Gendarmerie royale du Canada | Royal Canadian Mounted Police

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À :

Bid Receiving/Réception des soumissions

Réception des soumissions
Gendarmerie royale du Canada
Service des acquisitions et des marchés

Email/Courriel:

NWR_Procurement_Bids@rcmp-grc.gc.ca

REQUEST FOR PROPOSAL

DEMANDE DE PROPOSITION

Proposal to: Royal Canadian Mounted Police

We hereby offer to sell to His Majesty the King 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 aux : Gendarmerie royale du Canada

Nous offrons par la présente de vendre à Son Majesté le Roi du chef du Canada, aux conditions énoncées ou incluses par renvoi dans la présente et aux annexes 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 Solution de logiciel-service de planification des ressources pour les programmes de formation de l'École de la GRC (Division Dépôt)		**Date** 10 mai 2024
Solicitation No. – N° de l'invitation M5000-20-5233/A		
Client Reference No. – N° de référence du client : 202005233		
Solicitation Closes – L'invitation prend fin		
At /à :	2 :00 pm / 1400 heure	CST (Central Standard Time) HNC (Heure Normale du Centre)
On / le :	12 juin, 2024	

Delivery – Livraison See herein — Voir aux présentes	**GST – TPS** 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** Qyitayo Ziwa: Qyitayo.ziwa@rcmp-grc.gc.ca		
Telephone No. – N° de téléphone 639-625-4151	**Facsimile No. – N° de télécopieur**	

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. – N° de téléphone	**Facsimile No. – N° 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**

TABLE DES MATIÈRES

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

Liste des annexes

Liste des pièces jointes

Pièce jointe 2	Formulaire d'attestation de l'éditeur de la solution
Pièce jointe 3	Formulaire d'autorisation de l'éditeur de la solution
Pièce jointe 4	Formulaire d'autorisation du fournisseur de services infonuagiques du gouvernement du Canada

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

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 les instructions pour 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 relatives à la sécurité, exigences financières et autres exigences : comprend des exigences particulières auxquelles les soumissionnaires doivent répondre ; et

Partie 7 Clauses du contrat subséquent de l'éditeur de logiciel-service : contient les clauses et les conditions qui s'appliqueront au contrat subséquent de l'éditeur de logiciel-service

Les annexes comprennent notamment l'énoncé des travaux, la base de paiement, la Liste de vérification des exigences relatives à la sécurité (LVERS) et l'attestation d'absence de collusion dans l'établissement de la soumission.

1.2 Sommaire

1.2.1 L'École de la Gendarmerie royale du Canada (GRC) à la Division Dépôt a besoin d'une solution de logiciel-service de planification des ressources pour gérer ses programmes. Le système doit autoriser la GRC à gérer efficacement sa réserve de ressources : cadets, candidats, animateurs, installations et matériel.

La solution de logiciel-service de planification des ressources disponible sur le marché doit être offerte à quelque trente (30) utilisateurs. Elle doit notamment compter :

- un accès à la solution de logiciel-service de planification des ressources;
- des services de maintenance, de soutien et de documentation du logiciel;
- la formation des utilisateurs;
- la réalisation des travaux nécessaires pour accompagner les utilisateurs autorisés pendant le processus d'évaluation et d'autorisation de la sécurité (EAS).

La DDP vise l'attribution d'un contrat d'un an, plus quatre options irrévocables d'un an chacune, qui autorise le Canada à prolonger la durée du contrat. L'ensemble de la solution de logiciel-service de planification des ressources doit être à la disposition des utilisateurs clients 24 heures par jour, sept jours par semaine, 365 jours par année, en anglais, et doit fonctionner en permanence conformément à l'énoncé des travaux de l'environnement opérationnel du client décrit dans la DDP. Le terme « utilisateur » désigne les employés de la GRC.

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 de plus amples renseignements

sur les enquêtes de sécurité sur le personnel et les organismes, 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 Compte rendu

Les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Les soumissionnaires devraient 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. Mécanismes de recours

Si vous avez des préoccupations relativement au processus d'approvisionnement, veuillez-vous référer à la page Mécanismes de recours sur le site Achatsetventes.gc.ca. Veuillez noter qu'il y a des échéances strictes pour le dépôt des plaintes 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 est lancée par la Gendarmerie royale du Canada (GRC), il faut interpréter toute mention de Travaux publics et Services gouvernementaux Canada (TPSGC) ou de son 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 (2023-06-08) 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 : 250 jours

2.2 Présentation des soumissions

Les soumissions doivent être présentées uniquement au Module 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 obtenu l'approbation requise pour recevoir des soumissions par l'intermédiaire du Service Connexion de la Société canadienne des postes (SCP).

Les soumissions transmises par télécopieur à l'intention de la GRC 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 dix (10) 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 devraient citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. 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 » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un 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 transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet 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 Saskatchewan, 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 du dépôt direct

Les renseignements suivants 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. Communiquez 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, écrivez 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 contenus dans la DDP, sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la DDP. 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 pour autant qu'elles parviennent à l'autorité contractante au plus tard dix (10) jours avant la date de clôture des 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 (nombre de documents, d'utilisateurs et de super-utilisateurs) ont été fournies aux soumissionnaires afin de 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 cette demande de soumissions correspondra à ces données. Elles sont fournies à titre d'information seulement.

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 (une copie électronique en format PDF)

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

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

Section IV : Renseignements supplémentaires (une copie électronique en format PDF)

Section V : Exigences relatives à l'intégrité de la chaîne d'approvisionnement (une copie électronique en format PDF)

Remarque importante

Pour les soumissions transmises 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 présentation des soumissions);

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

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

e. la mauvaise identification de la soumission par le soumissionnaire;

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 (2023-06-08), 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 d'appel d'offres 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 bloquée par le système de courriel de la GRC sera considérée comme n'ayant pas été reçue. Le soumissionnaire doit veiller à la réception de sa soumission.

Les prix doivent figurer dans la soumission financière seulement. Aucun prix ne doit être indiqué dans une autre section de 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 DDP.

En avril 2006, le Canada a adopté une politique exigeant que les ministères et les 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.canada.ca/pol/doc-fra.aspx?id=32573). Pour aider le Canada à atteindre ses objectifs, les soumissionnaires doivent :

1. inclure toutes les certifications environnementales pertinentes pour leur organisation (p. ex. ISO 14001, Leadership in Energy and Environmental Design, Carbon Disclosure Project, p. ex.);

2. inclure toutes les certifications environnementales ou déclarations environnementales de produits propres à leur produit ou service (Forest Stewardship Council, ENERGY STAR, p. ex.);

3. sauf indication contraire, les soumissionnaires sont encouragés à présenter 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 x 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 : impression noir et blanc plutôt qu'en couleur, recto verso/à double face, broché ou agrafé, sans reliure Cerlox, reliure à attaches ou reliure à anneaux.

3.2 Section I : Soumission technique

3.2.1 Dans leur soumission technique, les soumissionnaires doivent démontrer qu'ils comprennent les exigences contenues dans la DDP et expliquer comment ils répondront à ces exigences de manière complète, concise et claire.

La soumission technique doit traiter clairement et de manière suffisamment approfondie des exigences 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 DDP. Afin de faciliter l'évaluation de la soumission, la GRC 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.

3.2.2La soumission technique consiste à présenter les éléments suivants.

a) **Accords sur les niveaux de service :** L'éditeur de logiciel-service doit présenter son accord sur les niveaux de service (ANS) publié, dans l'annexe F, Accords sur les niveaux de service.

En présentant une soumission, l'éditeur de logiciel-service reconnaît et convient que toutes les modalités contenues à l'annexe F, Accords sur les niveaux de service qui visent à interpréter le contrat, qui portent sur le même sujet ou un sujet semblable, ou qui sont liées aux modalités contenues dans les clauses du contrat, sont réputées être annulées et inopérantes. Les engagements relatifs au niveau de service (décrits dans les ANS) doivent inclure un soutien aux clients commerciaux qui prévoit, au minimum, un soutien publié et disponible sur le marché (garantie, maintenance et services de soutien) habituellement fourni aux clients qui fournissent une solution de logiciel-service.

Seules les modalités de l'ANS relatives aux niveaux de service et à la prestation de services s'appliqueront. Toute modalité de l'ANS non liée aux niveaux de service et à la prestation des services, telles qu'elles sont décrites ci-dessous, sera réputée annulée et ne s'appliquera pas.

b) **Droits d'utilisation du logiciel-service :** L'éditeur de logiciel-service peut soumettre d'autres modalités relatives aux droits d'utilisation du logiciel qui ne sont pas abordées. Ces modalités doivent être incluses à l'annexe G, Droits d'utilisation du logiciel-service. Toute modalité contenue à l'annexe G, Droits d'utilisation du logiciel-service, qui comprend des renseignements sur les prix, comme les modalités qui tentent d'imposer des conditions financières, des clauses de prix ou des pénalités de conformité, sera jugée comme étant supprimée, nulle et sans effet. Les conditions d'utilisation supplémentaires proposées doivent se limiter aux clauses habituelles généralement fournies aux clients commerciaux qui vendent la solution de logiciel-service. Si le Canada détermine qu'une modalité des droits d'utilisation du logiciel-service (DULS) proposée est inacceptable, il doit donner à l'éditeur de logiciel-service la possibilité de retirer cette disposition de sa soumission, ou la possibilité de proposer une formulation de remplacement, que le Canada examinera. L'acceptation de toute autre modalité proposée pour les DULS et l'ajout de cette modalité dans un contrat subséquent sont à l'entière discrétion du Canada. Les modalités comprises dans les DULS peuvent notamment comprendre :

(A) la définition des utilisateurs autorisés;
(B) les droits d'accès et d'utilisation;
(C) les restrictions d'accès et d'utilisation;
(D) l'utilisation des droits de vérification;

(E) les déclarations de garantie;
(F) l'indemnisation dans le cas d'une mauvaise utilisation par le client;
(G) les obligations et les responsabilités du client.

3.3 Section II : Soumission financière

3.3.1 Les soumissionnaires doivent présenter leur soumission financière conformément à la fiche de présentation de la soumission financière insérée à l'annexe B, Base de paiement.

3.3.2 Évaluation du prix – Soumissionnaires établis au Canada et à l'étranger

A0222T (2014-06-26), Évaluation du prix - soumissionnaires établis au Canada et à l'étranger

3.4 Section III : Attestations

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

3.5 Section IV : Renseignements supplémentaires

3.5.3 Sites ou locaux proposés par le soumissionnaire exigeant des mesures de protection

3.5.3.1 Comme indiqué dans la partie 6, à la rubrique sur les exigences relatives à la sécurité, le soumissionnaire doit fournir les adresses complètes de ses sites ou de ses locaux, ou de ceux des personnes proposées, pour lesquels des mesures de protection sont requises aux fins d'exécution des travaux :

Numéro civique/nom de la rue, numéro d'unité/de bureau/d'appartement
Ville, province, territoire ou état
Code postal
Pays

3.5.3.2 L'agent de sécurité d'entreprise doit veiller, par l'intermédiaire de la Sous-direction de la sécurité ministérielle de la GRC ou de ses sections régionales de la sécurité ministérielle que le soumissionnaire et les personnes proposées sont titulaires d'une cote de sécurité en vigueur et au niveau exigé, comme décrit à la partie 6, Exigences relatives à la sécurité, exigences financières et autres exigences.

3.6 Section V : Exigences relatives à l'intégrité de la chaîne d'approvisionnement

Les soumissionnaires doivent soumettre l'information sur la sécurité de la chaîne d'approvisionnement (ISCA) décrite en détail dans l'annexe E, Formulaire de présentation de l'information sur la sécurité de la chaîne d'approvisionnement, et la tenir à jour à la demande du responsable de la sécurité de la chaîne d'approvisionnement. Les fournisseurs doivent répondre aux exigences relatives à l'intégrité de la chaîne d'approvisionnement décrites aux critères S10 et S11 de l'annexe L, Critères d'évaluation des exigences relatives à la sécurité.

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Généralités

Les soumissions seront évaluées par rapport à l'ensemble des exigences de la DDP, y compris les critères d'évaluation technique et financière. Le processus d'évaluation comporte plusieurs étapes, lesquelles sont décrites ci-dessous. Même si l'évaluation et la sélection seront effectuées par étape, le fait que le Canada soit passé à une étape ultérieure ne signifie pas que ce dernier a irréfutablement déterminé que le

soumissionnaire a réussi toutes les étapes précédentes. Le Canada se réserve le droit d'exécuter parallèlement certaines étapes de l'évaluation.

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

A Étape I : Soumission technique

a. L'examen du Canada à l'étape I se limitera à une évaluation de la soumission technique afin de vérifier si le soumissionnaire a respecté tous les critères obligatoires admissibles. Cet examen n'évalue pas si la soumission technique répond à une norme ou à toutes les exigences de la soumission. Les exigences obligatoires d'admissibilité sont les critères techniques obligatoires décrits dans la présente DDP comme faisant partie de l'évaluation. Les critères techniques obligatoires qui ne sont pas identifiés dans la DDP comme faisant partie de l'évaluation ne seront pas évalués avant l'étape II.

b. Un soumissionnaire dont la soumission a été jugée recevable au regard des exigences examinées à l'étape I recevra un avis ou un rapport d'évaluation de la conformité (REC) qui précisera que sa soumission a été jugée recevable au regard des exigences examinées à cette étape. Un tel soumissionnaire ne doit pas être autorisé à présenter une réponse au REC.

c. Seules les soumissions jugées recevables conformément aux exigences examinées à l'étape I à la satisfaction du Canada seront examinées à l'étape II.

B Étape II : Contrôle de validation de la soumission

À l'étape II, la GRC réalisera un contrôle de validation de la soumission (CVS) pour vérifier les exigences obligatoires et évaluer les exigences cotées.
Le CVS sera donné en ligne et la GRC le visionnera à distance (par Microsoft Teams).

a. Le soumissionnaire doit donner accès à la solution afin de mettre à l'essai les fonctionnalités décrites dans les exigences obligatoires.

b. Le soumissionnaire doit pouvoir réaliser le CVS dans les 14 jours civils suivant la demande de la GRC.

C Étape III : Évaluation finale de la soumission

a. À l'étape III, le Canada évaluera toutes les soumissions jugées conformes aux exigences examinées à l'étape II. Les soumissions seront évaluées par rapport à l'ensemble des exigences de la DDP, dont les critères d'évaluation techniques et financiers.

b. Une soumission est irrecevable et sera rejetée d'emblée si elle ne satisfait pas à tous les critères d'évaluation obligatoires de la DDP.

4.2 Procédures d'évaluation

a. Les soumissions seront évaluées par rapport à l'ensemble des exigences de la DDP, y compris les critères d'évaluation technique et financière. Le processus d'évaluation comporte plusieurs étapes, lesquelles sont décrites ci-dessous. Même si l'évaluation et la sélection seront effectuées par étape, le fait que le Canada soit passé à une étape ultérieure ne signifie pas que ce dernier a irréfutablement déterminé que le soumissionnaire a réussi toutes les étapes précédentes. Le Canada se réserve le droit d'exécuter parallèlement certaines étapes de l'évaluation.

b. Une équipe d'évaluation formée de représentants de la GRC évaluera les soumissions.

c. En plus de tout autre délai établi dans la DDP :

i. **Demandes de précisions :** Si le Canada demande des précisions au soumissionnaire au sujet de sa soumission ou qu'il veut vérifier celle-ci, le soumissionnaire disposera d'un délai de cinq jours

ouvrables (ou d'un délai plus long précisé par écrit par l'autorité contractante) pour fournir les renseignements nécessaires au Canada. Si le soumissionnaire ne respecte pas ce délai, sa soumission sera déclarée non recevable.

ii. **Demandes de renseignements supplémentaires :** Si le Canada demande d'autres renseignements pour l'une des raisons qui suivent (selon la section intitulée « Déroulement de l'évaluation » du document 2003ACB, Instructions uniformisées d'AchatsCanada – biens ou services – besoins concurrentiels) :

- vérifier tout renseignement fourni par le soumissionnaire dans sa soumission;
- le soumissionnaire doit soumettre les renseignements demandés par le Canada dans les cinq jours ouvrables suivant la demande de l'autorité contractante.

iii. **Prolongation du délai :** Si le soumissionnaire a besoin de plus de temps, l'autorité contractante, à sa seule discrétion, peut accorder une prolongation du délai.

4.3 Soumission technique

a. Étape I : La note technique cotée sera calculée en additionnant les points de l'évaluation technique cotée. Toute soumission qui n'obtient pas un minimum de huit (8) points pour cette évaluation sera non recevable. Les soumissionnaires doivent répondre à chacun des critères d'évaluation dans leur soumission technique de manière claire et exhaustive. Pour prouver leur conformité, ils peuvent soumettre des captures d'écran, des renvois à des documents techniques (en indiquant les numéros de pages), des attestations ou encore des descriptions détaillées. Le simple fait de retranscrire les exigences indiquées dans la DDP n'est pas suffisant. Afin de faciliter le processus d'évaluation, les soumissionnaires doivent classer leurs réponses selon l'ordre des critères d'évaluation et utiliser la même numérotation. Pour éviter les répétitions, 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.

b. Étape II : La GRC réalisera un CVS pour vérifier la conformité des critères d'évaluation obligatoires indiqués à l'annexe J. Ce contrôle sera réalisé en ligne; la GRC le surveillera à distance à partir d'une plateforme comme Microsoft Teams. C'est l'occasion pour les soumissionnaires de montrer que leur solution de logiciel-service de planification des ressources est prête et respecte les exigences fonctionnelles techniques de l'énoncé des travaux.

4.4 Prise en compte des droits d'utilisation du logiciel (DULS) supplémentaires compris dans la soumission classée au premier rang (à la suite de l'évaluation financière)

(i) L'acceptation de l'ensemble des modalités figurant à la partie 7, Clauses du contrat subséquent (y compris les clauses relatives à la licence d'utilisation du logiciel et les clauses incorporées par renvoi) constitue une exigence obligatoire de la présente DDP.

(ii) Toutefois, les soumissionnaires peuvent, dans leur soumission, présenter des modalités supplémentaires d'utilisation du logiciel, comme il est décrit au sous-alinéa 3.2.2(b). L'inclusion ou non de ces modalités d'utilisation du logiciel dans tout contrat subséquent (en tant qu'annexe H, conformément à l'article intitulé « Ordre de priorité des documents » dans les clauses du contrat subséquent) sera déterminée à l'aide du processus décrit ci-après. Quant à savoir si les modalités supplémentaires d'utilisation du logiciel proposées sont acceptables pour le Canada, la décision est entièrement à la discrétion de ce dernier.

(iii) Voici le processus à suivre.

(A) Les soumissions peuvent comprendre des modalités supplémentaires d'utilisation du logiciel, qui sont proposées pour compléter les modalités des clauses du contrat subséquent. Les soumissionnaires ne doivent pas présenter les modalités standards de licence intégrales de l'éditeur de logiciel (car elles contiennent généralement des dispositions qui ne traitent pas uniquement de l'utilisation du logiciel; par exemple, elles traitent souvent de questions comme la limitation de la responsabilité ou la limite de garantie qui ne constituent pas des modalités d'utilisation du logiciel).

(B) Dans les cas où un soumissionnaire a présenté les modalités standards de licence intégrales de l'éditeur de logiciel, le Canada exigera que le soumissionnaire retire ces

modalités et qu'il présente seulement les modalités d'utilisation du logiciel qu'il souhaite que le Canada prenne en considération.

(C) Le Canada examinera les modalités d'utilisation du logiciel proposées par le soumissionnaire en tête (identifié après l'évaluation financière) afin de déterminer si certaines de ses dispositions proposées sont inacceptables pour le Canada.

(D) Si le Canada détermine qu'une modalité d'utilisation du logiciel proposée est inacceptable pour le pays, ce dernier avisera le soumissionnaire, par écrit, et lui fournira l'occasion de retirer cette disposition de sa soumission ou de proposer une formulation de remplacement pour examen par le Canada. Le Canada peut accorder un délai de réponse au soumissionnaire. Si le soumissionnaire présente une nouvelle formulation que le Canada juge inacceptable, le Canada n'est pas obligé de lui donner l'occasion de proposer une autre formulation.

(E) Si le soumissionnaire refuse de retirer de sa soumission les dispositions jugées inacceptables par le Canada dans le délai prescrit par celui-ci dans son avis, la soumission sera jugée irrecevable et rejetée; le Canada peut alors passer à la soumission classée au rang suivant.

(F) Si le soumissionnaire accepte de retirer les dispositions jugées inacceptables par le Canada et qu'il se voit attribuer un contrat subséquent, les modalités supplémentaires d'utilisation du logiciel (telles que modifiées) seront incorporées en tant qu'annexe H au contrat, conformément à l'article intitulé « Ordre de priorité des documents » des clauses du contrat subséquent.

(iv) Afin que seuls des logiciels supplémentaires qui utilisent des modalités approuvées par les deux parties soient incorporés dans le contrat subséquent, sauf si les logiciels supplémentaires utilisent des modalités proposées par le soumissionnaire qui sont incluses dans une annexe au contrat paraphée par les deux parties, elles ne seront pas considérées comme faisant partie du contrat subséquent (même si elles font partie de la soumission qui est incorporée en référence dans le contrat subséquent). L'inclusion de certaines modalités supplémentaires dans la soumission n'entraîne pas l'application de ses modalités au contrat subséquent, peu importe si le Canada s'oppose ou non à ces modalités conformément à la procédure ci-dessus.

4.5 Évaluation financière

4.5.1 Critères financiers obligatoires

Clause du Guide CCUA A0222T (2014-06-26), Évaluation du prix – soumissionnaires établis au Canada et à l'étranger.

4.6 Évaluation de la sécurité

Avant l'attribution du contrat, les exigences de sécurité ci-après doivent être respectées.

a. Critères de sécurité obligatoires

i. Chaque soumission sera examinée pour vérifier sa conformité avec les exigences de sécurité obligatoires de la DDP. Tout élément de la DDP désigné par les termes « doit », « doivent » ou « obligatoire » constitue une exigence de sécurité obligatoire. Les soumissions qui ne respectent pas toutes les exigences obligatoires décrites dans l'annexe L – Critères d'évaluation des exigences relatives à la sécurité seront déclarées non recevables et seront rejetées.

b. Les cotes de sécurité de l'organisation et du personnel, comme décrit à l'article 7.3, doivent être obtenus avant l'attribution du contrat.

c. L'évaluation de l'intégrité de la chaîne d'approvisionnement sera réalisée avant l'attribution du contrat (conformément aux articles 4.6 et 6.2).

4.7 Processus d'intégrité de la chaîne d'approvisionnement

(a) Le soumissionnaire doit réussir l'évaluation de l'intégrité de la chaîne d'approvisionnement de l'autorité de sécurité avant d'obtenir un contrat. Le Canada évaluera si, à son avis, la chaîne d'approvisionnement du soumissionnaire donne lieu à la possibilité que sa solution proposée compromette ou serve à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements appartenant au Canada, conformément à l'appendice A de l'annexe A, Définitions liées aux obligations en matière de sécurité et de confidentialité.

(b) Au cours du processus de DDP, de la période du contrat et de toute période d'option subséquente, l'autorité responsable de la sécurité de la chaîne d'approvisionnement désignée par le Canada peut évaluer l'ISCA du soumissionnaire, fournie en tant qu'annexe E, Formulaire de présentation de l'information sur la sécurité de la chaîne d'approvisionnement, en fonction de son mandat de sécurité nationale visant à protéger l'infrastructure de technologies de l'information (TI) du Canada, et à évaluer les menaces, les risques et les points faibles.

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

Les soumissionnaires doivent noter que l'attribution des contrats est assujettie au processus d'approbation interne du Canada, qui prévoit l'approbation obligatoire du financement selon le montant de tout contrat proposé. Même si un soumissionnaire a été recommandé pour l'attribution d'un contrat, un contrat sera attribué uniquement si l'approbation interne est obtenue conformément aux politiques internes du Canada. Si l'approbation n'est pas obtenue, aucun contrat ne sera attribué.

1. Pour être jugée recevable, une soumission doit :
   a. respecter toutes les exigences de la DDP;
   b. respecter tous les critères d'évaluation technique obligatoires;
   c. obtenir le nombre minimal de huit (8) points requis pour les critères d'évaluation cotés de l'annexe K, Critères d'évaluation cotés. L'échelle de notation compte 28 points.

2. Les soumissions ne répondant pas aux exigences du point (a), (b) ou (c) seront déclarées non recevables.

3. La sélection sera faite en fonction de la note combinée la plus élevée sur le plan du mérite technique et du prix. Une proportion de 70 % sera accordée au mérite technique et une proportion de 30 % sera accordée au 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 sera divisé par le nombre total de points pouvant être accordés, puis multiplié par 70 %.

5. Pour déterminer la note du prix, chaque soumission recevable sera évaluée proportionnellement au prix évalué le plus bas et au rapport de 30 %.

6. Pour chaque soumission recevable, la note combinée correspondra à la somme des notes du mérite technique et du prix.

7. La soumission retenue ne sera pas nécessairement celle ayant obtenu la note technique la plus élevée ni celle ayant le prix évalué le plus bas. La soumission recevable qui obtiendra la note combinée la plus élevée pour le mérite technique et le prix sera recommandée pour l'attribution d'un 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 rapport de 70/30 à l'égard du mérite technique et du prix, respectivement. Le nombre total de points possibles est de 28, et le prix évalué le plus bas s'établit à 145 000 $.

Méthode de sélection – Note combinée la plus élevée pour le mérite technique (70 %) et le prix (30 %)

		Soumissionnaire 1	Soumissionnaire 2	Soumissionnaire 3
Note d'évaluation du contrôle de validation de la soumission		20/28	15/28	10/28
Prix évalué de la soumission		155 000 $	150 000 $	145 000 $
Calculs	**Note d'évaluation du contrôle de validation de la soumission**	20/28 x 70 = 50	15/28 x 70 = 37,50	20/28 x 70 = 25
	Note du prix	145/155 x 30 = 28,06	145/150 x 30 = 29	145/145 x 30 = 30
Note combinée		**78,06**	**66,50**	**55,00**
Classement		1er	2e	3e

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 Canada peuvent faire l'objet d'une vérification à tout moment par ce dernier. Sauf indication contraire, le Canada déclarera qu'une soumission est non recevable ou qu'il y a manquement de la part du soumissionnaire s'il est établi qu'une attestation fournie avec sa soumission comprend de fausses déclarations, faites sciemment ou non, que ce soit pendant la période d'évaluation des soumissions ou pendant la durée du contrat.

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 du contrat et renseignements supplémentaires

Les attestations et les renseignements supplémentaires énumérés ci-après doivent être remplis et fournis avec la soumission, mais ils peuvent être fournis par après. 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. Si le soumissionnaire ne fournit pas les attestations et les renseignements supplémentaires énumérés ci-dessous dans le délai établi, sa soumission sera déclarée non recevable.

5.1.1 Dispositions relatives à l'intégrité

Conformément à la section Renseignements à fournir lors d'une soumission, de la passation d'un contrat ou de la conclusion d'un accord immobilier assujettie à la Politique d'inadmissibilité et de suspension (https://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html), le soumissionnaire doit fournir les documents exigés, selon le cas, afin que sa soumission ne soit pas rejetée du processus d'approvisionnement :

- 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 de plus amples détails (https://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 ni lui ni un membre de la coentreprise, si le soumissionnaire est une coentreprise, ne sont nommés dans la « liste des soumissionnaires à admissibilité limitée du PCF » (Programme de contrats fédéraux) qui figure au bas de la page du site Web d'Emploi et Développement social Canada – Programme de contrats fédéraux (https://www.canada.ca/fr/emploi-developpement-social/ministere/portefeuille/travail/programmes/equite-emploi/contrats-federaux.html).

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

5.1.3 Attestations additionnelles préalables à l'attribution du contrat

5.1.3.1 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) 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. Ce document vise à décourager le truquage des offres en obligeant les soumissionnaires à divulguer à l'autorité contractante tous les faits importants concernant les communications et les arrangements conclus par le soumissionnaire avec des concurrents à l'égard d'un appel d'offres.

5.1.3.2 Attestation ou autorisation de l'éditeur de logiciel-service

Si le soumissionnaire est l'éditeur de logiciel-service des produits logiciels privés proposés, le Canada exige que le soumissionnaire confirme, par écrit, qu'il est l'éditeur de logiciel. Les soumissionnaires doivent utiliser la pièce jointe 2, Formulaire d'attestation de l'éditeur de logiciel, qui accompagne la DDP. Bien qu'il soit nécessaire de fournir tous les renseignements exigés dans le formulaire d'attestation de l'éditeur de logiciel, il n'est pas obligatoire d'utiliser ce formulaire pour les fournir. Dans le cas des soumissionnaires qui utilisent un autre formulaire, il appartient entièrement au Canada, à sa seule discrétion, de déterminer si tous les renseignements exigés ont été fournis. Toute modification apportée aux énoncés du formulaire pourrait rendre la soumission non recevable.

Tout soumissionnaire qui n'est pas l'éditeur de logiciel-service de tous les produits logiciels privés proposés dans sa soumission doit présenter une preuve de l'autorisation de l'éditeur de logiciel-service, qui doit être signée par ce dernier (et non par le soumissionnaire). Aucun contrat ne sera attribué à un soumissionnaire qui n'est pas l'éditeur de logiciel-service de tous les logiciels privés proposés au Canada, sauf si une preuve de cette autorisation a été fournie au Canada. Si les logiciels privés proposés par le soumissionnaire proviennent de plusieurs éditeurs de logiciel-service, chacun d'eux doit fournir une autorisation. On demande aux soumissionnaires d'utiliser la pièce jointe 3, Formulaire d'autorisation de l'éditeur de logiciel joint à la DDP. Bien qu'il soit nécessaire de fournir tous les renseignements demandés dans le formulaire d'autorisation de l'éditeur de logiciel, il n'est pas obligatoire d'utiliser ce formulaire pour les fournir. Dans le cas des soumissionnaires et des éditeurs de logiciel-service qui utilisent un autre formulaire, le Canada déterminera, à sa seule discrétion, si tous les renseignements exigés ont été fournis. Toute modification apportée aux énoncés du formulaire pourrait rendre la soumission non recevable.

Dans le cadre de la présente DDP, « éditeur de logiciels-services » désigne le propriétaire de tout produit logiciel compris dans la soumission qui a le droit d'octroyer une licence (et d'autoriser d'autres personnes à octroyer une licence ou une sous-licence) pour ses produits logiciels.

Les autres documents d'attestation suivants sont exigés dans la soumission (au besoin) :

- Pièce jointe 2, Formulaire d'attestation de l'éditeur de la solution
- Pièce jointe 3, Formulaire d'autorisation de l'éditeur de la solution
- Pièce jointe 4, Formulaire d'autorisation du fournisseur de services infonuagiques du gouvernement du Canada

5.1.3.3 Le soumissionnaire atteste que la solution de logiciel-service est disponible sur le marché (produit commercial)

Tout le matériel et tous les logiciels proposés pour répondre à ce besoin doivent être des produits commerciaux (à moins d'un énoncé contraire dans la présente DDP), ce qui signifie que chaque élément de matériel et de logiciel est offert sur le marché, qu'il n'exige ni recherche ni développement supplémentaire et qu'il fait partie intégrante d'une gamme de produits existante dont le fonctionnement est éprouvé (c.-à-d. qu'ils n'ont pas simplement fait l'objet d'essais en laboratoire ou dans un environnement expérimental). Si le matériel ou le logiciel-service proposé est une extension entièrement compatible d'une gamme de produits éprouvés, il doit avoir été annoncé publiquement au plus tard à la date de clôture des soumissions. En déposant sa soumission, le soumissionnaire atteste que l'ensemble du matériel et le logiciel-service proposés sont des produits commerciaux.

5.1.3.4 Exigences relatives à la sécurité

Avant d'entamer tout travail où il aura accès à des renseignements confidentiels ou exclusifs appartenant à des tiers, ou encore à des renseignements générés ou produits dans le cadre des travaux, l'entrepreneur doit obtenir de ses employés et de ses sous-traitants l'entente de non-divulgation et l'entente de divulgation des conflits d'intérêts, incluses à l'annexe D, remplies et signées, et les remettre à l'autorité contractante.

L'entrepreneur doit remettre l'annexe D remplie et signée avant d'avoir accès aux renseignements liés aux travaux fournis par ou pour le Canada.

5.1.3.5 Ancien fonctionnaire

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-après avant l'attribution du contrat. Si les réponses aux questions et, s'il y a lieu, les renseignements requis n'ont pas été fournis à la date de fin de l'évaluation des soumissions, 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., 1985, ch. F-11, ou un ancien membre des Forces armées canadiennes ou de la GRC. Un ancien fonctionnaire peut être :

a. une personne;

b. une personne qui s'est incorporée;

c. une société de personnes 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'indemnité de cessation d'emploi, qui se mesure de façon similaire.

