivante : https://www.cyber.gc.ca/fr/orientation/nettoyage-des-supports-de-ti-itsp40006).

5.7.6. Il est interdit à l'entrepreneur et à son personnel de faire des copies des bases de données contenant des données organisationnelles ou de toute partie de ces bases de données en dehors des capacités de résilience des services réguliers et des espaces ou zones régionaux approuvés par la GRC.

5.7.7. L'entrepreneur et son personnel ne doivent pas déplacer ou transmettre des données organisationnelles inactives en dehors des régions de service convenues, sauf lorsqu'une autorisation à cet égard a été fournie par la GRC.

5.7.8. L'entrepreneur doit :

a) Mettre en œuvre un chiffrement de bout en bout pour toutes les données protégées en transit vers et depuis n'importe quel service infonuagique. Le chiffrement des données en transit doit respecter les exigences de la norme ITSP.40.111 – Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B ou ses versions ultérieures (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111-algorithms-unclassifiedprotected-and-protected-b-information-itsp40111).

b) Mettre en œuvre le chiffrement des données inactives pour tous les services hébergeant des données organisationnelles, y compris toutes les métadonnées ou tous les journaux dérivés des données organisationnelles ou liés à celles-ci, et le chiffrement des données inactives doit être effectif, ininterrompu et actif à tout moment, même en cas de défaillance de l'équipement ou de la technologie, comme spécifié dans la norme ITSP.40.111 – Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B ou ses versions ultérieures (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111-algorithms-unclassifiedprotected-and-protected-b-information-itsp40111).

c) Mettre en œuvre des contrôles de sécurité qui restreignent l'accès administratif aux données organisationnelles, y compris toutes les métadonnées ou tous les journaux dérivés des données et systèmes organisationnels ou liés à ceux-ci, par l'entrepreneur, et qui prévoient la possibilité d'exiger l'approbation de la GRC avant de pouvoir accéder aux données organisationnelles pour effectuer des activités de soutien, de maintenance ou d'exploitation.

d) Prendre des mesures raisonnables pour s'assurer que le personnel de l'entrepreneur ne dispose pas de droits d'accès permanents ou continus aux données organisationnelles sans besoin de connaître, y compris les ressources qui offrent un soutien technique ou à la clientèle selon l'approbation de la GRC.

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

5.8. *Emplacement des données (résidence)*

5.8.1. Toutes les données organisationnelles de nature délicate, y compris les données des copies de sauvegarde ou les données conservées à des fins de redondance, doivent se trouver à l'intérieur des frontières géographiques du Canada ou d'une ambassade ou d'un consulat du gouvernement du Canada situé à l'étranger.

5.9. *Traitement des données*

5.9.1. Toutes les données organisationnelles de nature délicate traitées par l'entrepreneur doivent l'être dans les limites géographiques du Canada*.

*Des exceptions pour le traitement des données organisationnelles de niveau Protégé A à l'extérieur du Canada peuvent être autorisées dans les pays du Groupe des cinq avec une évaluation de la sécurité de la GRC et l'approbation écrite de la GRC par le dirigeant principal de la sécurité ou son délégué.

5.10. *Transport et transmission de données*

5.10.1. S'il est nécessaire de transporter des données organisationnelles, celles-ci doivent être transportées à l'aide d'un dispositif de stockage portatif conforme à la norme FIPS 140-2 de niveau 2 ou supérieur fourni par la GRC. L'accès à ce dispositif doit être limité au personnel de l'entrepreneur ayant reçu une habilitation 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 remis en main propre ou expédié conformément aux instructions figurant à la section « Transport et transmission de biens matériels ».

5.10.2. Le mot de passe du dispositif de stockage portatif doit être fourni par des moyens hors bande, soit en personne ou par téléphone, uniquement au personnel de l'entrepreneur ayant reçu une habilitation de sécurité appropriée.

5.10.3. Lorsqu'il est nécessaire de transmettre des données organisationnelles, y compris toutes les métadonnées ou toutes les données de journal découlant des données organisationnelles ou liées à celles-ci, cela doit être fait de manière sécurisée, y compris par la mise en œuvre du chiffrement des données en transit, comme l'indique la section « Protection cryptographique ».

