

TABLE DES MATIÈRES

TABLE DES MATIÈRES	2
PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX.....	4
1.1 Introduction.....	4
1.2 Sommaire	4
1.3 Comptes rendus	5
1.4 Exigences obligatoires.....	5
PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES	6
2.1 Instructions, clauses et conditions uniformisées	6
2.2 Présentation des soumissions.....	6
2.3 Demandes de renseignements en période de soumission.....	6
2.4 Lois applicables	6
PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS	9
3.1 Instructions pour la préparation des soumissions	9
3.2 Section I : Soumission technique	9
3.3 Section II : Soumission financière	11
3.4 C3011T (2010-01-11) – Fluctuation du taux de change.....	13
3.5 Section III : Attestations et Renseignements supplémentaires	13
3.6 Section IV : Processus continu d'intégrité de la chaîne d'approvisionnement	13
PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION	14
4.1 Procédures d'évaluation	14
4.2 Évaluation technique	14
4.3 Évaluation financière	14
4.4 Processus d'intégrité de la chaîne d'approvisionnement.....	16
4.5 Méthode de sélection – Meilleure note combinée pour le mérite technique et le prix	16
PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES	18
5.1 Attestations exigées avec la soumission	18
5.2 Attestations préalables à l'attribution du contrat et renseignements supplémentaires	18
PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES	21
6.1 Exigences relatives à la sécurité	21
PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT	22
A1. Guide des clauses et conditions uniformisées d'achat.....	22
A2. Modalités du contrat	22
A3. Conditions générales.....	22
APPENDICE B – CONDITIONS SUPPLÉMENTAIRES	23
B1. Ordre de priorité des documents	23
B2. Clauses de CIC	23
B3. Clauses du Guide des CUA	23
B4. Exigences en matière de sécurité	23
B5. Période du contrat et Renouvellement automatique	23
B6. Résiliation avec avis de trente (30) jours.....	24
B7. Attestations / Conformité et renseignements supplémentaires	24
B8. Exigences en matière d'assurance.....	25
B9. Énoncé des travaux.....	25
B10. Responsables.....	25
B11. Divulgence proactive de marchés conclus avec d'anciens fonctionnaires.....	27
B12. Exigence.....	27
B13. Solution	27
B14. Services.....	28

B15.	Niveau de Service	30
B16.	Accords sur les niveaux de service (ANS)	30
B17.	Documentation	31
B18.	Travaux	32
B19.	Base de Paiement	33
B20.	Paiement	34
B21.	Responsabilité	35
B22.	Disposition générales	35
APPENDICE C – MODALITÉS DE PAIEMENT		36
C1.	Base de Paiement	36
C2.	Autorisation de tâches	36
C3.	Base de paiement – Tâches autorisées	37
C4.	Mode de paiement	37
C5.	Taxes applicables	38
C6.	Instructions relatives à la facturation	38
C7.	Frais de déplacement et de subsistance	39
C8.	Sous-traitance	39
APPENDICE D – ÉNONCÉ DES TRAVAUX		40
ANNEXE A à APPENDICE D –Énoncé des exigences de SGA IRCC		50
APPENDICE E – BASE DE PAIEMENT		51
APPENDICE F – LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA		57
SÉCURITÉ (LVERS).....		57
ANNEXE A à APPENDICE F		60
ANNEXE B À APPENDICE F – GUIDE DE CLASSIFICATION DE SÉCURITÉ		71
APPENDICE G – OBLIGATIONS EN MATIÈRE DE SÉCURITÉ ET PROTECTION DE LA VIE PRIVÉE		74
APPENDICE H – PROCESSUS D’INTÉGRITÉ DE LA CHAÎNE D’APPROVISIONNEMENT		99
APPENDICE I – FORMULAIRE D’AUTORISATION DE TÂCHES		103
APPENDICE J – ACCORDS SUR LES NIVEAUX DE SERVICE (ANS).....		105
APPENDICE K – ENTENTE DE NON-DIVULGATION DE SPAC RELATIF A L’INTÉGRITÉ DE LA CHAÎNE		106
D’APPROVISIONNEMENT		106
APPENDICE L – PROGRAMME D’ÉVALUATION DE LA SÉCURITÉ DES TI DES LOGICIELS-SERVICES :		107
PROCESSUS D’INTEGRATION		107
APPENDICE M – EXIGENCES RELATIFS A LA SÉCURITÉ NIVEAU 1		108
APPENDICE N – RENSEIGNEMENTS SUR LE FOURNISSEUR ET AUTORISATION.....		122
APPENDICE O – RENSEIGNEMENTS SUR LE FOURNISSEUR ET AUTORISATION		123



PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La demande de soumissions contient sept parties, ainsi que des pièces jointes et des appendices, 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: contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent.

1.2 Sommaire

1.2.1 La présente demande de soumission est émise pour répondre à un besoin du ministère de Citoyenneté et Immigration Canada HEREIN Immigration, Réfugiés et Citoyenneté Canada (IRCC) visant l'acquisition d'un système de gestion de l'apprentissage (SGA) qui peut être configuré pour répondre aux exigences spécifiques d'IRCC et permet la gestion, la prestation, le suivi, la production de rapports et l'évaluation de tout le contenu de formation et d'apprentissage.

L'état final sera un système infonuagique accessible par navigateur et reposant sur la technologie, disponible pour 12 000 employés ministériels. Ce système permettra aux employés d'accéder à du contenu d'apprentissage tout en conservant et en suivant leur progrès. L'application ou le système infonuagique doit offrir une expérience d'apprentissage simplifiée et améliorée de bout en bout et permettre un contrôle efficace, complet et global de la gestion, de l'analyse, de l'administration et de la communication du contenu pédagogique auprès des apprenants, des fournisseurs de services d'apprentissage et des décideurs. Aux fins de la présente demande de soumissions, les soumissionnaires doivent satisfaire aux exigences de sécurité identifiées au *Palier 1 – Exigences de sécurité pour logiciel-service*, mais peuvent être demandé de respecter le *Palier 2 – Exigences de sécurité pour logiciel-services* après l'attribution du contrat.

1.2.2 Contrat unique

Le Canada souhaite conclure un contrat pour un Solution de gestion de l'apprentissage, dont une portion des travaux sera effectués « sur demande » conformément à l'Appendice D – Énoncé des travaux, pour une période de six (6) années, périodes d'option comprises.

1.2.3 Exigences relatives à la sécurité

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, Appendice F et G. 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.

1.2.4 Accords commerciaux

Ce besoin est assujéti aux dispositions de l'Accord sur les marchés publics de l'Organisation mondiale du commerce (AMP-OMC), de l'Accord économique et commercial global entre le Canada et l'Union européenne (AECG), de l'Accord de libre-échange canadien (ALEC), de l'Accord de libre-échange Canada-Colombie, de l'Accord de libre-échange Canada-Chili, de l'Accord de libre-échange Canada-Pérou, de l'Accord de libre-échange Canada-Panama et de l'Accord de libre-échange Canada-Honduras.

1.2.5 Autorisations de tâches

La présente demande de soumissions vise à établir un contrat comportant des autorisations de tâches pour la livraison du besoin décrit dans la demande de soumissions aux utilisateurs désignés, et ce, partout au Canada, sauf dans les zones visées par des ententes sur les revendications territoriales globales (ERTG) au Yukon, dans les Territoires du Nord-Ouest, au Nunavut, au Québec et au Labrador. Toute demande de livraison dans les zones visées par des ERGT au sein du Yukon, des Territoires du Nord-Ouest, du Nunavut, du Québec ou du Labrador, devra faire l'objet de marchés distincts, attribués en dehors du contrat subséquent.