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

Ancien fonctionnaire touchant une pension

Selon les définitions précédentes, le soumissionnaire est-il un ancien fonctionnaire touchant une pension? **Oui** *( )* **Non** *( )*

Si oui, le soumissionnaire doit fournir les renseignements ci-après pour tous les anciens fonctionnaires touchant une pension, le cas échéant :

a. Nom de l'ancien fonctionnaire

b. Date de cessation d'emploi ou de départ à la retraite de la fonction publique

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

Directive sur le réaménagement des effectifs

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

Si oui, le soumissionnaire doit fournir les renseignements suivants :

a. Nom de l'ancien fonctionnaire

b. Conditions de l'incitatif versé sous forme de paiement forfaitaire

c. Date de la cessation d'emploi

d. Montant du paiement forfaitaire

e. Taux de rémunération qui a servi au calcul du paiement forfaitaire

f. Période correspondant au paiement forfaitaire, incluant la date du début, la date d'achèvement et le nombre de semaines

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

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

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

_____
(Nom du destinataire de la soumission)

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

en réponse à l'appel d'offres (ci-après « l'appel d'offres ») lancé par :

_____
(Nom de l'autorité contractante)

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

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

1. j'ai lu la présente attestation et j'en comprends le contenu;

2. je comprends que la soumission ci-jointe sera déclarée irrecevable si les déclarations contenues dans la présente attestation ne sont pas véridiques 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 la signature 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 toute personne, autre que le soumissionnaire, affilié ou non au soumissionnaire qui :
   (a) a été invité par l'appel d'offres à présenter une soumission;
   (b) pourrait présenter une soumission en réponse à l'appel d'offres compte tenu de ses compétences, 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 collusion et sans avoir communiqué ou établi d'entente ou d'arrangement avec un concurrent;

   (b) qu'il a établi la présente soumission sans avoir communiqué ou établi une entente ou un arrangement avec un ou plusieurs concurrents 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 communications, ententes ou arrangements;

7. sans limiter la généralité de ce qui précède aux alinéas 6(a) ou 6(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 répond 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 produits ou des services visés par le présent appel d'offres, sauf ceux qui ont été spécifiquement autorisés par l'autorité contractante 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 du poste) (Date)

PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES

6.1 Exigences relatives à la sécurité et autres exigences

(a) Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées.

(i) Chaque soumissionnaire faisant partie d'un partenariat de soumissionnaires doit détenir une attestation de sécurité de l'organisation et du personnel comme indiqué à la partie 7A ou 7B, Clauses du contrat subséquent.
(ii) Chaque lieu proposé par le soumissionnaire pour la réalisation des travaux et la sauvegarde des documents doit satisfaire aux exigences relatives à la sécurité comme indiqué à la partie 7A ou 7B, Clauses du contrat subséquent.
(iii) Chaque soumissionnaire doit fournir l'adresse des lieux proposés pour la réalisation des travaux et la sauvegarde des documents, comme indiqué à la partie 3, section IV, Renseignements supplémentaires.

(b) Conformément aux exigences du Programme de sécurité des contrats de SPAC (https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

(i) Les soumissionnaires canadiens doivent fournir avec leur soumission un formulaire de demande d'inscription (DI) du Programme de sécurité des contrats rempli. Le formulaire se trouve dans la pièce jointe 6.1.
(ii) Les soumissionnaires étrangers doivent fournir avec leur soumission un formulaire de filtrage initial de sécurité internationale rempli. Le formulaire se trouve dans la pièce jointe 6.2.

Chaque soumissionnaire doit obtenir rapidement la cote de sécurité requise et, le cas échéant, les capacités en matière de sécurité. Comme il est indiqué ci-dessus, les soumissionnaires qui ne fournissent pas toutes les informations requises à la clôture des soumissions auront la possibilité de remplir les informations manquantes du formulaire de DI dans un délai fixé par l'autorité contractante. Si ces renseignements ne sont pas fournis dans le délai établi par l'autorité contractante (y compris toute prolongation accordée par celle-ci, à sa discrétion), ou si le Canada a besoin d'autres renseignements de la part du soumissionnaire en lien avec l'évaluation de la demande d'autorisation de sécurité (c'est-à-dire des renseignements qui ne sont pas exigés par le formulaire de DI), le soumissionnaire sera tenu de soumettre ces renseignements dans le délai prescrit par l'autorité contractante, qui sera de 48 heures au minimum. Si, à quelque moment que ce soit, le soumissionnaire ne fournit pas les renseignements requis dans les délais fixés par l'autorité contractante, sa soumission sera déclarée non conforme. Si le soumissionnaire est une coentreprise, chacun des membres de celle-ci doit respecter les exigences relatives à la sécurité.

Le soumissionnaire retenu réalisera les travaux nécessaires pour accompagner les utilisateurs autorisés pendant le processus d'EAS de la Sécurité ministérielle et de la Section de la sécurité ministérielle de la GRC.

6.2 Exigences relatives à l'intégrité de la chaîne d'approvisionnement

Avant l'attribution d'un contrat, l'éditeur de logiciel-service doit avoir reçu la confirmation du Canada que l'évaluation de l'intégrité de la chaîne d'approvisionnement a été réalisée et que le fournisseur a été approuvé par ce dernier. Le processus d'évaluation de l'intégrité de la chaîne d'approvisionnement est défini à la section 4.6, Processus d'intégrité de la chaîne d'approvisionnement.

Si l'entrepreneur apporte des modifications importantes à sa chaîne d'approvisionnement, il doit en informer le Canada, car une nouvelle évaluation peut alors s'avérer nécessaire.

6.3 Exigence relative à l'attestation de sécurité des technologies de l'information

Avant l'attribution du contrat, l'éditeur de logiciel-service doit remplir l'une des deux conditions suivantes :

(a) détenir un accord-cadre infonuagique du gouvernement du Canada accordé aux fournisseurs de services infonuagiques (https://cloud-services-infonuagiques.canada.ca/s/gc-cloud-fa?language=fr) ou un arrangement en matière d'approvisionnement en logiciel-service infonuagique du gouvernement du Canada (https://cloud-services-infonuagiques.canada.ca/s/pspc-rfsa?language=fr) pour le stockage ou le traitement des renseignements « Protégé A » et « Protégé B » de tous les produits qui font partie du service;

(b) attester que la solution de logiciel-service de planification des ressources sera déployée par un fournisseur de services infonuagiques qui détient un accord-cadre infonuagique du gouvernement du Canada (https://cloud-services-infonuagiques.canada.ca/s/gc-cloud-fa?language=fr). L'attestation se trouve à la pièce jointe 4, Formulaire d'autorisation du fournisseur de services infonuagiques du gouvernement du Canada.

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

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

Le présent contrat est conclu le [DATE DU CONTRAT] entre [NOM DE L'ENTREPRENEUR] (l'« entrepreneur ») et la GRC (le « Canada »).

7.1 Besoin

7.1.1 Prix

L'entrepreneur accepte de fournir les services et d'exécuter les travaux décrits dans le contrat en conformité avec les prix établis dans l'annexe B, Base de paiement, et en fonction de ces prix.

7.1.2 Services

L'entrepreneur accepte de fournir les services décrits à l'annexe A, Énoncé des travaux, notamment :

- l'installation, le déploiement et la création de comptes utilisateurs;
- la configuration;
- la formation;
- la réalisation des travaux nécessaires pour accompagner les utilisateurs autorisés pendant le processus d'EAS.

7.1.3 Client

Dans le cadre du présent contrat, le client est la GRC.

7.1.4 Définitions des termes

Les termes et les expressions utilisés dans le contrat sont définis dans l'appendice A de l'annexe A.

7.1.5 Période du contrat

La période du contrat représente toute période au cours de laquelle l'entrepreneur est tenu de fournir les services et d'exécuter les travaux.

7.2 Exigences relatives à la sécurité

Les exigences relatives à la sécurité ci-après (LVERS et clauses connexes) s'appliquent et font partie intégrante du contrat.

7.2.1 Exigences relatives à la sécurité pour les soumissionnaires canadiens

a. L'entrepreneur doit détenir en permanence, pendant l'exécution du contrat, une attestation de vérification d'organisation désignée en vigueur ainsi qu'une cote de protection des documents approuvée au niveau « Protégé A », délivrées par la Section de la sécurité ministérielle de la GRC.

b. Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens de niveau « Protégé », ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau fiabilité tel que requis, délivrée ou approuvée par le PSC de SPAC.

c. L'entrepreneur NE DOIT PAS utiliser ses systèmes de TI pour traiter, produire ou stocker électroniquement des renseignements protégés tant qu'il n'en a pas reçu l'approbation écrite par le responsable de la sécurité du ministère client. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau « Protégé A », avec lien électronique au niveau « Protégé A ».

d. L'entrepreneur ou l'offrant doit respecter les dispositions des documents suivants :

   i. LVERS et guide de sécurité (s'il y a lieu), reproduits ci-joint à l'annexe M

   ii. Manuel de la sécurité industrielle (dernière édition)

   iii. Site Web de la DSSIO : Exigences de sécurité des contrats du gouvernement du Canada, à l'adresse https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html

7.2.2 Exigences relatives à la sécurité pour les fournisseurs étrangers

L'autorité de sécurité désignée canadienne (ADS canadienne) pour les questions de sécurité industrielle au Canada est le Secteur de la sécurité industrielle, SPAC, administré par la Direction de la sécurité industrielle internationale, SPAC. L'ADS canadienne est chargée d'évaluer la conformité des entrepreneurs et des sous-traitants aux exigences en matière de sécurité pour les fournisseurs étrangers. Les exigences suivantes en matière de sécurité s'appliquent aux entrepreneurs et aux sous-traitants étrangers destinataires constitués en société ou autorisés à faire des affaires dans un État autre que le Canada et qui livrent ou exécutent à l'extérieur du Canada les services infonuagiques décrits dans les solutions d'infonuagique, en plus des exigences en matière de confidentialité et de sécurité. Ces exigences en matière de sécurité s'ajoutent aux exigences figurant dans la section intitulée Protection et sécurité des données stockées dans des bases de données.

a. **L'entrepreneur ou le sous-traitant** atteste que la livraison et la prestation des services infonuagiques prévus par le présent contrat doivent provenir d'un pays membre de l'Organisation du Traité de l'Atlantique Nord, de l'Union européenne ou d'un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité. Dans le cadre du PSC, des accords internationaux bilatéraux en matière de sécurité ont été

conclus avec les pays énumérés sur le site Web https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html de SPAC, tel qu'il est mis à jour de temps à autre.

b. L'entrepreneur ou le sous-traitant étranger destinataire doit en tout temps, pendant la durée du contrat ou du contrat de sous-traitance, être inscrit auprès de l'autorité nationale de supervision appropriée des pays dans lesquels il est constitué en société, exerce ses activités et est autorisé à faire des affaires. Il doit fournir à l'autorité contractante et à l'ADS canadienne la preuve de son inscription auprès de l'autorité de surveillance compétente.

c. L'entrepreneur ou le sous-traitant étranger destinataire doit détenir en permanence, pendant l'exécution du contrat, une équivalence d'une attestation de vérification d'organisation désignée en vigueur, délivrée par l'ADS canadienne, comme suit :

   i. L'entrepreneur ou le sous-traitant étranger destinataire doit fournir une preuve qu'il est constitué en société ou autorisé à faire affaire sur son territoire de compétence.

   ii. L'entrepreneur ou le sous-traitant étranger destinataire doit désigner un agent de sécurité des contrats autorisé et un agent remplaçant de sécurité des contrats, au besoin, qui sera responsable du contrôle des exigences relatives à la sécurité, telles qu'elles sont définies dans le présent contrat. Cette personne sera nommée par le président-directeur général de l'entrepreneur ou du sous-traitant étranger destinataire qui présente une soumission ou par un cadre supérieur principal désigné, qui est soit propriétaire, dirigeant, agent, administrateur, directeur ou partenaire, et qui occupe un poste qui lui permettrait d'influer de manière négative sur les politiques ou les pratiques de l'organisation dans l'exécution du contrat.

   iii. L'entrepreneur ou le sous-traitant ne doit pas accorder l'accès à des renseignements ou des biens de niveau « Protégé » du Canada, sauf aux membres du personnel qui ont un besoin de savoir pour l'exécution du contrat et qui ont fait l'objet d'une vérification de sécurité conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=28115 ou qui utilisent des mesures équivalentes acceptables convenues par le MDN.

   iv. Les renseignements et les biens de niveau « Protégé » du Canada qui sont fournis à l'entrepreneur ou au sous-traitant étranger destinataire, ou qui sont produits par ce dernier :

      a) ne doivent pas être divulgués à un autre gouvernement, à une autre personne ou à une autre entreprise ou à un représentant de l'un ou de l'autre qui n'est pas directement lié à l'exécution du contrat, sans l'autorisation écrite préalable du Canada. Ce consentement doit être obtenu auprès de l'ADS canadienne en collaboration avec l'autorité contractante;

      b) ne doivent pas servir à un but autre que l'exécution du contrat sans l'approbation écrite préalable du Canada. Cette approbation doit être obtenue auprès de l'autorité contractante (en collaboration avec l'ADS canadienne).

d. L'entrepreneur ou le sous-traitant étranger destinataire NE DOIT PAS emporter de renseignements ou de biens de niveau « Protégé » du Canada hors des lieux de travail visés. Il doit également s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.

e. L'entrepreneur ou le sous-traitant étranger destinataire ne doit pas utiliser les renseignements ni les biens de niveau « Protégé » du Canada dans un but autre que l'exécution du contrat sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS canadienne.

f. L'entrepreneur ou le sous-traitant étranger destinataire doit détenir en permanence, pendant l'exécution du contrat, une autorisation de détenir des renseignements approuvés de niveau « Protégé A » du Canada.

g. L'entrepreneur ou le sous-traitant étranger destinataire doit se conformer aux dispositions de la LVERS figurant à l'annexe M.

h. Le Canada a le droit de rejeter toute demande présentée de manière distincte et indépendante de l'autorisation contenue dans le présent contrat relativement à l'autorisation de l'entrepreneur qui fournit les services infonuagiques d'accéder, de traiter, de produire, de transmettre ou de stocker électroniquement des données de niveau « Protégé » du Canada dans tout autre pays s'il y a lieu de craindre pour la sécurité, la confidentialité ou l'intégrité des renseignements.

7.3 Résiliation

7.3.1 Résiliation pour raisons de commodité

7.3.1.1 Le Canada peut résilier le contrat pour des raisons de commodité après avoir donné un avis écrit à l'entrepreneur ou en utilisant la fonctionnalité de résiliation ou d'annulation offerte sur le portail en ligne de l'entrepreneur, le cas échéant. Si le contrat est résilié en partie seulement, l'entrepreneur doit fournir les services infonuagiques qui ne sont pas touchés par l'avis de résiliation. À sa discrétion, l'entrepreneur peut se retirer du contrat en donnant à l'autorité contractante un avis écrit de cessation d'emploi de 30 jours. Une telle résiliation ne mettra pas fin aux services infonuagiques qui ne sont pas en lien avec l'avis de résiliation.

Si le Canada résilie le contrat pour des raisons de commodité, l'entrepreneur a le droit de se faire payer le solde dû pour tous les services infonuagiques fournis en vertu du contrat (moins tous les crédits applicables qu'il a demandés et qu'il a droit de recevoir).

7.3.1.2 Les sommes auxquelles l'entrepreneur a droit selon le présent article et les sommes versées, qui sont dues ou qui seront dues à l'entrepreneur ne doivent pas dépasser, au total, le prix du contrat.
Sauf dans la mesure prévue au présent article, l'entrepreneur n'aura aucun recours, notamment en ce qui concerne les dommages-intérêts, la compensation, la perte de profit et l'indemnité découlant de tout avis de résiliation donné par le Canada en vertu du présent article. L'entrepreneur convient de rembourser immédiatement au Canada toute partie de tout versement anticipé non liquidé à la date de la résiliation.

7.3.1.3 La résiliation du contrat pour raisons de commodité ne met pas fin aux services infonuagiques individuels pour raisons de commodité. Tous les services infonuagiques sont résiliés séparément pour raisons de commodité. La résiliation du contrat ne doit pas avoir d'effet sur un service infonuagique fourni avant la date de résiliation du contrat ou y mettre fin, à moins que le fait à l'origine de la résiliation du contrat entraîne directement un défaut de conformité des conditions de l'entrepreneur ou du Canada.

7.3.1.4 L'entrepreneur convient de rembourser immédiatement au Canada toute partie de tout versement anticipé non liquidé à la date de la résiliation.

7.3.1.5 Si, en vertu de l'alinéa 7.4.1.1, le Canada met fin à la totalité ou une partie des services, le Canada paiera à l'entrepreneur les coûts raisonnables liés à la cessation des services infonuagiques offerts par l'entrepreneur, à l'exclusion des coûts liés au licenciement des employés, à moins que l'entrepreneur ne démontre que ces coûts découlent d'obligations légales.

7.3.1.6 Les parties conviennent que ces montants représentent une estimation réelle des dommages et intérêts liquidés qui résulteraient pour l'entrepreneur d'une résiliation anticipée du contrat, et non une pénalité.

7.3.2 Résiliation pour inexécution

7.3.2.1 L'autorité contractante peut résilier le contrat avec effet immédiat en transmettant un avis de résiliation à l'entrepreneur, si les situations suivantes surviennent :

7.3.2.1.1 L'entrepreneur ne satisfait pas aux exigences de qualification continue décrites dans le présent contrat;

7.3.2.1.2 L'entrepreneur a enfreint l'une des conditions générales spécifiques détaillées dans le présent contrat;

7.3.2.1.3 L'entrepreneur fait faillite ou devient insolvable.

7.3.3 Avis de manquement

L'autorité contractante peut transmettre à l'entrepreneur un avis écrit de résiliation pour manquement de tout ou partie du contrat. L'avis indiquera la violation, les circonstances pertinentes, le délai proposé, les travaux ou les services touchés (en cas de résiliation partielle), les exigences relatives à un plan d'action, les services de transition ou de migration nécessaires, et la date d'entrée en vigueur de la résiliation. L'avis indiquera également si le Canada conserve d'autres réclamations de dommages-intérêts.

7.3.4 Conformité de l'entrepreneur

L'entrepreneur doit respecter les exigences en matière d'assurance prévues dans l'avis.

7.3.4.1 Violation totale

Si, de l'avis raisonnable du Canada, le manquement de l'entrepreneur constitue une violation totale ou substantielle du contrat, le Canada peut immédiatement résilier le contrat par l'avis. Par souci de clarté, l'avis du Canada peut être fondé sur les situations comme les suivantes :

7.3.4.1.1 l'entrepreneur ne respecte pas une obligation contractuelle substantielle;

7.3.4.1.2 l'entrepreneur semble irréfutablement incapable d'exécuter une obligation contractuelle substantielle, en raison de facteurs indépendants de sa volonté. Par souci de clarté, ceci comprend l'insolvabilité réelle ou apparente, l'incapacité répétée de remettre des produits livrables acceptables dans le cadre de ce contrat ou d'autres contrats similaires avec le Canada;

7.3.4.1.3 des violations non corrigées multiples ou répétées d'une obligation contractuelle intermédiaire par l'entrepreneur;

7.3.4.1.4 un manquement de l'entrepreneur qui a des répercussions négatives sur les activités du gouvernement.

7.4 Autre manquement

7.4.1 Si les manquements de l'entrepreneur ne sont pas des violations totales, le Canada déterminera le délai dans lequel l'entrepreneur doit corriger le manquement et peut exiger un plan d'action. Sauf dans le cas où ce manquement, par sa nature, ne peut être corrigé en 30 jours, la partie mettant fin au contrat doit donner à l'autre partie un préavis de 30 jours annonçant l'intention de résilier le contrat et la possibilité de corriger le manquement.

7.4.2 Si, en réponse à l'avis, l'entrepreneur indique son incapacité ou son refus de remédier au manquement, le Canada peut résilier immédiatement le contrat pour manquement.

7.4.3 Si le contrat précise qu'un manquement particulier ne permettra aucun délai, le Canada peut résilier le contrat pour manquement immédiatement sans fournir la possibilité de corriger le manquement.

7.4.4 Le Canada n'est pas tenu d'aviser l'entrepreneur des manquements. Les parties conviennent que le Canada peut choisir de ne pas utiliser ce processus d'avis officiel ou de prolonger le délai accordé à l'entrepreneur, et que ni l'un ni l'autre ne doit être interprété comme une renonciation du Canada à tout droit ou un acquiescement au manquement de l'entrepreneur.

7.4.5 Le Canada n'est pas tenu d'aviser l'entrepreneur des manquements. Les parties conviennent que le Canada peut choisir de ne pas utiliser ce processus d'avis officiel ou de prolonger le délai accordé à l'entrepreneur, et que ni l'un ni l'autre ne doit être interprété comme une renonciation du Canada à tout droit ou un acquiescement au manquement de l'entrepreneur.

7.4.6 Si le Canada résilie le contrat pour manquement, il ne paiera que les services infonuagiques livrés et acceptés avant la date de résiliation. Le Canada ne paiera aucun montant excédant la valeur des services infonuagiques acceptés. L'entrepreneur convient de rembourser immédiatement au Canada toute partie de tout versement anticipé non liquidé à la date de la résiliation.

7.5 Changement de contrôle

7.5.1 Récupération des données du Canada à la fin du contrat

7.5.1.1 N'importe quand au cours de la période visée par le contrat, le Canada doit pouvoir avoir accès à ses données stockées dans le service infonuagique et les extraire.

7.5.1.2 À la conclusion du contrat, l'entrepreneur doit garder les données du Canada stockées dans les services infonuagiques pendant au moins 90 jours civils et fournir au Canada un compte rendu limité semblable au compte principal du gouvernement qui donne au Canada la capacité d'extraire ses données au cours de la période en cause.

7.5.1.3 Le Canada doit avoir la capacité d'extraire de manière sécurisée ses données et ses métadonnées dans un format lisible et utilisable par machine et acceptable pour le Canada. Lorsque le contrat est résilié pour manquement, en partie ou en totalité, ces données doivent être fournies sans coût additionnel. À la fin de la période de conservation, l'entrepreneur peut, à la demande du Canada, désactiver le compte du Canada.

7.5.1.4 Si l'autorité contractante résilie le contrat pour des raisons de commodité, le Canada sera responsable de payer les honoraires et les frais entraînés jusqu'à la date d'extraction de ses données par le Canada.

7.6 Solution

7.6.1 Logiciel-service

L'entrepreneur fournira la solution à l'aide d'un modèle de prestation de solution de logiciel-service, permettant au Canada d'accéder à la solution hébergée par l'entrepreneur et de l'utiliser.

7.6.2 Services infonuagiques disponibles sur le marché

Le Canada reconnaît que la solution est une solution sur le marché offerte à d'autres clients. Dans le cadre de l'abonnement à la solution, l'entrepreneur s'engage à mettre à la disposition du Canada toutes les caractéristiques et fonctionnalités incluses dans la version commerciale de la solution, ainsi que les services d'infrastructure informatique accessoires et requis, qui sont tous inclus dans le prix de l'abonnement.

7.6.3 Évolution de l'application des services infonuagiques (caractéristiques ou fonctions)

Le Canada reconnaît que la solution, l'application de logiciel-service sous-jacente ou l'infrastructure associée peut évoluer pendant la durée du contrat. L'entrepreneur accepte de continuer de fournir les services à titre de solution disponible sur le marché, avec des fonctions ou des caractéristiques et à des conditions qui ne sont pas moins favorables du point de vue matériel qu'au moment de l'attribution du contrat.

7.6.4 Améliorations et évolution des services infonuagiques

Les parties reconnaissent que les technologies et les modèles opérationnels évoluent rapidement et qu'une solution fournie au début de la durée du contrat sera inévitablement différente d'une solution fournie à la fin de la durée du contrat, et que les méthodes par lesquelles tout périphérique potentiel est livré au Canada changeront ou évolueront probablement. Les parties reconnaissent aussi qu'au moment de conclure ce contrat, elles ne peuvent envisager tous les biens ou services qui peuvent être livrés dans le cadre du contrat, mis à part le fait qu'ils seront reliés à la livraison aux utilisateurs. Dans cette optique, les parties s'entendent sur ce qui suit :

a. L'entrepreneur doit maintenir et améliorer continuellement la solution et l'infrastructure pendant toute la durée du contrat, sur une base commerciale raisonnable, et il doit offrir ces améliorations au Canada dans le contexte de l'abonnement du Canada, sans ajustement de prix si ces améliorations sont également offertes à d'autres clients sans qu'il leur en coûte davantage.

b. Si l'entrepreneur retire des fonctions de l'offre commerciale de la solution et offre ces fonctions dans de nouveaux ou d'autres services ou produits, l'entrepreneur doit continuer de fournir ces fonctions au Canada dans le contexte de l'abonnement du Canada aux services, selon les modalités existantes du contrat, que ces autres services ou produits contiennent ou non des fonctions nouvelles ou supplémentaires. L'entrepreneur n'est pas obligé de se conformer à ce paragraphe si la solution acquise par le Canada est toujours offerte par l'entrepreneur parallèlement aux nouveaux services offerts à d'autres clients.

7.6.5 Déclassement

Si l'entrepreneur est incapable de fournir les services avec des caractéristiques et des fonctions qui ne sont pas moins favorables, l'entrepreneur transmettra au Canada un avis écrit indiquant les circonstances et des options de rechange, en plus d'inclure expressément une réduction de prix, et ce, 90 jours avant d'apporter les modifications. Si aucune option de rechange proposée n'est acceptable pour le Canada, l'entrepreneur consent à une résiliation du contrat et paie tous les coûts directs identifiables engagés par le Canada pour effectuer la migration et le stockage des données de client et pour acquérir des services de remplacement équivalents.

7.7 Services

7.7.1 Services de solution

a. Logiciel-service. L'entrepreneur fournira tous les services dont le Canada a besoin pour accéder à la solution et l'utiliser, selon ce qui est précisé à l'annexe A.

b. Autorisation. L'entrepreneur déclare et certifie qu'il possède ou a obtenu, et maintiendra pendant toute la durée du contrat, toutes les autorisations nécessaires, notamment les droits de propriété intellectuelle requis pour fournir les services d'après les modalités du contrat.

c. Indemnisation. L'entrepreneur accepte d'indemniser le Canada de toutes les pertes et les dépenses (y compris les frais juridiques) découlant de toute réclamation pour violation de propriété intellectuelle par un tiers fondée sur l'utilisation de la solution par le Canada.

d. Octroi des droits d'utilisation. L'entrepreneur accorde au Canada le droit non exclusif et incessible d'accéder à la solution et de l'utiliser à partir d'un nombre illimité d'endroits, d'appareils et d'environnements d'exploitation, par le biais d'une connexion sécurisée, sans fil, mobile ou autre, via Internet, un navigateur Web ou toute autre technologie de connexion d'accès qui pourrait être disponible.

Nonobstant toute disposition contraire, les droits seront accordés aux utilisateurs autorisés du Canada sans frais supplémentaires, y compris le droit :

i. d'utiliser les services pour tout but opérationnel légitime, quelle que soit l'utilisation décrite ou non dans la documentation, pourvu que le client se conforme aux conditions du présent accord;

ii. d'échanger un utilisateur autorisé pour un autre aussi souvent que nécessaire selon les fins commerciales du client.

e. Inclus. L'entrepreneur déclare et atteste que les services comprennent ce qui suit :

i. l'hébergement et la tenue à jour de la solution;

ii. la fourniture de tous les services d'infrastructure de la TI accessoires et supplémentaires requis, conformément à toutes les normes de sécurité requises;

iii. l'infrastructure technique qui respecte toutes les normes de sécurité requises, permettant au Canada d'utiliser les services infonuagiques pour traiter les données du Canada conformément à ses normes de sécurité exprimées;

iv. l'accès et l'utilisation absolus par le client, indépendamment de la quantité de données créées, traitées ou stockées par la solution;

v. nonobstant toute disposition contraire, toutes les données agrégées, codées et anonymisées que l'éditeur de logiciel-service peut recueillir au sujet de l'utilisation des services par les utilisateurs autorisés, y compris l'analyse des données, et qui ne contiennent pas de données relatives à des personnes identifiables (« données agrégées »), peuvent être communiquées à l'entrepreneur et à ses tierces parties (y compris les abonnées, les fournisseurs de services et les partenaires) pour diverses raisons, comme aider l'entrepreneur à mieux comprendre les besoins des abonnées et améliorer les services. L'entrepreneur accorde au Canada une licence perpétuelle et irrévocable d'utiliser les données agrégées à ses propres fins commerciales. Pour dissiper tout doute, le Canada n'aura plus accès aux données agrégées une fois le contrat achevé.

Tous ces éléments sont compris dans le prix.

f. Droits d'utilisation restreints. Le Canada reconnaît qu'en fournissant les services, l'entrepreneur ne cède pas de droits de propriété d'un produit logiciel-service, d'une composante de la solution ou de l'infrastructure utilisée par l'entrepreneur pour fournir les services, sauf ce qui est prévu expressément dans une autorisation écrite. Le Canada ne fera pas sciemment ce qui suit :

i. distribuer, octroyer une licence, prêter ou vendre la solution;

ii. porter atteinte aux mécanismes de sécurité de la solution ou les contourner;

iii. retirer, modifier ou obscurcir tout avis de droit d'auteur, de marque commerciale ou tout autre avis de propriété figurant sur ou dans la solution.

g. Modalités applicables. L'entrepreneur a indiqué, et le Canada a reconnu, que l'entrepreneur peut modifier unilatéralement les modalités selon lesquelles il fournit son offre commerciale de la solution, sans préavis à ses clients, dont le Canada. L'entrepreneur déclare et atteste que de telles modifications n'entraîneront pas des conditions moins favorables, plus précisément en ce qui concerne le prix, le niveau de service et les recours, sans égard à tout avis contraire.

h. Modalités supplémentaires. Les parties conviennent que toute modalité, y compris les « cliquer et suivre » ou les avis « contextuels » qui s'appliquent à l'offre commerciale de l'entrepreneur pour la solution, y compris les outils de tiers ou l'infrastructure connexe, ne s'appliquera pas à l'utilisation de la solution par le Canada si ces modalités entrent en conflit avec les conditions explicites du présent contrat. Les modalités des outils de tiers qui ne sont pas précisées dans l'annexe A ne sont pas assujetties à cette section.

i. Offre commerciale de logiciel-service. Le Canada reconnaît qu'il acceptera l'offre commerciale de logiciel-service de l'entrepreneur et déclare que, à moins qu'elle soit explicitement désignée comme travaux ou services à fournir en vertu du présent contrat, le Canada n'exige pas de développement personnalisé, de services de rechange, de niveaux de service, de fonctionnalités ou de caractéristiques.

j. Interfaces de programmation d'applications. L'entrepreneur doit :

i. fournir des services qui utilisent des interfaces de programmation d'applications (API) ouvertes, publiées, prises en charge et documentées pour exécuter des activités comme l'interopérabilité entre les composants et faciliter la migration des applications;

ii. fournir un moyen d'accéder aux applications de prestation de services via des API, et extraire les données de rapport, de facturation et de finances se rapportant à la solution de logiciel-service de planification des ressources utilisée par le Canada;

iii. prendre des mesures raisonnables pour protéger les API internes et externes grâce à des méthodes d'authentification sécurisées. Ceci comprend s'assurer que toutes les requêtes d'API exposées à l'externe nécessitent une authentification réussie pour pouvoir être utilisées et fournir au Canada la capacité de répondre aux normes du gouvernement du Canada sur les API (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/normes-gouvernement-canada-api.html);

iv. pour les services infonuagiques, fournir des API qui permettent :

a. d'interroger les données au repos dans la solution de logiciel-service de planification des ressources;

b. d'évaluer les événements et les incidents stockés dans les journaux liés à la solution de logiciel-service de planification des ressources louée au Canada.

k. Portail de services – Généralités.

Le fournisseur de services infonuagiques doit fournir un portail en ligne libre-service et sécurisé qui permet au Canada d'administrer à distance les services infonuagiques.

i. Ce portail doit comprendre, au minimum :

a. la prestation des services;

b. la gestion des problèmes avec notifications par courriel;

c. la gestion des comptes et l'approvisionnement pour les utilisateurs, y compris :

- la capacité de gérer les utilisateurs et les données associées;
- la création, la suppression et la modification des comptes utilisateurs et des droits d'accès;

d. l'authentification, dont la capacité de permettre l'authentification unique;

e. la capacité d'accéder en toute sécurité au portail en utilisant des mécanismes d'authentification à facteurs multiples pour authentifier les utilisateurs;

f. les renseignements sur la santé ou l'état du service, notamment des statistiques sur l'utilisation des ressources, des rapports sur le rendement, des seuils et des alertes;

g. la transition d'état du service, y compris le démarrage et l'arrêt;
le provisionnement et le déprovisionnement du service infonuagique doivent être disponibles sur une API. En outre, l'entrepreneur doit fournir des liens vers de la documentation, des articles, des tutoriels et d'autres formes d'orientation afin d'aider la GRC à utiliser les services de l'API.

l. Rapports du portail de services.

Le service doit permettre à la GRC de générer les rapports suivants.

i Rapports de gestion des services (p. ex. disponibilité des services, coût, utilisation ou consommation).

ii Rapports donnant de l'information au sujet de la gestion des biens et de la configuration, comme les rapports de vérification de la configuration, de modification de la configuration, d'inventaire ou de la surveillance de l'intégrité des dossiers.

iii Rapports sur les dossiers reçus par le bureau d'aide, les dossiers de demande de service et les dossiers de problèmes (qui ont ou non des répercussions sur les services), entre autres :

a. le nombre de dossiers ouverts;

b. le nombre de dossiers fermés;

c. le délai moyen de réponse aux dossiers (temps entre l'ouverture du dossier et le premier contact avec le client), le délai moyen de résolution des dossiers et la description du problème.

m. Gestion des comptes principaux.

L'entrepreneur doit veiller à protéger adéquatement le processus de gestion de comptes utilisé pour fournir et soutenir le service infonuagique pour le Canada. Ces mesures de sécurité doivent au moins comprendre :

(i) limiter l'accès aux seuls utilisateurs qui sont autorisés à exécuter des transactions et des fonctions comme la création et l'émission de comptes principaux;

(ii) veiller à bien délimiter les fonctions des personnes;

(iii) utiliser le principe de privilège minimal, y compris concernant les fonctions spécifiques de sécurité et les comptes privilégiés;

(iv) veiller à ce que les utilisateurs autorisés soient formés et sensibilisés à la sécurité dans le cadre de leur intégration à l'emploi et lorsque leurs rôles changent;

(v) créer, protéger et conserver les dossiers de vérification liés aux activités à l'appui de la gestion des comptes des services infonuagiques fournis au Canada;

(vi) fournir au Canada des rapports sur les événements vérifiés liés aux mesures relatives à l'accord et à la gestion des comptes principaux;

(vii) veiller à la protection des données du Canada durant et après les actions posées par le personnel, comme dans les cas de cessation d'emploi ou de mutation.