5.11. *Élimination des données et retour des dossiers*

5.11.1. L'entrepreneur doit procéder à l'effacement cryptographique des ressources (p. ex. l'équipement, les emplacements de stockage de données, les fichiers et la mémoire) qui contiennent des données organisationnelles et veiller à ce que les données stockées précédemment ne soient pas accessibles à d'autres clients. Sont visées toutes les copies des données organisationnelles qui sont effectuées à des fins de disponibilité élevée et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être conforme à l'un des points suivants :

a) Nettoyage des supports de TI (ITSP.40.006) [Centre canadien pour la cybersécurité];

b) Guidelines for Media Sanitization (NIST SP 800-88) [en anglais seulement];

c) à la demande de la GRC, l'entrepreneur doit fournir un document décrivant son processus d'élimination ou de réutilisation des ressources.

5.11.2. L'entrepreneur doit fournir à la GRC une confirmation, par le biais d'une lettre d'attestation ou d'entrées de journal, qui démontre que toutes les ressources ont été correctement éliminées, purgées ou détruites, selon le cas, et qui démontre la capacité d'empêcher le rétablissement de tout système, capacité (logiciel ou processus), donnée ou instance d'information supprimé ou détruit une fois que la GRC a cessé d'utiliser les services. La GRC peut exiger la preuve que les clés de chiffrement ont été détruites ou que les données ont bien fait l'objet d'un effacement cryptographique afin d'empêcher la récupération des données.

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

a) maintenir toutes les mesures de protection des données et de sécurité au niveau stipulé dans les présentes exigences relatives à la 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 lui permettant de récupérer toutes ces données auprès du contractant.

5.12. *Réponse aux incidents de sécurité*

5.12.1. Le National Institute of Standards and Technology (NIST) définit un incident de sécurité comme « un événement qui compromet réellement ou potentiellement la confidentialité, l'intégrité ou la disponibilité d'un système d'information ou de l'information que le système traite, stocke ou transmet ou qui constitue une violation ou une menace imminente de violation des politiques de sécurité, des procédures de sécurité ou des politiques d'utilisation acceptable » [Traduction]. L'entrepreneur doit donc aviser rapidement le responsable de la sécurité de la GRC (par téléphone et/ou par courriel) de toute compromission ou violation ou de tout signe de compromission ou de violation, notamment :

a) un incident de sécurité;

b) une défaillance de la sécurité de tout bien;

c) une fuite de données;

d) l'accès irrégulier ou non autorisé à tout bien;

e) la copie à grande échelle de renseignements;

f) toute autre activité irrégulière relevée par l'entrepreneur qui lui donne des motifs raisonnables de croire qu'un risque de compromission ou d'atteinte à la sécurité ou à la vie privée est ou peut être imminent, ou si les mesures de protection existantes ont cessé de fonctionner.

5.12.2. Si l'entrepreneur constate une compromission ou une atteinte à la sécurité entraînant, accidentellement ou illégalement, la destruction, la perte, l'altération ou la divulgation non autorisée de données du client ou de données personnelles ou l'accès à ces données tandis qu'elles sont traitées par l'entrepreneur (chacune de ces situations étant un « incident de sécurité »), l'entrepreneur doit, immédiatement ou au plus tard dans un délai de 24 heures :

a) signaler l'incident de sécurité au responsable de la sécurité de la GRC;

b) enquêter sur l'incident de sécurité et fournir à la GRC de l'information détaillée sur celui-ci;

c) prendre des mesures raisonnables pour atténuer la cause de l'incident de sécurité et minimiser les dommages qui en découlent.

5.13. *Impression, numérisation et photocopie*

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

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

a) disposer d'imprimantes, scanneurs ou photocopieurs supplémentaires ou dédiés qui ne sont pas directement connectés à un réseau, y compris à Internet. Des connexions locales dédiées entre ces dispositifs et les points terminaux de l'entrepreneur sont acceptables;

b) respecter les exigences définies à la section Sécurité physique en ce qui concerne le stockage, la production de renseignements ou d'autres biens sur support papier et la destruction;

c) nettoyer ou détruire les dispositifs d'impression, de numérisation et de photocopie (tels que les appareils multifonctions, les imprimantes, les photocopieuses) conformément à l'ITSP.40.006, Nettoyage des supports de TI (consulter le site https://www.cyber.gc.ca/fr/orientation/nettoyage-des-supports-de-ti-itsp40006 pour en savoir plus).