1.2.6 Programme de contrats fédéraux

Le Programme de contrats fédéraux pour l'équité en matière d'emploi s'applique au présent besoin; veuillez-vous référer à la Partie 5 – Attestations et renseignements supplémentaires, la Partie 7 – Clauses du contrat subséquent et l'annexe intitulée Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation.

1.2.7 Accessibilité

La prise en compte des critères et des caractéristiques d'accessibilité est obligatoire pour cette exigence. Pour obtenir de plus amples renseignements, veuillez consulter la [Politique sur les marchés du Conseil du Trésor](#).

1.2.8 Diversité

IRCC est résolu à assurer un processus d'approvisionnement qui reflète la diversité du Canada. Nous nous efforçons de cerner et de réduire les obstacles dans nos processus d'approvisionnement. Nous continuons d'améliorer les pratiques afin qu'elles permettent d'assurer une bonne représentation des groupes visés par l'équité. À cette fin, nous encourageons les entreprises appartenant à des minorités visibles à soumissionner dans le cadre de nos processus.

1.3 Comptes rendus

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.

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).

1.4 Exigences obligatoires

Lorsque les mots « doit », « devrait » ou « devra » apparaissent dans la présente DP, on doit considérer cette disposition comme une exigence obligatoire.

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

Toutes les instructions, clauses et conditions d'Immigration, Réfugiés et Citoyenneté Canada (IRCC) identifiées dans la demande de soumissions par un numéro, une date et un titre sont reproduites sur le site [Web d'IRCC](#).

Toutes les clauses du Guide des clauses et conditions uniformisées d'achat (CCUA) qui portent sur des instructions particulières ne faisant pas partie des instructions uniformisées identifiées par un numéro, une date et un titre sont reproduites dans [le Guide des clauses et conditions uniformisées d'achat](#) de Travaux publics et Services gouvernementaux Canada (TPSGC).

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 intitulé *Instructions uniformisées de CIC – Biens ou services – Besoins concurrentiels* [CIC-SI-001 \(2016-05-26\)](#) est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

La sous-section 5.4 des Instructions uniformisées CIC-SI-001 (2016-05-26) - Biens ou services - Besoins concurrentiels, est modifiée comme suit:

Supprimer: 90 jours

Insérer: 250 jours

2.2 Présentation des soumissions

Les soumissions doivent être envoyées uniquement à l'Immigration, Réfugiés et Citoyenneté Canada au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la présente invitation à soumissionner.

En raison de la nature de la demande de soumissions, les soumissions transmises par télécopieur ne seront pas acceptées.

2.3 Demandes de renseignements en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins 5 jours civils avant la clôture de la demande de soumissions. Toute demande reçue après ce délai pourrait ne pas être répondue.

Les soumissionnaires devraient citer le plus fidèlement possible l'article numéroté dans la demande de soumissions auquel se rapporte la demande de renseignements. Ils devraient également énoncer chaque question de manière suffisamment détaillée pour que les représentants du gouvernement du Canada puissent 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 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 permettrait pas de les diffuser à tous les soumissionnaires.

2.4 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur en Ontario.

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 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 demande de soumissions sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la demande de soumissions. Les soumissionnaires doivent indiquer de façon claire les améliorations proposées, ainsi que les motifs de celles-ci.

Les suggestions, qui ne restreignent pas la concurrence ou qui ne favorisent pas un soumissionnaire en particulier, seront examinées à la condition d'être soumises à l'autorité contractante, conformément au moins cinq (5) jours avant la clôture de la demande de soumissions. Le Canada aura le droit d'accepter ou de rejeter n'importe laquelle ou la totalité des suggestions proposées

2.6 Ancien fonctionnaire

Les contrats attribués à des 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 des anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée ci-dessous avant l'attribution du contrat. Si la réponse aux questions et, s'il y a lieu les renseignements requis, n'ont pas été fournis par le temps où l'évaluation des soumissions est complétée, le Canada informera le soumissionnaire du délai à l'intérieur duquel l'information doit être fournie. Le défaut de se conformer à la demande du Canada et satisfaire à l'exigence dans le délai prescrit rendra la soumission non recevable.

Définition

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, un ancien membre des Forces armées canadiennes ou de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être :

- a. un individu;
- b. un individu qui s'est incorporé;
- c. une société de personnes constituée d'anciens fonctionnaires; ou
- d. une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.

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

« 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, et 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 ci-dessus, est-ce que le soumissionnaire est un ancien fonctionnaire touchant une pension? **Oui** () **Non** ()

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

- a. le nom de l'ancien fonctionnaire;
- b. la date de cessation d'emploi dans la fonction publique ou de la retraite.

En fournissant cette information, les soumissionnaires acceptent que le statut du soumissionnaire retenu, en tant qu'ancien fonctionnaire touchant une pension en vertu de la LPFP, soit publié dans les rapports de divulgation proactive des marchés, sur les sites Web des ministères, et ce conformément à l'[Avis sur la Politique des marchés : 2012-2](#) et les [Lignes directrices sur la divulgation des marchés](#).

Directive sur le réaménagement des effectifs

Est-ce que le soumissionnaire est un ancien fonctionnaire qui a reçu un paiement forfaitaire en vertu de la Directive sur le réaménagement des effectifs? **Oui** () **Non** ()

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

- a. le nom de l'ancien fonctionnaire;
- b. les conditions de l'incitatif versé sous forme de paiement forfaitaire;
- c. la date de la cessation d'emploi;
- d. le montant du paiement forfaitaire;
- e. le taux de rémunération qui a servi au calcul du paiement forfaitaire;
- f. la période correspondant au paiement forfaitaire, incluant la date du début, 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.

Pour tous les contrats attribués pendant la période du paiement forfaitaire, le montant total des honoraires qui peut être payé à un ancien fonctionnaire qui a reçu un paiement forfaitaire est limité à 5 000 \$, incluant les taxes applicables.



PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

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

- Section I : Soumission technique (une (1) copie électronique par courriel)
- Section II : Soumission financière (une (1) copie électronique par courriel)
- Section III : Attestations et Renseignements supplémentaires (une (1) copie électronique par courriel)
- Section IV : Information sur l'intégrité de la chaîne d'approvisionnement (une (1) copie électronique par courriel)

En raison de la nature de la demande de soumissions, les soumissions transmises par les services epost Connect et par télécopieur ne seront pas acceptées. Conformément à la section 2.2, les offres seront transmises par courrier électronique.

Le Canada demande que les répondants soumettent leur réponse par courriel, en format PDF non protégé (c.-à-d. sans mot de passe). La taille complète des courriels contenant une réponse ne doit pas dépasser 10 Mo. Les courriels dépassant 10 Mo ne seront pas reçus. Si la taille des courriels dépasse 10 Mo, les répondants doivent communiquer avec l'autorité contractante au moins 48 heures avant la date de clôture pour discuter des solutions de rechange.

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 demande de soumissions;
- b) paginer chacune des pages de la proposition dans le coin inférieur droit.