7.8 Durée du contrat

7.8.1 Période du contrat.

La période du contrat représente toute période au cours de laquelle l'entrepreneur est tenu de fournir les services et d'exécuter les travaux.

7.8.2 Durée initiale

Le présent contrat entre en vigueur à la date d'attribution du contrat et prend fin 12 mois plus tard.

7.8.3 Option de prolongation du contrat.

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

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

7.8.4 Changement en matière de consommation

L'entrepreneur accorde au Canada l'option irrévocable d'augmenter ou de diminuer la consommation des services infonuagiques décrite à l'annexe A au moment du renouvellement. Dans les cas où la consommation des services infonuagiques du Canada diminue, l'entrepreneur convient qu'aucune pénalité ne s'applique, quoique le prix par unité peut être modifié en raison de la diminution de la consommation.

7.8.5 Retrait de renouvellement automatique

Par la présente, le Canada avise l'entrepreneur qu'il refuse tout renouvellement automatique de la période obligatoire. L'entrepreneur accuse réception de l'avis et déclare que le présent contrat sera valide seulement jusqu'à la fin de la période du contrat définie ci-dessus.

7.9 Conformité de l'entrepreneur

L'entrepreneur doit respecter les exigences en matière d'assurance prévues dans l'avis.

7.9.1 Violation totale. Si, de l'avis raisonnable du Canada, le manquement de l'entrepreneur est une violation totale ou substantielle du contrat, le Canada peut immédiatement résilier le contrat au moyen d'un avis. Par souci de clarté, l'avis du Canada peut être fondé sur des situations comme les suivantes :

7.9.2 l'entrepreneur ne respecte pas une obligation contractuelle substantielle;

7.9.3 l'entrepreneur semble irréfutablement incapable d'exécuter une obligation contractuelle substantielle, en raison de facteurs indépendants de sa volonté. Par souci de clarté, ceci comprend l'insolvabilité réelle ou apparente, l'incapacité répétée de remettre des produits livrables acceptables dans le cadre de ce contrat ou d'autres contrats similaires avec le Canada;

7.9.4 des violations non corrigées multiples ou répétées d'une obligation contractuelle intermédiaire par l'entrepreneur;

7.9.5 un manquement de l'entrepreneur qui a des répercussions négatives sur les activités du gouvernement.

7.10 Certitude de vérification et vérifications externes de conformité

L'entrepreneur doit accepter que la GRC effectue des examens et des évaluations indépendants au moins une fois par année pour s'assurer de repérer les non-conformités des politiques, des normes, des procédures et des obligations de conformité établies.

Le signalement des incidents et interventions en investigation informatique et criminalistique infonuagique se fera au moyen de la gestion régulière des rapports d'incident de la GRC.

La criminalistique infonuagique est un sous-ensemble de la criminalistique de réseau qui utilise la criminalistique numérique dans l'infonuagique. La criminalistique infonuagique peut être utilisée dans les situations suivantes.

7.10.1 Enquête : Enquêter sur la criminalité en nuage et les infractions aux politiques dans des environnements multilocataires et pluri-gouvernementaux, les transactions, les opérations et les systèmes douteux dans le nuage pour intervenir en cas d'incident ou reconstruire des événements dans le nuage.

7.10.2 Dépannage : Rechercher des données et les héberger physiquement et virtuellement dans des environnements en nuage. Repérer la cause fondamentale des tendances et des incidents isolés, et élaborer de nouvelles stratégies qui aideront à empêcher d'autres événements semblables de se produire. Rechercher et surveiller un événement, et évaluer son état actuel.

7.10.3 Surveillance des journaux : Recueillir, analyser et mettre en corrélation les entrées de journaux dans plusieurs systèmes hébergés dans le nuage, dont les aides à la vérification, la diligence raisonnable et la conformité réglementaire.

7.10.4 Récupération de données et de systèmes : Récupérer des données dans le nuage, qu'elles aient été accidentellement ou intentionnellement modifiées ou supprimées. Déchiffrer les données chiffrées dans le nuage si la clé de chiffrement est déjà perdue.

7.10.5 Diligence raisonnable et conformité réglementaire : Faire preuve de diligence raisonnable et respecter les exigences liées à la protection des renseignements de nature délicate, à la tenue à jour de certains dossiers nécessaires à la vérification, ainsi qu'à la transmission d'avis aux parties concernées lorsque des renseignements confidentiels sont dévoilés ou compromis.

7.11 Accord sur les niveaux de service

7.11.1 L'accord sur les niveaux de service infonuagique de l'entrepreneur est joint à l'annexe F. Les engagements relatifs au niveau de service (décrits dans l'annexe F) doivent comprendre un soutien aux clients commerciaux qui prévoit, au moins, un soutien publié et disponible sur le marché (c.-à-d. garantie, maintenance et services de soutien) habituellement offert aux clients qui fournissent des services infonuagiques.

7.11.2 Les modalités suivantes doivent être abordées dans l'annexe F, Accord sur les niveaux de service, selon le cas :

7.11.2.1 période pendant laquelle l'entrepreneur assurera la garantie et le soutien;
7.11.2.2 coordonnées et renseignements concernant la procédure d'obtention de soutien;
7.11.2.3 procédures de résolution de problèmes;
7.11.2.4 délais de réponse;
7.11.2.5 procédures relatives au traitement (quand et comment répondre) des communications par téléphone, par télécopieur ou par courriel;
7.11.2.6 recours et procédures de renvoi;
7.11.2.7 définition des temps d'arrêt, prévus et imprévus ;
7.11.2.8 système de reprise après sinistre disponible;
7.11.2.9 crédits de service – déclencheurs et calculs, et services de maintenance (p. ex. correctifs, mises à jour, versions majeures ou mineures, etc.).

7.12 Responsables

7.12.1 Autorité contractante

L'autorité contractante pour le contrat est :

Nom *:* Qyitayo Ziwa
Gendarmerie royale du Canada
Nº de téléphone : 639-625-4151
Adresse électronique : 2Qyitayo.ziwa@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.

7.12.2 Chargé de projet *(à insérer à l'attribution du contrat)*

Le chargé de projet pour le contrat est :

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____

Téléphone : ___ ___ _____
Télécopieur : ___ ___ _____
Courriel : _____

Le chargé de projet représente le ministère ou l'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. De tels changements peuvent être effectués uniquement au moyen d'une modification de contrat émise par l'autorité contractante.

7.12.3 Représentant de l'entrepreneur *(à insérer à l'attribution du contrat)*

7.13 Divulgation proactive de marchés 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.

7.14 Paiements

7.14.1 Factures

a. Présentation des factures. L'entrepreneur doit présenter des factures pour tous les services infonuagiques et les travaux visés par le paiement conformément au contrat. L'entrepreneur doit fournir la version originale de chaque facture au responsable du projet.

b. **Instructions relatives à la facturation.**

i. Tous les prix facturés et les paiements doivent être inscrits en dollars canadiens.

ii. En présentant des factures (portant sur des articles qui ne font pas l'objet d'un paiement anticipé), l'entrepreneur atteste que les services infonuagiques ont été fournis et que tous les frais sont calculés, conformément au contrat.

c. Exigences de facturation. Les factures doivent être soumises au nom de l'entrepreneur et doivent contenir :

i. la date, le nom et l'adresse du ministère client, les numéros d'article ou de référence, les produits livrables et la description des services infonuagiques, ainsi que le numéro de contrat;

ii. des renseignements sur les dépenses (comme le nom des articles et leur quantité, l'unité de distribution, le prix unitaire, les tarifs horaires fermes, le niveau d'effort et les contrats de sous-traitance, selon le cas) conformément à la base de paiement, excluant les taxes applicables;

iii. les taxes applicables doivent être indiquées sur une ligne distincte avec les numéros d'enregistrement correspondants des autorités fiscales, et tous les éléments qui sont détaxés, exonérés ou auxquels les taxes applicables ne s'appliquent pas doivent être désignés comme tels sur toutes les factures;

iv. les déductions correspondant à la retenue de garantie, s'il y a lieu;

v. le report des totaux, s'il y a lieu.

d. Taxes

Paiement des taxes. Les taxes applicables seront payées par le Canada conformément aux dispositions de l'article sur la présentation de factures. Il revient à l'entrepreneur de facturer les taxes applicables selon le taux approprié, conformément aux lois en vigueur. L'entrepreneur accepte de remettre aux autorités fiscales concernées les sommes acquittées ou exigibles au titre de taxes applicables.

e. Certification des factures. En présentant une facture, l'entrepreneur atteste que la facture correspond aux travaux qui ont été livrés et qu'elle est conforme au contrat.

7.14.2 Mode de paiement

H1001C (2008-05-12) Paiements multiples

1. Accès au service, stockage des données et soutien de la solution de logiciel-service de planification des ressources lors des périodes du contrat initiales et facultatives

a. Le Canada versera le paiement anticipé annuel à l'entrepreneur pour les services d'abonnement, le stockage des données et le soutien de la solution de logiciel-service de planification des ressources dans les 30 jours qui suivent la date de réception de la facture complète (et de toute pièce justificative exigée).

b. Si le Canada s'oppose au contenu de la facture pour quelque motif que ce soit, il s'engage à régler à l'entrepreneur la tranche de la facture non contestée, à la condition que les articles non contestés soient indiqués distinctement sur la facture et que leur paiement soit exigible en vertu du contrat. Dans le cas des factures contestées, elles ne seront réputées reçues aux fins de l'article des conditions générales intitulé « Intérêts sur les comptes en souffrance » qu'une fois le litige réglé.

L'entrepreneur reconnaît qu'il s'agit d'un paiement anticipé et, malgré toute indication contraire dans le contrat, le Canada n'exécutera les procédures d'acceptation qu'une fois les biens fournis ou les services rendus, peu importe si le paiement a déjà été versé. L'entrepreneur convient que tout paiement anticipé autorisé et versé conformément aux modalités du contrat ne constitue pas une acceptation des biens et des services à l'égard desquels le paiement a été versé. De plus, le versement d'un paiement anticipé n'empêche pas le Canada d'exercer un recours à l'égard de ce paiement ou d'une partie des travaux, si les travaux exécutés par la suite s'avèrent inacceptables.

1. Prestation de la solution de logiciel-service de planification des ressources

Le Canada versera des paiements conformément aux indications de l'annexe B, Base de paiement, et aux modalités de paiement du contrat si :

a. une facture exacte et complète et tous les autres documents exigés par l'autorité contractante ont été présentés, conformément aux instructions relatives à la facturation contenues dans le contrat.

7.15 Attestations et renseignements supplémentaires

7.15.1 Conformité

Sauf indication contraire, 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 peuvent faire l'objet d'une vérification par le Canada pendant toute la durée du contrat.

7.16 Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur Saskatchewan, et les relations entre les parties seront déterminées par ces lois.

7.17 Ordre de priorité des documents

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

Les conditions, y compris les appendices, les annexes, les modifications et ce qui est attribué au contrat;

a. Annexe A Énoncé des travaux
b. Appendice A de l'annexe A – Définitions liées aux obligations en matière de sécurité et de confidentialité
c. Annexe B Base de paiement
d. Annexe C Obligations en matière de sécurité et de confidentialité
e. Annexe E Formulaire de présentation de l'information sur la sécurité de la chaîne d'approvisionnement
f. Annexe F Accord sur les niveaux de service
g. Annexe G Droits d'utilisation du logiciel
h. Annexe H Conditions supplémentaires d'utilisation du logiciel
i. Annexe M Liste de vérification des exigences relatives à la sécurité et guide de sécurité
j. Soumission de l'entrepreneur en date du ----------

7.18. Ombudsman de l'approvisionnement

7.18.1 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 découlant du 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/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'entremise 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.

7.18.2 Administration du contrat

Les parties reconnaissent que l'ombudsman de l'approvisionnement nommé en vertu du paragraphe 22.1(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.

Le Bureau de l'ombudsman de l'approvisionnement peut être joint par téléphone, au 1-866-734-5169, par courriel à l'adresse boa.opo@boa-opo.gc.ca, ou par l'entremise de son site Web à l'adresse www.opo-boa.gc.ca pour le dépôt d'une plainte.

7.19 Exigences en matière d'assurance

L'entrepreneur doit décider si une couverture supplémentaire est nécessaire pour remplir ses obligations en vertu du contrat et se conformer aux lois applicables. Toute assurance souscrite ou maintenue par

l'entrepreneur est assumée par lui seul, à son propre bénéfice et pour sa seule protection. Elle ne dégage pas l'entrepreneur de sa responsabilité aux termes du contrat ni ne la diminue.

7.20 Limitation de responsabilité

7.20.1 Responsabilité de la première partie

7.20.1.1 Exécution du contrat : L'entrepreneur est entièrement responsable envers le Canada de tous les dommages résultant de l'exécution ou l'inexécution du contrat par l'entrepreneur.

7.20.1.2 Violation des données : L'entrepreneur est entièrement responsable envers le Canada de tous les dommages qui résultent d'un manquement qu'il a commis aux obligations en matière de sécurité ou de confidentialité et qui entraîne un accès non autorisé à des documents, des données ou de l'information appartenant au Canada ou à un tiers, ou leur divulgation non autorisée.

7.20.1.3 Limitation par incident : Sous réserve de l'article suivant, quel que soit le fondement ou la nature de la réclamation, la responsabilité totale de l'entrepreneur par incident n'excédera pas la valeur cumulative des factures contractuelles pour les douze (12) mois précédant l'incident.

7.20.1.4 Aucune limite : La limite fixée ci-dessus pour la responsabilité de l'entrepreneur ne s'applique pas aux éléments suivants :
inconduite volontaire ou actes délibérément fautifs;tout manquement aux obligations relatives à la garantie.

7.20.2 Responsabilité envers les tiers

Que la réclamation d'un tiers soit faite au Canada, à l'entrepreneur ou aux deux, chaque partie convient qu'elle acceptera l'entière responsabilité des dommages qu'elle cause au tiers dans le cadre du contrat. La répartition de la responsabilité correspondra au montant convenu par les parties ou déterminé par la cour. Les parties conviennent de se rembourser pour tout paiement à un tiers relativement aux dommages causés par l'autre. L'autre partie accepte d'effectuer promptement le remboursement pour sa part de responsabilité.

7.21 Inspection et acceptation

Le responsable technique est le responsable de l'inspection. Tous les rapports, produits livrables, documents, biens et services fournis conformément au contrat peuvent être soumis à l'inspection du responsable de l'inspection ou de son représentant. Si un rapport, document, bien ou service ne respecte pas les exigences de l'énoncé des travaux et n'est pas jugé satisfaisant, tel qu'il est présenté, par le responsable de l'inspection, ce dernier aura le droit de les rejeter ou d'en demander la correction, entièrement aux frais de l'entrepreneur, avant d'en recommander le paiement.

7.22 Considérations environnementales

S'il y a lieu, on invite les fournisseurs à prendre en compte les facteurs environnementaux suivants.

Produits livrables

- Le cas échéant, imprimer les documents papier sur du papier dont au moins 30 % du contenu est recyclé, ou sur du papier certifié, répondant aux normes d'aménagement forestier durable.
- Recycler les documents imprimés inutiles (conformément aux exigences relatives à la sécurité).

Déplacements

- Préférablement, tenir les réunions par téléphone, par téléconférence ou par vidéo afin de limiter les déplacements requis.
- On invite les entrepreneurs à accéder au Répertoire des établissements d'hébergement et des entreprises de location de véhicules de SPAC, lequel contient une liste d'établissements ayant une cote écologique. Au moment de chercher un lieu d'hébergement, les entrepreneurs peuvent consulter le lien suivant pour trouver des propriétés ayant une cote écologique. Ces propriétés sont identifiées par une cote clé verte ou une cote feuille verte et honorent le prix accordé aux entrepreneurs.
- Les entrepreneurs sont invités à utiliser le transport en commun/écologique, dans la mesure du possible

ANNEXE A

ÉNONCÉ DES TRAVAUX

1. TITRE

Solution de logiciel-service de planification des ressources pour les programmes de formation de l'École de la GRC (Division Dépôt)

2. CONTEXTE

La Division Dépôt de la GRC, située à Regina, en Saskatchewan, est chargée de la tâche cruciale qu'est la formation de tous les membres du service de police national du Canada. Le principal volet de la formation de base de l'École de la GRC, Division Dépôt, est le Programme de formation des cadets (PFC). Le PFC comporte des exigences de planification uniques par rapport aux programmes universitaires conventionnels.

Chaque année financière, il forme plusieurs troupes composées d'environ 32 cadets chacune. Ces cadets suivent un programme de formation intensif de 26 semaines qui prévoit des activités variées réalisées dans divers établissements et généralement avec la participation d'animateurs multiples.

De plus, la Division Dépôt offre ses services de formation à un grand nombre d'organismes nationaux et internationaux du maintien de l'ordre et de la réglementation. Ces cours de formation spécialisés variés peuvent durer d'une seule journée à plusieurs semaines.

Au-delà des exigences de planification du PFC, la Division Dépôt effectue aussi des tâches de planification pour les logements, les réunions et conférences, les événements et les séminaires sur le perfectionnement des employés.

Contrairement au modèle semestriel typique des universités, l'arrivée des troupes à la Division Dépôt ne suit pas un calendrier académique commun. Elle se déroule plutôt de manière échelonnée, souvent à des intervalles d'une semaine. Même si la durée et le contenu de la formation sont les mêmes, les dates de début et de fin varient d'une troupe à l'autre. Il en résulte un chevauchement des moments où diverses troupes se trouvent à la Division Dépôt dans le cadre de leur programme de formation.

Afin de renforcer l'efficacité opérationnelle, il est urgent d'établir un système de planification plus efficace, capable d'assurer la gestion de cette structure rotative. Le système doit exceller dans l'affectation des ressources, assurer une utilisation et une disponibilité optimales, et favoriser une planification dynamique pour les troupes, les animateurs, les installations et toutes les autres ressources.

3. OBJECTIF

La GRC est à la recherche d'une solution de logiciel-service de planification des ressources qui peut être configurée pour répondre aux besoins spécifiques de l'organisation et assurer une planification automatisée de son bassin de ressources (cadets et candidats, animateurs, installations, matériel et logements).

La solution de logiciel-service de planification des ressources doit, à tout le moins :

a. fournir une plateforme pour la planification, la gestion et l'affectation des ressources;
b. offrir aux utilisateurs un accès sécurisé et adapté à leur rôle;
c. fournir une plateforme efficace et conviviale pour une planification des ressources simplifiée;
d. être une solution de logiciel-service infonuagique;
e. pouvoir prendre en charge jusqu'à trente (30) utilisateurs simultanés, avec des possibilités d'extension au cours de la période du contrat;
f. appuyer l'intégration de l'interface API afin de faciliter l'échange bidirectionnel des données avec les systèmes organisationnels actuels;
g. offrir aux gestionnaires de ressources des outils analytiques et administratifs.

4. Portée du travail

L'éditeur de logiciel-service de planification des ressources (l'entrepreneur) doit fournir, exploiter et entretenir une solution complète de logiciel-service de planification des ressources pour toute la durée du contrat, y compris les années d'option. Ceci comprend l'accès à l'environnement de la solution de logiciel-service, la création et la configuration des comptes d'utilisateur, la formation et les services de soutien.

4.1 Solution de logiciel-service de planification des ressources pleinement fonctionnelle

La solution doit comprendre la configuration d'un système qui offrira à la GRC les éléments et fonctionnalités générales figurant ci-dessous.

1. Gestion de l'accès par les utilisateurs
   - Données d'accès individuelles;
   - Contrôle d'accès basé sur les rôles pour les animateurs, apprenants, administrateurs et autres membres du personnel.

2. Gestion du bassin de ressources
   - Suivi et gestion des ressources matérielles (armes, véhicules, équipement);
   - Mises à jour de l'inventaire en temps réel et alertes automatisées indiquant quand les stocks d'un article sont limités;
   - Suivi de l'entretien et de la réparation du matériel.

3. Gestion du calendrier
   - Vues adaptées pour la planification des ressources (animateurs, séances de formation, etc.);
   - Vues affichant les calendriers individuels des troupes et des animateurs;
   - Outils pour la résolution automatisée des conflits en cas de chevauchements d'horaires;
   - Vérification des disponibilités en temps réel (salles de classe, champs de tir et autres installations de formation);
   - Envoi d'avis automatisés par l'intermédiaire des systèmes de messagerie électronique actuels (rappels concernant les activités à venir, avis de changements aux calendriers).

4. Établissement de rapports et analyses
   - Rapports personnalisables sur les calendriers et l'utilisation des ressources;
   - Analyse des données pour le repérage de tendances et l'amélioration de l'affectation des ressources.

4.2 Disponibilité de l'environnement

Dans les deux semaines suivant l'attribution du contrat, l'entrepreneur doit veiller à mettre la solution de logiciel-service de planification des ressources à la disposition de la GRC. Ceci comprend la création des comptes d'utilisateur ou d'un compte d'administration qui permettra à la GRC de créer les comptes d'utilisateur.

La solution de logiciel-service de planification des ressources doit être hébergée au Canada, et elle doit être installée et configurée de sorte que toutes les données, y compris les sauvegardes de données, demeurent au Canada.

4.3 Fonctionnement du service

4.3.1 Heures de service

L'environnement de la solution de logiciel-service de planification des ressources doit être accessible à la GRC en tout temps (24 heures par jour, 7 jours par semaine et 365 jours par année), à l'exception des périodes d'entretien prévues ou des pannes inattendues qui ne dépassent pas le temps d'arrêt autorisé, précisé dans l'ANS.

4.3.2 Surveillance du service

L'entrepreneur doit continuellement surveiller la santé et le rendement global du service. Il doit veiller au maintien constant du rendement du système pour toute la durée du contrat.

4.3.1 Services de soutien

L'entrepreneur doit fournir, sur demande, des conseils techniques spécialisés et des instructions concernant la solution de logiciel-service de planification des ressources afin de veiller à ce qu'elle soit programmée, configurée et mise en œuvre conformément aux pratiques exemplaires de l'entrepreneur, et d'assurer qu'elle continue de répondre à toutes les exigences (en matière de sécurité, de niveau de service, etc.) du contrat subséquent de l'éditeur de logiciel-service.

4.4 Formation

L'entrepreneur doit être disponible pour animer des séances de formation des utilisateurs finaux dans les huit (8) semaines suivant l'attribution du contrat. Il est tenu de renseigner les utilisateurs sur les caractéristiques, les fonctionnalités et les pratiques exemplaires du système. Les séances de formation comprendront :

- un plan de cours, un programme et des documents de formation (fournis sept [7] jours avant la première séance;
- une formation à distance (en temps réel) sur la solution et des documents à l'appui;
- une formation destinée à deux groupes principaux (indiqués ci-dessous).

4.4.1 Formation

Description de la formation	**Nombre estimé de participants**	**But ou objectif**
Administrateurs	4	Former un petit groupe d'utilisateurs responsables de gérer les comptes d'utilisateur et d'offrir un soutien technique de base à la GRC.
Utilisateurs finaux	Jusqu'à 15	Former les utilisateurs finaux du système sur ses caractéristiques, fonctionnalités et pratiques exemplaires.

5. LANGUE DE TRAVAIL

La langue de travail et des produits livrables est l'anglais.

6. DÉPLACEMENTS

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

7. RÉUNIONS

L'entrepreneur sera tenu d'assister aux réunions par voie virtuelle, à la demande du responsable technique de la GRC ou de son représentant désigné.

APPENDICE A DE L'ANNEXE A

DÉFINITIONS LIÉES AUX OBLIGATIONS EN MATIÈRE DE SÉCURITÉ ET DE CONFIDENTIALITÉ

Terme	Définition
Mandataire	Un mandataire autorisé par l'entrepreneur à exécuter une ou plusieurs des tâches ci-après dans le cadre des modalités de l'accord-cadre et de toute commande de service correspondante : 1) Fournir des renseignements sur la facturation; 2) S'occuper de la facturation; 3) Fournir des services de rapports sur la consommation; 4) Recevoir le paiement au nom de l'entrepreneur. Un agent n'a pas accès aux comptes principaux de SPC et n'y donne pas non plus accès, pas plus qu'il n'a accès au locataire d'un client, aux données d'un client ni aux comptes principaux d'un client.
Données du Canada	L'information ou les données, y compris tous les fichiers texte, musicaux ou vidéo, les images, les logiciels et les métadonnées connexes, peu importe leur forme ou leur format : a) communiquées par le personnel, les clients, les partenaires, les participants à une coentreprise, les concédants de licence, les vendeurs ou les fournisseurs du Canada au moyen de services infonuagiques; b) communiquées par les utilisateurs finaux des services infonuagiques; c) recueillies, utilisées, traitées ou stockées dans un environnement infonuagique, qui sont communiquées directement ou indirectement à l'entrepreneur ou aux sous-traitants par le Canada ou en son nom, ou encore par l'entremise des services infonuagiques. Cela comprend toute information ou donnée : i) à laquelle l'entrepreneur ou tout sous-traitant a accès intentionnellement ou par inadvertance; ii) transitant sur un réseau ou conservée dans un système ou du matériel utilisé et géré pour le Canada par l'entrepreneur en vue d'assurer la prestation des services infonuagiques et de l'entrepreneur, y compris l'infrastructure de l'entrepreneur.
Infonuagique	Un modèle qui permet, de façon omniprésente, pratique et à la demande, l'accès réseau à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peuvent rapidement être fournies et mises à jour tout en exigeant très peu d'efforts de gestion ou de contacts avec le fournisseur de services. Définition tirée de la publication SP 800-145 du National Institute of Standards and Technology (NIST), accessible à la page suivante (en anglais seulement) : https://csrc.nist.gov/pubs/sp/800/145/final
Fournisseur de services infonuagiques (FSI)	Une entité (pouvant être composée d'au moins une personne physique, une société, un partenariat, une société à responsabilité limitée, etc.) à l'origine du *service infonuagique public* dans son ensemble.
Offert sur le marché	Un service auquel le public peut accéder pour l'utilisation ou la consommation.
Compromission	Brèche de sécurité au gouvernement qui comprend, entre autres : • un accès non autorisé à des renseignements ou des biens de nature délicate, ou la communication, la modification, l'utilisation, l'élimination ou la destruction de renseignements ou de biens de nature délicate, qui pourraient occasionner une perte de confidentialité, d'intégrité, de disponibilité ou de valeur; • tout agissement, comportement, menace ou geste d'une personne à l'égard d'un employé à son lieu de travail ou d'une personne dans les installations fédérales qui a créé un dommage ou un préjudice à cet employé ou à cette personne; • les événements entraînant une perte de l'intégrité ou de la disponibilité des services ou des activités du gouvernement. (Référence : Plan de gestion des événements de cybersécurité du gouvernement du Canada)
Entrepreneur	Une entité (peut comprendre une ou plusieurs personnes physiques, des sociétés, des partenariats, des sociétés à responsabilité limitée, etc.) qui fournit les services infonuagiques à la GRC et à ses partenaires. Il s'agit de

Terme	Définition
	l'entité approuvée et désignée comme « entrepreneur » dans le contrat éventuel.
Utilisateur final	Toute personne, ou tout processus système agissant au nom d'une personne, que le Canada autorise à accéder aux services infonuagiques.
Fuite d'information	Incidents lors desquels un actif informationnel est déposé par inadvertance dans un dispositif ou dans un système qui n'est pas autorisé à traiter ces renseignements (voir la Ligne directrice sur la sécurité de la technologie de l'information-33, IR-9).
Compte principal	Un compte doté de privilèges de base pour générer des comptes clients ou des sous-comptes qui permettront au ministère d'accéder à des services infonuagiques publics offerts sur le marché.
Métadonnées	Information décrivant les caractéristiques des données, y compris, par exemple, les métadonnées structurelles décrivant les structures de données (comme le format des données, la syntaxe et la sémantique) et les métadonnées descriptives décrivant le contenu des données (comme les étiquettes de sécurité de l'information). (Référence : NIST SP 800-53, révision 4)
Renseignements personnels	Information qui a trait à une personne identifiable et qui est consignée dans tous les formats possibles, conformément à l'article 3 de la *Loi sur la protection des renseignements personnels*. Il s'agit, par exemple, des renseignements relatifs à la race, à l'origine nationale ou ethnique, à la religion, à l'âge, à la situation de famille, à l'adresse, à l'éducation ainsi que les renseignements relatifs au dossier médical, au casier judiciaire, aux opérations financières et les antécédents professionnels. Les renseignements personnels comprennent également tout numéro ou symbole d'identification, comme le numéro d'assurance sociale, attribué à une personne. (Référence : https://laws-lois.justice.gc.ca/fra/lois/p-21/section-3.html)
Atteinte à la vie privée	Une atteinte à la vie privée suppose la collecte, l'usage, la communication, la conservation ou le retrait inappropriés ou non autorisés de renseignements personnels. (Référence : Lignes directrices sur les atteintes à la vie privée du Secrétariat du Conseil du Trésor)
Services infonuagiques publics	Le nuage public est une infrastructure infonuagique fournie à l'usage général du public. Il peut appartenir à une ou plusieurs entreprises, à un établissement scolaire ou à un organisme gouvernemental, ou encore à un regroupement de ces intervenants. Il se trouve dans les locaux du fournisseur de services infonuagiques. Les services infonuagiques publics désignent un bassin de modèles de services d'infonuagique accessible par Internet aux utilisateurs à titre de libre-service rapide, sur demande et élastique au moyen des serveurs d'un fournisseur d'infonuagique, par opposition aux services fournis par les propres serveurs d'une entreprise, qui se trouvent dans ses locaux.
Dossier	Tout document sur papier ou tout groupement de données lisible par machine qui contient des renseignements personnels.
Évaluation et autorisation de la sécurité (EAS)	Le mécanisme grâce auquel on comprend, atténue et gère, de façon uniforme et mesurable, le risque visant un système de TI, et ce, tout au long de son cycle de vie.
Événement de sécurité	Tout événement, acte, omission ou situation pouvant nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité. Les événements de cybersécurité comprennent notamment la divulgation des nouvelles vulnérabilités, la fourniture de renseignements indiquant qu'un auteur de menace planifie possiblement une attaque contre le système d'information du gouvernement du Canada (p. ex. attaque par déni de service distribué) ou encore des tentatives pour porter atteinte au périmètre de réseau.

Terme	Définition
	(Référence : Plan de gestion des événements de cybersécurité du gouvernement du Canada)
Registre des incidents de sécurité	Tout incident, avis ou alerte qu'un dispositif, un système ou un logiciel peut techniquement produire en ce qui concerne son état, ses fonctions et ses activités. Les registres des incidents de sécurité ne se limitent pas aux dispositifs de sécurité; ils s'appliquent à tous les dispositifs, systèmes et logiciels ayant techniquement la capacité de produire des registres sur les incidents pouvant être utilisés dans les enquêtes sur la sécurité, les vérifications et les activités de surveillance. Voici une liste non exhaustive d'exemples de systèmes pouvant produire des registres des incidents de sécurité : pare-feu, systèmes de prévention d'intrusion, routeurs, commutateurs, filtrage de contenu, registres du flux de trafic d'un réseau, réseaux, services d'authentification, services de répertoire, protocoles DHCP, systèmes DNS, plateformes matérielles, plateformes de virtualisation, serveurs, systèmes d'exploitation, serveurs Web, bases de données, applications, pare-feu à couche application (couche 7).
Incident de sécurité	Un événement (ou un ensemble d'événements), un acte, une omission ou une situation qui a entraîné une compromission. Exemples d'incidents de sécurité cybernétique : exploitation active d'une ou de plusieurs vulnérabilités connues, exfiltration de données, défaillance d'un contrôle de sécurité, atteinte d'un service du GC géré ou hébergé dans le nuage, etc. (Référence : Plan de gestion des événements de cybersécurité du gouvernement du Canada)
Événement de sécurité	Tout événement, acte, omission ou situation pouvant nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité. Les événements de cybersécurité comprennent notamment la divulgation des nouvelles vulnérabilités, la fourniture de renseignements indiquant qu'un auteur de menace planifie possiblement une attaque contre le système d'information du gouvernement du Canada (p. ex. attaque par déni de service distribué) ou encore des tentatives pour porter atteinte au périmètre de réseau. (Référence : Plan de gestion des événements de cybersécurité du gouvernement du Canada)
Accord sur les niveaux de service (ANS)	Contrat entre un fournisseur de services (interne ou externe) et l'utilisateur final qui définit le niveau de service attendu du fournisseur de services.
Emplacement de service	Toute installation ou tout site ou endroit que le fournisseur ou qu'un sous-traitant ultérieur du fournisseur possède, loue, fournit ou occupe autrement et à partir duquel le fournisseur ou tout sous-traitant ultérieur du fournisseur fournit des services.
Sous-traitant	Toute personne à qui l'entrepreneur confie en sous-traitance la prestation des services de l'entrepreneur, en tout ou en partie.
Sous-traitant ultérieur	Personne physique ou morale, autorité publique, organisme ou autre organisation effectuant le traitement des données personnelles au nom d'un contrôleur des données ou d'un entrepreneur.

ANNEXE B
BASE DE PAIEMENT

1. BESOIN INITIAL

1.1 Le paiement du prix de lot ferme pour la solution de logiciel-service de planification des ressources dépendra de l'atteinte de toutes les étapes de prestation.

1.2 Pour la solution de logiciel-service de planification des ressources, une fois les deux premières étapes terminées, le Canada paiera un certain montant fondé sur le prix annuel ferme divisé par 365 jours, puis multiplié par le nombre de jours restants avant la date anniversaire du début du contrat. Pour toute année subséquente où le Canada peut exercer son option pour l'obtention des services de solution de logiciel-service de planification des ressources, le montant complet s'appliquera.

AUX FINS D'ÉVALUATION SEULEMENT
L'annexe B doit être remplie dans son intégralité, y compris la période optionnelle. Si tous les tableaux ne sont pas remplis, la soumission sera jugée non recevable et rejetée.