5.14. *Gestion de l'identité et de l'accès*

5.14.1. S'il est nécessaire d'utiliser l'équipement de la GRC, les membres du personnel de l'entrepreneur se verront attribuer des justificatifs d'identité leur permettant d'accéder aux biens protégés de la GRC. Les justificatifs d'identité de la GRC ne doivent être utilisés que dans le cadre de l'exécution des tâches décrites dans les documents du contrat et doivent être révoqués à la fin du présent contrat.

5.15. *Licenciements et résiliation du contrat*

5.15.1. L'entrepreneur doit avoir mis en œuvre une procédure documentée de licenciement ou de changement de statut pour le personnel. La procédure doit comprendre, au minimum, les éléments suivants :

a) la transmission d'un avis de licenciement au chargé de projet le jour même du licenciement;

b) la suppression de l'accès au système d'information le jour même du licenciement;

c) la résiliation ou la révocation de tous les identifiants ou justificatifs associés à la personne concernée dans les 24 heures;

d) la réalisation d'une entrevue de départ qui comprend une discussion sur les points cernés dans la *Norme sur le filtrage de sécurité* du Secrétariat du Conseil du Trésor et sur toute disposition connexe du Programme de la sécurité industrielle;

e) la soumission du formulaire 330-47 – Certificat d'enquête de sécurité et profil de sécurité pour la résiliation de l'habilitation de sécurité de l'entrepreneur;

f) la récupération de tous les biens liés à la sécurité des systèmes d'information de la GRC, y compris les cartes d'accès, dans les 24 heures;

g) la conservation de l'accès à l'information et aux systèmes d'information de la GRC précédemment contrôlés par la personne licenciée.

5.15.2. En cas de résiliation du contrat pour quelque raison que ce soit, le personnel de l'entrepreneur est tenu de remettre au chargé de projet de la GRC tous les appareils fournis par la GRC, y compris, sans s'y limiter :

a) les ordinateurs portatifs;

b) les téléphones cellulaires;

c) les clés USB;

d) les cartes à puce.

6. Obligations de sécurité relatives aux logiciels en tant que service et plateformes en tant que service

Sont présentées ci-dessous les obligations de sécurité supplémentaires qui doivent être respectées lorsqu'un entrepreneur doit, dans le cadre d'un contrat, utiliser ou développer un logiciel en tant que service ou une plateforme en tant que service non contrôlé par la GRC pour la prestation des services énoncés dans le contrat.

6.1. *Sécurité des réseaux et des communications*

6.1.1. Assurer la sécurité des connexions aux services, notamment en protégeant les données en transit entre la GRC et le service à l'aide du protocole TLS 1.2 (ou versions subséquentes).

6.1.2. Utiliser des protocoles, des algorithmes de chiffrement et des certificats à jour et pris en charge, comme l'indiquent les documents ITSP.40.062 (https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062) et ITSP.40.111 (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111) du CST.

6.1.3. Utiliser des certificats correctement configurés dans les connexions TLS conformément aux directives du CST énoncées dans le document ITSP.40.062 (https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062).

6.1.4. S'assurer que ces certificats fonctionnent avec la solution d'agent de sécurité d'accès au nuage de la GRC.

6.2. *Développement sécurisé*

6.2.1. S'il y a lieu, l'entrepreneur doit mettre en œuvre un cycle de développement de logiciel et de système qui applique les principes techniques de sécurité des systèmes d'information tout au long du cycle de vie du système d'information et au développement des logiciels, des sites Web et des services, et qui respecte les normes et les pratiques exemplaires de l'industrie, notamment :

a) les normes du NIST;
b) la norme ISO 27034;
c) la norme ITSG-33;
d) SAFECode;
e) les normes de l'Open Web Application Security Project (OWASP), telles que l'Application Security Verification Standard (ASVS);
f) toute norme équivalente approuvée par écrit par la GRC.

6.2.2. À la demande de la GRC, l'entrepreneur doit fournir un document décrivant son approche et son processus documentés relativement au cycle de vie du développement des logiciels et des systèmes.