Conformément à la [Politique sur les marchés du Conseil du Trésor](#) et à la *Loi canadienne sur l'accessibilité*, les ministères et organismes fédéraux doivent tenir compte des critères et des caractéristiques d'accessibilité lorsqu'ils achètent des biens ou des services. Par conséquent, les soumissionnaires sont encouragés à mettre en évidence toutes les caractéristiques et composantes liées à l'accessibilité dans leur proposition pour l'énoncé des travaux (EDT) et doivent :

- (i) démontrer en quoi les biens ou les services proposés par le soumissionnaire satisfont aux exigences en matière d'accessibilité au moment de la livraison; ou
- (ii) décrire comment, aux termes d'un contrat subséquent, le soumissionnaire livrerait ses biens ou ses services d'une manière qui satisfait à l'exigence obligatoire

3.2 Section I : Soumission technique

- a) Dans leur soumission technique, les soumissionnaires devraient démontrer leur compréhension des exigences contenues dans la demande de soumissions et expliquer comment ils répondront à ces exigences. Les soumissionnaires devraient démontrer leur capacité de façon complète, concise et claire pour effectuer les travaux.
- b) La soumission technique devrait traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les



soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

- c) Le soumission technique comprend les éléments suivants :
- i. **Justification de la conformité technique** : La soumission technique doit prouver que le SGA proposé par le soumissionnaire est conforme aux paragraphes de l'annexe A à l'appendice D – *Énoncé des exigences*
 - ii. **Formulaire d'attestation de l'éditeur de logiciels-services (Formulaire 1)**: Si l'éditeur du logiciel-service (défini comme l'entité ou la personne titulaire du droit d'auteur sur toute solution de logiciel-service incluse dans la soumission et qui a le droit de: la licence et autoriser des tiers à utiliser sa solution de logiciel-service et tous les composants sous-jacents) a l'intention de soumettre une soumission et de se qualifier en tant que fournisseur de plein droit, cet éditeur de solution de logiciel-service doit soumettre le formulaire de certification 1.
 - iii. **Formulaire d'autorisation de l'éditeur de logiciels-services (Formulaire 2)**: S'il s'agit d'un revendeur (un tiers qui n'est pas l'éditeur de solutions de logiciel-service, mais est autorisé à distribuer et à revendre les solutions logiciels-services au tiers partie) a l'intention de soumettre une soumission et de se qualifier de fournisseur à part entière; ce revendeur doit alors certifier que son éditeur, conformément au formulaire 2, certifie qu'il a été autorisé à fournir le logiciel en mode de logiciel-service de l'éditeur de solution de logiciel-service.
 - iv. **Justification de la conformité aux exigences relatives à la sécurité à l'assurance de niveau 1**: les fournisseurs doivent justifier de la conformité aux exigences de qualification énoncées à l'appendice M – Niveau 1 Exigences relatives à la sécurité à l'assurance de niveau 1. La justification ne doit pas être simplement une répétition des exigences, mais doit expliquer et démontrer comment le fournisseur répond à ces exigences. Indiquer simplement que le fournisseur ou la solution de logiciels-services proposée est conforme n'est pas suffisant. Lorsque le Canada détermine que la justification n'est pas complète, la soumission sera déclarée non recevable et rejetée
 - v. **Documentation technique** : Le soumissionnaire doit fournir les documents techniques, comme les manuels de l'utilisateur, les captures d'écran, les documents de conception ou de gestion du système (ou d'autres sources d'information), à l'appui de la réponse du soumissionnaire à chaque exigence identifiée à l'Annexe A à l'appendice D – *Énoncé des exigences* (une copie électronique des documents techniques à l'appui de la soumission technique est acceptable). La documentation technique doit démontrer comment la solution proposée par les soumissionnaires répond aux critères obligatoires. L'indication de liens vers des sites Web n'est pas acceptable, et dans le cas où une telle indication sert à confirmer une exigence obligatoire, la soumission sera considérée comme non recevable. Le soumissionnaire devrait indiquer l'endroit exact où figure le document de référence, y compris le titre du document, la page et le numéro d'article. Tout document de référence indiqué par le soumissionnaire pour attester la conformité doit accompagner la soumission (copie papier ou électronique). Un document qui n'est pas joint à la soumission ne sera pas pris en considération par le Canada. Lorsque la référence n'est pas suffisamment précise, le Canada peut demander que le soumissionnaire dirige le Canada vers l'endroit approprié dans le document.
 - vi. **Accords sur les niveaux de service (ANS)**: Les fournisseurs doivent soumettre des accords sur les niveaux de service (ANS) publiés décrivant les accords de niveaux de service à inclure dans l'Appendice J - Accords sur les niveaux de service (ANS).

En présentant une soumission, l'entrepreneur reconnaît et accepte que toutes les conditions contenues dans l'Appendice J - Accords de niveau de service de solution ANS qui visent à



interpréter le contrat, sont le même objet ou un objet similaire, ou sont liées aux conditions contenues dans les clauses du contrat, sont considérés comme frappés et sont sans effet.

Les engagements en matière de niveau de service (précisés dans les accords sur les niveaux de service publiés) doivent offrir aux clients commerciaux un soutien qui comprend, au minimum, le soutien offert sur le marché et rendu public (c.-à-d. la garantie et les services de maintenance et de soutien) généralement fourni aux clients des Solutions de logiciels-services.

Voici des exemples de modalités pouvant faire partie des ANS du soumissionnaire :

- A. la période durant laquelle le fournisseur offrira du soutien aux Clients;
- B. les coordonnées et les renseignements concernant la procédure pour accéder aux services de soutien;
- C. les procédures de résolution de problèmes;
- D. les temps de réponse;
- E. les procédures sur la façon et le moment de répondre à toutes les communications par téléphone, télécopieur ou courriel;
- F. la disponibilité du site Web de soutien pour les clients (par exemple: jour et nuit, 365 jours par an, 99.9 % du temps); et
- G. droits de maintenance (par exemple des correctifs, mises à jour majeures/mineures de presse, etc)

En soumettant une soumission en matière d'approvisionnement, le fournisseur reconnaît et accepte que toutes les modalités contenues dans l'annexe l'Appendice J - Accords sur les niveaux de service (ANS) de la Solution de logiciels-services visant à interpréter la DDP, ou qui relèvent d'un sujet identique ou similaire ou en lien avec, les conditions contenues dans la DDP et les clauses du contrat subséquent sont considérées comme nulles ou sans effet.

- vii. **Conformité à l'Appendice G - Obligations en matière de sécurité et protection de la vie privée:** Les fournisseurs doivent se conformer aux obligations de sécurité et de confidentialité figurant à l'Appendice G - Obligations en matière de sécurité et protection de la vie privée. Les fournisseurs doivent fournir les preuves écrites ou les documents de certification attestant de leur conformité aux obligations en matière de sécurité et de confidentialité.

En présentant une soumission, le fournisseur reconnaît et accepte que toutes les autres conditions soumises dans le cadre de la soumission technique sont considérées comme nulles et ne font aucunement partie de l'AMA.

3.3 Section II : Soumission financière

- a) Dans la soumission financière, les soumissionnaires doivent soumettre un Solutions de logiciels-services comportant leurs prix commerciaux ainsi que leurs prix ou tarifs applicables pour les services professionnels qui doivent être fournis par les soumissionnaires, en plus de la ou des solutions logiciels-services proposées. La section Catalogue des solutions logiciels-services et des prix commerciaux de la soumission doit obligatoirement être soumise selon le modèle fourni dans en vertu du Barème de prix fourni dans l'**Appendice E – Base de paiement**. La soumission financière doit être clair et traiter de façon suffisamment approfondie les points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée.
- b) Les renseignements suivants doivent figurer dans l'**Appendice E, Base de paiement** :
 - i. **N° de pièce de l'éditeur de logiciels-services:** Le soumissionnaire doit inscrire le numéro de pièce utilisé par l'éditeur de logiciels-services pour identifier la Solution de logiciels services commercialement;



- ii. **Nom de la Solution de logiciels-services:** Le soumissionnaire doit indiquer le nom commercial utilisé par l'éditeur de logiciels-services pour identifier commercialement la Solution de logiciels-services.
- iii. **Nom de l'éditeur de logiciels-services:** Le soumissionnaire doit inscrire le nom de l'éditeur de logiciels-services qui possède les droits de propriété intellectuelle de la Solution de logiciels-services;
- iv. **Fournisseur de services d'infonuagiques :** Le soumissionnaire doit identifier le fournisseur de services infonuagiques (CSP) dont les services infonuagiques sont utilisés pour fournir au Canada la Solution de logiciel-service proposée.
- v. **Prix :** Le soumissionnaire doit soumettre les prix p pour la solution de logiciels-services et leurs prix ou tarifs applicables pour les services professionnels à l'appendice E, Base de paiement. Les prix doivent respecter les conditions suivantes:
 - A. la tarification commerciale du soumissionnaire moins le pourcentage de rabais applicable
 - B. prix exprimés en dollars canadiens;
 - C. exclure la taxe sur les produits et services (TPS) ou la taxe de vente harmonisée (TVH).
- vi. **Unité de mesure :** Le soumissionnaire entrez l'unité de mesure pour le logiciel-service, telle que «par utilisateur», «par entité», etc. et abonnement, durée;
- vii. **Langue(s) disponible(s) :** Le soumissionnaire doit fournir la ou les langue(s) disponible(s) pour la Solution de logiciels-services, en indiquant « AN » pour anglais, « FR » pour français, ou « AN FR » pour les deux;
- viii. **Information sur les Solutions de logiciels-services:** Le fournisseur doit inscrire une adresse de site Web affichant l'information sur la Solution de logiciels-services;

Les soumissionnaires doivent présenter leur soumission financière en conformité avec l'appendice E – Base de paiement. Le montant total des taxes applicables doit être indiqué séparément, s'il y a lieu.