Les quantités estimées sont fournies aux fins d'évaluation seulement. Ces quantités représentent l'utilisation estimée aux fins de l'évaluation des coûts seulement et ne constituent pas une garantie ni un engagement de la part du Canada quant à la quantité qu'on doit commander.

1.1 Prestation de la solution de logiciel-service de planification des ressources

Tableau 1 : Prestation de la solution de logiciel-service de planification des ressources		
Point	**Étapes**	**Prix**
1	• Déployer et configurer la solution de logiciel-service de planification des ressources • Formation • Assurer la transition vers les opérations • Réaliser les travaux nécessaires pour accompagner les utilisateurs autorisés pendant le processus d'EAS.	
Prix total de la prestation de la solution de logiciel-service de planification des ressources		

1.2 Accès et soutien à la solution de logiciel-service de planification des ressources

Tableau 2 : Licence annuelle pour l'accès et le soutien à la solution de logiciel-service de planification des ressources		
Point	**Licences d'abonnement annuelles**	**Prix**
An 1	La licence pour l'accès et le soutien à la solution de logiciel-service de planification des ressources permettant d'utiliser la solution conformément aux modalités du contrat. De 1 à 30 utilisateurs	$
Année d'option 1	La licence annuelle pour la solution de logiciel-service de planification des ressources permettant d'utiliser la solution conformément aux modalités du contrat. De 1 à 30 utilisateurs	$
Année d'option 2	La licence pour l'accès et le soutien à la solution de logiciel-service de planification des ressources permettant d'utiliser la solution conformément aux modalités du contrat. De 1 à 30 utilisateurs	$
Année d'option 3	La licence pour l'accès et le soutien à la solution de logiciel-service de planification des ressources permettant d'utiliser la solution conformément aux modalités du contrat. De 1 à 30 utilisateurs	$
Année d'option 4	La licence pour l'accès et le soutien à la solution de logiciel-service de planification des ressources permettant d'utiliser la solution conformément aux modalités du contrat. De 1 à 30 utilisateurs	$

Table 7 – Aux fins d'évaluation seulement		
Point	**Description**	**Prix calculé**
1	Tableau 1 : Prestation	$
2	Tableau 2 : Licence annuelle pour l'accès et le soutien à la solution de logiciel-service de planification des ressources	$
Prix total évalué (en dollars canadiens)		$

ANNEXE C
OBLIGATIONS EN MATIÈRE DE SÉCURITÉ ET DE CONFIDENTIALITÉ

Partie 1 – Obligations en matière de sécurité pour les services infonuagiques commerciaux (jusqu'au niveau « Protégé A », inclusivement)

1. Généralités

1.1 *Objet*

La présente annexe a pour objet d'énoncer les obligations de l'entrepreneur en ce qui a trait à la bonne gestion des données du Canada, notamment afin de les protéger contre tout accès, modification ou exfiltration non autorisés, conformément à l'entente, à la présente partie et aux mesures de sécurité de l'entrepreneur (collectivement, les « **obligations en matière de sécurité** »).

1.2 *Transfert des obligations en matière de sécurité*

Les obligations de l'entrepreneur contenues dans les présentes obligations en matière de sécurité doivent être transférées par l'entrepreneur à tout sous-traitant, le cas échéant.

1.3 *Gestion du changement*

L'entrepreneur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir à jour les exigences relatives à la sécurité afin de se conformer aux pratiques exemplaires en matière de sécurité et aux normes de l'industrie, énoncées dans la présente partie.

L'entrepreneur doit informer le Canada de tout changement qui pourrait nuire de manière importante aux services infonuagiques présentés dans le présent contrat, y compris les changements ou améliorations de nature technologique, administrative ou autre. L'entrepreneur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier, sans supplément pour le Canada.

2. Reconnaissance

Les parties reconnaissent que :

(a) les données du Canada sont assujetties à ces obligations en matière de sécurité.

(b) nonobstant toute autre disposition de la présente partie, les parties partagent la responsabilité de l'élaboration et du maintien des politiques, des procédures et des contrôles de sécurité relatifs aux données du Canada.

(c) l'entrepreneur ne doit pas avoir ou tenter d'obtenir la garde de données du Canada, ni permettre à un membre du personnel des services infonuagiques d'accéder aux données du Canada avant la mise en œuvre des exigences en matière de sécurité, comme l'exige la présente partie, au plus tard à l'attribution du contrat.

(d) Les obligations en matière de sécurité s'appliquent aux **services infonuagiques commerciaux** (jusqu'au niveau « Protégé A/Intégrité moyenne/Disponibilité moyenne » ou « Préjudice moyen », inclusivement), sauf indication contraire.

3. Protection des données du Canada

(1) L'entrepreneur doit protéger les données du Canada contre toute modification, toute exfiltration et tout accès non autorisé. Ceci comprend la mise en œuvre et le maintien

des mesures de sécurité techniques et organisationnelles appropriées, notamment des politiques, des procédures et des contrôles de sécurité de l'information afin de préserver la confidentialité, l'intégrité et la disponibilité des données du Canada.

4. Rôles et responsabilités liés à la sécurité

(1) L'entrepreneur doit clairement définir les rôles et responsabilités relatifs aux contrôles et aux fonctions de sécurité des services infonuagiques pour lui-même et pour le Canada. Ceci comprend, à tout le moins, les rôles et les responsabilités pour : i) la gestion des comptes; ii) la protection des frontières; iii) la sauvegarde des actifs et des systèmes d'information; iv) la gestion des incidents; v) la surveillance du système; et vi) la gestion de la vulnérabilité.

(2) L'entrepreneur doit fournir au Canada un document à jour qui définit les rôles et les responsabilités : i) à l'attribution du contrat; ii) annuellement; iii) lorsqu'il y a des changements importants à ces rôles et responsabilités à la suite d'un changement aux services; ou iv) à la demande du Canada.

5. Assurance d'une tierce partie : Certifications et rapports

(1) L'entrepreneur doit s'assurer que les données du Canada, l'infrastructure de l'entrepreneur (y compris tout service d'infrastructure-service, de plateforme-service ou de logiciel-service fourni au Canada) et les emplacements de service sont protégés par des mesures de sécurité appropriées qui respectent les exigences établies dans les pratiques et politiques en matière de sécurité de l'entrepreneur.

(2) L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et les rapports de vérification suivants en présentant des rapports d'évaluation ou des certifications de tierce partie indépendante pour chaque niveau de service (p. ex. infrastructure-service, plateforme-service ou logiciel-service) au sein des services infonuagiques :

(a) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Certification obtenue par un organisme de certification accrédité (ou versions ultérieures); OU

(b) Service Organization Control (SOC) 2 de type II de l'AICPA Rapport de vérification 2 de type II pour les principes de confiance en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité – émis par un expert-comptable agréé indépendant;

(c) L'autoévaluation de l'entrepreneur selon la matrice des contrôles infonuagiques de la Cloud Security Alliance, version 4 (ou versions ultérieures).

(3) Chaque certification ou rapport de vérification présenté doit : i) déterminer la dénomination commerciale officielle de l'entrepreneur ou du sous-traitant concerné; ii) déterminer la date de certification de l'entrepreneur ou du sous-traitant et le statut de cette certification; iii) déterminer les services inclus dans le cadre du rapport de certification. Si la méthode déterminée est utilisée pour exclure les sous-traitants comme l'hébergement de centres de données, le rapport d'évaluation du sous-traitant doit être inclus.

(4) Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être mis à la disposition du Canada. Les certifications doivent être accompagnées de preuves à l'appui, comme le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO, et doivent indiquer clairement toutes les constatations importantes faites par le vérificateur. L'entrepreneur doit corriger rapidement et à la satisfaction du vérificateur les problèmes soulevés dans tout rapport de vérification et fournir au Canada des preuves à l'appui des mesures correctives mises en place ou la

confirmation par le vérificateur que les problèmes ont été corrigés à sa satisfaction.

(5) Chaque rapport de vérification SOC 2 de type II doit avoir été réalisé dans les 12 mois précédant le début du contrat. Une lettre de pont pourrait être fournie afin de démontrer que l'entrepreneur procède au renouvellement dans les cas où il y a un écart entre la date du rapport de l'organisme de services et la fin d'année de l'organisme utilisateur (c.-à-d. fin de l'année civile ou de l'exercice financier).

(6) L'entrepreneur doit conserver les certifications ISO 27001 ou SOC 2 de type II, le cas échéant, pour toute la durée du contrat. L'entrepreneur doit fournir, au moins une fois par année et rapidement à la demande du Canada, tous les rapports ou les documents pouvant être raisonnablement exigés pour démontrer que l'entrepreneur possède les certifications actuelles.

6. Vérification de la conformité

(1) L'entrepreneur doit veiller à ce que les vérifications de confidentialité et de sécurité, de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter et protéger les données du Canada soient effectuées comme suit :

(a) Lorsqu'une norme ou un cadre prévoit des vérifications, une vérification de cette norme ou de ce cadre de contrôle sera entreprise au moins une fois par année;

(b) Chaque vérification sera effectuée conformément aux normes et aux règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable;

(c) Chaque vérification sera effectuée par un vérificateur tiers indépendant qui i) est qualifié selon l'AICPA, CPA Canada ou le régime de certification ISO et ii) se conforme à la norme ISO/IEC 17020 sur les systèmes de gestion de la qualité, selon le choix et aux frais de l'entrepreneur;

(2) Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être mis à la disposition du Canada. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le vérificateur tiers. L'entrepreneur doit, à ses frais, corriger rapidement et à la satisfaction du vérificateur les problèmes et les lacunes soulevés dans tout rapport de vérification.

(3) À la demande du Canada, l'entrepreneur ou un sous-traitant peut fournir des preuves supplémentaires, y compris des plans de sécurité du système, des conceptions ou des documents d'architecture qui fournissent une description complète du système, afin d'achever les rapports de certification et de vérification décrits à la section 5 (Assurance d'une tierce partie) et de démontrer la conformité de l'entrepreneur avec les certifications requises de l'industrie. Ceci comprend les cas où l'entrepreneur est un fournisseur de logiciel-service ou de plateforme-service qui utilise des centres de données physiques fournis par un fournisseur d'infrastructure-service tiers.

7. Programme d'évaluation de la sécurité des TI des fournisseurs de services infonuagiques

(1) L'entrepreneur doit démontrer qu'il respecte les exigences de sécurité sélectionnées à l'annexe A, Profil de contrôle de la sécurité infonuagique – FAIBLE, du Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103) du Centre canadien pour la cybersécurité (CCC) (https://www.cyber.gc.ca/fr/orientation/guide-sur-la-categorisation-de-la-securite-des-services-fondes-sur-linfonuagique https://www.cyber.gc.ca/fr/orientation/guide-sur-la-categorisation-de-la-securite-des-services-fondes-sur-linfonuagique) pour la portée

des services infonuagiques fournis par l'entrepreneur. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications de l'industrie applicables énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants.

La conformité sera évaluée et validée par l'entremise du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux FSI (ITSM.50.100) du CCC (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, c'est-à-dire qu'il a intégré le programme, qu'il y a participé et qu'il l'a terminé. Il doit notamment fournir les documents suivants :

(i) Une copie du dernier rapport d'évaluation rempli fourni par le Canada;
(ii) Une copie du dernier rapport sommaire fourni par le Canada.

L'entrepreneur qui souhaite en savoir plus sur le processus d'évaluation des TI du CCC doit communiquer avec le gouvernement du Canada.
L'entrepreneur des services infonuagiques proposés a l'obligation continue d'aviser le gouvernement du Canada lorsqu'il y a d'importants changements à la prestation des services de sécurité des technologies de l'information (STI) à l'appui des services offerts par l'entrepreneur.

(3) Dans les cas où l'entrepreneur est un fournisseur de logiciel-service utilisant un fournisseur d'infrastructure-service approuvé par le gouvernement du Canada qui se conforme déjà aux exigences de l'article 5 – Assurance d'une tierce partie et des sous-sections (1) et (2) de l'article 7 – Programme d'évaluation de la sécurité des TI des fournisseurs de services infonuagiques, le fournisseur de logiciel-service doit présenter au Canada une copie d'un message électronique fourni par le CCC, confirmant que l'entrepreneur a terminé le Programme d'évaluation de la STI s'appliquant aux FSI du CCC.

Le message doit énoncer que le FSI a été évalué par le Programme d'évaluation de la STI s'appliquant aux FSI et qu'il a obtenu un rapport définitif concernant l'évaluation. Pour toute question, il est possible de communiquer avec le CCC par courriel à l'adresse contact@cyber.gc.ca.

8. Protection des données

(1) L'entrepreneur doit :

(a) mettre en œuvre le chiffrement des données au repos pour les services infonuagiques qui hébergent les données du Canada dans les cas où le chiffrement des données au repos demeure en vigueur, ininterrompu et actif à tout moment, même dans l'éventualité de panne d'équipement ou de technologie, conformément à l'article 13 – Protection cryptographique;

(b) transmettre les données du Canada d'une manière sécuritaire qui offre au GC la possibilité de mettre en œuvre le chiffrement des données en transit pour toutes les transmissions des données du Canada, conformément à l'article 13 – Protection cryptographique et à l'article 21 – Sécurité des réseaux et des communications.

(2) L'entrepreneur doit :

(a) mettre en œuvre des contrôles de sécurité qui restreignent l'accès administratif de l'entrepreneur aux données du Canada et aux systèmes et lui permettent d'exiger l'approbation écrite du Canada avant que l'entrepreneur puisse avoir accès aux données du Canada pour effectuer des activités opérationnelles, de soutien ou de maintenance;

(b) prendre des mesures raisonnables pour s'assurer que le personnel de l'entrepreneur n'a

pas de droits d'accès permanents ou continus aux données du Canada, et que l'accès est limité au personnel de l'entrepreneur doté du besoin de savoir, notamment les ressources qui offrent un soutien technique ou à la clientèle, sur approbation du Canada.

(3) L'entrepreneur ne doit pas faire de copies des bases de données ou de toute partie de ces bases de données contenant des données du Canada au-delà des capacités habituelles de résilience des services et à l'intérieur des zones ou des espaces régionaux protégés au Canada.

(4) L'entrepreneur ne doit pas déplacer ou transmettre les copies approuvées à l'extérieur des régions de service convenues, à moins d'avoir obtenu l'approbation écrite du Canada.

(5) À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit toutes les métadonnées supplémentaires créées à partir des données du Canada.

(6) L'entrepreneur n'est pas autorisé à divulguer des données organisationnelles ou des renseignements secondaires fournis par la GRC à tout sous-traitant sans EAS adéquat.

9. Séparation des données

(1) L'entrepreneur doit mettre en place des contrôles afin d'assurer une séparation appropriée des ressources, de sorte que les données du gouvernement du Canada ne se retrouvent pas mêlées à celles d'autres locataires sans contrôle à cet effet, et ce, pendant l'utilisation, le stockage ou le transfert, et dans tous les aspects des fonctions et de l'administration du système des services infonuagiques et de l'infrastructure de l'entrepreneur. Il doit notamment mettre en place des contrôles d'accès et une séparation logique ou physique adéquate à l'appui de :

(a) la séparation entre l'administration interne de l'entrepreneur et les ressources utilisées par ses clients;

(b) la séparation des ressources des clients dans les environnements multilocataires afin d'empêcher que les activités d'un client malveillant ou compromis aient des répercussions sur le service ou les données d'un autre;

(c) la capacité du GC de soutenir l'isolation dans un environnement à locataires géré par le GC (pour l'infrastructure-service).

(2) À la demande du Canada, l'entrepreneur doit fournir au Canada un document qui décrit l'approche permettant d'assurer la séparation voulue des ressources, de manière à ce que les données du Canada ne soient pas mêlées à celles d'un autre locataire pendant leur utilisation, stockage ou transit.

10. Emplacement des données

(1) L'entrepreneur doit avoir la capacité de stocker et de protéger les données du Canada, au repos, y compris les données sauvegardées ou conservées aux fins de redondance. Ceci comprend la capacité d'isoler les données au Canada dans des centres de données approuvés. Un centre de données approuvé est défini comme suit :

(a) Un centre de données qui répond à toutes les exigences et certifications de sécurité décrites à l'article 30 pour la sécurité physique (centre de données ou installations);

(b) Il garantit l'impossibilité de trouver les données d'un client en particulier sur des supports physiques;

(c) Il emploie le chiffrement pour s'assurer qu'aucune donnée n'est écrite sur disque sous une forme non chiffrée, conformément à l'article 13 – Protection cryptographique.

(2) À la demande du Canada, l'entrepreneur doit :

(a) fournir au GC une liste à jour des emplacements physiques, y compris la ville, qui peuvent contenir les données du Canada pour chaque centre de données qui sera utilisé pour fournir les services infonuagiques;

(b) indiquer les parties des services infonuagiques qui sont fournies à partir de l'extérieur du Canada, y compris tous les endroits où les données sont stockées et traitées et d'où l'entrepreneur gère le service.

(3) L'entrepreneur des services infonuagiques proposés a l'obligation continue d'aviser le Canada par écrit lorsqu'il y a des mises à jour de la liste des emplacements physiques qui peuvent contenir des données du Canada.

11. Transfert et récupération des données

L'entrepreneur doit offrir au Canada les capacités, y compris les outils et services, qui lui permettent de procéder aux opérations suivantes :

(a) Extraire toutes les données du Canada en ligne, pseudo-directes et hors ligne, y compris, notamment, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activités infonuagiques, les codes sources hébergés dans un référentiel de codes du Canada et les configurations réseau, de sorte que tout utilisateur final du Canada puisse se servir de ces instructions pour effectuer la migration d'un environnement à un autre;

(b) Effectuer le transfert sécurisé de toutes les données du Canada, y compris les données de contenu et les métadonnées associées, dans un format lisible et utilisable par machine, notamment le format CSV, conformément aux Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires à valeur continue de Bibliothèque et Archives Canada (https://bibliotheque-archives.canada.ca/fra/services/gouvernement-canada/information-disposition/gestion-documents-administratifs/lignes-directrices-information/Pages/lignes-directrices-formats-fichier-ressources-documentaires.aspx?wbdisable=true).

12. Disposition des dossiers et remise des dossiers au Canada

(1) L'entrepreneur doit éliminer ou réutiliser en toute sécurité les ressources (p. ex. l'équipement, les unités de stockage, les fichiers et la mémoire) qui contiennent des données du Canada et s'assurer que les données précédemment stockées ne peuvent pas être consultées par d'autres clients après leur diffusion. Cela comprend toutes les copies des données du Canada qui sont créées à des fins de disponibilité accrue et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être harmonisée à l'un des documents suivants :
(i) Manuel d'utilisation du Programme national de sécurité industrielle (DoD 5220.22-M6); (ii) Lignes directrices pour l'assainissement des supports (NIST SP 800-88); ou (iii) Effacement et déclassification des supports d'information électroniques (CSTC ITSG-06).

À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit le processus d'élimination ou de réutilisation des ressources de l'entrepreneur.

(2) L'entrepreneur doit fournir au Canada une confirmation écrite démontrant qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de tout système, de toute capacité (logiciel ou processus), de toute donnée ou de toute information retirés ou détruits après que le Canada ait cessé d'utiliser les services infonuagiques.

13. Protection cryptographique

L'entrepreneur doit :

(a) configurer toute solution cryptographique qui est adoptée à l'égard des services et qui est utilisée dans le cadre de la mise en œuvre de mesures de protection de la confidentialité ou de l'intégrité ou encore d'un mécanisme d'authentification (p. ex. solutions liées au réseau privé virtuel, protocole de sécurité de la couche transport [protocole TLS], modules logiciels, indicateurs de rendement clés et jetons d'authentification, le cas échéant). Ceci doit être fait en conformité avec les algorithmes cryptographiques, les tailles des paramètres cryptographiques, les longueurs de clés de chiffrement et les périodes de validité des clés approuvés par le Centre de la sécurité des télécommunications (CST), comme il est indiqué dans les documents « Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B » (ITSP.40.111) et « Conseils sur la configuration sécurisée des protocoles réseau » (ITSP.40.062), ou dans des versions ultérieures publiées sur https://cyber.gc.ca/fr/;

(b) utiliser des algorithmes cryptographiques approuvés par le CST qui ont été validés par le Programme de validation des algorithmes cryptographiques (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program), avec les tailles de paramètres cryptographiques et les longueurs de clés de chiffrement précisées dans le document ITSP.40.111 ou dans des versions ultérieures de ce document publiées sur https://cyber.gc.ca/fr/;

(c) veiller à ce que l'utilisation des algorithmes cryptographiques, les tailles de paramètres cryptographiques, les longueurs de clés de chiffrement et les périodes de validité des clés soient configurables et puissent être mis à jour au sein des protocoles, des applications et des services conformément aux directives en matière de transition, à temps pour respecter les dates de transition indiquées dans les documents ITSP.40.444 et ITSP.40.062 ou dans des versions ultérieures de ce document publiées sur https://cyber.gc.ca/fr/. Les entrepreneurs devraient appuyer la transition vers la cryptographie à résistance quantique, conformément aux directives des documents ITSP.40.444 et ITSP.40.062 et de leurs versions ultérieures;

(d) s'assurer que les modules cryptographiques validés par le Programme de validation des modules cryptographiques (PVMC) sont utilisés lorsqu'un chiffrement est nécessaire et qu'ils sont mis en œuvre, configurés et exploités conformément à la politique sur la sécurité des modules cryptographiques figurant sur la liste des modules validés par le PVMC (https://csrc.nist.gov/Projects/cryptographic-module-validation- program/validated-modules), dans un mode approuvé ou autorisé afin de fournir un degré élevé de certitude que le module cryptographique validé par le PVMC fournit les services de sécurité prévus de la manière prévue;

(e) s'assurer que tous les modules cryptographiques utilisés ont une certification active, à jour et valide du PVMC. Les produits validés par le PVMC seront accompagnés d'un numéro de certification dans la liste des modules validés (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules).

14. Gestion des clés

L'entrepreneur doit mettre en œuvre un service de gestion des clés pour la solution de logiciel-service de planification des ressources et l'organisation de l'entrepreneur. Ce service doit être conforme au document ITSP.50.106 Guide sur le chiffrement des services infonuagiques (https://www.cyber.gc.ca/fr/orientation/guide-sur-le-chiffrement-des-services-infonuagiques-itsp50106) du CCC et à ses versions ultérieures publiées sur https://cyber.gc.ca/fr/. Ceci comprend :

(a) la capacité de créer ou générer et de supprimer des clés de chiffrement, à la demande du gouvernement du Canada;

(b) la définition et l'application de politiques particulières qui contrôlent la manière dont les clés peuvent être utilisées;

(c) la protection de l'accès au matériel relatif aux clés, y compris la prévention de l'accès non autorisé au matériel relatif aux clés de manière non chiffrée;

(d) la capacité de vérifier tous les événements liés aux services de gestion des clés, y compris l'accès par l'entrepreneur, pour que le Canada puisse les examiner.

15. Protection des points terminaux

L'entrepreneur doit mettre en œuvre, gérer et surveiller les points d'accès sécurisés dotés de protection active par le système d'hébergement afin de prévenir les logiciels malveillants, les attaques et les abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide to General Server Security [guide relatif à la sécurité générale des serveurs]), des points de référence du Center for Internet Security ou d'une norme équivalente approuvée par écrit par le Canada.

16. Développement sécurisé

L'entrepreneur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : i) NIST, ii) ISO 27034, iii) ITSG-27034, iv) SAFECode ou v) Open Web Application Security Project (p. ex. Application Security Verification Standard) ou une norme équivalente approuvée par le Canada par écrit. À la demande du Canada, l'entrepreneur doit fournir un document qui décrit le logiciel documenté de l'entrepreneur, ainsi que l'approche et le processus adoptés relativement au cycle de vie du développement du système.

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

(1) L'entrepreneur doit procurer au Canada la capacité de soutenir un accès sécurisé aux services, y compris la capacité de configurer :

(a) l'authentification multifactorielle à l'épreuve de l'hameçonnage, conformément à l'ITSP.30.031 V3 du CST ou à ses versions ultérieures (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs - dans-les-systemes-de-technologie-de) à l'aide d'identifiants approuvés par le gouvernement du Canada;

(b) un accès en fonction du rôle;

(c) les contrôles d'accès aux objets entreposés;

(d) les politiques d'autorisation granulaire pour permettre ou limiter l'accès.

(2) L'entrepreneur doit être en mesure d'établir des paramètres par défaut pour l'ensemble de l'organisme aux fins de la gestion des politiques des locataires.

18. Fédération

(1) L'entrepreneur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment :

(a) prendre en charge les normes ouvertes relatives aux protocoles d'authentification tels que le Security Assertion Markup Language 2.0 et l'OpenID Connect 1.0 (ou leurs versions ultérieures) où les justificatifs et authentificateurs des utilisateurs du GC pour les services infonuagiques sont contrôlés uniquement par le Canada;

(b) permettre d'associer les identifiants uniques du Canada (p. ex. un numéro d'identification unique du Canada, une adresse de courriel du Canada) aux comptes d'utilisateurs des services infonuagiques correspondants.

19. Gestion des accès privilégiés

(1) L'entrepreneur doit :

(a) mettre en œuvre des politiques et des procédures de contrôle d'accès pour l'intégration, le départ, la transition d'un rôle à l'autre, les examens périodiques des accès afin de repérer tout privilège ou contrainte inutile, et le contrôle de l'utilisation des privilèges d'administrateur;

(b) gérer et surveiller l'accès privilégié aux services infonuagiques pour s'assurer que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC;

(c) restreindre et minimiser l'accès aux services infonuagiques et aux données du Canada seulement aux appareils autorisés et aux utilisateurs finaux ayant explicitement besoin de cet accès;

(d) appliquer et vérifier les autorisations d'accès aux services infonuagiques et aux données du Canada;

(e) confiner tous les accès aux interfaces de service qui hébergent les biens et les données du Canada à des utilisateurs finaux, des dispositifs et des processus (ou des services) identifiés, authentifiés et autorisés de manière unique;

(f) mettre en œuvre des politiques sur les mots de passe afin de protéger les justificatifs d'identité contre les attaques en ligne ou hors ligne et de détecter ces attaques en consignant et en surveillant des événements tels que (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle de ces derniers et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément à la version 3 (ou aux versions ultérieures) des Normes ITSP.30.031 du CCC (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification- des-utilisateurs-dans-les-systemes-de-technologie-de);

(g) mettre en place des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs ayant des privilèges d'accès, conformément à la norme ITSP.30.031 V3 du CCC (ou à ses versions ultérieures) (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification- des-utilisateurs-dans-les-systemes-de-technologie-de);

(h) mettre en place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux données du Canada;

(i) définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, les rôles de développement des rôles opérationnels et les rôles de gestion de l'accès des autres rôles opérationnels;

(j) adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services infonuagiques et aux données du Canada;

(k) utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (par exemple un point terminal dédié qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) pour offrir le soutien et l'administration des services infonuagiques et de l'infrastructure de l'entrepreneur;

(l) mettre en place un processus automatisé pour effectuer une vérification périodique de la création, de la modification, de l'activation, de la désactivation et de la suppression de comptes, au minimum;

(m) révoquer, en cas de cessation d'emploi, les authentifiants et les justificatifs d'accès associés à tout personnel de services.

(2) À la demande du Canada, l'entrepreneur doit fournir un document qui décrit son approche et son processus pour la gestion et la surveillance des accès privilégiés aux services infonuagiques.

20. Gestion à distance

(1) L'entrepreneur doit gérer et surveiller l'administration à distance des services infonuagiques qui sont utilisés pour héberger les services du GC, en plus de prendre des mesures raisonnables pour :

(a) mettre en place des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs d'accès à distance, conformément à la norme ITSP.30.031 V3 du CCC (ou à ses versions ultérieures) (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification- des-utilisateurs-dans-les-systemes-de-technologie-de);

(b) employer des mécanismes cryptographiques pour protéger la confidentialité des séances d'accès à distance, conformément à l'article 13 (Protection cryptographique);

(c) acheminer tout l'accès à distance par des points de contrôle des accès gérés, surveillés et vérifiés;

(d) déconnecter ou désactiver rapidement les connexions non autorisées de gestion à distance ou d'accès à distance;

(e) autoriser l'exécution à distance des commandes privilégiées et l'accès à distance aux informations relatives à la sécurité.

(2) À la demande du Canada, l'entrepreneur doit fournir un document qui décrit son approche et son processus pour la gestion et la surveillance de l'administration à distance des services infonuagiques.

21. Sécurité des réseaux et des communications

L'entrepreneur doit :

(a) permettre au Canada d'établir des connexions sécurisées aux services infonuagiques, notamment en assurant la protection des données en transit entre le Canada et le service infonuagique au moyen de TLS 1.2 ou de versions ultérieures;

(b) employer des protocoles ainsi que des algorithmes et des certificats cryptographiques pris en charge et à jour, comme le décrivent les normes 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);

(c) utiliser des certificats correctement configurés dans les connexions TLS conformément aux directives du CCC;

(d) Permettre au Canada de mettre en œuvre des contrôles d'accès au réseau et des règles de sécurité qui limitent l'accès aux ressources canadiennes aux appareils et réseaux autorisés.

22. Journalisation et vérification

(1) L'entrepreneur doit mettre en œuvre des pratiques et des contrôles de production et de gestion de journaux pour toutes les composantes du service infonuagique qui stockent ou traitent les données du Canada, et qui sont conformes aux normes et aux pratiques exemplaires de l'industrie, comme celles de NIST 800-92 (Guide to Computer Security Log Management), ou une norme équivalente approuvée par écrit par le Canada. À la demande du Canada, l'entrepreneur doit fournir un document qui décrit les pratiques et les contrôles de production ainsi que de gestion de journaux documentés de l'entrepreneur.

(2) L'entrepreneur doit permettre au Canada d'exécuter la gestion et la configuration centralisées du contenu devant être saisi dans les rapports de vérification de multiples composantes (p. ex. réseau, données, stockage, calcul, etc.) des services infonuagiques utilisés par le Canada, de sorte qu'il puisse assurer la surveillance de la sécurité, la production de rapports, l'analyse, les enquêtes et la mise en œuvre de mesures rectificatives, au besoin. Ceci comprend la capacité du Canada :

(a) d'enregistrer et de détecter les événements de vérification tels que (i) les tentatives de connexion réussies ou non, (ii) la gestion des comptes, (iii) l'accès aux objets et changement de politique, (iv) les fonctions de privilèges et de suivi des processus, (v) les événements système, (vi) la suppression des données, conformément au Guide sur la consignation d'événements du gouvernement du Canada (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/guide-sur-la-consignation-evenements.html);

(b) d'enregistrer dans des journaux (ou fichiers journaux) des événements de vérification qui sont synchronisés et horodatés en temps universel coordonné et protégés contre l'accès, la modification ou la suppression non autorisés, que ces données soient en transit ou inactives;

(c) d'émettre des alertes en temps réel, en cas d'échec d'événements de vérification, à l'intention du personnel muni des pouvoirs lui permettant de résoudre de tels échecs;

(d) de repérer des incidents de sécurité et des journaux de bord distincts pour les différents comptes du Canada afin de permettre au Canada de surveiller et de gérer les événements à l'intérieur de ses frontières qui ont une incidence sur l'instance d'un service infonuagique d'infrastructure-service, de plateforme-service ou de logiciel-service qui lui est rendu par l'entrepreneur ou un sous-traitant;

(3) L'entrepreneur doit permettre au Canada d'exporter les journaux d'événements de sécurité au moyen d'interfaces d'établissement de rapports, de protocoles et de formats de données (Common Event Format, Syslog et autres formats communs) ainsi que d'interfaces API normalisées qui permettent la récupération à distance des données de journaux (p. ex. par l'intermédiaire d'une interface de base de données qui utilise SQL, etc.) pour les services infonuagiques utilisés, en appui des opérations du GC telles que la surveillance des services infonuagiques et pour la preuve électronique et la mise en suspens pour raisons juridiques.

(4) Pour le logiciel-service, l'entrepreneur doit fournir des API qui permettent :

(a) d'inspecter et d'interroger les données au repos dans les applications de logiciel-service;

(b) d'évaluer les événements tels que l'accès et le comportement des utilisateurs, l'accès et le comportement des administrateurs, et les modifications de l'accès aux interfaces de protocole d'application de tiers, enregistrés dans les journaux d'application de logiciel-service.

23. Surveillance continue

(1) L'entrepreneur doit continuellement gérer, surveiller et maintenir la posture de sécurité de l'infrastructure du fournisseur et des emplacements de service qui hébergent les données du Canada pendant toute la durée du contrat, et s'assurer que les services infonuagiques fournis au Canada sont conformes aux présentes obligations en matière de sécurité. Dans le cadre de l'obligation, l'entrepreneur doit :

(a) surveiller activement et continuellement les menaces et les vulnérabilités pesant sur l'infrastructure de l'entrepreneur, les emplacements de service ou les données du Canada;

(b) effectuer régulièrement des analyses de vulnérabilité et des tests d'intrusion de l'infrastructure de l'entrepreneur et des emplacements de service, en vue de déterminer les lacunes et les mesures correctives à prendre pour empêcher l'accès non autorisé aux renseignements de nature délicate, le contournement des contrôles d'accès et l'élévation des privilèges, ainsi que l'exploitation des vulnérabilités pour accéder aux systèmes ou aux renseignements;

(c) faire de son mieux pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le refus de service;

(d) faire de son mieux pour détecter les attaques, les incidents de sécurité et autres événements anormaux;

(e) détecter l'utilisation et l'accès non autorisés à tous les services infonuagiques, données et composants pertinents aux services infonuagiques d'infrastructure-service, de plateforme-service ou de logiciel-service du Canada;

(f) gérer et appliquer les correctifs et les mises à jour liés à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de remédier à

tout problème signalé publiquement dans les services infonuagiques ou les bibliothèques que les services utilisent, et fournir des avis préalables liés aux correctifs conformément aux engagements convenus relatifs au niveau de service;

(g) répondre aux menaces et aux attaques contre les services infonuagiques du fournisseur, les contenir et veiller à la récupération;

(h) au besoin, prendre des contre-mesures proactives, y compris des mesures de prévention et d'intervention permettant d'atténuer les menaces.