6.2.3. L'entrepreneur doit nommer par écrit la personne qui sera responsable de la sécurité globale des processus de développement, de gestion et de mise à jour des applications pendant toute la durée du contrat.

6.2.4. Le personnel de l'entrepreneur qui travaille sur les biens de TI de la GRC dans l'environnement de développement de la GRC est tenu de suivre les processus de développement de la GRC et de respecter toutes ses structures de gouvernance de la GI-TI.

6.3. *Processus d'évaluation et d'autorisation de la sécurité des TI*

6.3.1. S'il y a lieu, l'entrepreneur doit démontrer qu'il respecte les exigences de sécurité choisies par la GRC pour la portée des services fournis par l'entrepreneur. La conformité devra être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications tierces applicables (c.-à-d. ISO 27001, SOC 2 Type 2). Pour l'information non classifiée, la validation des contrôles de sécurité par la présentation de preuves directement à la GRC peut être acceptable (c.-à-d. le Consensus Assessment Initiative Questionnaire [questionnaire sur l'initiative d'évaluation du consensus] de la Cloud Security Alliance).

6.3.2. La conformité sera évaluée et validée par la GRC au moyen de son processus d'évaluation de la sécurité et d'autorisation ou d'un processus tiers déterminé par la GRC.

6.3.3. Dans le cas où l'entrepreneur a été évalué et validé au moyen du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100) du Centre canadien pour la cybersécurité (https://www.cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux), l'entrepreneur doit démontrer qu'il a participé au processus en adhérant avec succès au programme, en y participant et en le terminant. À cette fin, il doit fournir les documents suivants à la GRC :

a) une copie de la lettre de confirmation indiquant qu'il a été admis au programme;

b) une copie du dernier rapport d'évaluation rempli fourni par le Centre canadien pour la cybersécurité;

c) une copie du dernier rapport sommaire fourni par le Centre canadien pour la cybersécurité.

6.3.4. Il incombe à l'entrepreneur d'aviser la GRC avant de mettre en production tout système ou service nouveau ou modifié de façon importante et, sur demande de la GRC, l'entrepreneur doit, à ses frais, se soumettre à tout processus d'évaluation de la sécurité ou à toute vérification supplémentaire jugée nécessaire par la GRC.

6.3.5. Le personnel de l'entrepreneur doit participer à tout processus d'évaluation et d'autorisation de sécurité jugé nécessaire par le chargé de projet ou la Sécurité ministérielle.

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

6.4. *Gestion de l'identité et de l'accès*

6.4.1. Lorsque l'entrepreneur fournit un service à la GRC, il doit se conformer à la section sur la gestion de l'identité et de l'accès. Si les justificatifs d'identité de la GRC ne sont pas requis, l'entrepreneur doit mettre en œuvre ce qui suit :

a) l'authentification multifactorielle conformément au document ITSP.30.031 V3 du CST (ou versions ultérieures) [https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de] à l'aide de justificatifs approuvés par le gouvernement du Canada;

b) l'accès fondé sur le rôle;

c) le contrôle de l'accès aux objets stockés;

d) des politiques d'autorisation détaillées permettant d'autoriser ou de limiter l'accès.

6.5. *Gestion de l'accès privilégié*

6.5.1. Lorsque l'entrepreneur ou son personnel, y compris les sous-traitants, accèdent à des services gérés par la GRC, l'entrepreneur doit permettre à la GRC de gérer et de surveiller l'accès privilégié de l'entrepreneur à tous les services, y compris les services offerts à partir d'un locataire de la GRC.

6.5.2. Lorsque l'entrepreneur ne réalise pas ses opérations à partir d'un locataire géré par la GRC, il doit :

a) gérer et surveiller l'accès privilégié aux données organisationnelles dans les services autres que ceux de la GRC afin de s'assurer que toutes les interfaces de service dans un environnement multilocataires, y compris celles qui sont utilisées pour héberger les services de la GRC, sont protégées contre les accès non autorisés;

b) restreindre et minimiser l'accès aux services et aux données organisationnelles aux appareils et utilisateurs finaux autorisés ayant explicitement besoin de cet accès;

c) appliquer et vérifier les autorisations d'accès aux services et aux données organisationnelles;

d) limiter l'accès aux interfaces de services hébergeant des données organisationnelles aux utilisateurs finaux, dispositifs et processus (ou services) identifiés, authentifiés et autorisés au moyen d'un identifiant unique;