Les soumissionnaires doivent fournir les renseignements suivants dans leur soumission financière en remplissant l'Appendice O – Renseignements sur le fournisseur et autorisation, qui doit être intégrée à leur soumission :

1. Leur dénomination sociale;
2. Leur [numéro d'entreprise](#); et
3. Le nom de la personne-ressource (y compris son adresse postale, ses numéros de téléphone et télécopieur, et son adresse de courriel) autorisée par le soumissionnaire à communiquer avec le Canada relativement :
 - a) à la soumission;
 - b) à tout contrat subséquent pouvant découler de la soumission.

Dans les propositions financières, il faut clairement nommer le personnel proposé et la catégorie associée aux fins de l'évaluation seulement. Les tarifs journaliers ou prix fermes proposés doivent être indiqués en dollars canadiens.

Le taux proposé par le soumissionnaire en réponse à une demande de proposition et pour les contrats subséquents doit comprendre les coûts généraux et administratifs, les coûts indirects et la marge bénéficiaire. Les coûts suivants engagés lors de la prestation des services doivent être inclus : le local pour bureau, l'équipement informatique et les logiciels, le traitement de texte, la préparation des rapports, les services de photocopie, de messagerie, de télécopie et de téléphone, les frais liés aux déplacements locaux et les frais administratifs relatifs aux dépenses liées aux déplacements extérieurs. Le mot « local » utilisé dans la présente fait référence à l'endroit où les travaux seront effectués au Canada, selon les précisions de la demande de proposition et le ou les contrats subséquents.

Les soumissionnaires doivent fournir dans leur soumission financière une ventilation des prix, comme il est précisé à l'Appendice E – Base de paiement.

Clauses du Guide des CUA



3.4 C3011T (2010-01-11) – Fluctuation du taux de change

Le besoin ne prévoit aucune protection relative à la fluctuation du taux de change. Aucune demande de protection contre la fluctuation du taux de change ne sera prise en considération. Toute soumission incluant une disposition en ce sens sera déclarée non recevable.

3.5 Section III : Attestations et Renseignements supplémentaires

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

3.6 Section IV : Processus continu d'intégrité de la chaîne d'approvisionnement

- a) Les soumissionnaires doivent soumettre des renseignements précis concernant chaque composante de la chaîne d'approvisionnement qu'ils proposent. Cette information est appelée (« Information sur la sécurité de la chaîne d'approvisionnement » ou « ISCA »), comme le précise la section 1.1 de l'Appendice H, Processus d'intégrité de la chaîne d'approvisionnement.
- b) Les soumissionnaires doivent soumettre l'information sur la sécurité de la chaîne d'approvisionnement dans le formulaire 3 - formulaire de soumission SCI. Le Canada utilisera cette information pour évaluer si, à son avis, la chaîne d'approvisionnement proposée par une soumissionnaire pourrait faire en sorte que la solution proposée par le soumissionnaire compromette ou serve à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, conformément à l'évaluation de l'ISCA décrite à l'**Appendice H, Processus d'intégrité de la chaîne d'approvisionnement**.
- c) En soumettant ISCA, et compte tenu de cette opportunité à participer dans le processus d'acquisition, le fournisseur convient à se conformer aux conditions de l'accord de non-divulgence dans L'Appendice K -Chaîne d'approvisionnement et accord de non-divulgence.



PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

- a) Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les critères d'évaluation technique et financière.
- b) une équipe d'évaluation composée de représentants du Canada évaluera les soumissions.
- c) **Demande de précisions** : Si le Canada demande des précisions au fournisseur sur sa soumission ou s'il veut vérifier celui-ci, le fournisseur disposera d'un délai de deux (2) jours ouvrables (ou d'un délai plus long précisé par écrit par le responsable de la soumission en matière d'approvisionnement) pour fournir les renseignements nécessaires au Canada. Le défaut de respecter les délais rendra la soumission non recevable, causera sa suspension ou retardera l'attribution du contrat.
- d) **Droits du Canada**
 - a. Le Canada se réserve le droit de refuser tout produit proposé par un fournisseur et de négocier les prix prévus à l'Appendice E, Base de paiement;
 - b. Le Canada se réserve le droit de refuser ou de négocier les modalités proposées par un fournisseur et soumises à l'Appendice J, Accords sur les niveaux de service (ANS). Aucun contrat ne sera attribué avant que le Canada approuve toutes les modalités.

4.2 Évaluation technique

4.2.1 Critères techniques obligatoires

Les soumissions doivent satisfaire à tous les critères techniques obligatoires indiqués à l'Annexe A à l'Appendice D – *Énoncé des exigences - Réponse du soumissionnaire Tableau A – Exigences obligatoires*. Le soumissionnaire doit soumettre la documentation nécessaire afin de démontrer qu'il satisfait à cette exigence.

Les exigences obligatoires sont évaluées selon le simple principe de la réussite ou de l'échec. Si le soumissionnaire ne satisfait à aucune des exigences obligatoires, la proposition sera déclarée **non recevable et ne sera plus prise en considération**. Il faut absolument traiter les exigences obligatoires dans tout processus d'approvisionnement. Chaque critère technique obligatoire devrait être traité séparément.

Les exigences techniques obligatoires sont les suivantes :

- i. Justification de la conformité à l'annexe A de l'appendice D Énoncé des exigences - Réponse du soumissionnaire Tableau A - Exigences obligatoires
- ii. Justification de la conformité aux exigences de sécurité de niveau 1, conformément au paragraphe 3.2 (c) (iv);
- iii. Accords sur le niveau de service (ANS), conformément au paragraphe 3.2. (c) (vii);
- iv. Attestations, conformément à la Partie 5;

4.2.2 Critères techniques cotés

Chaque soumission technique qui répond aux exigences obligatoires précisées ci-dessus sera évaluée et notée conformément aux critères d'évaluation cotés indiqués à l'Annexe A à l'Appendice D – *Énoncé des exigences – Réponse du soumissionnaire Tableau B – Exigences cotés*. Chaque critère technique coté doit être traité séparément.

4.3 Évaluation financière

Seules les propositions techniques jugées recevables feront l'objet d'une évaluation financière.



Le prix des soumissions sera évalué en dollars canadiens, les taxes applicables non comprise.

Pour les besoins de cette évaluation, l'Appendice E – Base de paiement, sera utilisée. Le soumissionnaire doit fournir des prix unitaires tout compris pour les logiciels-services et les applicables services professionnels pour lesquelles il propose des ressources conformément à la demande de soumissions, pour la période de contrat initiale et les périodes d'option.

Les données volumétriques comprises dans le barème de prix de l'Appendice E – Base de paiement, sont fournies uniquement à des fins de détermination du prix évalué de la soumission. Elles ne doivent pas être considérées comme une garantie contractuelle.