(2) Les services infonuagiques de l'entrepreneur doivent permettre de copier les données des applications (infrastructure-service, plateforme-service et logiciel-service) et le trafic réseau (infrastructure-service et plateforme-service) du gouvernement du Canada dans les services infonuagiques hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du gouvernement).

(3) Dans le cas du logiciel-service, les services infonuagiques de l'entrepreneur doivent permettre au Canada de déployer et d'utiliser des logiciels de sécurité pour assurer la surveillance avancée et l'atténuation des cybermenaces pour les services infonuagiques du Canada, pour les composants gérés par le Canada seulement.

24. Gestion des incidents de sécurité

(1) Le processus d'intervention de l'entrepreneur en cas d'incident de sécurité pour les services infonuagiques doit englober le cycle de vie de la gestion des incidents de sécurité des TI et les pratiques de prise en charge des activités de préparation, de détection, d'analyse, de confinement et de reprise. Ce processus comprend ce qui suit :

(a) Un processus d'intervention en cas d'incident de sécurité publié et documenté aux fins d'examen par le Canada, qui est conforme à l'une des normes suivantes : i) ISO/IEC 27035:2011 Technologies de l'information – Techniques de sécurité – Management des incidents liés à la sécurité de l'information; ou ii) NIST SP800-612, Computer Security Incident Handling Guide; ou iii) Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html); ou (iv) autres pratiques exemplaires des principaux fournisseurs de services si le Canada détermine, à sa discrétion, que celles-ci respectent ses exigences en matière de sécurité.

(b) Des processus et des procédures documentés sur la façon dont l'entrepreneur détectera les incidents de sécurité de l'information, y donnera suite, les corrigera, les signalera et en fera part au Canada, notamment : (i) la portée des incidents de sécurité de l'information que l'entrepreneur signalera au Canada; (ii) le niveau de divulgation de la détection des incidents de sécurité de l'information et des réponses associées; (iii) le délai cible dans lequel la notification des incidents de sécurité de l'information aura lieu; (iv) la procédure de notification des incidents de sécurité de l'information; (v) les coordonnées pour le traitement des problèmes liés aux incidents de sécurité de l'information, conformément aux procédures de déclaration décrites dans le PGEC GC (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html); et (vi) tout recours qui s'applique si la sécurité de l'information se produit;

(c) La capacité de l'entrepreneur d'appuyer les efforts d'enquête du Canada dans le cas de toute compromission des utilisateurs ou des données du service relevé;

(d) L'autorisation uniquement des représentants désignés et préautorisés du client (p. ex. le CCC ou d'autres organisations approuvées par le gouvernement du Canada), émise par le responsable technique :

(i) pour demander et recevoir un accès et des renseignements confidentiels en ce qui a trait aux données du client (données des utilisateurs, journaux d'événements du système et de sécurité, saisies de paquets du réseau ou de l'hôte, journaux de composants de sécurité comme des systèmes de détection et de prévention d'intrusion et des pare-feu, etc.), dans un format non chiffré, à des fins de réalisation d'enquêtes;
(ii) pour effectuer le suivi d'un événement signalé lié à la sécurité de l'information.

(e) Des procédures permettant de répondre aux demandes de preuves numériques potentielles ou d'autres renseignements provenant de l'environnement des services infonuagiques et conformes aux normes et bonnes pratiques de l'industrie, notamment la norme ISO 22095:2020 Chaîne de contrôle – Terminologie générale et modèles (https://www.iso.org/fr/standard/72532.html), y compris les procédures médico-légales appropriées et les garanties pour ce qui suit :

(i) Le maintien d'une chaîne de contrôle pour les renseignements sur la vérification;
(ii) La collecte, la conservation et la présentation de preuves démontrant l'intégrité des preuves;

(2) Un document décrivant le processus de réponse aux incidents de sécurité de l'entrepreneur, y compris les coordonnées. L'entrepreneur doit fournir ce document dans les 10 jours suivant la date d'entrée en vigueur du contrat. Ce processus, y compris les coordonnées, doit rester à jour et, au minimum, être validé sur une base annuelle et être approuvé par le Canada.

(3) L'entrepreneur doit :

(a) Travailler avec le ou les centres des opérations de sécurité (COS) du Canada (p. ex. le COS du gouvernement du Canada, les équipes ministérielles de sécurité des TI) et les principaux intervenants du PGEC GC (c.-à-d. le CCC et le Secrétariat du Conseil du Trésor du Canada), sur le confinement des incidents de sécurité, leur éradication et le rétablissement, conformément au processus d'intervention en cas d'incident de sécurité et le PGEC GC (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html);

(b) Tenir un registre des violations de la sécurité comprenant une description de la violation, la période, les conséquences de la violation, le nom de la personne ayant signalé la violation et celui de la personne à qui la violation a été signalée, la procédure pour rétablir les données ou le service, et des enregistrements d'activités liées à la gestion de l'incident de sécurité, y compris les communications internes et externes (p. ex. dans le cas d'un logiciel de rançon, toutes les communications, y compris les demandes de rançon, etc.). Cette information doit être fournie au Canada sur demande;

(c) Assurer le suivi, ou permettre au Canada d'assurer le suivi, des divulgations de données canadiennes, y compris les données qui ont été divulguées, à qui, et à

quel moment.

(4) Dans le cadre des enquêtes de sécurité, le Canada peut exiger des preuves médico-légales de la part de l'entrepreneur pour contribuer à une enquête du gouvernement du Canada. L'entrepreneur doit :

(a) conserver les rapports d'enquête liés à une enquête de sécurité pendant une période de deux ans après la fin de l'enquête ou les fournir au Canada à des fins de conservation;

(b) fournir un soutien d'enquête raisonnable aux représentants désignés et préautorisés du Canada tels que le CCC et la Gendarmerie royale du Canada;

(c) maintenir la chaîne de contrôle des preuves conformément aux pratiques exemplaires comme celles décrites dans la norme ISO 22095:2020;

(d) prendre en charge l'investigation électronique;

(e) maintenir des mises en suspens pour des raisons juridiques afin de répondre aux besoins des enquêtes et des demandes judiciaires.

(5) Si l'entrepreneur fait appel à une entreprise externe dans le cadre de ses activités d'intervention en cas d'incident, il doit s'assurer que les dispositions de la section 24 – Gestion des incidents de sécurité et de la section 25 – Intervention en cas d'incident de sécurité s'appliquent également à l'équipe externe d'intervention en cas d'incident et qu'elles sont documentées dans le processus de l'entrepreneur.

25. Intervention en cas d'incident de sécurité

(1) L'entrepreneur doit alerter et aviser promptement le Canada (par téléphone ou par courriel), conformément aux procédures de rapport du paragraphe (25), de toute compromission, de toute violation ou de toute preuve comme i) un incident de sécurité, ii) une défectuosité liée à la sécurité d'un actif, iii) l'accès irrégulier ou non autorisé à un actif, iv) la copie à grande échelle d'un actif d'information ou v) toute autre activité illégale recensée par l'entrepreneur, portant ce dernier à croire de manière raisonnable que le risque de compromission, d'atteinte à la sécurité ou à la vie privée est ou pourrait être imminent, ou si les mesures de protection existantes ont cessé de fonctionner, au cours de la période suivante (tous les jours, 24 heures par jour, 365 jours par année), et sans tarder, dans tous les cas, dans les 72 heures, et conformément aux engagements convenus relatifs au niveau de service.

(2) Si l'entrepreneur prend connaissance d'une compromission ou violation de la sécurité entraînant accidentellement ou illégalement la destruction, la perte, l'altération, la divulgation non autorisée des données ou l'accès aux données du client ou à des données personnelles pendant le traitement par l'entrepreneur (chacun étant un « incident de sécurité »), l'entrepreneur doit rapidement et sans tarder (i) informer le Canada de cet incident de sécurité; (ii) mener une enquête et fournir au Canada des renseignements détaillés sur cet incident de sécurité; (iii) prendre les mesures nécessaires pour en atténuer les causes et minimiser les dommages découlant de l'incident de sécurité.

(3) L'entrepreneur doit signaler les incidents majeurs aux services de police compétents à la demande du Canada.

26. Fuite d'information

(1) L'entrepreneur doit avoir un processus documenté qui énonce son approche en cas d'incident de fuite d'information. Le processus doit être harmonisé avec i) les directives de la section IR-9 intitulée « Intervention en cas de fuite d'information » du

document ITSG-33, ou ii) une autre pratique exemplaire du secteur approuvée par écrit par le Canada. Nonobstant ce qui précède, le processus d'intervention en cas de fuite d'information de l'entrepreneur doit comprendre, à tout le moins :

(a) un processus d'identification des éléments de données précis utilisés dans la contamination d'un système;

(b) un processus visant à isoler et à éradiquer un système contaminé;

(c) un processus d'identification des systèmes pouvant avoir été subséquemment contaminés et toute autre mesure prise pour empêcher la propagation de la contamination.

(2) À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit le processus d'intervention en cas de fuite d'information de l'entrepreneur.

27. Essais de sécurité et validation

(1) L'entrepreneur doit disposer d'un processus qui permet d'effectuer une analyse de vulnérabilité ou un essai de pénétration non perturbateur et non destructif visant le service infonuagique qui héberge les données du Canada. Ceci comprend la capacité de réaliser régulièrement des analyses internes et externes du nuage du gouvernement du Canada, et lorsque des modifications importantes sont apportées à la plateforme principale, la capacité de détecter toute vulnérabilité potentielle du système liée à la location du Canada au moyen :

(i) d'analyses de vulnérabilité;
(ii) d'analyses d'application Web;
(iii) d'essais de pénétration.

(2) L'entrepreneur doit mettre en place un plan d'action et des jalons afin de consigner les mesures correctives qu'il envisage de prendre pour corriger les faiblesses ou les lacunes de la plateforme principale, afin de réduire et d'éliminer les vulnérabilités du système, ou celles qui pourraient être liées aux services infonuagiques où sont hébergées et utilisées les données du Canada dans le cadre de sa location.

(3) À la demande du Canada, l'entrepreneur doit fournir les résultats des essais réalisés sur la plateforme, ainsi que le plan d'action et les documents sur les jalons, à des fins de planification et d'examen.

(4) L'entrepreneur doit offrir la possibilité de mettre en place un outil libre-service de vérification de l'état de la sécurité ou un outil de notation qui permet de mesurer la posture de sécurité des services infonuagiques configurés par le Canada

28. Filtrage de sécurité du personnel

(1) L'entrepreneur doit mettre en place des mesures de sécurité qui permettent d'accorder et de maintenir le niveau de filtrage de sécurité requis pour le personnel de l'entrepreneur engagé dans la fourniture de services d'infonuagique et le personnel des sous-traitants en fonction de leurs privilèges d'accès aux biens des systèmes d'information sur lesquels les données du Canada sont stockées et traitées.

(2) Les mesures de contrôle de l'entrepreneur doivent être appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs- sct.canada.ca/pol/doc- fra.aspx?id=28115), ou utiliser un équivalent acceptable convenu par le Canada.

(3) À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit le processus de filtrage de sécurité du personnel de l'entrepreneur. Le processus doit offrir au minimum :

(a) une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux données du client ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services infonuagiques;

(b) une description des activités et des pratiques de filtrage de sécurité, y compris les procédures de notification qui doivent être suivies si le filtrage n'a pas été achevé ou si les résultats causent des doutes ou des préoccupations;

(c) une description de la sensibilisation et la formation en matière de sécurité dans le cadre de l'intégration à l'emploi, lorsque les rôles des employés et des sous-traitants changent, et de façon continue, pour s'assurer que les employés et les sous-traitants connaissent, comprennent et respectent leurs responsabilités en matière de sécurité de l'information;

(d) une description du processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi;

(e) l'approche de détection et d'atténuation des menaces internes potentielles et les contrôles de sécurité mis en œuvre pour atténuer le risque d'accès aux données du gouvernement du Canada ou de dommage à la fiabilité des services infonuagiques hébergeant les données du Canada.

29. Sécurité matérielle (centre des données et installations)

(1) L'entrepreneur doit mettre en place des mesures de sécurité matérielle qui assurent la protection des installations de TI et des biens du système d'information dans lesquels les données du Canada sont stockées et protégées contre toute forme de manipulation, de perte, de dommage et de saisie. Des mesures de protection physique visant toutes les installations qui abritent des données du MDN doivent être appliquées conformément à une approche fondée sur les risques reposant sur la prévention, la détection, l'intervention et la récupération en matière de sécurité physique ou utiliser une telle approche, conformément aux mesures de contrôle et aux pratiques en matière de sécurité physique figurant dans la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor (https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=12329). Les mesures de sécurité exigées en vertu de cette disposition comprennent, à tout le moins :

(i) des capacités suffisantes de redondance et de reprise dans les installations de l'entrepreneur et entre celles-ci, qui sont suffisamment disparates sur le plan géographique pour que la perte d'une installation n'empêche pas la récupération des données et des données du Canada conformément aux engagements sur les niveaux de service convenus;

(ii) l'utilisation adéquate des supports de TI;

(iii) le contrôle de la maintenance de tous les systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue;

(iv) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada;

(v) la restriction de l'accès physique aux données du Canada et aux emplacements de services infonuagiques au personnel de service autorisé en fonction du poste ou du rôle et du principe du besoin d'accès, validé par deux formes d'identification;

(vi) l'escorte des visiteurs et la surveillance de leurs activités;

(vii) l'application de mesures de protection des données du gouvernement du Canada à d'autres lieux de travail (p. ex. les sites de télétravail);

(viii) la consignation et la surveillance de tous les accès physiques aux points de service et de tous les accès par voie électronique aux systèmes qui hébergent les données du Canada, au moyen d'une combinaison de registres d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions;

(ix) la réalisation de vérifications de sécurité continues à la limite des emplacements de service et des installations afin de détecter toute exfiltration interdite d'information ou de composantes du système.

(2) À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit les mesures de sécurité matérielle de l'entrepreneur.

(3) L'entrepreneur doit aviser le Canada de tout changement apporté aux mesures de sécurité matérielle qui pourrait nuire de manière importante à la sécurité matérielle.

30. Gestion des risques liés à la chaîne d'approvisionnement

(1) L'entrepreneur doit prendre des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services infonuagiques. En font notamment partie la protection tout au long du cycle de développement des systèmes par la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement; la sensibilisation aux cybermenaces, l'éducation des effectifs d'approvisionnement sur les menaces, les risques et les contrôles de sécurité requis; et l'exigence que les entités de la chaîne d'approvisionnement mettent en œuvre les mesures de sécurité nécessaires.

(2) L'entrepreneur doit avoir une approche de gestion des risques de la chaîne d'approvisionnement (GRCA), dont un plan de GRCA qui est conforme à l'une des pratiques exemplaires suivantes :

(i) ISO/IEC 27 036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4);

(ii) NIST Special Publication 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations;

(iii) Contrôle de sécurité ITSG-33 pour SA-12 lorsque les garanties de sécurité définies sont documentées dans un plan de gestion des risques liés à la chaîne d'approvisionnement.

(3) Dans les 90 jours suivant l'attribution du contrat, l'entrepreneur doit :

(a) présenter une preuve confirmant que l'approche et le plan de GRCA ont été évalués et validés par un tiers indépendant certifié selon les exigences de l'AICPA, de CPA Canada ou du régime de certification ISO;

OU

(b) présenter au Canada une copie du plan de GRCA, annuellement ou sur demande du Canada.

(4) Dans les cas où l'entrepreneur est un fournisseur de logiciel-service utilisant un fournisseur d'infrastructure-service approuvé par le GC qui se conforme déjà aux exigences de l'article 31 – Exigences relatives à la gestion des risques de la chaîne d'approvisionnement, dans les 90 jours suivant l'attribution du contrat, le fournisseur de logiciel-service utilisant un fournisseur d'infrastructure-service approuvé par le GC doit fournir dans les 90 jours suivant l'attribution du contrat une liste de produits de technologie de communication de l'information (TCI) qui décrit l'équipement de TCI déployé dans l'environnement d'infrastructure-service approuvé par le GC pour un examen de l'intégrité de la chaîne d'approvisionnement.
Cet examen sera effectué au plus tôt tous les trois ans.

31. Sous-traitants

(1) L'entrepreneur doit fournir une liste de sous-traitants auxquels il pourrait faire appel pour exécuter n'importe quelle partie des travaux en fournissant le service au Canada. La liste doit comprendre les renseignements suivants : (i) le nom du sous-traitant; (ii) la description des travaux qui seraient exécutés par le sous-traitant; et (iii) les emplacements où le sous-traitant exécuterait les travaux.

(2) L'entrepreneur doit fournir une liste des sous-traitants dans les dix jours suivant la date d'entrée en vigueur du contrat. Le fournisseur doit informer le Canada (en mettant à jour le site Web et en fournissant au client un mécanisme lui permettant d'obtenir un avis lié à cette mise à jour) de tout nouveau sous-traitant au moins 14 jours avant de fournir aux sous-traitants l'accès aux données du client ou aux données personnelles. Le fournisseur doit aider le Canada à mener les vérifications visant les sous-traitants dans les dix jours ouvrables.

32. Programme de sécurité industrielle – Exigences relatives à la sécurité pour les fournisseurs canadiens

(1) L'entrepreneur ou l'offrant doit détenir en tout temps pendant l'exécution du contrat, de l'offre à commandes ou de l'accord d'approvisionnement une vérification d'organisation désignée valide avec une cote de protection des documents approuvée au niveau « PROTÉGÉ A ou B » (selon les besoins) délivrée par le Programme de sécurité des contrats (PSC) de SPAC.

(2) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens de niveau « PROTÉGÉ », ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau « SECRET », délivrée ou approuvée par le PSC de SPAC.

(3) L'entrepreneur NE DOIT PAS utiliser ses systèmes de TI pour traiter, produire ou stocker électroniquement des renseignements protégés tant qu'il n'en a pas reçu l'approbation écrite par le responsable de la sécurité du ministère client. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau « PROTÉGÉ A ou B » (selon les besoins), avec lien électronique au niveau pertinent.

(4) L'entrepreneur ne peut pas accorder de contrat de sous-traitance comportant des exigences relatives à la sécurité sans l'autorisation écrite préalable du PSC de SPAC.

(5) L'entrepreneur ou l'offrant doit respecter les dispositions des documents suivants :

(a) LVERS et guide de sécurité (s'il y a lieu), reproduits ci-joint à l'annexe M;

(b) Manuel de la sécurité des contrats (dernière édition);

(c) Exigences de sécurité des contrats du gouvernement du Canada, à l'adresse https://www.tpsgc-pwgsc.gc.ca/esc- src/index-fra.html (site Web du PSC).

REMARQUE : Il y a des niveaux multiples de contrôle de sécurité du personnel associé à ce dossier. Dans le cas présent, un guide de sécurité doit être ajouté à la LVERS afin de clarifier ces niveaux d'enquête de sécurité. Le guide de sécurité est normalement rédigé par le chargé de projet ou le responsable de la sécurité de l'organisation.

33. Programme de sécurité industrielle – Exigences relatives à la sécurité pour les fournisseurs étrangers

L'administration désignée en matière de sécurité canadienne (ADS canadienne) pour les questions de sécurité industrielle au Canada est le Secteur de la sécurité industrielle, SPAC, administrée par la Direction de la sécurité industrielle internationale, SPAC. L'ADS canadienne est chargée d'évaluer la conformité des **entrepreneurs** et des **sous-traitants** aux exigences en matière de sécurité pour les fournisseurs étrangers. Les exigences suivantes en matière de sécurité s'appliquent aux **entrepreneurs** et **sous-traitants** étrangers destinataires constitués en société ou autorisés à faire des affaires dans un État autre que le Canada et qui livrent ou exécutent à l'extérieur du Canada les services infonuagiques décrits dans les solutions d'infonuagique, en plus des exigences en matière de confidentialité et de sécurité. Ces exigences en matière de sécurité s'ajoutent aux exigences figurant dans la section intitulée Protection et sécurité des données stockées dans des bases de données.

(1) L'entrepreneur ou le sous-traitant atteste que la livraison et la prestation des services infonuagiques prévus par le présent contrat doit provenir d'un pays membre de l'Organisation du Traité de l'Atlantique Nord, de l'Union européenne ou d'un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité. Dans le cadre du PSC, des accords internationaux bilatéraux en matière de sécurité ont été conclus avec les pays énumérés sur la page https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html de SPAC. La liste est mise à jour périodiquement.

(2) L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit en tout temps, au cours de la durée du **contrat** ou du **contrat de sous-traitance**, être inscrit auprès de l'autorité nationale de supervision appropriée des pays dans lesquels il est constitué en société, exerce ses activités et est autorisé à faire des affaires. Il doit fournir à l'autorité contractante et à l'ADS canadienne la preuve de son inscription auprès de l'autorité de surveillance compétente.

(3) L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit fournir une preuve qu'il est constitué en société ou autorisé à faire affaire sur son territoire de compétence.

(4) L'entrepreneur étranger destinataire ne doit pas entreprendre les travaux, fournir les services ou assurer toute autre prestation tant que l'ADS canadienne n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le contrat. L'ADS canadienne fournira, par écrit, à l'entrepreneur étranger destinataire un formulaire d'attestation qui confirmera la conformité et l'autorisation de fournir les services prévus.

(5) L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit désigner un agent de sécurité des contrats autorisé et un agent remplaçant de sécurité des contrats, au besoin, qui sera responsable du contrôle des exigences relatives à la sécurité, telles qu'elles sont définies dans le présent contrat. Cette personne sera nommée par le président-directeur général de l'**entrepreneur** ou du **sous-traitant** étranger destinataire qui présente une soumission ou par un cadre supérieur principal désigné, qui est soit propriétaire, dirigeant, agent, administrateur, directeur ou partenaire, et qui occupe un poste qui lui permettrait d'influer de manière négative sur les politiques ou les pratiques de l'organisation dans l'exécution du contrat.

(6) L'**entrepreneur** ou le **sous-traitant** ne doit pas accorder l'accès à des renseignements ou des biens de niveau **« PROTÉGÉ B » AU CANADA**, sauf aux membres du personnel qui ont un besoin de savoir pour l'exécution du contrat et qui ont fait l'objet d'une vérification de sécurité conformément à la définition et aux

pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.canada.ca/pol/doc- fra.aspx?id=28115), ou qui utilisent des mesures équivalentes acceptables convenues par le Canada.

(7) L'information et les biens de niveau **« PROTÉGÉ » AU CANADA** fournis à l'**entrepreneur** ou au **sous-traitant** étranger destinataire ou produits par l'**entrepreneur** ou **sous-traitant** destinataire étranger :

i. ne doivent pas être divulgués à un autre gouvernement, à une autre personne ou à une autre entreprise ou à un représentant de l'un ou de l'autre qui ne soit pas directement lié à l'exécution du **contrat**, sans l'autorisation écrite préalable du gouvernement. Ce consentement doit être obtenu auprès de l'ADS canadienne en collaboration avec l'autorité contractante;

ii. ne doivent pas servir à un but autre que l'exécution du contrat sans l'approbation écrite préalable du Canada. Cette approbation doit être obtenue auprès de l'autorité contractante (en collaboration avec l'ADS canadienne).

(8) L' **entrepreneur** ou le **sous-traitant** étranger destinataire NE DOIT PAS emporter de renseignements ou de biens de niveau **« PROTÉGÉ » AU CANADA** hors des lieux de travail visés, et l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.

(9) L'**entrepreneur** ou le **sous-traitant** étranger destinataire ne doit pas utiliser les renseignements ni les biens de niveau **« PROTÉGÉ » AU CANADA** dans un but autre que l'exécution du **contrat** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS canadienne.

(10) L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit détenir en permanence, pendant l'exécution du **contrat**, une autorisation de détenir des renseignements approuvée de niveau **« PROTÉGÉ B » AU CANADA**.

(11) L'entrepreneur étranger destinataire doit signaler immédiatement à l'ADS canadienne tous les cas connus ou soupçonnés où des renseignements et des biens de niveau « PROTÉGÉ » AU CANADA dans le cadre du présent contrat auraient été compromis.

(12) L'entrepreneur étranger destinataire doit assurer une protection des renseignements et biens de niveau « PROTÉGÉ » AU CANADA aussi stricte que celle assurée par le gouvernement du Canada, conformément aux politiques nationales ainsi qu'aux lois et règlements en matière de sécurité nationale, et dans le respect des prescriptions prévues par l'ADS canadienne.

(13) À la fin des travaux, l'entrepreneur étranger destinataire doit remettre au gouvernement du Canada tous les renseignements et biens de niveau « PROTÉGÉ » AU CANADA fournis ou produits en vertu du contrat, y compris tous les renseignements et biens de niveau « PROTÉGÉ » AU CANADA remis à ses sous-traitants ou produits par eux.

(14) L'entrepreneur étranger destinataire qui doit accéder à des renseignements ou à des biens de niveau « PROTÉGÉ » AU CANADA ou à des sites à accès restreint au Canada, en vertu du présent contrat, doit présenter une demande pour l'accès au site au chef de la sécurité de [nom du ministère ou de l'organisation] Canada.

(15) L'entrepreneur étranger destinataire NE DOIT PAS utiliser ses systèmes de

technologie de l'information pour traiter, produire ou stocker dans un système informatique (et transférer au moyen d'un lien électronique) des renseignements de niveau « PROTÉGÉ B » AU CANADA avant que l'ADS canadienne lui en donne le droit.

(16) Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE DOIVENT PAS être attribués sans qu'on ait obtenu au préalable l'autorisation écrite de l'ADS canadienne.

(17) Tous les contrats de sous-traitance attribués à un entrepreneur étranger destinataire ne doivent PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne afin de confirmer les exigences de sécurité à imposer aux sous-traitants.

(18) Tous les contrats de sous-traitance attribués par un entrepreneur étranger destinataire ne doivent PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne afin de confirmer les exigences de sécurité à imposer aux sous-traitants.

(19) L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit se conformer aux dispositions de la LVERS figurant à l'annexe M.

(20) Malgré tout article des conditions générales relatif à la sous-traitance, l'entrepreneur étranger destinataire ne peut confier à un sous-traitant (y compris à une société affiliée) aucune fonction qui permet d'accéder aux données du contrat sans le consentement écrit préalable de l'autorité contractante (en collaboration avec l'ADS canadienne).

(21) Le Canada a le droit de rejeter toute demande présentée de manière distincte et indépendante de l'autorisation contenue dans le présent contrat relativement à l'autorisation de l'entrepreneur qui fournit les services infonuagiques d'accéder, de traiter, de produire, de transmettre ou de stocker électroniquement des données de niveau **« PROTÉGÉ » AU CANADA** dans tout autre pays s'il y a lieu de craindre pour la sécurité, la confidentialité ou l'intégrité des renseignements.

Partie 2 – Obligations en matière de confidentialité pour le niveau 2 (jusqu'au niveau « Protégé A », inclusivement)

1. Généralités

1.1 *Objet*

La présente partie a pour objet d'énoncer les obligations de l'entrepreneur en matière de confidentialité en ce qui a trait à l'utilisation, à la collecte, au traitement, à la transmission, au stockage ou à l'élimination des données du Canada qui contiennent des renseignements personnels. Tous les renseignements personnels qui sont stockés dans les systèmes de l'entrepreneur ou que l'entrepreneur est tenu de gérer (recueillir, conserver, utiliser, divulguer et supprimer) doivent être protégés à tout moment par la mise en œuvre de mesures de protection administratives, matérielles et techniques qui sont nécessaires pour assurer la protection des renseignements personnels selon un niveau correspondant à l'ampleur des préjudices pouvant résulter de l'atteinte à la vie privée, conformément à l'entente sur la gestion des données de l'entrepreneur, à la présente partie et aux mesures particulières de l'entrepreneur en matière de confidentialité (collectivement, les « **obligations en matière de confidentialité** »).

1.2 *Transfert des obligations en matière de confidentialité*

Les obligations de l'entrepreneur contenues dans les présentes obligations en matière de confidentialité doivent être transférées par l'entrepreneur aux sous-traitants, le cas échéant.

2. Reconnaissance

Les parties reconnaissent que :

(a) toutes les données du Canada qui contiennent des renseignements personnels sont assujetties à ces obligations en matière de confidentialité.

(b) nonobstant toute autre disposition de la présente partie, les parties partagent la responsabilité de l'élaboration et du maintien des politiques, des procédures et des contrôles de confidentialité relatifs aux données du Canada.

(c) l'entrepreneur ne doit pas avoir ou tenter d'obtenir la garde de données du Canada, ni permettre à un membre du personnel de l'entrepreneur d'accéder aux données du Canada avant la mise en œuvre des obligations en matière de confidentialité, comme l'exige la présente partie, au plus tard à la date de l'attribution du contrat.

3. Propriété des données

(1) Le Canada demeurera en tout temps le contrôleur des renseignements personnels traités par l'entrepreneur dans le cadre du contrat. Le Canada doit veiller à respecter ses obligations en matière de confidentialité à titre de contrôleur en vertu des lois applicables sur la protection des données, particulièrement pour justifier la transmission de renseignements personnels à l'entrepreneur (cela comprend de fournir tout avis requis et de recueillir toute autorisation ou tout consentement requis, ou autrement d'obtenir un fondement juridique convenable en vertu des lois applicables sur la protection des données), et les décisions et mesures du Canada en ce qui concerne le traitement de telles données personnelles.

(2) L'entrepreneur est un agent de traitement et le demeurera à tout moment en ce qui concerne les données concernant des renseignements personnels fournies à l'entrepreneur par le Canada dans le cadre du contrat. L'entrepreneur est responsable de respecter ses obligations en vertu de l'entente sur la gestion des données de l'entrepreneur ainsi que de respecter ses obligations à titre d'agent de traitement en vertu des lois applicables sur la confidentialité (p. ex. *Loi sur la protection des renseignements personnels et les documents électroniques*).

(3) L'entrepreneur doit s'abstenir d'utiliser ou d'autrement traiter les données du Canada qui contiennent des renseignements personnels ou d'en tirer de l'information à des fins de partage des données, publicitaires ou commerciales semblables. Entre les parties, le Canada conserve tous les droits, titres et intérêts relatifs aux données clients. L'entrepreneur n'acquiert aucun droit sur les données du client, à l'exception des droits que le client accorde à l'entrepreneur afin de fournir les services infonuagiques au client.

(4) Toutes les données qu'il stocke, héberge ou traite au nom du Canada demeurent la propriété du Canada.

4. Demandes de renseignements personnels

(1) Le Canada et l'entrepreneur doivent établir selon des conditions mutuellement acceptables un processus de traitement des demandes de communication de dossiers en vertu de la *Loi sur l'accès à l'information* ainsi que des demandes d'accès aux renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels* (demandes d'accès).

5. Assurance d'une tierce partie : Certifications

(1) L'entrepreneur doit s'assurer, à l'égard des renseignements personnels contenus dans les données du Canada qu'il peut héberger, stocker ou traiter, que l'infrastructure de l'entrepreneur (y compris tout service d'infrastructure-service, de plateforme-service ou de logiciel-service fourni au Canada) et les emplacements de service sont protégés par des mesures de sécurité et de confidentialité appropriées et qui respectent les exigences établies dans les pratiques et politiques en matière de confidentialité de l'entrepreneur.

(2) L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications suivantes en présentant des rapports d'évaluation ou des certifications de tierce partie indépendante pour chaque niveau de service (p. ex. infrastructure-service, plateforme-service, logiciel-service) au sein des services infonuagiques, y compris :

(a) ISO/IEC 27018:2014 Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables dans l'informatique en nuage public agissant comme processeur de ces informations – Certification obtenue par un organisme de certification accrédité.

(3) Chaque certification présentée doit :

(i) indiquer la dénomination commerciale officielle de l'entrepreneur ou du sous-traitant concerné;
(ii) déterminer la date de certification de l'entrepreneur ou du sous-traitant et le statut de cette certification.

6. Conformité aux exigences en matière de confidentialité

(1) L'entrepreneur doit démontrer, au moyen de rapports d'évaluation et de rapports de vérification de tiers, qu'il :

(a) limite la création, la collecte, la réception, la gestion, l'accès, l'utilisation, la conservation, l'envoi, la communication et l'élimination des renseignements personnels à ce qui est nécessaire pour la prestation des services infonuagiques;

(b) a mis en œuvre des processus et des contrôles de sécurité à jour tels que les contrôles de gestion de l'accès, la sécurité des ressources humaines, la cryptographie et la sécurité physique, opérationnelle et des communications qui préservent l'intégrité, la confidentialité et l'exactitude de toutes les informations, données et métadonnées, peu importe leur format.

7. Protection de la confidentialité dès la conception

L'entrepreneur doit démontrer qu'il met en œuvre une confidentialité par conception au cours du cycle de vie du développement de son logiciel, conformément à la partie 1 – Obligations en matière de sécurité, article 16 (développement sécurisé).

8. Atteinte à la vie privée

(1) L'entrepreneur doit rapidement évaluer les incidents qui éveillent des soupçons, qui indiquent un accès non autorisé aux renseignements personnels ou le traitement de ceux-ci (« **incident** ») et y répondre. Dans la mesure où :

l'entrepreneur a connaissance d'un incident et qu'il établit que celui-ci constitue une atteinte à la vie privée entraînant le détournement ou la destruction, la perte, la modification, la divulgation non autorisée ou l'accès accidentel ou illégal aux renseignements personnels transmis, stockés ou traités dans les systèmes de l'entrepreneur ou dans l'environnement des services infonuagiques de façon à compromettre la sécurité, la confidentialité ou l'intégrité de ces renseignements personnels (« atteinte aux renseignements personnels »), l'entrepreneur avisera le Canada sans délai de l'atteinte aux renseignements personnels, conformément à l'article 26 de la partie 1 – Obligations en matière de sécurité.