e) mettre en œuvre des politiques de mot de passe pour protéger les justificatifs d'identité contre la compromission par des attaques en ligne ou hors ligne et pour détecter ces attaques en consignant et en surveillant des événements tels que : (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle des justificatifs d'identité et (iii) l'accès à la base de données des mots de passe et l'exfiltration de mots de passe de celle-ci, conformément à la norme ITSP.30.031 V3 (ou version subséquente) du CST (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);

f) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément à la norme ITSP.30.031 V3 (ou version subséquente) du CST (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);

g) mettre en œuvre des mécanismes de contrôle de l'accès fondés sur les rôles afin d'attribuer des privilèges qui constituent la base de l'accès aux données de l'organisation;

h) définir et mettre en œuvre la séparation des tâches afin de séparer, au minimum, les rôles de gestion et d'administration des services des rôles de soutien des systèmes d'information, les rôles de développement des rôles opérationnels, et les rôles de gestion de l'accès des autres rôles opérationnels;

i) respecter les principes du droit d'accès minimal et du besoin de savoir lors de l'octroi de l'accès aux services et aux données organisationnelles;

j) exiger, si nécessaire, une double autorisation pour les actions considérées par la GRC comme étant de nature très délicate ou à haut risque;

k) s'il y a lieu, utiliser des points d'extrémité à sécurité élevée (p. ex. des ordinateurs, des dispositifs d'utilisateur final, des serveurs intermédiaires) qui sont configurés de manière à offrir des fonctionnalités minimales afin de fournir un soutien et de permettre l'administration des services et de l'infrastructure de l'entrepreneur et à empêcher l'utilisation de dispositifs de stockage de masse USB;

l) mettre en œuvre un processus automatisé pour vérifier périodiquement, au minimum, les actions de création, de modification, d'activation, de désactivation et de suppression de comptes;

m) en cas de cessation d'emploi, révoquer les authentifiants et les justificatifs d'identité associés à tout membre du personnel de l'entrepreneur;

n) à la demande de la GRC, fournir un document décrivant son approche et son processus de gestion et de surveillance de l'accès privilégié aux services.

6.5.3. Les membres du personnel de l'entrepreneur se verront attribuer des rôles au sein de l'infrastructure de la GRC en fonction de leurs tâches. Les membres du personnel de l'entrepreneur ne doivent en aucun cas disposer d'un accès au compte principal ou au compte racine.

6.6. *Gestion du compte principal*

6.6.1. L'entrepreneur doit veiller à protéger adéquatement le processus de gestion de compte utilisé pour fournir les services à la GRC et soutenir ceux-ci. Les mesures de sécurité doivent comprendre ce qui suit, sans s'y limiter :

a) fournir des privilèges de compte principal uniquement au personnel de la GRC de sorte que le vendeur cède tout contrôle du service à la GRC;

b) lorsque le personnel de l'entrepreneur doit ou souhaite avoir accès au compte principal, l'entrepreneur doit :

i) limiter l'accès aux utilisateurs habilités et autorisés par la GRC à exécuter des transactions et des fonctions telles que la création et l'émission d'un compte principal;

ii) assurer la séparation des tâches des personnes;

iii) appliquer le principe du droit d'accès minimal, y compris pour des fonctions de sécurité spécifiques et les comptes privilégiés;

iv) veiller à ce que les utilisateurs autorisés reçoivent une formation sur la sécurité et soient sensibilisés à celle-ci dans le cadre de l'intégration professionnelle et lorsque leur rôle change;

v) créer, protéger et conserver les dossiers de vérification relatifs aux activités qui soutiennent la gestion des comptes pour les services fournis à la GRC;

vi) fournir à la GRC des rapports sur les événements vérifiés ayant trait aux actions liées à la création et à la gestion de comptes principaux;

vii) veiller à ce que les données organisationnelles soient protégées pendant et après la prise de mesures touchant le personnel, comme les licenciements et les transferts.