Le « PRIX TOTAL ÉVALUÉ » à l'Appendice E, Base de paiement, taxes en sus, sera utilisé pour établir la note de l'évaluation financière.

Le « PRIX TOTAL ÉVALUÉ » à l'Appendice E, Base de paiement, sera calculé en additionnant le total de la période initiale du contrat (Tableaux 1 et 2) et le total des années d'options (Tableaux 3 et 4). La somme des quatre tableaux sera utilisée pour déterminer l'évaluation financière.

Tableau 5, Accès pour les utilisateurs supplémentaires ne sera pas considérée lors de l'évaluation financière. Toutefois, si l'on exerce l'achat des articles durant la période initiale et optionnelle, les prix de ceux-ci ne peuvent pas excéder au-delà de 3% par année.

4.3.1 Formule dans le barème de prix

Si le barème de prix fourni aux soumissionnaires comprend une formule, le Canada peut entrer les prix fournis par les soumissionnaires dans un nouveau tableau, si le Canada estime que la formule ne fonctionne plus correctement selon la version fournie par le soumissionnaire.

4.3.2 Justification des taux pour les services professionnels

Selon l'expérience du Canada, les soumissionnaires proposent de temps à autre des tarifs au moment de déposer une soumission pour une ou plusieurs catégories de ressources qu'ils refusent de respecter par la suite, parce que ces tarifs ne leur permettent pas de recouvrer leurs propres coûts ou de réaliser un profit. Au moment d'évaluer les taux pour les services professionnels, le Canada peut, sans toutefois y être obligé, demander une justification des prix pour les taux proposés (soit pour l'ensemble des catégories de ressources ou pour certaines d'entre elles). Des exemples de justification des prix acceptables pour le Canada seraient :

- a) des documents (notamment des factures) indiquant que le soumissionnaire a récemment fourni et facturé à un autre client (avec lequel le soumissionnaire fait affaire sans lien de dépendance) des services similaires à ceux qui seraient fournis par la catégorie pertinente de ressources, lorsque ces services ont été fournis pendant au moins un mois et que les frais imputés sont égaux ou inférieurs aux tarifs offerts au Canada (afin de protéger les renseignements personnels du client, le soumissionnaire peut noircir le nom et les renseignements personnels du client sur la facture soumise au Canada);
- b) un contrat signé, conclu entre le soumissionnaire et une personne qualifiée (selon les qualifications précisées dans la demande de soumissions), pour travailler dans la catégorie de ressources appropriée, où le montant devant être versé à la ressource par le soumissionnaire est égal ou inférieur aux taux offerts pour cette catégorie de ressources;
- c) un contrat signé avec un sous-traitant qui effectuera les travaux prévus par le contrat, où le montant devant être versé pour les services est égal ou inférieur aux taux offerts pour cette catégorie de ressources (et où la ressource en question satisfait aux qualifications précisées dans la demande de soumissions);
- d) des données sur le salaire versé et les avantages offerts aux personnes au service du soumissionnaire compétent (selon les qualifications décrites dans la demande de soumissions) pour travailler dans la catégorie de ressources appropriée, où la rémunération, une fois convertie en taux horaires ou journaliers (le cas échéant), est égale ou inférieure aux taux offerts pour cette catégorie de ressources.



Lorsque le Canada demande une justification des taux offerts pour une catégorie de ressources particulière, il revient uniquement au soumissionnaire de présenter l'information (soit l'information précitée dans les exemples ou d'autres renseignements qui démontrent qu'il sera en mesure de recouvrer ses propres frais au moyen des taux proposés) qui permettra au Canada de déterminer s'il peut compter en toute confiance sur la capacité du soumissionnaire à offrir les services requis aux taux indiqués tout en recouvrant, au minimum, les coûts engagés. Si le Canada détermine que l'information fournie par le soumissionnaire ne démontre pas que celui-ci sera en mesure de recouvrer ses frais en offrant les ressources proposées, le Canada pourra déclarer que la proposition est irrecevable si le tarif proposé est d'au moins **20 %** inférieur à la médiane des taux offerts par les soumissionnaires conformes pendant la première année du contrat subséquent pour la ou les ressources pertinentes. Seuls les taux journaliers fermes des propositions recevables sur le plan technique seront pris en considération.

4.4 Processus d'intégrité de la chaîne d'approvisionnement

- a. Durant le processus de DDP, la période de la chaîne d'approvisionnement et celle de contrat subséquent, l'autorité en matière de sécurité de la chaîne d'approvisionnement, comme identifié par le Canada, peut, sur la base du mandat en matière de la sécurité nationale consistant à protéger l'infrastructure informatique du Canada, évaluer les menaces, risques et vulnérabilités et de même pour le fournisseur SCI.
- b. Le Canada évaluera si, à son avis, la chaîne d'approvisionnement du fournisseur crée la possibilité que la solution proposée par le soumissionnaire puisse compromettre ou soit utilisée pour compromettre l'intégrité de la sécurité de équipements, micro logiciels, logiciels, systèmes ou informations, conformément à la section 2.4 de l'Appendice H, Processus d'intégrité de la chaîne d'approvisionnement.
- c. Il est une condition préalable pour toute adjudication du contrat que le fournisseur doit satisfaire à l'évaluation de l'autorité en matière de sécurité de la chaîne d'approvisionnement.

4.5 Méthode de sélection – Meilleure note combinée pour le mérite technique et le prix

4.5.1 Pour être déclarée recevable, une soumission doit :

- a) respecter toutes les exigences de la demande de soumissions;
- b) respecter tous les critères obligatoires; et
- c) obtenir le nombre minimal de points, soit **1608**, pour l'ensemble des critères d'évaluation technique cotés.

L'échelle de cotation compte **2403** points.

4.5.1.2 Les soumissions qui ne répondent pas aux points (a) ou (b) ou (c) seront déclarées non recevables.

4.5.1.3 La sélection sera faite en fonction de la meilleure note combinée pour le mérite technique et le prix. Une proportion de 70% sera accordée au mérite technique et une proportion de 30% sera accordée au prix.

4.5.1.4 Pour établir la note du mérite technique, la note technique globale de chaque soumission recevable sera déterminée comme suit : nombre total de points obtenus/nombre maximum de points possible, multiplié par 70%.

4.5.1.5 Pour déterminer la note relative au prix, la note de chaque soumission recevable sera calculée au prorata par rapport au prix évalué le plus bas, multiplié par 30%.

4.5.1.6 Pour chaque soumission recevable, les notes attribuées au mérite technique et au prix seront additionnées afin d'obtenir la note combinée.

4.5.1.7 Le contrat ne sera pas nécessairement attribué au soumissionnaire dont la soumission recevable présente la note la plus élevée sur le plan technique ou présente le prix le plus bas. La soumission



recevable qui obtiendra la meilleure note combinée 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 ratio de 70/30 à l'égard du mérite technique et du prix, respectivement. Le nombre total de points pouvant être accordé est de 135, et le prix évalué le plus bas est de 45 000 \$ (45).

Méthode de sélection – Meilleure note combinée pour le mérite technique (70 %) et le prix (30 %)

		Soumissionnaire 1	Soumissionnaire 2	Soumissionnaire 3
Note technique globale		115/135	89/135	92/135
Évaluation du prix de la soumission		55 000 \$	50 000 \$	45 000 \$
Calculs	Note pour le mérite technique	$115/135 \times 70 = 59.63$	$89/135 \times 70 = 46.15$	$92/135 \times 70 = 47.70$
	Note pour le prix	$45/55 \times 30 = 24.55$	$45/50 \times 30 = 27.00$	$45/45 \times 30 = 30.00$
Note combinée		84.18	73.15	77.70
Évaluation globale		1 ^{er}	3 ^e	2 ^e



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 le Canada. À moins d'indication contraire, le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur s'il est établi qu'une attestation du soumissionnaire est fautive, 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 exigées avec la soumission

Les soumissionnaires doivent fournir les attestations suivantes dûment remplies avec leur soumission.