(2) L'entrepreneur doit :

(a) assurer le suivi, ou permettre au Canada d'assurer le suivi, des divulgations de données canadiennes, y compris les données qui ont été divulguées, à qui, et à quel moment.

9. Renseignements personnels

Les sous-sections suivantes s'appliquent dans les cas où l'entrepreneur confirme qu'il détient l'accès, la garde et le contrôle des données du Canada.

9.1 Propriété des renseignements personnels et des dossiers

9.1.1 Pour exécuter les services infonuagiques, l'**entrepreneur** ou le **sous-traitant** étranger destinataire se verra remettre ou recueillera des renseignements personnels de tiers. L'**entrepreneur** ou le **sous-traitant** étranger destinataire reconnaît qu'il n'a aucun droit sur ces renseignements personnels ou dossiers et que ces derniers appartiennent au Canada. L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit rendre disponibles, sur demande du Canada, tous les renseignements personnels et dossiers dans un format acceptable pour le Canada.

9.2 Utilisation des renseignements personnels

9.2.1 L'**entrepreneur** ou le **sous-traitant** étranger destinataire convient de créer, de recueillir, de recevoir, de gérer, d'utiliser et de conserver des renseignements personnels et des dossiers de même que d'y avoir accès et d'en disposer uniquement pour exécuter les services infonuagiques conformément au **contrat**.

9.3 Collecte de renseignements personnels

9.3.1 Si l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit obtenir des renseignements personnels d'un tiers dans le cadre des services infonuagiques, il ne

doit recueillir que les renseignements personnels lui permettant d'exécuter les services infonuagiques. L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit recueillir les renseignements personnels auprès de l'individu concerné et l'informer (au moment de la collecte ou préalablement) de ce qui suit :

9.3.1.1 les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;

9.3.1.2 les usages qui seront faits des renseignements personnels recueillis;

9.3.1.3 la divulgation des renseignements personnels est volontaire ou, s'il existe une obligation juridique de divulguer les renseignements personnels, les fondements de cette obligation juridique;

9.3.1.4 les conséquences, le cas échéant, du refus de fournir les renseignements;

9.3.1.5 l'individu a le droit de consulter et de corriger les renseignements personnels le concernant;

9.3.1.6 les renseignements personnels feront partie d'un fichier de renseignements personnels particulier (au sens de la *Loi sur la protection des renseignements personnels*), et fournir à l'individu de l'information concernant l'institution fédérale qui gère le fichier de renseignements personnels, si l'autorité contractante a fourni ces renseignements à l'**entrepreneur** ou au **sous-traitant** étranger destinataire.

9.3.2 L'**entrepreneur** ou le **sous-traitant** étranger destinataire et leurs employés respectifs doivent s'identifier auprès des individus desquels ils recueillent des renseignements personnels et leur donner le moyen de vérifier qu'ils sont autorisés à recueillir les renseignements personnels conformément à un contrat passé avec le Canada.

9.3.3 Si l'autorité contractante l'exige, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit élaborer un formulaire de demande de consentement à utiliser lors de la collecte de renseignements personnels ou un texte dans le cas de la collecte de renseignements personnels par téléphone. L'**entrepreneur** ou le **sous-traitant** étranger destinataire ne peut utiliser le formulaire ou le texte sans avoir obtenu l'approbation écrite préalable de l'autorité contractante. Il doit aussi obtenir le consentement de l'autorité contractante avant de modifier le formulaire ou le texte.

9.3.4 Si, au moment de la collecte de renseignements personnels auprès d'un individu, l'**entrepreneur** ou le **sous-traitant** étranger destinataire soupçonne que cet individu n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit demander des directives à l'autorité contractante.

9.4 Exactitude, confidentialité et intégrité des renseignements personnels

9.4.1 L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit veiller à ce que les renseignements personnels soient aussi exacts, complets et à jour que possible. L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit veiller à protéger la confidentialité des renseignements personnels. À cette fin, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit au moins :

9.4.1.1 ne pas utiliser de données d'identification personnelle (p. ex. le numéro d'assurance sociale) pour lier de nombreuses bases de données qui comprennent des renseignements personnels;

9.4.1.2 isoler tous les dossiers des renseignements et des dossiers de l'**entrepreneur** ou du **sous-traitant** étranger destinataire;

9.4.1.3 ne donner l'accès aux renseignements personnels et aux dossiers qu'aux personnes qui en ont besoin aux fins d'exécution des services infonuagiques (par exemple, en utilisant des mots de passe ou un accès biométrique);

9.4.1.4 donner de la formation à toute personne à laquelle l'**entrepreneur** ou le **sous-traitant** étranger destinataire donne accès aux renseignements personnels concernant l'obligation d'assurer la confidentialité et de ne l'utiliser qu'aux fins de l'exécution des services infonuagiques.

L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit donner cette formation avant d'autoriser l'accès aux renseignements personnels et préparer à cet effet un dossier accessible à l'autorité contractante, sur demande;

9.4.1.5 à la demande de l'autorité contractante, demander aux personnes ayant accès aux renseignements personnels de reconnaître, par écrit (sous une forme approuvée par l'autorité contractante), leurs responsabilités en matière de confidentialité des renseignements personnels, avant de leur en donner l'accès;

9.4.1.6 garder un registre de toutes les demandes faites par un individu pour la révision de ses renseignements personnels et toutes les demandes de correction d'erreurs ou d'omissions concernant les renseignements personnels (que les demandes soient faites directement par un individu ou par le Canada au nom d'un individu);

9.4.1.7 joindre une note à tout dossier qu'un individu a demandé de corriger, mais que l'**entrepreneur** ou le **sous-traitant** étranger destinataire a décidé, pour quelque raison que ce soit, de ne pas corriger. Lorsque cela se produit, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit immédiatement informer l'autorité contractante de la correction demandée et des raisons de l'**entrepreneur** ou du **sous-traitant** étranger destinataire de ne pas l'effectuer. Si l'autorité contractante demande que la correction soit effectuée, l'entrepreneur a l'obligation de le faire;

9.4.1.8 garder un registre de la date et de l'auteur de la dernière mise à jour de chaque dossier;

9.4.1.9 maintenir un journal de vérification électronique qui enregistre tous les accès et les tentatives d'accès des dossiers électroniques. Le journal de vérification doit être dans un format qui peut être lu par l'**entrepreneur** ou le **sous-traitant** étranger destinataire et le Canada en tout temps;

9.4.1.10 sécuriser et contrôler l'accès à tout exemplaire papier des dossiers.

9.5 Protection des renseignements personnels

9.5.1 L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit protéger les renseignements personnels à tout moment en prenant toutes les mesures raisonnablement nécessaires pour les protéger et en protéger l'intégrité et la confidentialité, conformément aux mesures de sécurité décrites à la partie 1 – Obligations en matière de sécurité.

9.6 Obligations législatives

9.6.1 L'**entrepreneur** ou le **sous-traitant** étranger destinataire reconnaît que le Canada est tenu de traiter tous les renseignements personnels et les dossiers conformément aux dispositions de la *Loi sur la protection des renseignements personnels*, L.R.C. 1985, ch. P-21, de la *Loi sur l'accès à l'information*, L.R.C. 1985, ch. A-1 et de la *Loi sur la Bibliothèque et les Archives du Canada*, L.C. 2004, ch. 11. L'**entrepreneur** ou le **sous-traitant** étranger destinataire convient de se conformer aux exigences établies par l'autorité contractante qui sont requises pour permettre au Canada de remplir ses obligations en vertu de ces lois et de toute autre loi qui entre en vigueur lorsqu'il y a lieu.

9.6.2 L'**entrepreneur** ou le **sous-traitant** étranger destinataire reconnaît que les obligations dont il doit s'acquitter en vertu du **contrat** s'ajoutent à toutes celles qui lui incombent en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, ou d'une loi similaire en vigueur dans une province ou un territoire du Canada. Si l'**entrepreneur** ou le **sous-traitant** étranger destinataire croit que l'une ou l'autre des obligations du **contrat** l'empêche de respecter ses obligations en vertu de ces lois, il doit immédiatement aviser l'autorité contractante de la disposition particulière du **contrat** et de l'obligation particulière prévue par la loi qui lui semble contraire.

9.7 Obligation juridique de divulguer les renseignements personnels

9.7.1 Si l'entrepreneur reçoit une assignation ou une ordonnance judiciaire, administrative ou arbitrale de la part d'un organisme exécutif ou administratif, d'un organisme de réglementation ou de toute autre instance gouvernementale en ce qui concerne le traitement des renseignements personnels (« demande de divulgation »), il transférera rapidement cette demande de divulgation au Canada sans y répondre, sauf disposition contraire des lois applicables (notamment dans le cas d'un accusé de réception qui doit être fourni à l'autorité qui a fait la demande de divulgation).

9.7.2 À la demande du Canada, l'entrepreneur fournira au Canada des renseignements raisonnables en sa possession qui pourraient répondre à la demande de divulgation, ainsi que toute aide raisonnablement nécessaire pour que le Canada réponde à la demande rapidement.

9.8 Plaintes

Le Canada et l'entrepreneur ou le sous-traitant destinataire étranger conviennent de s'informer immédiatement et mutuellement de la réception d'une plainte en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* ou de toute autre loi pertinente concernant les renseignements personnels. Les parties conviennent de s'échanger toute information nécessaire pour faciliter le règlement de la plainte et de s'informer immédiatement l'une l'autre de son dénouement.

9.9 Exception

Les obligations énoncées dans ces conditions générales supplémentaires ne s'appliquent pas aux renseignements personnels qui sont déjà du domaine public, du moment qu'elles ne sont pas devenues du domaine public, à la suite d'une faute ou d'une omission de l'entrepreneur ou de tout sous-traitant, agent ou représentant de l'entrepreneur ou de leurs employés.

ANNEXE D
ENTENTE DE NON-DIVULGATION AVEC LE CLIENT

Entente de non-divulgation, numéro de contrat :

1. Je soussigné(e), _____, (insérer le nom de l'employé ou du sous-traitant) reconnais que, dans le cadre de mon travail à titre d'employé ou de sous-traitant de _____ (insérer le nom de l'entrepreneur), je peux avoir le droit d'accès à des renseignements fournis par ou pour le Canada relativement aux travaux, en vertu du contrat portant le numéro de série 21120-221210 entre Sa Majesté le Roi du chef du Canada, représentée par le ministre des Travaux publics et des Services gouvernementaux et _____ (insérer le nom de l'entrepreneur), y compris des renseignements confidentiels ou des renseignements protégés par des droits de propriété intellectuelle appartenant à des tiers, ainsi que ceux qui sont conçus générés ou produits par l'entrepreneur pour l'exécution des travaux.

2. Aux fins du présent accord, sont compris, sans s'y limiter, les renseignements suivants :

   2.1 documents et données;

   2.2 conseils, instructions et lignes directrices;

   2.3 énoncé des travaux ou exigences, plans détaillés et dessins, spécifications ou normes techniques ou de rendement, et critères d'évaluation;

   2.4 autres renseignements reçus verbalement, sous forme imprimée ou électronique ou autre, et considérés ou non comme exclusifs ou de nature délicate, qui sont divulgués à _____ (insérer le nom de l'entrepreneur) ou à moi-même, ou dont _____ (insérer le nom de l'entrepreneur) ou moi-même prend connaissance pendant l'exécution du contrat.

3. J'accepte de ne pas reproduire, copier, utiliser, divulguer, diffuser ou publier, en tout ou en partie, de quelque manière ou forme que ce soit les renseignements décrits ci-dessus sauf à une personne employée par le Canada qui est autorisée à y avoir accès. Je m'engage également à protéger les renseignements et à prendre toutes les mesures nécessaires et appropriées, y compris celles énoncées dans toute instruction écrite ou verbale émise par le Canada, pour prévenir la divulgation ou l'accès à ces renseignements en contravention du présent accord.

4. Je reconnais également que les renseignements fournis à _____ (insérer le nom de l'entrepreneur) ou à moi-même par ou pour le Canada ne doivent être utilisés qu'aux seules fins du contrat et que ces renseignements demeurent la propriété du Canada ou d'un tiers, selon le cas.

5. Je conviens que l'obligation énoncée dans le présent accord demeurera en vigueur à la fin du contrat portant le numéro suivant :

Nom en caractères d'imprimerie : _____

Numéro de téléphone en caractères d'imprimerie : _____

Dénomination sociale de l'employeur en caractères d'imprimerie : _____

Titre en caractères d'imprimerie : _____

Date : _____

Signature : _____

ANNEXE E
FORMULAIRE DE PRÉSENTATION DE L'INFORMATION SUR LA SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT
(Joint séparément en format Excel)

ANNEXE F
ACCORD SUR LES NIVEAUX DE SERVICE

Seules les modalités de l'accord sur les niveaux de service relatives aux niveaux de service et à la prestation de services seront intégrées au contrat, telles qu'elles sont décrites à l'article 3.2.2 de la section 1 : Soumission technique.

En présentant une soumission, le soumissionnaire reconnaît et convient que toutes les modalités contenues à l'annexe F – Accord sur les niveaux de service qui visent à interpréter le contrat, qui sont le même sujet ou un sujet semblable, ou qui sont liées aux modalités contenues dans les clauses du contrat, sont réputées être annulées et inopérantes. De même, toute clause contenue à l'annexe F – Accord sur les niveaux de service qui comprend des renseignements sur les prix, comme (notamment) celles qui tentent d'imposer des conditions financières, des modalités de prix ou des pénalités de conformité, sera réputée être annulée et inopérante.

Aucune modalité n'est censée abréger ou proroger les délais pour introduire une action pour violation, une action en responsabilité délictuelle, ou d'autres actions de tout type.

ANNEXE G
DROITS D'UTILISATION DU LOGICIEL

Seules les modalités contenues dans les droits d'utilisation du logiciel-service (DULS), décrites en détail à l'alinéa 3.2.3(b) de la section I : Soumission technique, s'appliqueront. Toute modalité et condition des DULS non liée aux droits d'utilisation du logiciel-service sera jugée comme étant supprimée et ne s'appliquera pas. Les fournisseurs peuvent soumettre leurs DULS au moyen d'URL. Les fournisseurs sont autorisés à mettre à jour leurs DULS de façon continue, à condition que les changements apportés ne représentent pas une diminution des niveaux de service et que les changements sont acceptés par le Canada. Les modalités intégrées par renvoi par le truchement d'adresses URL, de fichiers « Lisez-moi » ou d'autres moyens, comme indiqué dans les DULS du contrat. Les fournisseurs peuvent mettre à jour leurs conditions intégrées par référence à l'aide d'URL, de fichiers « Lisez-moi » ou d'autres moyens, comme indiqué dans les DULS, de façon continue, à condition que les changements apportés n'auront pour conséquence qu'une amélioration et une augmentation des services. Aucune modalité n'est censée abréger ou proroger les délais pour introduire une action pour violation, une action en responsabilité délictuelle, ou d'autres actions de tout type.

ANNEXE H
CONDITIONS SUPPLÉMENTAIRES D'UTILISATION DU LOGICIEL

ANNEXE I
LISTE DE VÉRIFICATION DE LA PRÉSENTATION DE LA SOUMISSION

Les soumissions doivent être présentées uniquement au Groupe de la 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 propositions.

Les pages suivantes dûment remplies doivent être jointes à votre soumission :

- ☐ Page couverture de la demande de propositions, signée et datée
- ☐ Annexe B – Base de Paiement
- ☐ Annexe J – Critères d'évaluation obligatoires
- ☐ Annexe K – Critères d'évaluation cotés

Les documents suivants peuvent être présentés avec la soumission, ou plus tard, à la demande de l'autorité contractante :

- ☐ Page couverture de la demande de propositions (le cas échéant), signée et datée
- ☐ Pièce jointe 1 – Attestation d'absence de collusion dans l'établissement de soumission
- ☐ Pièce jointe 2 – Formulaire d'attestation de l'éditeur de logiciels
- ☐ Pièce jointe 3 – Formulaire d'autorisation de l'éditeur de logiciels
- ☐ Pièce jointe 4 – Formulaire d'autorisation du fournisseur de services infonuagiques du gouvernement du Canada
- ☐ Annexe E – Formulaire de présentation de l'information sur la sécurité de la chaîne d'approvisionnement

Remarque : Veiller à ce que tous les coûts liés aux activités soient inclus dans le prix de la soumission.
(*y compris les exigences en matière d'assurance)

ANNEXE J
CRITÈRES D'ÉVALUATION OBLIGATOIRES

1. Exigence obligatoire

La soumission technique doit traiter clairement et de manière suffisamment approfondie des exigences faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Pour prouver leur conformité, les soumissionnaires peuvent soumettre des captures d'écran, des renvois à des documents techniques (en indiquant les numéros de pages), des attestations ou encore des descriptions détaillées. Il ne suffit pas de reprendre simplement les énoncés contenus dans la DDP. Afin de faciliter l'évaluation de la soumission, la GRC 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.

Le contrôle de validation de la soumission (CVS) sera réalisé afin de vérifier les exigences obligatoires 1 à 29. Le CVS sera donné en ligne et la GRC le visionnera à distance (par Microsoft Teams), tandis que le soumissionnaire démontrera sa conformité aux exigences obligatoires.

- Le soumissionnaire doit pouvoir réaliser le CVS dans les 14 jours ouvrables suivant la demande de la GRC.

Toute soumission qui ne satisfait pas aux éléments obligatoires sera jugée non recevable et sera rejetée d'emblée.

Tableau 1 – Exigence obligatoire

Élément	Critère obligatoire (O)	Page de référence
Infrastructure		
O1	La solution de logiciel-service de planification des ressources doit être compatible avec les navigateurs Web 64 bits actuels qui utilisent Chromium (Microsoft Edge ou Google Chrome).	
Planification de la formation		
O2	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des entités de base de données qui représentent les étudiants aux propriétés adéquates. Notamment : a) Numéro d'identification b) Nom c) Âge d) Sexe	
O3	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des entités de base de données qui représentent les instructeurs aux propriétés adéquates. Notamment : a) Numéro d'identification b) Nom c) Unité d) Qualifications	
O4	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des entités de base de données qui représentent les groupes de classe. Notamment : a) Numéro d'identification b) Date de début c) Date d'obtention du diplôme	
O5	La solution de logiciel-service de planification des ressources doit avoir la capacité de diviser un groupe de classe en plusieurs sous-groupes de classe. Par exemple, la troupe 10 peut être divisée en : groupe A, groupe B et groupe C.	

O6	La solution de logiciel-service de planification des ressources doit avoir la capacité d'assigner un sous-groupe de classe à différentes séances simultanément.	
O7	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des entités de base de données qui représentent des modules. Notamment : a) Numéro du module b) Nom du module c) Nom du sujet d) Modules préalables e) Catégorie de modules f) Ordre des modules	
O8	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des entités de base de données qui représentent des séances. Notamment : a) Module parent b) Numéro de la session c) Nom de la séance d) Durée e) Séances préalables f) Ordre des séances g) Ressources nécessaires	
O9	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des entités de base de données qui représentent des immeubles ou installations aux propriétés adéquates. Notamment : a) Nom de l'immeuble b) Type d'immeuble c) Emplacement d) Salles	
O10	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des entités de base de données qui représentent des salles (ou des lieux) aux propriétés adéquates. Notamment : a) Numéro de la salle b) Type de salle (salle de conférence, salle de classe standard, salle d'informatique, gymnase, piscine, salle de cours d'autodéfense, salle de tir, mess, salle d'exercices, cafétéria) c) Immeuble d) Capacité (sièges) e) Ressources (ordinateurs, imprimantes, projecteurs, marqueurs à essuyage à sec, tableau interactif, connexion pour portables, téléconférence, vidéoconférence, accès au système ROSS, accès Internet, réseau Wi-Fi, microphone, caméra vidéo, lecteur Blue Ray, scène, gradins, taille des affichages)	
O11	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer plusieurs programmes de formation.	
O12	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des règles opérationnelles qui définissent les contraintes liées à la planification.	
O13	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer un calendrier (programme). Le calendrier consistera en la réservation de ressources et de places (groupes de classe, instructeurs) pour une séance. Le logiciel signalera aux utilisateurs les conflits d'horaire et les avertira des problèmes ou des conflits qui surviennent.	
O14	La solution de logiciel-service de planification des ressources doit avoir les fonctionnalités qui permettent d'automatiser la planification des tâches. Au moyen de règles opérationnelles personnalisées, le logiciel doit avoir la capacité de planifier les séances, en s'assurant qu'il n'y a pas de conflit d'horaire ou de problème sur le plan de la disponibilité des instructeurs.	

O15	La solution de logiciel-service de planification des ressources doit appuyer le programme de formation par rotation de la GRC tel qu'il est défini dans l'énoncé des travaux.	
O16	La solution de logiciel-service de planification des ressources doit fournir un accès aux groupes de classe et aux instructeurs afin que ceux-ci puissent voir les calendriers par l'intermédiaire d'un portail Web.	
O17	Les instructeurs doivent avoir accès à leur calendrier, à leur calendrier des unités et aux horaires des installations à partir d'un portail Web.	
O18	Les instructeurs doivent recevoir une notification lorsqu'ils sont inscrits au calendrier.	
O19	Les groupes de classe doivent avoir accès à leur calendrier par l'intermédiaire d'un portail Web.	
Hébergement/Réservations		
O20	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de créer, de modifier et de supprimer des entités de base de données qui représentent des logements aux propriétés adéquates. Notamment : a) Immeuble b) Numéro de la chambre c) Nombre de lits d) Type de logement	
O21	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs de réserver la place d'étudiants et de non-étudiants pour des logements manuellement à partir d'une liste de logements disponibles.	
O22	La solution de logiciel-service de planification des ressources doit avoir la capacité de réserver des logements pour des groupes de classe avant qu'on sache qui y séjournera.	
O23	La solution de logiciel-service de planification des ressources doit pouvoir fournir de l'information en temps réel sur le taux d'occupation du bâtiment.	
O24	La solution logicielle doit fournir un accès utilisateur basé sur le groupe ou sur le rôle.	
Niveaux de service		
O25	L'accord sur les niveaux de service (ANS) du vendeur doit comprendre des dispositions sur le temps d'accès au système, qui garantissent un temps d'accès minimal de 95 %.	
O26	L'ANS du vendeur doit comprendre des dispositions sur le temps d'arrêt du système à des fins de maintenance. Il doit garantir un préavis d'au moins 7 jours avant tout arrêt du système, et assurer que le temps d'arrêt ne dépasse pas 4 heures par mois.	
O27	La solution de logiciel-service de planification des ressources doit être accessible 24 heures sur 24, 7 jours sur 7, à l'exception des interruptions prévues.	
O28	Les vendeurs doivent offrir un soutien technique et aux utilisateurs pour la solution 5 jours par semaine (du lundi au vendredi), de 8 h à 17 h (HNC).	
O29	La solution de logiciel-service de planification des ressources doit respecter les exigences du GC en matière de conformité et les Lignes directrices sur les ententes de services (https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=25761).	

ANNEXE K
CRITÈRES D'ÉVALUATION COTÉS

1. Exigences cotées

Le Canada utilisera les critères ci-après pour évaluer chaque proposition qui satisfait à tous les critères obligatoires.

Les soumissionnaires doivent obtenir au moins huit (8) points sur un total de vingt-huit (28) points. Toute soumission qui n'obtient pas la note minimale de huit (8) points pour les critères cotés sera jugée non recevable et sera rejetée d'emblée.

Les propositions seront évaluées en fonction des critères suivants.

Tableau 1 : Critères cotés

Numéro de l'exigence	Description de l'exigence	Pondération : 28 points
Généralités		
C1	La solution de logiciel-service de planification des ressources doit avoir des fonctionnalités qui permettent d'importer en lot ou de mettre à jour l'information sur le cours, l'étudiant, le cadet et l'instructeur à partir d'une source externe.	Oui = 1 point Non = 0 point
C2	La solution de logiciel-service de planification des ressources doit permettre aux utilisateurs administrateurs de créer et d'exécuter des rapports personnalisés dans le système, ou fournir l'accès à des ensembles de données qui permettent d'élaborer des rapports personnalisés.	Oui = 2 points Non = 0 point
Formation		
C5	La solution de logiciel-service de planification des ressources doit avoir la capacité de repérer les instructeurs qui possèdent les qualifications requises pour enseigner un module ou une séance planifié(e).	Oui = 2 points Non = 0 point
C6	La solution de logiciel-service de planification des ressources doit avoir la capacité d'indiquer lorsque des instructeurs sont en congé et ne sont pas disponibles pour la planification.	Oui = 1 point Non = 0 point
C7	La solution de logiciel-service de planification des ressources doit avoir la capacité de répartir le temps en classe de façon égale entre les instructeurs qualifiés disponibles.	Oui = 1 point Non = 0 point
C8	La solution de logiciel-service de planification des ressources doit avoir la capacité d'analyser les données de planification passées pour prévoir l'utilisation future des ressources.	Oui = 1 point Non = 0 point
C9	La solution de logiciel-service de planification des ressources doit avoir la capacité d'analyser les données de planification passées pour déterminer les manques de ressources éventuels.	Oui = 1 point Non = 0 point
Hébergement		
C10	La solution de logiciel-service de planification des ressources doit aider à répartir uniformément l'utilisation des logements au moment de la réservation.	Oui = 1 point Non = 0 point
C11	La solution de logiciel-service de planification des ressources doit avoir la capacité d'envoyer automatiquement aux cadets/invités avant leur arrivée un courriel comprenant une « trousse de bienvenue ». Le courriel doit comprendre les renseignements suivants : a) Indications sur l'endroit où aller une fois arrivé b) Dates d'enregistrement à l'arrivée et au départ	Oui = 1 point Non = 0 point

C12	La solution de logiciel-service de planification des ressources doit comporter un portail Web pour l'enregistrement des personnes à leur arrivée à la Division Dépôt.	Oui = 1 point Non = 0 point
C13	La solution de logiciel-service de planification des ressources doit avoir la capacité de réserver ou d'assigner plusieurs logements à la fois. Par exemple, on doit pouvoir réserver un bloc de chambres pour l'hébergement d'un groupe de classe qui arrive.	Oui = 2 points Non = 0 point
C14	La solution de logiciel-service de planification des ressources doit avoir des fonctionnalités qui permettent de déplacer ou de modifier des logements en bloc (déplacer un groupe de classe d'un endroit à un autre, changer la date de départ d'un groupe de classe en entier).	Oui = 2 points Non = 0 point
C15	La solution de logiciel-service de planification des ressources doit avoir la capacité de créer et de gérer des factures. (1 point) Les factures doivent être calculées automatiquement en fonction du type de logement, du bâtiment et de la durée du séjour. (1 point) La solution de logiciel-service de planification des ressources doit permettre d'ajouter des suppléments à la facture (p. ex. repas). (1 point)	1 point par élément (3 points maximum)
C16	La solution de logiciel-service de planification des ressources doit avoir la capacité de signaler les salles qui nécessitent un entretien.	Oui = 1 point Non = 0 point
C17	La facilité d'utilisation ainsi que l'aspect et la convivialité de la solution de logiciel-service de planification des ressources proposée seront évalués en même temps que les exigences fonctionnelles. L'interface doit être facile à comprendre et aider l'utilisateur à atteindre ses objectifs dans le logiciel le plus aisément et efficacement possible. Des points sont alloués si la tâche peut être menée à bien en moins de quatre (4) étapes (ne comprend pas la connexion et l'entrée des données sur le terrain) : a) Réserver une chambre pour un invité b) Réserver une salle pour une séance c) Créer un groupe de classe d) Assigner un instructeur à une séance e) Assigner un groupe de classe à une séance f) Communiquer le taux d'occupation d'un bâtiment g) Indiquer qu'un instructeur est en congé ou non disponible	1 point pour chaque tâche (8 points maximum)

ANNEXE L
CRITÈRES D'ÉVALUATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

Les **quinze (15) exigences de sécurité** suivantes doivent être respectées afin de démontrer la conformité au 1er niveau d'assurance **(données jusqu'au niveau « Protégé A », inclusivement)**.

1. 1er niveau d'assurance (données jusqu'au niveau « Protégé A », inclusivement)

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au niveau 1
O1	**Rôles et responsabilités liés à la sécurité**	Le fournisseur doit s'assurer que les rôles et responsabilités relatifs aux contrôles et aux fonctions de sécurité de la solution sont clairement définis pour lui-même et pour le Canada (ainsi que pour tout sous-traitant, s'il y a lieu).	Il doit indiquer, à tout le moins, les rôles et les responsabilités des parties pour : i) la gestion des comptes; ii) la protection des frontières; iii) la sauvegarde des actifs et des systèmes d'information; iv) la gestion des incidents; v) la surveillance du système; et vi) la gestion de la vulnérabilité.
O2	**Protection des données**	Les emplacements physiques du logiciel-service public commercial (qui peut contenir les données du Canada) doivent être situés au sein du Groupe des cinq, une alliance des services de renseignements de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis.	Le fournisseur doit présenter une documentation démontrant la façon dont le logiciel-service public commercial proposé satisfait aux exigences en matière de protection des données. Pour être jugés conformes, les documents doivent comporter les éléments suivants : Une liste à jour des emplacements physiques (y compris la ville et le pays) de chaque centre de données susceptible de contenir des données du Canada, y compris des données sauvegardées ou redondantes. Les explications nécessaires sur les exigences de protection des données. Il ne suffit pas de reprendre l'exigence obligatoire. Le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les

			documents mentionnés, leur titre et les numéros de page et de paragraphe.
O2	**Installations des centres de données**	Le fournisseur du logiciel-service public commercial proposé doit mettre en place des mesures de sécurité qui assurent la protection des installations de TI et des biens du système d'information dans lesquels les données du gouvernement du Canada sont stockées et protégées contre toute forme de manipulation, de perte, de dommages et de saisie, et qui sont fondées sur une approche de détection et de récupération préventive en matière de sécurité physique. Ceci doit inclure, à tout le moins, les éléments qui suivent : a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont notamment suffisamment disparates sur le plan géographique pour que la perte d'un centre de données n'empêche pas la récupération des données conformément à l'ANS prescrit; b) l'utilisation adéquate des supports de TI; c) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; d) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; e) la restriction de l'accès physique aux biens des systèmes d'information aux employés autorisés et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, validé par deux formes d'identification; f) l'escorte des visiteurs et la surveillance de leurs activités; g) la tenue de registres de vérification de l'accès physique; h) le contrôle et la gestion des dispositifs d'accès physique; i) l'application des mesures de protection des données du GC à d'autres lieux de travail (p. ex. les sites de télétravail); j) la consignation et la surveillance de tous les accès physiques aux installations des centres de données et de tous les accès par voie électronique aux composants des systèmes d'information qui hébergent les données du Canada, au moyen d'une combinaison de registres d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.	Le fournisseur doit présenter une documentation démontrant la façon dont le fournisseur du logiciel-service (et, le cas échéant, l'autre fournisseur de services) des services proposés respecte les exigences des installations des centres de données. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) les documents de système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, les processus et les procédures servant à protéger les installations de TI et les biens du système d'information dans lesquels les données du gouvernement du Canada sont stockées et protégées contre toute forme de manipulation, de perte, de dommage et de saisie, et qui sont fondées sur une approche de détection et de récupération préventive en matière de sécurité physique. OU b) la pièce jointe 4 remplie attestant que la solution de logiciel-service de planification des ressources est hébergée par un fournisseur de services infonuagiques approuvé par le GC et qui détient un accord-cadre infonuagique du GC (https://cloud-services-infonuagiques.canada.ca/s/gc-cloud-fa?language=fr). Pour la documentation sur les exigences relatives aux installations du centre de données, il ne suffit pas de

			reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service public commercial satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O4	**Sécurité du personnel**	Le fournisseur du logiciel-service public commercial proposé doit mettre en place des mesures de sécurité qui accordent et maintiennent le niveau de filtrage de sécurité requis pour son personnel respectif ainsi que pour le personnel de tout sous-traitant, en fonction de leurs privilèges d'accès aux biens des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Les mesures de contrôle doivent être appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115), ou utiliser un équivalent acceptable convenu par le Canada. Ces mesures comprennent, au minimum : a) une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux données du Canada ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services; b) le processus visant à s'assurer que les employés et les entrepreneurs connaissent, comprennent et respectent leurs responsabilités en matière de sécurité de l'information et que le rôle que l'on compte leur confier leur convient; c) le processus relatif à la sensibilisation et à la formation en matière de sécurité dans le cadre de l'intégration à l'emploi et lorsque les rôles des employés et des sous-traitants changent; d) le processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi; e) une approche de détection des initiés malveillants potentiels et des contrôles mis en œuvre pour atténuer le risque d'accès aux données du GC ou d'incidence sur la fiabilité du logiciel-service hébergeant les biens et les données du gouvernement du Canada.	Le fournisseur doit présenter une documentation démontrant la façon dont le fournisseur du logiciel-service public commercial respecte les exigences relatives à la sécurité du personnel. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, les processus et les procédures utilisés pour accorder et maintenir le niveau de filtrage de sécurité requis pour le personnel du fournisseur ainsi que pour le personnel de tout sous-traitant, en fonction de leurs privilèges d'accès aux biens des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Pour la documentation sur les exigences relatives à la sécurité du personnel, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service public commercial proposé satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des