7. Sécurité du personnel

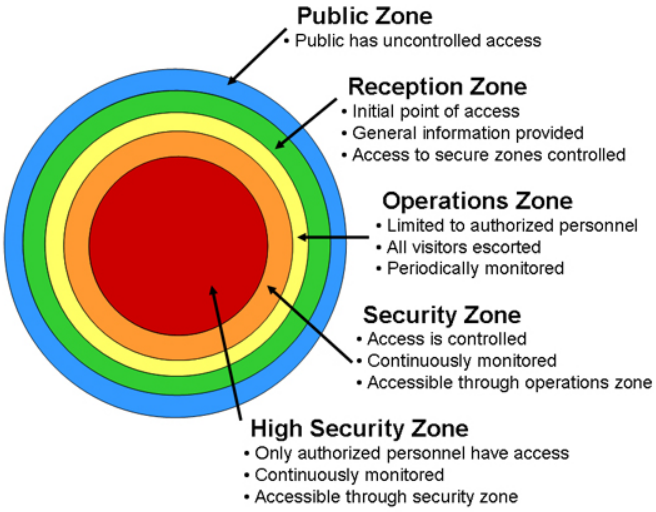
Le personnel de l'entrepreneur aura accès à des renseignements de nature délicate de la GRC; il doit donc posséder une habilitation de sécurité de niveau appropriée ou une habilitation équivalente approuvée par la GRC*. Le personnel de l'entrepreneur doit se soumettre à une vérification par la GRC avant de se voir accorder l'accès à des renseignements, systèmes, biens ou installations de nature délicate. La GRC se réserve le droit de refuser l'accès à tout membre du personnel de l'entrepreneur, et ce, en tout temps. En cas d'incident de sécurité ou de tout autre type d'incident, la GRC a le droit de refuser ou de suspendre l'accès à ses emplacements, services ou données en attendant un examen de l'incident, si la situation le justifie.

Pour ce besoin, nous avons déterminé qu'aucune habilitation de sécurité n'est requise pour le personnel, mais qu'il existe des exigences relatives aux TI qui nécessitent de suivre des directives en matière de sécurité.

Appendice A – Concept de zone 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 ».

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



ANGLAIS	FRANÇAIS
Public zone	Zone d'accès public
Public has uncontrolled access	Zone où l'accès est libre pour le public
Reception zone	Zone d'accueil
Initial point of access	Point d'accès initial
General information provided	Transmission de renseignements généraux
Access to secure zones controlled	Accès aux zones sécurisées contrôlé
Operations Zone	Zone de travail
Limited to authorized personnel	Limité au personnel autorisé
All visitors escorted	Tous les visiteurs sont accompagnés
Periodically monitored	Surveillance périodique
Security Zone	Zone de sécurité
Access is controlled	Accès contrôlé
Continuously monitored	Surveillance continue
Accessible through operations zone	Accessible par la zone de travail
High Security Zone	Zone de haute sécurité
Only authorized personnel have access	Accès limité au personnel autorisé
Continuously monitored	Surveillance continue
Accessible through security zone	Accessible par la zone de travail

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 – endroit où la transition d'une zone d'accès public à une zone à accès restreint est délimitée et contrôlée. Elle est généralement située à l'entrée de l'immeuble, où survient le premier contact entre le public et le ministère; il peut s'agir d'un endroit 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 – secteur dont l'accès est limité au personnel qui y travaille et aux visiteurs accompagnés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée sur une base périodique. Exemples : un espace à bureaux à aire ouverte typique ou le local typique des installations électriques.

Zone de sécurité – zone dont l'accès est limité au personnel autorisé et aux visiteurs autorisés et accompagnés comme il se doit; elle doit être indiquée par un périmètre reconnaissable et surveillée continuellement (24 heures sur 24, 7 jours sur 7). Exemple : une zone où des renseignements secrets sont traités ou conservés.

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

L'accès aux zones devrait être fondé sur le concept du « besoin de connaître » et sur la restriction de l'accès pour protéger le personnel et les biens de valeur. Pour obtenir de plus amples renseignements, veuillez consulter le document de la GRC G1-026 Guide pour l'établissement des zones de sécurité matérielle.

Annexe D – Critères d'évaluation

1. INSTRUCTIONS À L'INTENTION DU SOUMISSIONNAIRE

1. Le soumissionnaire doit fournir une réponse aux Critères d'évaluation ou d'indiquer en quoi il répond aux critères en indiquant l'emplacement (p. ex. numéro de section/volume, onglet, numéro de page, paragraphe du résumé, etc.) dans la colonne « Justification ».