5.1.1 Dispositions relatives à l'intégrité - déclaration de condamnation à une infraction

Conformément aux dispositions relatives à l'intégrité des instructions uniformisées, tous les soumissionnaires doivent présenter avec leur soumission, **s'il y a lieu**, le formulaire de déclaration d'intégrité disponible sur le site Web [Intégrité – Formulaire de déclaration](http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html) (<http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-fra.html>), afin que leur soumission ne soit pas rejetée du processus d'approvisionnement.

5.1.2 Attestations additionnelles requises avec la soumission

Les certifications additionnelles ci-dessous sont requises dans le cadre de la soumission :

1. Formulaire 1 - Formulaire d'attestation de l'éditeur de logiciels-services
2. Formulaire 2 – Formulaire d'autorisation de l'éditeur de logiciels-services
3. Formulaire 3 – Formulaire de soumissionnaire SCI

5.2 Attestations préalables à l'attribution du contrat et renseignements supplémentaires

Les attestations et les renseignements supplémentaires énumérés ci-dessous devraient être remplis et fournis avec la soumission mais ils peuvent être fournis plus tard. Si l'une de ces attestations ou renseignements supplémentaires ne sont pas remplis et fournis tel que demandé, l'autorité contractante informera le soumissionnaire du délai à l'intérieur duquel les renseignements doivent être fournis. À défaut de fournir les attestations ou les renseignements supplémentaires énumérés ci-dessous dans le délai prévu, la soumission sera déclarée non recevable.

5.2.1 Dispositions relatives à l'intégrité – documentation exigée

Conformément à l'article intitulé Renseignements à fournir lors d'une soumission, de la passation d'un contrat ou de la conclusion d'un accord immobilier de la [Politique d'inadmissibilité et de suspension](#), le soumissionnaire doit présenter la documentation exigée, s'il y a lieu, afin que sa soumission ne soit pas rejetée du processus d'approvisionnement.

5.2.2 Dispositions relatives à l'intégrité – Liste de noms

Conformément aux Dispositions relatives à l'intégrité des Instructions générales, tous les soumissionnaires doivent fournir une liste de noms dûment remplie dans le formulaire de vérification de l'intégrité se trouvant sur



le site [Web du régime d'intégrité](#), afin que leur proposition soit prise en compte dans le cadre du processus d'approvisionnement.

5.2.3 Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation de sousmission

En présentant une soumission, le soumissionnaire atteste que le soumissionnaire, et tout membre de la coentreprise si le soumissionnaire est une coentreprise, n'est pas nommé dans la liste des « soumissionnaires à admissibilité limitée du PCF » du Programme de contrats fédéraux (PCF) pour l'équité en matière d'emploi disponible au bas de la page du site Web [d'Emploi et Développement social Canada \(EDSC\) – Travail](#).

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.

Le Canada aura aussi le droit de résilier le contrat pour manquement si l'entrepreneur, ou tout membre de la coentreprise si l'entrepreneur est une coentreprise, figure dans la liste des « [soumissionnaires à admissibilité limitée du PCF](#) » pendant la durée du contrat.

Le soumissionnaire doit fournir à l'autorité contractante l'annexe intitulée [Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation](#) remplie avant l'attribution du contrat. Si le soumissionnaire est une coentreprise, il doit fournir à l'autorité contractante l'annexe Programme de contrats fédéraux pour l'équité en matière d'emploi - Attestation remplie pour chaque membre de la coentreprise.

Je, soumissionnaire, en présentant les renseignements suivants à l'autorité contractante, atteste que les renseignements fournis sont exacts à la date indiquée ci-dessous. Les attestations fournies au Canada peuvent faire l'objet d'une vérification à tout moment. Je comprends que le Canada déclarera une soumission non recevable, ou un entrepreneur en situation de manquement, si une attestation est jugée fautive, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat. Le Canada aura le droit de demander des renseignements supplémentaires pour vérifier les attestations d'un soumissionnaire. À défaut de répondre à toute demande ou exigence imposée par le Canada, la soumission peut être déclarée non recevable ou constituer un manquement aux termes du contrat.

Pour obtenir de plus amples renseignements sur le Programme de contrats fédéraux pour l'équité en matière d'emploi, visitez le site Web [d'Emploi et Développement social Canada \(EDSC\) – Travail](#).

Date : _____ (AAAA/MM/JJ) [si aucune date n'est indiquée, la date de clôture de la demande de soumissions sera utilisée]

Compléter à la fois A et B.

A. Cochez seulement une des déclarations suivantes :

- A1. Le soumissionnaire atteste qu'il n'a aucun effectif au Canada.
 - A2. Le soumissionnaire atteste qu'il est un employeur du secteur public.
 - A3. Le soumissionnaire atteste qu'il est un [employeur sous réglementation fédérale](#), dans le cadre de la [Loi sur l'équité en matière d'emploi](#).
 - A4. Le soumissionnaire atteste qu'il a un effectif combiné de moins de 100 employés permanents à temps plein et/ou permanents à temps partiel au Canada.
- A5. Le soumissionnaire a un effectif combiné de 100 employés ou plus au Canada; et
- A5.1. Le soumissionnaire atteste qu'il a conclu un [Accord pour la mise en œuvre de l'équité en matière d'emploi](#) valide et en vigueur avec EDSC – Travail.

ou



() A5.2. Le soumissionnaire a présenté [l'Accord pour la mise en oeuvre de l'équité en matière d'emploi \(LAB1168\)](#) à EDSC - Travail. Comme il s'agit d'une condition à l'attribution d'un contrat, remplissez le formulaire intitulé Accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168), signez-le en bonne et due forme et transmettez-le à EDSC – Travail.

B. Cochez seulement une des déclarations suivantes :

() B1. Le soumissionnaire n'est pas une coentreprise.

OU

() B2. Le soumissionnaire est une coentreprise et chaque membre de la coentreprise doit fournir à l'autorité contractante l'annexe Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation. (Consultez la section sur les coentreprises des instructions uniformisées.)

5.2.4 Confirmation de l'inscription au Programme d'évaluation de la sécurité des logiciels-services:

La réponse doit comprendre la documentation confirmant que le soumissionnaire est inscrit au processus d'évaluation de la sécurité des logiciels-services décrit à l'Appendice L, Programme d'évaluation de la sécurité informatique des logiciels-services : Processus d'intégration.

Attestation

En présentant sa soumission, le soumissionnaire atteste que les renseignements qu'il a fournis pour répondre aux exigences ci-dessus sont exacts et complets.



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

6.1 Exigences relatives à la sécurité

1 Avant l'attribution du contrat, les conditions suivantes doivent être respectées :

- (a) le soumissionnaire doit détenir une attestation de sécurité d'organisme valable, conformément à la partie 7 – Clauses du contrat subséquent;
- (b) les personnes proposées par le soumissionnaire qui doivent avoir accès à des renseignements ou à des biens de nature classifiée ou protégée ou à des établissements de travail dont l'accès est réglementé doivent chacune posséder une attestation de sécurité au niveau exigé dans la partie 7 – Clauses du contrat subséquent;
- (c) le soumissionnaire doit fournir le nom de toutes les personnes qui devront avoir accès à des renseignements ou à des biens de nature classifiée ou protégée ou à des établissements de travail dont l'accès est réglementé.
- (d) le lieu proposé par le soumissionnaire pour la réalisation des travaux et la sauvegarde des documents doit satisfaire aux exigences relatives à la sécurité précisées à la Partie 7– Clauses du contrat subséquent;
- (e) le soumissionnaire doit fournir l'adresse du ou des lieux proposés pour la réalisation des travaux et la sauvegarde des documents, tel qu'indiqué en bas.