			documents techniques et des documents destinés à l'utilisateur final. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O5	**Assurance d'une tierce partie**	Le logiciel-service doit être conçu et développé pour assurer la sécurité du logiciel-service public commercial proposé, y compris la mise en œuvre de politiques, de procédures et de contrôles de sécurité de l'information.	Le fournisseur doit présenter une documentation au Canada démontrant la façon dont le fournisseur du logiciel-service public commercial respecte les exigences relatives à l'assurance d'une tierce partie. La conformité doit être démontrée par la présentation d'au moins une des certifications de l'industrie énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants. Le fournisseur doit présenter les certifications suivantes de l'industrie afin de démontrer la conformité de la solution proposée : 1) Un des éléments suivants : i) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences; Le soumissionnaire détient une certification ISO 27001 ou une lettre de pont confirmant que la certification est en cours de renouvellement. ii) contrôle de l'organisation des services (SOC) de l'AICPA – rapports des SOC 2 de type II; 2) une autoévaluation de ses services par rapport à la version 3.01 (ou une version ultérieure) de la matrice des contrôles infonuagiques de la Cloud Security Alliance. Chaque rapport de certification et d'évaluation fourni doit :

			a) être valide à la date de présentation; b) indiquer la dénomination sociale du fournisseur proposé et du sous-traitant du fournisseur, s'il y a lieu, y compris le fournisseur de services infonuagiques; c) indiquer la date ou l'état de la certification actuelle; d) comprendre la liste des biens, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification; e) indiquer les emplacements et les services offerts par le fournisseur proposé. Si la méthode déterminée est utilisée pour exclure les organisations de services en sous-traitance, comme l'hébergement de centres de données, le rapport d'évaluation de l'organisation sous-traitante doit être inclus; f) être délivré par un tiers indépendant qualifié au titre de l'AICPA ou de CPA Canada ou du régime de certification ISO, et respecter la norme ISO/IEC 17020 relativement aux systèmes de gestion de la qualité. Remarque • Des certifications doivent être fournies pour chaque partie des services proposés. • Les certifications doivent être accompagnées de rapports d'évaluation complets. • Les certifications doivent être valides dans les 12 mois précédant le début du contrat.
O6	**Gestion de la chaîne d'approvisionnement**	Le fournisseur doit fournir une liste de fournisseurs tiers contenant des renseignements sur tout tiers (p. ex. filiales, sous-traitants, fournisseurs de services infonuagiques, etc.) qui fournirait au Canada le logiciel sous forme de service commercialement disponible. Pour les besoins de cette exigence, une entreprise qui fournit des biens au fournisseur du logiciel-service sous forme de service public commercial proposé, mais qui n'effectue pas une partie de la chaîne d'approvisionnement qui pourrait fournir au Canada le logiciel sous forme de	Le fournisseur doit présenter une liste de tous les sous-traitants auxquels il pourrait faire appel pour exécuter n'importe quelle partie des services rendus au Canada. La liste doit comprendre les renseignements suivants : (i) le nom du sous-traitant; (ii) la description des activités qui seraient réalisées par le sous-traitant; et (iii) le ou les lieux où le sous-traitant réaliserait les

		service public commercial proposé, n'est pas considérée comme un tiers. Les exemples de tiers comprennent les techniciens qui pourraient être déployés ou entretenir le logiciel-service public commercial proposé par le fournisseur. Remarque Les fournisseurs sont informés que les étapes d'approvisionnement subséquentes peuvent exiger que le fournisseur avise périodiquement le Canada en cas de mise à jour de la liste des fournisseurs tiers.	activités requises à l'appui des services. (1) L'entrepreneur doit démontrer, pour la solution d'infrastructure-service ou de plateforme-service utilisée par les services : (a) que les sous-traitants ont été évalués par le programme d'intégrité de la chaîne d'approvisionnement du CCC; (b) que le fournisseur respecte les obligations des sous-traitants en matière de sécurité, définies par le fournisseur, pour toute la durée du contrat. Si le fournisseur ne fait appel à aucun tiers pour effectuer une partie quelconque de la chaîne d'approvisionnement en mesure de fournir au Canada le logiciel sous forme de service public commercial proposé, le fournisseur doit l'indiquer dans sa réponse à cette exigence.
O7	**Gestion des risques liés à la chaîne d'approvisionnement**	Le fournisseur du logiciel-service public commercial proposé doit mettre en œuvre des mesures de protection afin de réduire les vulnérabilités de la chaîne d'approvisionnement des services de TI et les menaces qui la guettent. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.	Le fournisseur doit démontrer la façon dont le fournisseur du logiciel-service public commercial respecte les exigences relatives à la gestion des risques de la chaîne d'approvisionnement, comme le précise le programme d'évaluation de la sécurité de la TI du fournisseur du logiciel-service. Pour être jugée conforme, la documentation fournie doit démontrer la conformité du fournisseur à l'une des trois normes suivantes : 1. ISO/IEC 27 036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4); ou 2. Publication spéciale 800-161 du NIST – Supply Chain Risk Management Practices for Federal Information Systems and Organizations (pratiques de

			gestion des risques de la chaîne d'approvisionnement pour les systèmes d'information et organisations du fédéral); ou 3. Catalogue des contrôles de sécurité ITSG-33, sections SA-12 et SA-12(2), où les mesures de sécurité définies et organisées sont documentées dans un plan de gestion des risques de la chaîne d'approvisionnement (GRCA). Le plan de GRCA doit décrire la démarche du fournisseur du logiciel-service en matière de GRCA et démontrer la façon dont le fournisseur du logiciel-service public commercial proposé réduira et atténuera les risques de la chaîne d'approvisionnement.
O8	**Gestion des accès privilégiés**	Le fournisseur du logiciel-service public commercial proposé doit fournir des documents de système démontrant la façon dont le logiciel-service est en mesure de répondre aux exigences de sécurité suivantes en matière de gestion de l'accès privilégié : a) Gérer et surveiller l'accès privilégié à la solution (infrastructure sous-jacente comprise) pour s'assurer que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC; b) Restreindre et réduire au minimum l'accès aux services et aux données du Canada aux seuls dispositifs autorisés et aux utilisateurs finaux ayant un besoin explicite d'y avoir accès; c) Faire respecter et vérifier les autorisations d'accès aux services et aux données du Canada; d) Limiter tous les accès aux interfaces de service qui hébergent les biens et les données du Canada aux utilisateurs finaux, dispositifs et processus (ou services) désignés, authentifiés et autorisés de façon unique; e) Mettre en œuvre des politiques relatives aux mots de passe afin de protéger les identifiants contre les attaques en ligne ou hors ligne et de détecter ces attaques en enregistrant et en surveillant des événements tels que : i) l'utilisation réussie des identifiants de connexion, ii) l'utilisation inhabituelle des identifiants de connexion et iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);	Le fournisseur doit démontrer sa conformité en fournissant de la documentation qui décrit la capacité du logiciel sous forme de service commercialement disponible de répondre aux exigences de sécurité liées aux exigences en matière de gestion de l'accès privilégié : Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Une documentation du système ou un livre blanc décrivant les politiques, les processus et les procédures utilisés pour prendre en charge la gestion de l'accès privilégié. La justification demandée pour la documentation sur la gestion de l'accès privilégié ne doit pas simplement reprendre l'exigence obligatoire; elle doit expliquer et démontrer la façon dont le logiciel-service disponible sur le marché satisfait à l'exigence, en indiquant exactement où le matériel de référence figure dans la soumission (titre du document, numéros de page et de paragraphe). Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final.

		(f) Mettre en place des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs ayant des privilèges d'accès, conformément à la norme ITSP.30.031 V2 (ou une 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 place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux biens et aux renseignements du GC; h) Définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, les rôles de développement des rôles opérationnels et les rôles de gestion de l'accès des autres rôles opérationnels; i) Adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services, aux biens et aux renseignements; j) Contrôler l'accès aux objets stockés et aux politiques d'autorisation granulaires pour autoriser ou limiter l'accès; k) Utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (par exemple un point terminal dédié qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) pour offrir le soutien et l'administration des services et de l'infrastructure du fournisseur; l) Mettre en place un processus automatisé pour effectuer une vérification périodique de la création, de la modification, de l'activation, de la désactivation et de la suppression de comptes, au minimum; m) Révoquer, en cas de cessation d'emploi, les authentificateurs et les justificatifs d'accès associés au personnel de service.	Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

O9	**Fédération de l'identité**	**Fédération de l'identité** Le fournisseur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment : a) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de); b) prendre en charge le Security Assertion Markup Language (SAML) 2.0 et l'OpenID Connect 1.0, où les justificatifs et authentificateurs des utilisateurs du GC pour les services d'infonuagique sont contrôlés uniquement par le Canada; c) pouvoir associer les identifiants uniques du Canada (p. ex. un numéro d'identification unique du Canada, une adresse de courriel du Canada) aux comptes d'utilisateurs des services d'infonuagique correspondants.	Le fournisseur des services proposés doit fournir une documentation qui démontre comment il se conforme aux exigences énoncées à la rubrique Fédération de l'identité. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la protection de la fédération de l'identité. Pour les exigences relatives à la fédération de l'identité, il ne suffit pas de reprendre l'exigence obligatoire. On doit expliquer et démontrer la façon dont le logiciel sous forme de service commercialement disponible satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

O10	**Protection des points terminaux**	**Protection des points terminaux** Le fournisseur doit mettre en œuvre, gérer et surveiller les points d'accès sécurisés afin de prévenir les attaques et les abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide to General Server Security [guide relatif à la sécurité générale des serveurs]), des points de référence du Center for Internet Security ou d'une norme équivalente approuvée par écrit par le Canada.	Le fournisseur des services proposés doit fournir une documentation qui démontre comment il se conforme aux exigences énoncées à la rubrique Protection des points terminaux. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la protection des points terminaux. La justification demandée pour la protection des points terminaux ne doit pas simplement reprendre l'exigence obligatoire; elle doit expliquer et démontrer la façon dont le logiciel-service commercial satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

O11	**Développement sécurisé**	**Développement sécurisé** Le fournisseur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : i) NIST, ii) ISO, iii) ITSG-33, iv) SAFECode ou v) Open Web Application Security Project (p. ex. Application Security Verification Standard) ou une norme équivalente approuvée par le Canada par écrit.	Le fournisseur des services proposés doit présenter une documentation qui démontre comment il se conforme aux exigences énoncées à la rubrique Développement sécurisé. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer le développement sécurisé. La justification demandée pour le développement sécurisé ne doit pas simplement reprendre l'exigence obligatoire; elle doit expliquer et démontrer la façon dont le logiciel-service commercial satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

O12	**Gestion à distance du fournisseur**	**Gestion à distance du fournisseur** Le fournisseur doit gérer et surveiller l'administration à distance des services du fournisseur qui sont utilisés pour héberger les services du GC, en plus de prendre des mesures raisonnables pour : a) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs utilisant l'accès à distance, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de); b) employer des algorithmes et mécanismes cryptographiques approuvés par le CST en vertu du document ITSP.40.111 https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111 afin de protéger la confidentialité des séances d'accès à distance; c) acheminer tout l'accès à distance par des points de contrôle des accès gérés, surveillés et vérifiés; d) déconnecter ou désactiver rapidement les connexions non autorisées de gestion à distance ou d'accès à distance; e) autoriser l'exécution à distance des commandes privilégiées et l'accès à distance aux informations relatives à la sécurité.	Le fournisseur des services proposés doit fournir une documentation qui démontre comment il se conforme aux exigences énoncées à la rubrique Gestion à distance du fournisseur. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la gestion à distance du fournisseur La justification demandée pour la gestion à distance du fournisseur ne doit pas simplement reprendre l'exigence obligatoire; elle doit expliquer et démontrer la façon dont le logiciel-service commercial satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

O13	**Fuite d'information**	**Fuite d'information** Le fournisseur doit fournir au Canada un document décrivant le processus qu'il suit pour répondre à un incident de fuite d'information. Le processus doit être harmonisé : (i) aux directives de la section IR−9 intitulée « Intervention en cas de fuite d'information » du document ITSG−33; ou (ii) à une autre pratique exemplaire des principaux fournisseurs de services approuvés par écrit par le Canada. Sans égard à ce qui précède, le processus d'intervention en cas de fuite d'information du fournisseur doit comprendre, à tout le moins : a) un processus d'identification de l'actif d'information précis concerné par la contamination d'un actif ou d'un système; b) un processus visant à isoler et à éradiquer un actif ou un système contaminé; c) une description du processus d'identification des actifs ou systèmes qui ont pu avoir été subséquemment contaminés et de toute autre mesure prise pour empêcher la propagation de la contamination. (2) Le fournisseur doit transmettre au Canada un processus d'intervention en cas de fuite d'information à jour, chaque année ou immédiatement à la suite d'importantes modifications apportées au processus.	Le fournisseur des services proposés doit fournir une documentation qui démontre comment il se conforme aux exigences énoncées à la rubrique Fuite d'information. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la protection contre les fuites d'information. La justification demandée pour la fuite d'information ne doit pas simplement reprendre l'exigence obligatoire; elle doit expliquer et démontrer la façon dont le logiciel-service commercial satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

O14	Protection cryptographique	**Protection cryptographique** Le fournisseur doit fournir au Canada un document décrivant le processus qu'il suit pour répondre à une protection cryptographique de l'information. a) configurer toute solution cryptographique qui est adoptée à l'égard des services et qui est utilisée dans le cadre de la mise en œuvre de mesures de protection de la confidentialité ou de l'intégrité ou encore d'un mécanisme d'authentification (p. ex. solutions liées au réseau privé virtuel, protocole TLS, modules logiciels, indicateurs de rendement clés et jetons d'authentification, le cas échéant), conformément avec les algorithmes cryptographiques, les tailles de clés de chiffrement et les périodes de validité des clés approuvés par le CST; b) utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui ont été validés par le Programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/), et précisés dans le document ITSP.40.111 Algorithmes cryptographiques pour l'information « Non classifié », « Protégé A » et « Protégé B » ou dans des versions subséquentes de ce document (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111); c) s'assurer que la cryptographie validée selon la norme FIPS 140 est utilisée lorsqu'un chiffrement est nécessaire et qu'elle est mise en œuvre, configurée et exploitée dans un module cryptographique, validé par le Programme de validation des modules cryptographiques (https://www.cse-cst.gc.ca/fr/groupgroupe/programme-validation-modules-cryptographiques-pvmc), dans un mode approuvé ou autorisé afin de fournir un degré élevé de certitude que le module cryptographique validé FIPS 140-2 fournit les services de sécurité prévus de la manière prévue; d) s'assurer que tous les modules FIPS 140-2 utilisés ont une certification active, à jour et valide. Les produits conformes ou validés selon la norme FIPS 140 auront un numéro de certificat.	Le fournisseur des services proposés doit fournir une documentation qui démontre comment il se conforme aux exigences énoncées à la rubrique Protection cryptographique. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la protection cryptographique. La justification demandée pour la protection cryptographique ne doit pas simplement reprendre l'exigence obligatoire; elle doit expliquer et démontrer la façon dont le logiciel-service commercial satisfait à l'exigence. Pour étayer sa réponse, le fournisseur peut fournir des captures d'écran, des documents techniques et des documents destinés à l'utilisateur final. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Le fournisseur doit indiquer à quel endroit dans la soumission se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

O15	**Séparation des données**	Le fournisseur doit mettre en place des contrôles afin d'assurer un isolement approprié des ressources, afin que les actifs d'information ne se retrouvent pas mêlés aux données d'autres locataires, et ce, pendant l'utilisation, le stockage ou le transfert, et dans tous les aspects des fonctions et de l'administration du système du service et de l'infrastructure du fournisseur. Il doit notamment mettre en place des contrôles d'accès et une séparation logique ou physique adéquate à l'appui de : (a) la séparation de l'administration interne du fournisseur des ressources utilisées par ses clients; **(b)** b) la séparation des ressources des clients dans les environnements multilocataires afin d'empêcher que les activités d'un client malveillant ou compromis aient des répercussions sur le service ou les données d'un autre.	Le fournisseur des services proposés doit fournir une documentation qui démontre comment il se conforme aux exigences énoncées à la rubrique Protection cryptographique.

A ANNEX M
SECURITY REQUIREMENTS CHECK LIST (SRCL) & SECURITY GUIDE

PIÈCE JOINTE 2 – FORMULAIRE D'ATTESTATION DE L'ÉDITEUR DE LA SOLUTION

SaaS Publisher Certification Form

(to be used where the Supplier itself is the SaaS Publisher)

The Supplier certifies that it is the Software as a Service (SaaS) Publisher of all the following SaaS Solutions and that it has all the rights necessary to license them in accordance with the terms and conditions of the Bid Solicitation to Canada:

_____

_____

_____

_____

_____

[Suppliers should add or remove lines as needed, or attach the product list as an appendix.]

Name of SaaS Publisher _____

Signature of authorized signatory of SaaS Publisher _____

Print Name of authorized signatory of SaaS Publisher _____

Print Title of authorized signatory of SaaS Publisher _____

Address for authorized signatory of SaaS Publisher _____

Telephone no. for authorized signatory of SaaS Publisher _____

Email for authorized signatory of SaaS Publisher _____

Date signed _____

Solicitation Number: _____

PIÈCE JOINTE 3 – FORMULAIRE D'AUTORISATION DE L'ÉDITEUR DE LA SOLUTION

SaaS Publisher Authorization Form

(to be used where the Supplier is not the SaaS Publisher)

This confirms that the Software as a Service (SaaS) Publisher identified below understands and acknowledges that the Supplier named below has submitted a Submission in response to the Request for Proposal (RFP) dated _____, reference number _____ issued by Public Services and Procurement Canada (PSPC).

The SaaS Publisher hereby confirms that:

(i) The Supplier named below is authorized to supply the SaaS Publisher listed below or attached; and
(ii) The SaaS Publisher agrees to grant all licenses to be acquired under the Contract in accordance with the resulting Contract's terms and conditions set out.

The SaaS Publisher acknowledges that the reseller has proposed to the Crown, in response to the Bid Solicitation, the following SaaS Solutions and other proprietary products of the Corporation.

[*Identify all of the proprietary SaaS Solutions that are proposed by the Supplier*]

_____

_____

_____

_____

[*Suppliers should add or remove lines as needed,* or attach the product list as an appendix.]

Name of Supplier _____

Name of SaaS Publisher _____

Signature of authorized signatory of SaaS Publisher

_____

Print Name of authorized signatory of SaaS Publisher

_____

Print Title of authorized signatory of SaaS Publisher

_____

Address for authorized signatory of SaaS Publisher

_____

Telephone no. for authorized signatory of SaaS Publisher

_____

Email for authorized signatory of SaaS Publisher _____

Date signed _____

Solicitation number _____

PIÈCE JOINTE 4 – FORMULAIRE D'AUTORISATION DU FOURNISSEUR DE SERVICES INFONUAGIQUES DU GOUVERNEMENT DU CANADA

Le fournisseur de services infonuagiques (FSI) du gouvernement du Canada (GC) reconnaît que le soumissionnaire nommé ci-dessous a présenté une soumission en réponse à la demande de propositions (numéro de référence M5000-20-5233/A), conformément aux procédures énoncées dans cette dernière. Cette soumission concerne la solution de logiciel-service de planification des ressources suivante proposée pour un déploiement sur le nuage approuvé par le GC, présenté plus bas.

Le FSI du GC confirme par la présente que :

(i) le soumissionnaire nommé ci-dessous est autorisé à déployer sa solution de logiciel-service au moyen du FSI indiqué ci-dessous;

(ii) le FSI indiqué ci-dessous, au moyen duquel la solution de logiciel-service proposée sera déployée et hébergée, concorde avec le profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html).

Nom de la solution de logiciel-service : _____

Nom du FSI approuvé par le GC : _____

Nom du soumissionnaire : _____

Nom du FSI du GC : _____

Signature du signataire autorisé du FSI du GC : _____

Titre en caractères d'imprimerie du signataire autorisé du FSI du GC :
_____

Adresse du signataire autorisé du FSI du GC :
_____

Nº de tél. du signataire autorisé du FSI du GC :
_____

Adresse courriel du signataire autorisé du FSI du GC : _____

Date : _____

Guide de sécurité de la liste de vérification des exigences relatives à la sécurité des services infonuagiques

Solution de planification des ressources
Division Dépôt
Nº LVERS :

Préparé par :
Sécurité ministérielle
Gendarmerie royale du Canada

1. Préambule

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

1.2. Tous les entrepreneurs employés dans le cadre du présent contrat doivent soutenir et maintenir l'environnement de sécurité de la Gendarmerie royale du Canada (GRC) en se conformant aux exigences décrites dans le présent document. Des obligations de sécurité plus complètes seront fournies lors de la phase de Demande de propositions, le cas échéant. Le présent guide de sécurité ne couvre que les services ou le personnel qui stockent ou traitent de l'information de nature délicate jusqu'au niveau « Protégé B », inclusivement.

2. Définitions

Infonuagique : Modèle qui permet, de façon omniprésente, pratique et sur demande, l'accès réseau à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peuvent rapidement être fournies et mises à jour tout en exigeant très peu d'efforts de gestion ou de contacts avec le fournisseur de services.

Fournisseur de services infonuagiques (FSI) : Entité (pouvant être composée d'au moins une personne physique, une société, un partenariat, un partenariat à responsabilité limitée, etc.) à l'origine du service infonuagique public dans son ensemble.

Compromission : Brèche de sécurité au gouvernement qui comprend, entre autres :

- l'accès non autorisé, la divulgation, la modification, l'utilisation, l'interruption, l'élimination ou la destruction de renseignements ou d'actifs de nature délicate, qui pourraient occasionner une perte de confidentialité, d'intégrité, de disponibilité ou de valeur;
- les agissements, comportements, menaces ou gestes d'une personne à l'égard d'un membre du personnel à son lieu de travail ou d'une personne dans les installations fédérales qui a créé un dommage ou un préjudice à ce membre du personnel ou à cette personne;
- les événements entraînant une perte de l'intégrité ou de la disponibilité des services ou des activités du gouvernement.

Entrepreneur : Entité (peut comprendre une ou plusieurs personnes physiques, des sociétés, des partenariats, des partenariats à responsabilité limitée, des fournisseurs de services, des vendeurs, etc.) qui fournit les services à la GRC et à ses partenaires. Il s'agit de l'entité approuvée et désignée comme « entrepreneur » dans le contrat subséquent.

Utilisateur final : Toute personne, ou tout processus système agissant au nom d'une personne, autorisée par la GRC à accéder aux services infonuagiques.

Fuite d'information : Incident lors duquel un actif informationnel est déposé par inadvertance dans un dispositif ou dans un système qui n'est pas autorisé à traiter ces renseignements (consulter la Ligne directrice sur la sécurité de la technologie de l'information LDSTI-33, IR-9).

Compte principal : Compte doté de privilèges de base pour générer des comptes clients ou des sous-comptes qui permettront au ministère d'accéder à des services infonuagiques publics offerts sur le marché.

Métadonnées : Informations décrivant les caractéristiques des données, y compris, par exemple, les métadonnées structurelles décrivant les structures de données (comme le format des données, la syntaxe et la sémantique) et les métadonnées descriptives décrivant le contenu des données (comme les étiquettes de sécurité de l'information).

Données organisationnelles : Données créées et détenues par ou pour la GRC ou le Canada. Lorsque les services infonuagiques sont utilisés, cela comprend tous les fichiers texte, les sons, les vidéos, les images, les données de journaux, les noms et mots de passe d'utilisateurs, les logiciels et les métadonnées connexes, peu importe leur forme ou leur format : a) communiquées par le personnel de la GRC, les clients, les partenaires, les coentreprises en participation, les concédants de licence, les vendeurs ou les fournisseurs; b) communiquées par les utilisateurs finaux des services infonuagiques; c) recueillies, utilisées, traitées ou stockées dans un environnement infonuagique, qui sont communiquées directement ou indirectement à l'entrepreneur ou aux sous-traitants par la GRC ou en son nom, ou encore par l'entremise des services infonuagiques. Cela comprend toute information ou donnée : i) à laquelle l'entrepreneur ou tout sous-traitant accède intentionnellement ou par inadvertance; ii) transitant sur un réseau ou conservée dans un système ou du matériel utilisé et géré pour la GRC par l'entrepreneur en vue d'assurer la prestation des services infonuagiques et de l'entrepreneur, y compris l'infrastructure de l'entrepreneur.

Renseignements personnels : Information qui a trait à une personne identifiable et qui est consignée dans tous les formats possibles, conformément à l'article 3 de la *Loi sur la protection des renseignements personnels.* Il s'agit notamment des renseignements relatifs à l'ethnie, à la nationalité, à la religion, à l'âge, à l'état civil, à l'adresse, à l'éducation ainsi que les renseignements relatifs au dossier médical, au casier judiciaire, aux opérations financières et les antécédents professionnels. Les renseignements personnels comprennent également tout numéro ou symbole d'identification, comme le numéro d'assurance sociale attribué à une personne.

Chargé de projet : Entité responsable de la gestion du contrat. Toute modification au contrat doit être autorisée par écrit par le chargé de projet, et l'entrepreneur ne doit pas exécuter de travaux en sus ou en dehors du cadre ou de la portée du contrat à la suite de demandes ou d'instructions verbales ou écrites d'une personne autre que le chargé de projet.

Renseignements « Protégé B » : Renseignements ou actifs dont la compromission pourrait causer un préjudice grave à un individu, à une organisation ou au gouvernement.

Informations protégées : Informations ou actifs qui, si compromis, pourraient raisonnablement causer un préjudice à un intérêt non national, c'est-à-dire un intérêt individuel tel qu'une personne ou un organisme.

Enregistrement : Tout document sur papier ou tout groupement de données lisible par machine qui contiennent des renseignements personnels.

Responsable de la sécurité : Entité au sein d'un organisme qui est autorisée à approuver la sécurité du contrat et qui détient le pouvoir signataire autorisé de la LVERS.

Autorisation de sécurité : Cote 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 inclure certaines des étapes ou toutes les étapes de vérification de sécurité énumérées dans la clause de sécurité appropriée.

Événement de sécurité : Tout événement, omission ou situation pouvant nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité.

Incident de sécurité : Tout événement (ou série d'événements), acte, omission ou situation qui entraîne une compromission. Exemples d'incidents de cybersécurité : exploitation active d'une ou de plusieurs vulnérabilités connues, exfiltration de données, défaillance d'un contrôle de sécurité, atteinte d'un service du gouvernement du Canada (GC) géré ou hébergé dans le nuage, etc.

Sous-traitant : Toute personne à qui l'entrepreneur confie en sous-traitance la prestation de ses services, en entier ou en partie.

Sous-traitant : Désigne une personne physique ou morale, une autorité publique, un organisme ou une autre organisation effectuant le traitement des données personnelles au nom d'un contrôleur des données ou d'un entrepreneur.

Télétravail : Entente entre l'employé d'un entrepreneur et le chargé de projet permettant d'effectuer certaines ou l'ensemble de ses tâches à partir d'un emplacement éloigné. Le télétravail nécessite la conclusion d'une entente de télétravail entre l'employé et le chargé de projet.

3. Exigences générales en matière de sécurité

3.1. Toutes les données organisationnelles, y compris la documentation papier et tout autre actif de nature délicate dont la GRC a la responsabilité, doivent être communiquées à l'entrepreneur conformément aux processus déjà approuvés.

3.2. Les renseignements divulgués par la GRC seront gérés, mis à jour et éliminés conformément au cadre du contrat.

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

3.4. Il est interdit de prendre des photos dans les installations de la GRC. Si des photos sont requises, 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 secondaires fournis par la GRC à tout sous-traitant sans l'évaluation et l'autorisation de sécurité de la GRC.

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

3.7. Toutes les données organisationnelles doivent être protégées par des moyens cryptographiques. Il faut utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui sont conformes au document ITSP.40.111 Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B, ou dans des versions subséquentes de ce document.

3.8. Les exigences d'autorisation de sécurité du personnel de l'entrepreneur seront fondées sur les rôles prévus et l'accès aux données et aux systèmes du GC. Au besoin, un guide de classification de sécurité sera ajouté au présent guide de sécurité pour indiquer clairement les exigences en matière d'autorisation de sécurité du personnel.

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

3.10. Les lieux de travail de l'ensemble du personnel de l'entrepreneur doivent être clairement indiqués à l'annexe B – Guide de classification de sécurité et énoncé des travaux (EDT). L'entrepreneur doit produire régulièrement un rapport sur les lieux de travail, ce qui comprend les lieux de télétravail du personnel et le nombre de jours travaillés. Si l'on s'attend à ce que le lieu de travail change pendant la durée du contrat, il faut également l'indiquer de manière explicite. Les lieux de travail peuvent comprendre : i) les installations de la GRC; ii) les lieux d'où s'effectue le télétravail; iii) un hybride des deux. Le télétravail doit être effectué au Canada. Des exceptions pour le télétravail à l'extérieur du Canada peuvent être accordées dans les pays du Groupe des cinq moyennant une évaluation de sécurité de la GRC et l'approbation écrite du dirigeant principal de la sécurité (DPS) ou de son délégué. Les contrôles et les exigences de sécurité seront déterminés au cours de l'évaluation de sécurité pour chaque lieu de travail.

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

3.12. Les lieux de travail de tout le personnel de l'entrepreneur doivent être clairement indiqués dans le Guide de classification de sécurité et dans l'EDT. L'entrepreneur doit produire régulièrement un rapport sur les lieux de travail, ce qui comprend les lieux de télétravail du personnel et le nombre de jours travaillés. Si l'on s'attend à ce que le lieu de travail change pendant la durée du contrat, il faut également l'indiquer de manière explicite. La GRC doit être avisée de tout changement de lieu de travail qui n'est pas indiqué dans le guide de classification et l'EDT, car cela nécessitera un examen et une approbation du contrat. Le télétravail doit être conforme aux directives de la section sur la gestion du télétravail. Toutes les exigences énoncées à l'annexe C (Lignes directrices de la GRC sur le lieu de télétravail) doivent être respectées pendant le télétravail.

4. Sécurité matérielle

4.1. *Entreposage*

4.1.1. Pendant les travaux dans les installations de l'entrepreneur, les données et les actifs organisationnels doivent être entreposés dans un contenant approuvé par le responsable de la sécurité de la GRC. Le contenant doit être situé (au minimum) à l'intérieur d'une « zone de travail ». En conséquence, les installations de l'entrepreneur doivent être dotées d'une aire ou d'une salle répondant aux critères du tableau suivant.

Zone de travail	
a) Définition	1) Une zone où l'accès est limité aux : i) membres du personnel autorisés à y travailler; ii) visiteurs accompagnés des personnes appropriées en tout temps. 2) Le personnel travaillant dans la zone de travail doit posséder une autorisation valide conformément à l'annexe B – Guide de classification de sécurité.
b) Périmètre	1) Doit être délimitée par un périmètre visible ou par un périmètre de sécurité, selon les besoins du projet. Par exemple, les commandes doivent se trouver dans une pièce ou dans un bureau fermé à clé. 2) La zone de travail peut faire l'objet d'un examen par l'unité de la sécurité matérielle, et peut également exiger des mesures de protection supplémentaires ou des recours hiérarchiques jugés nécessaires par l'unité de la sécurité matérielle de la GRC en fonction de l'évaluation de l'espace, des zones avoisinantes, des conditions propres au site, etc.
c) Surveillance	1) Surveillance périodique par le personnel autorisé. Par exemple, des utilisateurs du local qui travaillent sur les lieux sont en mesure de repérer toute atteinte à la sécurité.

Remarque : Consulter l'annexe A pour obtenir plus de renseignements sur le concept de zone de sécurité.

4.1.2. Lorsque les entrepreneurs sont autorisés à travailler à partir d'un certain lieu de télétravail, les données organisationnelles de nature délicate non chiffrées ou sur papier sont interdites. Tous les actifs de la GRC doivent être entreposés dans un endroit qui répond aux critères du tableau suivant.

Zone de télétravail	
a) Définition	1) Toute zone au Canada* où l'accès est limité au personnel qui participe au contrat et aux visiteurs escortés. Remarque : Le personnel travaillant dans la zone de télétravail doit : i) posséder une autorisation valide conformément à l'annexe B – Guide de classification de sécurité;

	ii) posséder une autorisation équivalente approuvée par la GRC conformément à l'annexe B – Guide de classification de sécurité; iii) être escorté par une personne détentrice d'une autorisation conformément à l'annexe B – Guide de classification de sécurité.
b) Périmètre	1) Lorsque les entrepreneurs travaillent dans une zone de télétravail donnée, les travaux doivent être effectués dans un espace réservé aménagé de telle sorte que les personnes partageant le même espace ne puissent ni voir ni entendre ce qui s'y passe, et que l'on ne puisse pas voir par les fenêtres.
c) Surveillance	1) L'entrepreneur doit surveiller régulièrement les renseignements et les actifs de la GRC. Par exemple, des utilisateurs du local qui travaillent sur les lieux sont en mesure d'observer toute atteinte à la sécurité et de la signaler.

**La zone de télétravail doit être située au Canada. Des exceptions pour le télétravail à l'extérieur du Canada peuvent être permises dans les pays du Groupe des cinq moyennant une évaluation de sécurité de la GRC et l'approbation écrite du DPS ou de son délégué.*

4.1.3. En ce qui concerne les lieux de télétravail, l'entrepreneur doit prendre des mesures raisonnables pour protéger les renseignements et les actifs contre la divulgation non autorisée, la perte, le vol, l'incendie, la destruction, les dommages ou les modifications.

4.1.4. Les lieux de télétravail doivent se trouver dans des endroits fermés et privés, jamais à l'extérieur ou dans un lieu public.

4.1.5. Lorsqu'ils travaillent, les entrepreneurs doivent être conscients de leur environnement en tout temps, ainsi qu'être en mesure de fermer immédiatement tout programme ou toute application et de verrouiller l'ordinateur au besoin.

4.2. *Discussions*

4.2.1. Lorsque des conversations de nature délicate sont prévues dans les installations de l'entrepreneur, les zones de travail doivent être dotées de barrières acoustiques continues qui s'étendent d'une dalle à l'autre et qui ont une cote acoustique correspondant à la protection du caractère délicat de la conversation.