2. Pour que le Canada tienne compte de l'expérience de travail, la soumission technique ne doit pas simplement indiquer le titre d'un sujet, mais doit décrire en détail le sujet et la durée de son offre.

3. Le soumissionnaire doit également utiliser le numéro unique du point ainsi que le titre/la description correspondant dans ses réponses aux critères d'évaluation.

   Exemple : *M1 : sujet X : onglet nº 3, description du sujet X, page 6, paragraphe 4.*

4. Des expressions comme « au cours des cinq (5) dernières années » utilisées dans la présente demande de soumissions signifient « au cours des cinq (5) années précédant la date de clôture de la demande de propositions ». Si la date de clôture de la demande de propositions est changée après la publication initiale de celle-ci, la durée de l'expérience sera mesurée à partir de la date de clôture finale, à moins d'indication contraire dans une modification à la demande de propositions.

5. Pour démontrer son expérience, le soumissionnaire doit fournir les renseignements suivants sur la façon dont l'expérience mentionnée a été acquise :

   i. les dates de début et de fin (AAAA-MM) de chaque sujet;

   ii. les documents de référence décrivant en détail les sujets offerts.

1. CRITÈRES D'ÉVALUATION OBLIGATOIRES

Dans leur proposition, les soumissionnaires doivent montrer par écrit qu'ils satisfont aux critères obligatoires ci-dessous. Toute soumission qui ne satisfait pas aux critères obligatoires sera jugée non recevable et sera rejetée d'emblée. Les liens vers les pages Web ne sont pas acceptés et recevront la mention « NON SATISFAIT ».

	CRITÈRE	**JUSTIFICATION** **Indiquer les pages pertinentes de la proposition** **[Rempli par le soumissionnaire]**	**ÉVALUATION DES RISQUES** **SATISFAIT/ NON SATISFAIT** **[Rempli par l'évaluateur de la GRC]**
O1	Le soumissionnaire doit démontrer, en fournissant des copies des programmes de cours et des documents sur les sujets précédents, qu'il a offert au moins dix (10) sujets propres à l'aviation, accessibles en ligne et à rythme libre, pendant au moins trois (3) ans au cours des cinq (5) dernières années. Pour être considéré comme étant conforme, le soumissionnaire doit respecter les exigences suivantes : 1. les dates de début et de fin (MM-AAAA) de chaque sujet doivent s'échelonner sur une période d'au moins trois (3) ans; 2. chacun des dix (10) sujets présentés comme preuve doit être différent; 3. les sujets doivent figurer dans les sujets énumérés dans l'énoncé des travaux.		

2. CRITÈRES D'ÉVALUATION COTÉS PAR POINTS

Les soumissions qui répondent à tous les critères techniques obligatoires seront évaluées et cotées selon les critères qui figurent dans les tableaux ci-dessous.

	CRITÈRES D'ÉVALUATION COTÉS PAR POINTS	Limite maximale	Structure de répartition des points	JUSTIFICATION Indiquer les pages pertinentes de la proposition [Rempli par le soumissionnaire]	ÉVALUATION DES RISQUES [Rempli par l'évaluateur de la GRC]
C1	Le soumissionnaire doit démontrer, en fournissant des copies des programmes de cours, des documents de cours et des examens précédents, qu'il peut offrir la formation en français.	**10**	10 points pour les documents présentés en français		
C2	Le soumissionnaire doit démontrer, en fournissant suffisamment de documents, qu'il peut offrir un soutien technique en français. Pour satisfaire à ce critère coté, la documentation doit au moins fournir des détails sur les types de soutien technique en français disponibles (p. ex. téléphone, courriel, clavardage en ligne), la façon de communiquer avec le soutien technique en français et les heures de disponibilité. La disponibilité devrait être de 9 h à 17 h, heure de l'Est, du lundi au vendredi.	**10**	2 points pour le soutien par téléphone 2 points pour le soutien par courriel 2 points pour le soutien par clavardage en ligne 2 points pour d'autres options de soutien 2 points pour les heures de disponibilité de 9 h à 17 h, heure de l'Est, du lundi au vendredi		
	TOTAL	20			