N° civique / nom de la rue, unité / N° de bureau / d'appartement
Ville, province, territoire / État
Code postal / code zip
Pays

L'agent de sécurité d'entreprise doit s'assurer, par l'entremise du [Programme de sécurité des contrats](#) que le soumissionnaire et les individus proposés sont titulaires d'une cote de sécurité en vigueur et au niveau exigé.

6.2 Assurance

L'entrepreneur est responsable de décider s'il doit s'assurer pour remplir ses obligations en vertu du contrat et pour se conformer aux lois applicables. Toute assurance souscrite ou maintenue par l'entrepreneur est à sa charge ainsi que pour son bénéfice et sa protection. Elle ne dégage pas l'entrepreneur de sa responsabilité en vertu du contrat, ni ne la diminue.



PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

APPENDICE A – CONDITIONS GÉNÉRALES

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

A1. Guide des clauses et conditions uniformisées d'achat

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 (CCUA) de Travaux publics et Services gouvernementaux Canada (TPSGC) et dans le Manuel des modalités et des conditions contractuelles de Citoyenneté et Immigration Canada.

A1.1 Une version électronique du [Guide des CCUA](#) est accessible sur le site Web Achats.

A1.2 Une version électronique du Manuel des modalités et des conditions contractuelles d'Immigration, Réfugiés et Citoyenneté Canada (IRCC) est accessible sur le site [Web d'IRCC](#).

A2 Modalités du contrat

A2.1 Les instructions, clauses et conditions générales identifiées dans la demande de soumissions par un numéro, une date et un titre sont incorporées par renvoi dans le présent contrat et en font partie intégrante, comme si elles y étaient formellement reproduites, sous réserve des autres conditions contenues dans la présente.

A3. Conditions générales

A3.1 Le document [CIC-GC-001 \(2020-12-02\)](#), Conditions générales – Marchés de biens et de services de complexité moyenne ou élevée, s'applique au présent contrat et en fait partie intégrante.

APPENDICE B – CONDITIONS SUPPLÉMENTAIRES

B1. Ordre de priorité des documents

En cas d'incompatibilité entre le libellé des textes énumérés dans la liste, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte.

- a) Les articles de la convention;
- b) Appendice B – Conditions supplémentaires;
- c) Appendice A – Conditions générales;
- d) Appendice G - Obligations en matière de sécurité et protection de la vie privée
- e) Appendice D – Énoncé des travaux;
- f) Annexe A à l'Appendice D – Énoncé des exigences
- g) Appendice C – Modalités de paiement – Autorisations de tâches;
- h) Appendice E – Base de paiement;
- i) Appendice M – Exigences relatives à la sécurité niveau 1
- j) Appendice F – Liste de vérification des exigences relatives à la sécurité (LVERS)
- k) Appendice H – Processus d'intégrité de la chaîne d'approvisionnement;
- l) Appendice J – Accords sur les niveaux de service (ANS);
- m) Appendice K – Chaîne d'approvisionnement et accord de non-divulgaration; et
- n) La proposition de l'entrepreneur datée du _____ (*à déterminer*).

B2. Clauses de CIC

Les modalités et conditions de Citoyenneté et Immigration Canada qui suivent sont incorporées par renvoi et font partie intégrante du présent contrat.

N°	Date	Titre
CIC-SC-001 (2015-02-16), L'entrepreneur détient les droits de propriété intellectuelle (PI) sur les renseignements originaux		

B3. Clauses du Guide des CUA

Les clauses suivantes du Guide des CUA sont incorporées par renvoi et font partie intégrante du présent contrat.

N°	Date	Titre
A9117C	2007-11-30	T1204 – Demande directe du ministère client
A9116C	2007-11-30	T1204 – Information à transmettre par l'entrepreneur
C0705C	2010-01-11	Vérification discrétionnaire des comptes

B4. Exigences en matière de sécurité

Les exigences relatives à la sécurité suivantes (LVERS – Appendice F) et clauses connexes (Annexe A à Appendice F) et Appendice G, annexe 1 tel que prévu par le Programme de sécurité des contrats s'appliquent et font partie intégrante du contrat.

B5. Période du contrat et Renouvellement automatique

Durée du contrat : La durée du contrat comprend la période pendant laquelle l'entrepreneur est tenu de fournir les services et d'effectuer les travaux.

Durée initiale : le présent contrat entre en vigueur à la date d'attribution du contrat et se termine trois (3) ans plus tard.



B5.1 Option de prolongation du contrat

L'entrepreneur accorde au Canada le droit irrévocable de prolonger la durée du contrat pour au plus trois (3) périodes supplémentaires d'une (1) années chacune, selon les mêmes conditions. L'entrepreneur accepte, au cours de la durée prolongée du contrat, d'être payé conformément aux dispositions applicables prévues à l'Appendice E – Base de paiement.

Le Canada peut exercer cette option à n'importe quel moment, en envoyant un avis écrit à l'entrepreneur au moins dix (10) jours civils avant la date d'expiration 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.

B5.2 Option d'accroître le niveau d'effort du contrat

L'entrepreneur accorde au Canada l'option irrévocable d'accroître le niveau d'effort du contrat, conformément à l'annexe E – Base de paiement, pendant la période contractuelle, selon les mêmes conditions. L'entrepreneur accepte, au cours de la période prolongée du contrat, d'être payé conformément aux dispositions applicables, telles qu'elles sont définies dans la base de paiement.

Le Canada pourra se prévaloir de cette option à n'importe quel moment, en adressant à l'entrepreneur un avis écrit au moins dix (10) jours civils avant la date d'expiration 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.

B5.3 Changement de consommation

L'entrepreneur accorde au Canada l'option irrévocable d'augmenter ou de réduire sa consommation des produits ou logiciels-services décrits à l'Appendice D. Lorsque la consommation canadienne des produits ou logiciels-services est diminuée, l'entrepreneur convient qu'aucune pénalité ou augmentation du prix unitaire s'appliquera en conséquence.

B5.4 Option de non-participation au renouvellement automatique

Par les présentes, le Canada avise l'entrepreneur qu'il renonce à tout renouvellement automatique de l'obligation à terme. L'entrepreneur accuse réception de l'avis et déclare que le présent contrat ne sera valide que jusqu'à l'expiration du contrat, comme indiqué précédemment.

B6. Résiliation avec avis de trente (30) jours

1. Le Canada se réserve le droit de résilier à n'importe quel moment le contrat, en tout ou en partie, en donnant par écrit un avis de trente (30) jours civils à l'entrepreneur.
2. En cas de résiliation, le Canada paiera uniquement les coûts engagés pour les services rendus et acceptés par le Canada avant la date de la résiliation. Malgré toute autre disposition du contrat, aucun autre coût résultant de la résiliation ne sera payé à l'entrepreneur.

B7. Attestations / Conformité et renseignements supplémentaires

À moins d'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 pourront faire l'objet de vérifications par le Canada pendant toute la durée du contrat.

B7.1 Programme de contrats fédéraux pour l'équité en matière d'emploi – Manquement de la part de l'entrepreneur

Lorsqu'un Accord pour la mise en oeuvre de l'équité en matière d'emploi a été conclu avec Emploi et Développement social Canada (EDSC) – Travail, l'entrepreneur reconnaît et s'engage, à ce que cet accord demeure valide pendant toute la durée du contrat. Si l'Accord pour la mise en oeuvre de l'équité en matière



d'emploi devient invalide, le nom de l'entrepreneur sera ajouté à la liste des « [soumissionnaires à admissibilité limitée du PCF](#) ». L'imposition d'une telle sanction par EDSC fera en sorte que l'entrepreneur sera considéré non conforme aux modalités du contrat.