4.2.2. Dans les lieux de télétravail, il faut tenir les discussions dans un espace réservé aménagé de telle sorte que les personnes partageant le même espace ne puissent ni voir ni entendre ce qui s'y passe, et que l'on ne puisse pas voir par les fenêtres. Assurez-vous qu'aucune information de nature délicate en arrière-plan ne soit transmise par vidéo ou audio. Toutes les discussions de

nature délicate doivent être protégées. Consulter l'annexe C – Lignes directrices de la GRC sur le lieu de télétravail.

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

4.3.1. La production (création ou modification) de données organisationnelles sur papier ou d'actifs doit se faire dans une aire répondant aux critères exigés pour 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 des documents papier contenant des données organisationnelles pendant la durée du présent contrat, toutes les ébauches ou erreurs d'impression (copies endommagées ou copies en trop) doivent être détruites par l'entrepreneur.

4.4.2. Les données organisationnelles stockées dans un lieu d'entreposage transitoire 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 (déchiqueteuse) ou le système employé pour détruire les documents de nature délicate doit être coté conformément au degré de destruction requis; conformément au Guide de sélection de l'équipement de déchiquetage Guide de sélection de l'équipement de déchiquetage (rcmp-grc.gc.ca);
b) les degrés de destruction approuvés pour le niveau « Protégé B » exigent une dimension de résidu inférieure à 2 mm x 15 mm (lambeaux). **Remarque** : Si l'entrepreneur n'est pas en mesure de satisfaire aux exigences de la GRC en matière de destruction, il doit retourner tous les renseignements et les actifs de nature délicate à la GRC afin qu'ils puissent être détruits selon les règles;
c) les ébauches ou les erreurs d'impression de nature délicate en attente d'élimination doivent être protégées conformément à sa catégorisation de sécurité jusqu'à sa destruction.

4.5. *Transport et transmission des actifs matériels*

4.5.1. L'échange physique d'actifs et de renseignements sur papier de nature délicate doit être sécurisé avant le transport et la transmission. Lorsqu'un service de livraison est utilisé, il doit fournir une preuve d'expédition, ainsi qu'un suivi pendant l'expédition et une attestation de livraison.

a) Transport	1) Transport : transmission d'actifs et de renseignements sur papier de nature délicate, jusqu'au niveau « Protégé B » inclusivement, d'une personne ou d'un lieu à un autre par l'entremise d'une personne **qui a besoin de connaître** les renseignements ou d'accéder aux actifs. 2) Préparation : enveloppe simple, sceau de papier gommé ou mallette verrouillée ou autre contenant de résistance égale ou supérieure. 3) Méthode de livraison : Personnel autorisé.
b) Transmission	1) Transmission : transmission d'actifs et de renseignements de nature délicate, jusqu'au niveau « Protégé B » inclusivement, d'une personne ou d'un lieu à un autre par l'entremise d'une personne **qui n'a pas besoin de connaître** les renseignements ou d'accéder aux actifs. 2) Adresser de façon non spécifique. Ajouter la mention « Ne doit être ouvert que par », en raison des principes du besoin de connaître ou du besoin d'accéder si justifié. 3) Préparation : enveloppe simple, sceau de papier gommé. 4) Méthode de livraison : courrier recommandé, poste prioritaire, messagerie commerciale ou courrier de première classe.

5. Mesures de contrôle générales en sécurité des TI

5.1. *Transfert des obligations en matière de sécurité*

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

5.2. *Rôles et responsabilités liés à la sécurité*

5.2.1. L'entrepreneur doit clairement définir les rôles et responsabilités relatifs aux contrôles et aux fonctions de sécurité de la solution prévue pour lui-même et pour la GRC. Ceci comprend, à tout le moins, les rôles et les responsabilités pour :

a) la gestion des comptes;
b) la protection des frontières;
c) la sauvegarde des actifs et des systèmes d'information;
d) la gestion des incidents;
e) le contrôle du système;
f) la gestion des vulnérabilités.

5.3. *Recours à des sous-traitants ou des sous-sous-traitants*

5.3.1. L'entrepreneur doit fournir une liste des sous-traitants et des sous-sous-traitants qui pourraient être utilisés pour exécuter toute partie du travail visant à fournir le service à la GRC ou qui sont

liés à une enquête sur un événement ou un incident de sécurité susceptible d'avoir une incidence sur les données organisationnelles de la GRC. La liste doit comporter les renseignements suivants :

a) le nom des sous-traitants ou des sous-sous-traitants;
b) le travail qui serait effectué ou le service qui serait fourni par les sous-traitants ou les sous-sous-traitants;
c) l'endroit où les sous-traitants ou les sous-sous-traitants effectueraient le travail.

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

5.3.3. L'entrepreneur doit aviser la GRC de tout nouveau sous-traitant ou sous-sous-traitant au moins 14 jours avant de lui donner accès aux données organisationnelles.

5.4. *Gestion du télétravail*

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

5.4.2. Les lieux de travail peuvent comprendre : i) les installations de la GRC; ii) les lieux d'où s'effectue le télétravail; iii) un hybride des deux. Lorsque le lieu de travail est hybride, le chargé de projet doit fournir un calendrier détaillé indiquant les dates auxquelles le personnel travaillera dans quelle catégorie. Le télétravail comprend tout emplacement se trouvant à l'extérieur d'une installation de la GRC. Le télétravail doit être effectué au Canada, mais des exceptions pour le télétravail à l'extérieur du Canada peuvent être permises dans les pays du Groupe des cinq moyennant une évaluation de sécurité de la GRC et l'approbation écrite du DPS ou de son délégué. Peu importe le lieu de travail à distance, toutes les directives de sécurité énoncées dans le présent document s'appliquent. Ceci comprend les travaux réalisés dans les installations de l'entrepreneur, dans la résidence du personnel de l'entrepreneur ou dans tout autre lieu de travail à distance.

5.4.3. Lorsque l'utilisation de l'équipement fourni par la GRC est requise, le chargé de projet et l'entrepreneur doivent :

a) gérer et surveiller l'accès à distance par l'entrepreneur aux systèmes de la GRC ou à ses données organisationnelles;
b) exécuter l'ensemble des tâches prévues pendant toute la durée du contrat en utilisant l'équipement fourni;
c) fournir de l'équipement standard de la GRC pour le travail à distance, y compris un ordinateur portable imagé de la GRC avec chiffrement complet approuvé du disque;
d) utiliser l'authentification à facteurs multiples avec l'authentifiant standard fournis par la GRC pour toutes les exigences d'accès sécurisé (p. ex. accès au RPV);
e) s'assurer que l'entrepreneur a lu et signé la politique d'utilisation acceptable de la GRC;
f) s'assurer que l'équipement de la GRC demeure en tout temps dans les lieux de travail indiqués.

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

5.5. *Protection des points terminaux*

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

5.6. *Protection cryptographique*

5.6.1. Le personnel de l'entrepreneur doit :

a) configurer toute solution cryptographique qui est utilisée dans le cadre de la mise en œuvre de mesures de protection de la confidentialité ou de l'intégrité ou encore d'un mécanisme d'authentification (p. ex. solutions liées au RPV, TLS, modules logiciels, infrastructure à clé publique et jetons d'authentification, le cas échéant), conformément avec les algorithmes cryptographiques, les tailles de clés cryptographiques et les périodes de validité des clés approuvées par le Centre de la sécurité des télécommunications (CST);
b) utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui ont été validés par le Programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/) et précisés dans le document ITSP.40.111 Algorithmes cryptographiques pour l'information Non classifié,

Protégé A et Protégé B ou dans des versions subséquentes de ce document (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111linformation-non-classifie-protege-https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111-protege-b).

5.7. *Protection des données*

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

a) gérer et surveiller l'accès à distance par l'entrepreneur aux systèmes de la GRC ou à ses données organisationnelles;
b) exécuter l'ensemble des tâches prévues pendant toute la durée du contrat en utilisant l'équipement fourni;
c) fournir de l'équipement standard de la GRC pour le travail à distance, y compris un ordinateur portable imagé de la GRC avec chiffrement complet approuvé du disque;
d) utiliser l'authentification à facteurs multiples avec l'authentifiant standard fournis par la GRC pour toutes les exigences d'accès sécurisé (p. ex. accès au RPV);
e) s'assurer que l'entrepreneur a lu et signé la politique d'utilisation acceptable de la GRC;
f) s'assurer que l'équipement de la GRC demeure en tout temps dans les lieux de travail indiqués.

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

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

5.7.4. Toutes les données organisationnelles au repos hébergées dans un service infonuagique sont nécessaires pour mettre en œuvre un chiffrement qui répond aux exigences de la GRC, ce qui comprend toutes les métadonnées ou tous les journaux dérivés des données organisationnelles ou liés à celles-ci.

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

5.7.6. Les dossiers électroniques et les dispositifs multimédias doivent être nettoyés ou détruits conformément au document ITSP.40.006 Nettoyage des supports de TI (consulter le https://www.cyber.gc.ca/fr/orientation/nettoyage-des-supports-de-ti-itsp40006 pour en savoir plus).

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

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

5.7.9. L'entrepreneur doit :

a) mettre en œuvre un chiffrement de bout en bout pour toutes les données protégées en mouvement vers et depuis tous les services infonuagiques. Tout chiffrement des données en mouvement doit satisfaire aux exigences du document ITSP.40.111 Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B, ou des versions ultérieures (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111-);
b) mettre en œuvre le chiffrement des données au repos pour tous les services qui hébergent des données organisationnelles, y compris toutes les métadonnées ou tous les journaux dérivés des données organisationnelles ou liés à celles-ci, lorsque le chiffrement des données inactives demeure en vigueur, ininterrompu et actif en tout temps, même en cas de panne d'équipement ou de technologie, conformément au document ITSP.40.111 Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B, ou des versions ultérieures (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111);
c) mettre en place des contrôles de sécurité qui restreignent l'accès administratif aux données organisationnelles, y compris à toutes les métadonnées ou à tous les journaux dérivés des données et des systèmes organisationnels ou connexes par l'entrepreneur et qui permettent d'exiger l'approbation de la GRC avant que l'entrepreneur puisse accéder aux données organisationnelles pour effectuer des activités de soutien, d'entretien ou d'exploitation;
d) prendre des mesures raisonnables pour s'assurer que le personnel de l'entrepreneur n'a pas de droits d'accès permanents ou continuels aux données organisationnelles, sans un besoin de connaître, y compris les ressources qui fournissent un soutien technique ou à la clientèle, en fonction de l'approbation de la GRC;

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

5.8. *Emplacement des données (résidence)*

5.8.1. Toutes les données organisationnelles de nature délicate, y compris les données de sauvegarde ou les données conservées à des fins de redondance, doivent se trouver dans les frontières géographiques du Canada ou dans une ambassade ou 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 doivent être traitées par l'entrepreneur dans les frontières géographiques du Canada*.

*Des exceptions pour le traitement de données organisationnelles de niveau « Protégé A » à l'extérieur du Canada peuvent être permises à partir des pays du Groupe des cinq moyennant une évaluation de sécurité de la GRC et l'approbation écrite du DPS ou de son délégué.

5.10. *Transport et transmission des données*

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

5.10.2. Le mot de passe pour le dispositif de stockage portatif doit être fourni hors bande, soit en personne ou par téléphone, et uniquement aux membres du personnel de l'entrepreneur ayant obtenu la cote de sécurité appropriée.

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

5.11. *Élimination des données et retour des dossiers*

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

a) Nettoyage des supports de TI (ITSP.40.006);
b) Guidelines for Media Sanitization (NIST SP 800-88);
c) À la demande de la GRC, l'entrepreneur doit produire un document qui décrit son processus d'élimination ou de réutilisation des ressources.

5.11.2. L'entrepreneur doit confirmer à la GRC, par la présentation d'une lettre d'attestation ou d'entrées de journal, qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon les moyens appropriés, et qu'il est en mesure d'empêcher le rétablissement de tout système retiré ou détruit, de toute capacité (logiciel ou processus), de toute donnée ou de toute information une fois que la GRC a cessé d'utiliser les services. La GRC peut exiger une preuve que les clés de chiffrement ont été détruites ou que les données ont subi un crypto-déchiquetage avec succès pour 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 tous les contrôles de protection des données et de sécurité au même niveau décrit en détail pour ces exigences de sécurité pendant la période où la GRC récupère les données organisationnelles;
b) fournir à la GRC l'accès à ses données organisationnelles pendant une période qui permet à la GRC de récupérer toutes les données organisationnelles de l'entrepreneur.

5.12. *Intervention en cas d'incident de sécurité*

5.12.1. Le *National Institute of Standards and Technology* (NIST) définit un incident de sécurité comme suit : « Un incident 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 infraction ou une menace imminente d'infraction des politiques de sécurité, des procédures de sécurité ou des politiques d'utilisation acceptable. » En conséquence, l'entrepreneur doit alerter rapidement le responsable de la sécurité de la GRC (par téléphone ou par courriel) de toute compromission, de toute atteinte ou de toute preuve d'un tel événement, notamment :

a) tout incident de sécurité;
b) toute défaillance de la sécurité d'un actif;
c) toute fuite de données;
d) tout accès irrégulier ou non autorisé à un actif;
e) toute copie à grande échelle d'un actif informationnel;
f) toute autre activité irrégulière relevée par l'entrepreneur qui l'amène à croire raisonnablement que le risque de compromission ou d'atteinte à la sécurité ou à la vie privée est ou peut être imminent, ou que les mesures de protection existantes ont cessé de fonctionner.

5.12.2. Si l'entrepreneur prend connaissance d'une compromission ou d'une atteinte à la sécurité entraînant la destruction, la perte, la modification, la divulgation non autorisée ou l'accès accidentel ou illégal des données du client ou personnelles, pendant le traitement par l'entrepreneur, chacun étant un « incident de sécurité », il doit immédiatement ou au moins dans les 24 heures :

a) aviser le responsable de la sécurité de la GRC de l'incident de sécurité;
b) enquêter sur l'incident de sécurité et fournir à la GRC des renseignements détaillés sur cet incident;
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 photocopies*

5.13.1. L'impression, la numérisation ou 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, de numériseurs ou de photocopieurs supplémentaires réservés à ces fonctions qui ne sont pas directement connectés à un réseau, y compris Internet. Les connexions locales réservées de ces appareils aux points terminaux de l'entrepreneur sont acceptables;
b) respecter les exigences énoncées dans la section Sécurité matérielle sur l'entreposage, la production de renseignements sur papier ou d'autres actifs et la destruction;
c) nettoyer ou détruire les appareils d'impression, de numérisation et de photocopie (comme les appareils multifonctions, les imprimantes, les photocopieurs) conformément au document ITSP.40.006 Nettoyage des supports de TI (consulter le 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. Lorsque l'utilisation de l'équipement de la GRC est requise, le personnel de l'entrepreneur se verra attribuer des authentifiants de la gestion des identités et de l'accès (IAM) leur permettant d'accéder aux actifs protégés de la GRC. L'authentifiant IAM de la GRC ne doit être utilisé que dans le cadre de l'exécution des tâches décrites dans les documents contractuels et doit être révoqué à la fin du présent contrat.

5.15. *Résiliation*

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

a) transmettre un avis de résiliation au chargé de projet le jour même de la résiliation;
b) retirer l'accès au système d'information le jour même de la résiliation;
c) résilier ou révoquer l'identifiant ou l'authentifiant associé à la personne dans un délai de 24 heures;
d) mener des entrevues de fin de contrat qui comprennent une discussion sur les éléments énoncés dans la Norme sur le filtrage de sécurité du Secrétariat du Conseil du Trésor (SCT) et toute disposition connexe du Programme de sécurité industrielle;
e) soumettre le formulaire d'information sur la sécurité 330-47 pour la résiliation de l'autorisation de sécurité de l'entrepreneur;
f) récupérer tous les actifs liés au système d'information de la GRC se rattachant à la sécurité, y compris les cartes d'accès, dans un délai de 24 heures;
g) conserver l'accès à l'information et aux systèmes d'information de la GRC qui étaient sous le contrôle de la personne faisant l'objet de la résiliation.

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

a) ordinateurs portatifs;
b) téléphones cellulaires;
c) clés USB;
d) cartes à puce.

6. Obligations en matière de sécurité des logiciels-services et plateformes-services

Les obligations de sécurité supplémentaires suivantes doivent être respectées lorsqu'un entrepreneur ou un contrat met en cause l'utilisation ou le développement d'environnements de logiciels-services ou de plateformes-services non contrôlés par la GRC pour l'exécution de services contractuels.

6.1. *Sécurité des réseaux et des communications*

6.1.1. L'entrepreneur doit mener à bien les tâches suivantes :

a) établir des connexions sécurisées aux services, notamment en assurant la protection des données en mouvement entre la GRC et le Service au moyen du protocole TLS 1.2 ou de versions ultérieures;
b) utiliser des protocoles ainsi que des algorithmes et des certificats cryptographiques pris en charge et à jour, comme le décrivent les normes ITSP.40.062 (https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062) et ITSP.40.111 (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b) du CST;
c) utiliser des certificats correctement configurés dans les connexions TLS, conformément aux directives du CST, ITSP.40.062 (https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062);
d) s'assurer qu'il peut travailler avec la solution de courtier 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 vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, notamment :

a) NIST;
b) norme ISO 27034;
c) ITSG-33;
d) SAFECode;
e) norme d'Open Web Application Security Project (OWASP) comme l'Application Security Verification Standard (ASVS);
f) norme équivalente approuvée par écrit par la GRC.

6.2.2. À la demande de la GRC, l'entrepreneur doit produire un document qui décrit son logiciel documenté, ainsi que l'approche et le processus adoptés relativement au cycle de vie du développement du système.

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

6.2.4. Le personnel de l'entrepreneur qui travaille sur les actifs de TI de la GRC dans l'environnement de développement de la GRC doit suivre les processus de développement de la GRC et respecter toutes les structures de gouvernance de la gestion de l'information et technologie de l'information (GI-TI) de la GRC.

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

6.3.1. S'il y a lieu, l'entrepreneur doit démontrer sa conformité aux exigences de sécurité choisies par la GRC pour la portée des services fournis par l'entrepreneur. La conformité devra être démontrée par la schématisation des contrôles de sécurité avec les certifications de tiers applicables (c.-à-d. IOS 27001, SOC 2 de type 2). Dans le cas des renseignements non classifiés, la validation des contrôles de sécurité par la présentation de preuves directement à la GRC peut être acceptable (c.-à-d. CAIQ de la CSA).

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

6.3.3. Dans le cas où l'entrepreneur ou le service a été évalué et validé au moyen du processus d'évaluation de la sécurité des technologies de l'information (TI) s'appliquant aux entrepreneurs fournissant des solutions de sécurité en infonuagique (ITSM.50.100) du Centre canadien pour la cybersécurité (CCC) (https://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. Il doit notamment fournir à la GRC une copie des documents suivants :

a) lettre de confirmation qui indique qu'il a adhéré au programme;
b) rapport d'évaluation le plus récent fourni par le CCC;
c) rapport sommaire le plus récent fourni par le CCC.

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 entièrement ou en partie par des entrepreneurs ne soient transférées dans un environnement de production, une autorisation provisoire d'exploiter ou une autorisation d'exploitation (AE) complète doit être accordée. L'obtention AE complète ou provisoire nécessite une évaluation de sécurité dans le cadre du processus d'évaluation et autorisation de la sécurité, 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 authentifiants de la GRC ne sont pas requis, l'entrepreneur doit mettre en œuvre ce qui suit :

a) l'authentification à facteurs multiples conformément à la norme ITSP.30.031 V3 du CST (ou à ses versions ultérieures) (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de) au moyen d'authentifiants approuvés par le GC;
b) l'accès en fonction du rôle;
c) les contrôles d'accès aux objets entreposés;
d) les politiques d'autorisation granulaire pour permettre ou limiter l'accès.

6.5. *Gestion d'accès privilégié*

6.5.1. Lorsque l'entrepreneur ou son personnel, y compris les sous-traitants, accèdent aux 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 par tout locataire de la GRC.

6.5.2. Lorsque l'entrepreneur n'exerce pas ses activités dans un local 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 pour s'assurer que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services de la GRC;
b) restreindre et minimiser l'accès aux services et aux données organisationnelles seulement aux appareils autorisés et aux utilisateurs finaux ayant explicitement besoin de cet accès;
c) appliquer et vérifier les autorisations d'accès aux services et aux données organisationnelles;
d) limiter tous les accès aux interfaces de service qui hébergent les données organisationnelles à des utilisateurs finaux, des dispositifs et des processus (ou des services) identifiés, authentifiés et autorisés de manière unique;
e) mettre en œuvre des politiques sur les mots de passe afin de protéger les authentifiants contre les attaques en ligne ou hors ligne et de détecter ces attaques en consignant et en surveillant des événements tels que (i) l'utilisation réussie des authentifiants (ii) l'utilisation inhabituelle de ces derniers et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément à la version 3 (ou aux versions ultérieures) des Normes ITSP.30.031 du CST (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);

f) mettre en place des mécanismes d'authentification à facteurs multiples pour authentifier les utilisateurs finaux ayant des privilèges d'accès, conformément à la norme ITSP.30.031 V3 du CST (ou à ses versions ultérieures) (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);
g) mettre en place des mécanismes de contrôle d'accès fondés sur le rôle qui forment la base de l'accès aux données organisationnelles;
h) définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, les rôles de développement des rôles opérationnels et les rôles de gestion de l'accès des autres rôles opérationnels;
i) adhérer aux principes du moindre privilège et du besoin de connaître pour accorder l'accès aux services et aux données organisationnelles;
j) appliquer, si elle est requise, une double autorisation pour les mesures jugées très délicates ou à risque élevé par la GRC;
k) utiliser des points terminaux sécurisés (p. ex. ordinateurs, appareils des utilisateurs finaux, serveurs de secours) configurés de manière à offrir une fonctionnalité minimale afin d'assurer le soutien et l'administration des services et de l'infrastructure de l'entrepreneur et qui interdisent l'utilisation de dispositifs de stockage de masse USB, s'il y a lieu;
l) mettre en œuvre un processus automatisé pour vérifier périodiquement, au minimum, la création, la modification, l'activation, la désactivation et la suppression de comptes;
m) révoquer, en cas de cessation d'emploi, les identifiants et les authentifiants d'accès associés à tout personnel de l'entrepreneur;
n) produire un document qui décrit l'approche et le processus de l'entrepreneur pour la gestion et la surveillance des accès privilégiés aux services, à la demande de la GRC.

6.5.3. Le personnel de l'entrepreneur se verra attribuer des rôles au sein de l'infrastructure de la GRC en fonction de ses tâches. Sous aucune circonstance le personnel de l'entrepreneur ne doit avoir accès au compte principal ou au compte doté de privilèges de base.

6.6. *Gestion des comptes principaux*

6.6.1. L'entrepreneur doit veiller à protéger adéquatement le processus de gestion de comptes utilisé pour fournir et soutenir le service pour la GRC. Ces mesures de sécurité doivent au minimum :

a) accorder les privilèges de compte principal exclusivement au personnel de la GRC de manière à ce que le fournisseur remette l'entièreté du contrôle du service à la GRC;
b) convenir lorsque le personnel de l'entrepreneur doit ou souhaite accéder à un compte principal. L'entrepreneur doit alors :
    i) limiter l'accès aux seuls utilisateurs autorisés et approuvés par la GRC auxquels la GRC permet d'effectuer des transactions et de remplir des fonctions, comme celles de créer et d'accorder des comptes principaux;

ii) garantir la séparation des fonctions des personnes;
iii) utiliser le principe de privilège minimal, y compris en ce qui concerne les fonctions spécifiques de sécurité et les comptes privilégiés;
iv) veiller à ce que les utilisateurs autorisés soient formés et sensibilisés à la sécurité dans le cadre de leur intégration à l'emploi et lorsque leurs rôles changent;
v) créer, protéger et conserver les dossiers de vérification liés aux activités à l'appui de la gestion des comptes du service fourni à la GRC;
vi) fournir à la GRC des rapports sur les événements vérifiés liés aux mesures relatives à l'accord et à la gestion des comptes principaux;
vii) veiller à la protection des données organisationnelles durant et après les actions posées par le personnel, comme dans les cas de cessation d'emploi ou de mutation.

7. Sécurité du personnel

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

7.2. Lorsque la GRC détermine, par exemple, qu'une autorisation d'accès à l'installation (niveau 2), une cote de fiabilité approfondie, ou une cote de fiabilité approfondie avec autorisation de niveau secret est nécessaire, elle invite les entrepreneurs à visiter son portail en ligne pour y remplir les formulaires d'autorisation.

7.3. Tout le personnel et tous les sous-traitants de l'entrepreneur doivent maintenir une autorisation de sécurité correspondant au caractère délicat des travaux à réaliser tout au long du cycle de vie du contrat (conformément aux dispositions de la LVERS).

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

7.5. Lorsque du personnel non présélectionné est requis, les rôles doivent être identifiés et approuvés au préalable par la GRC dans la LVERS une fois le fournisseur retenu choisi.

7.6. L'entrepreneur sera tenu d'informer la GRC de toute modification au personnel en ce qui concerne les exigences relatives à la sécurité. Par exemple : Lorsqu'un employé détenant une attestation de sécurité quitte l'entreprise ou ne participe plus à l'exécution du contrat de la GRC, lorsqu'un nouvel employé doit obtenir une attestation de sécurité, ou encore lorsqu'un employé doit faire renouveler son attestation de sécurité.

7.7. La GRC procédera à des vérifications de filtrage de sécurité du personnel dépassant les exigences de sécurité prescrites par la Politique sur la sécurité du gouvernement.

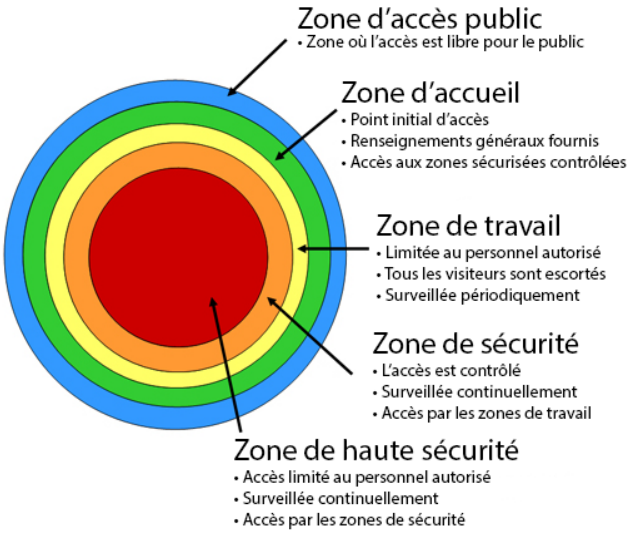
7.8. La GRC se réserve le droit d'augmenter ou de modifier les niveaux de sécurité requis, selon ce qu'elle juge approprié, lorsque les rôles professionnels auront été mieux définis.

**Les équivalences de cote ou d'autorisation de sécurité doivent être approuvées par écrit par le DPS ou son délégué au nom de la GRC.*

Annexe A – Concept des zones de sécurité

La *Politique sur la sécurité du gouvernement (section 10.8 – Limites à l'accès)* stipule que « les ministères doivent limiter l'accès aux renseignements classifiés et protégés et autres actifs aux seules personnes qui ont besoin de les connaître et qui ont la cote de fiabilité ou de sécurité appropriée ».

La *Norme opérationnelle sur la sécurité matérielle (section 6.2, Hiérarchie des zones)* stipule que « les ministères doivent assurer l'accès aux actifs protégés et classifiés et leur protection en fonction d'une hiérarchie de zones clairement reconnaissables. »



La zone d'accès public est une zone où l'accès est libre pour le public et qui entoure habituellement un immeuble gouvernemental ou en fait partie. Par exemple, les terrains entourant un bâtiment ou les corridors publics et les vestibules d'ascenseur dans les immeubles à locataires multiples.

La zone d'accueil est une zone 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 se fait le premier contact entre les visiteurs et le Ministère, y compris des endroits où des services sont fournis et où des renseignements sont échangés. L'accès du public peut y être restreint à certaines heures de la journée ou pour des motifs particuliers.

La zone de travail est une zone dont l'accès est limité au personnel qui y travaille et aux visiteurs dûment escortés; elle doit être indiquée par un périmètre reconnaissable et surveillée sur une base périodique. Par exemple, un espace à bureaux à aire ouverte typique ou le local des installations électriques typique.

La zone de sécurité est une zone dont l'accès est limité au personnel autorisé et aux visiteurs autorisés dûment escortés; elle doit être indiquée par un périmètre reconnaissable et être surveillée continuellement (24 heures par jour et 7 jours par semaine). Par exemple, une zone où des renseignements secrets sont traités ou conservés.

La zone haute sécurité est une zone dont l'accès est limité au personnel autorisé ayant fait l'objet d'un contrôle approprié et aux visiteurs autorisés et dûment escortés; elle doit être indiquée par un périmètre construit conformément aux spécifications recommandées dans l'évaluation de la menace et des risques (EMR), être surveillée continuellement (24 heures par jour et 7 jours par semaine), et être une zone où les détails d'accès sont enregistrés et vérifiés. Par exemple, une zone où des actifs de grande valeur sont manipulés par des membres du personnel sélectionnés.

L'accès aux zones devrait reposer sur le concept du « besoin de connaître », et la restriction de l'accès sert à protéger le personnel et les actifs de valeur. Consultez le Guide G1-026 de la GRC, Guide pour l'établissement des zones de sécurité matérielle pour des renseignements plus détaillés.

Annexe B – Guide de classification de sécurité

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

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

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

Rôle ou fonction	Type de données consultées	Lieu de travail (inclure la ville si elle se trouve à l'extérieur du Canada)	Description et détails du rôle	Niveau de sécurité
Développeur d'applications	*« Protégé B » – production de données, configurations, code, accès au système en continu tout au long du contrat*	*À distance – au Canada*	- *Architecture du système* - *Développement d'applications dans les locaux de la GRC* - *Dépannage et maintenance du système*	

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

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

Des contrôles d'accès doivent être mis en œuvre pour restreindre l'accès à l'information aux personnes de bonne foi avec le « besoin de connaître ».

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

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

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

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

Le responsable de la sécurité de la GRC est le premier point de contact pour fournir, aux entrepreneurs, des conseils et une orientation sur les exigences et les contrôles de la politique de sécurité.

Travail sans papier

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

L'impression, la numérisation et la photocopie de renseignements papier de nature délicate sont interdites sans l'approbation de la GRC et sont interdites à l'extérieur d'une zone de travail (p. ex. maison, hôtel, espace de travail partagé).

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

- Le chiffrement complet du disque est requis pour tous les appareils qui traitent des données organisationnelles de nature délicate.
- Toutes les données organisationnelles de nature délicate doivent être chiffrées au minimum au moyen de l'algorithme de norme de chiffrement avancé (AES) dont la longueur des clés est de 128 (AES-128).

L'authentification à facteurs multiples est requise pour l'accès à des données organisationnelles de nature délicate.

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

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

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

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

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

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

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

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

Contrôle de l'espace de travail

Le personnel contractuel doit :

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

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

- utiliser exclusivement de l'équipement et des logiciels approuvés;
- utiliser des casques d'écoute pour l'audio ainsi qu'un espace de travail à l'abri des regards, ou une pièce fermée aménagée de telle sorte que des personnes partageant le même espace ne puissent ni voir ni entendre ce qui s'y passe, et que l'on ne puisse pas voir par les fenêtres;
- activer les caméras Web uniquement lorsqu'elles sont utilisées;
- désactiver le microphone au moment opportun et procéder rapidement au blocage visuel de la caméra au besoin;
- ne pas discuter de données organisationnelles de nature délicate de niveau supérieur à « Protégé B »;
- s'assurer que les appareils mobiles sont laissés à l'extérieur des zones où des discussions de nature délicate ont lieu;
- éteindre les appareils sans fil permettant la transmission de la voix ou désactiver les microphones de ces appareils pendant les réunions où il est question de données organisationnelles de nature délicate.

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

Exigences supplémentaires pour les télétravailleurs contractuels utilisant de l'équipement de la GRC

Lorsqu'il utilise l'équipement de technologies de l'information et des communications de la GRC, le personnel de l'entrepreneur doit :

- lire et signer les pratiques d'utilisation acceptable pour la technologie de l'information de la GRC;
- respecter les politiques et les normes de la GRC en matière de TI et de sécurité.

Résiliation ou expiration du contrat

Au moment d'une résiliation ou d'une expiration visant tout personnel de l'entrepreneur, l'entrepreneur doit immédiatement aviser le chargé de projet de la GRC, récupérer tout l'équipement de TI de la GRC ainsi que toute information connexe, et les soumettre au chargé de projet de la GRC aux fins d'élimination ou de retrait de l'information liée aux contrats de la GRC.

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
2021-1117913
Security Classification / Classification de sécurité unclassified

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	2. Branch or Directorate / Direction générale ou Direction
RCMP/GRC	Informatics/2. Informatique
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant
	Resource Scheduling Vendor unknown at this time/Planification des ressources –

4. Brief Description of Work / Brève description du travail

Setup and configuration of a SaaS solution. This solution is for Depot Resource Scheduling application that is RFP currently with PWGSC.

4. Installation et configuration d' une solution SaaS. Cette solution concerne l' application de planification des ressources – Division Dépôt, qui fait actuellement l' objet d' une DP avec TPSGC.

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

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

PROTECTED A / PROTÉGÉ A ☑	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) ☐

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

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

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

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

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

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

☑ RELIABILITY STATUS COTE DE FIABILITÉ	☐ CONFIDENTIAL CONFIDENTIEL	☐ SECRET SECRET	☐ TOP SECRET TRÈS SECRET
☐ TOP SECRET– SIGINT TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL NATO CONFIDENTIEL	☐ NATO SECRET NATO SECRET	☐ COSMIC TOP SECRET COSMIC TRÈS SECRET
☐ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

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

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

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

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 TRES SECRET
Information / Assets Renseignements / Biens	✔															
Production																
IT Media / Support TI	✔															
IT Link / Lien électronique	✔															

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

☑ 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).