B8. Exigences en matière d'assurance

L'entrepreneur est responsable de décider s'il doit s'assurer pour remplir ses obligations en vertu du contrat et pour se conformer aux lois applicables. Toute assurance souscrite ou maintenue par l'entrepreneur est à sa charge ainsi que pour son bénéfice et sa protection. Elle ne dégage pas l'entrepreneur de sa responsabilité en vertu du contrat, ni ne la diminue.

B9. Énoncé des travaux

L'entrepreneur doit exécuter les travaux conformément à l'énoncé des travaux qui se trouve à l'Appendice D.

B10. Responsables

<Tous les responsables pour le contrat doit être désigner lors de l'attribution du contrat.>

B10.1 Autorité contractante

L'autorité contractante pour le contrat est :

Nom :
Titre :
Organisation :
Adresse :
Téléphone :
Télécopieur :
Courriel

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 qui dépassent la portée du contrat ou qui n'y sont pas prévus, à la suite de demandes ou instructions verbales ou écrites de toute personne autre que l'autorité contractante.

B10.2 Chargé de projet

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 n'a pas le pouvoir d'autoriser des changements concernant la portée des travaux. Les changements de cet ordre peuvent uniquement être effectués au moyen d'une modification au contrat émise par l'autorité contractante.

B10.3 Responsable technique

Le responsable technique pour le contrat est :

Nom :
Titre :



Organisation :
Adresse :
Téléphone :
Télécopieur :
Courriel :

Le responsable technique est chargé de fournir des conseils sur les exigences techniques et les livrables.

B10.4 Personne-ressource administrative du client

La personne-ressource administrative du client pour le contrat est :

Nom :
Titre :
Organisation :
Adresse :
Téléphone :
Télécopieur :
Courriel :

La personne-ressource administrative du client doit recevoir la facture originale. Toutes les demandes de renseignements relatives aux demandes de paiement doivent être adressées à la personne-ressource administrative du client.

B10.5 Autorité sur la sécurité de la chaîne d'approvisionnement

L'autorité de sécurité de la chaîne d'approvisionnement est :

Nom :
Titre :
Organisation :
Adresse :
Téléphone :
Télécopieur :
Courriel :

L'autorité sur la sécurité de la chaîne d'approvisionnement est le représentant d'IRCC et est responsable pour ce qui concerne au processus d'intégrité sur la chaîne d'approvisionnement dans le cadre du contrat. Ni l'autorité contractante ni l'autorité technique ne sont habilités à conseiller ou à autoriser des informations relatives au processus d'intégrité de la chaîne d'approvisionnement. Toutes les autres questions liées à la sécurité relèvent de la responsabilité de l'autorité sur la sécurité de la chaîne d'approvisionnement.

B10.6 Représentant de l'entrepreneur

Le représentant de l'entrepreneur est :

Nom :
Titre :
Téléphone :
Télécopieur :
Courriel :



B11. Divulgence 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 : 2012-2](#) du Secrétariat du Conseil du Trésor du Canada.

B12. Exigence

B12.1 L'entrepreneur convient de fournir les services et d'exécuter les travaux décrits dans le contrat conformément aux spécifications dans l'Appendice A – Énoncé des travaux et aux prix énoncés dans l'Appendice E – Base de paiement. **Toute information sur les prix incluse ailleurs dans le contrat, y compris dans l'Appendice J – Contrat de niveau de service du logiciel-service sera réputée radiée et est sans force ni effet.**

B12.2 Services : L'entrepreneur accepte de fournir les services suivants, identifiées à l'Appendice D, qui inclut au minimum :

- a. accorder des droits d'utilisation sur les applications logicielles («solution (s)») identifiées au Appendice D fournies ou hébergées par l'entrepreneur;
- b. fournir la documentation de la solution;
- c. assurer la maintenance, la mise à niveau et la mise à jour de la solution;
- d. gérer les incidents et les défauts pour s'assurer que la ou les solutions fonctionnent aux niveaux de service applicables;
- e. fournir des services d'infrastructure de technologie de l'information accessoires et additionnelle requis.
- f. Services d'infrastructure requis pour livrer la solution.
- g. Fournir des services professionnels et de la formation, à la demande de Canada

B12.3 Services professionnels : L'entrepreneur s'engage à fournir les services professionnels suivants, sur demande du Canada, en utilisant le processus d'autorisation de tâches :

- a. la trousse de formation et de services Guide de démarrage rapide (« GDR »);
- b. les services de mise en œuvre;
- c. les services de formation;
- d. les services d'épuration, de migration et de transition des données;
- e. les services consultatifs.

B12.4 Client : Conformément au contrat, le « client » est Citoyenneté et Immigration Canada, ci-après appelé Immigration, Réfugiés et Citoyenneté Canada (IRCC)

B12.5 Réorganisation des clients. Toute forme de restructuration ou de réaménagement du client n'aura aucune incidence sur l'obligation de l'entrepreneur en ce qui a trait aux travaux et à la prestation des services (et ne donnera pas lieu non plus au paiement d'honoraires additionnels). Le Canada peut désigner une autorité contractante ou un responsable technique de remplacement.

B13. Solution

B13.1 Logiciel-service. L'entrepreneur fournira la solution en mode de prestation de logiciels-services, ce qui permettra au Canada d'accéder à la solution hébergée par l'entrepreneur et de l'utiliser.

B13.2 Solution commercialement disponible. Le Canada reconnaît que la solution est une solution commercialement disponible 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 commercialement disponible de la solution, ainsi que les services d'infrastructure informatique accessoires et requis, qui sont tous inclus dans le prix de l'abonnement.



B13.3 Évolution du logiciel; caractéristiques ou fonctionnalités. Le Canada reconnaît que la solution ou l'infrastructure connexe peut évoluer au cours de la durée du contrat. L'entrepreneur convient de continuer à fournir les services sous forme de solution commercialement disponible, avec des fonctionnalités ou des caractéristiques et à des conditions qui ne sont pas moins favorables qu'au moment de l'attribution du contrat.

B13.4 Améliorations et évolution de la solution. Les parties reconnaissent que la technologie et les modèles d'affaires évoluent rapidement et que toute solution fournie au début de la durée du contrat sera inévitablement différente de la solution fournie à la fin de la durée du contrat, et que la ou les méthodes par lesquelles la solution et tout périphérique potentiel sont livrés au Canada soient susceptibles de changer ou d'évoluer et que, au moment de la conclusion du présent contrat, les parties ne puissent envisager tous les biens ou services qui peuvent être livrés aux termes du présent contrat, mis à part le fait qu'ils seront livrés aux utilisateurs. Dans cet esprit, les parties s'entendent sur ce qui suit:

- a) L'entrepreneur doit maintenir et améliorer continuellement la solution et l'infrastructure tout au long de la durée du contrat sur une base commercialement raisonnable, et doit fournir ces améliorations au Canada dans le cadre de l'abonnement du Canada, sans ajustement de prix si ces améliorations sont également offertes aux autres clients sans frais additionnel.
- b) Si l'entrepreneur supprime des fonctions de l'offre commerciale de la solution et les offres dans tout autre service ou produit, ou tout service ou produit nouveau, l'entrepreneur doit continuer de les fournir au Canada dans le cadre de l'abonnement du Canada aux services, selon les modalités actuelles du contrat, peu importe si ces autres services ou produits contiennent également des fonctions nouvelles ou additionnelles. L'entrepreneur n'est pas tenu de se conformer au présent paragraphe si la solution acquise par le Canada est toujours offerte par l'entrepreneur parallèlement aux nouveaux services offerts aux autres clients.

B13.5 Option de déclassement. Si l'entrepreneur n'est pas en mesure de fournir les services avec des caractéristiques et des fonctionnalités non moins favorables, il doit en aviser le Canada par écrit en précisant les circonstances et les autres options possibles, notamment une réduction du prix. Si aucune autre option n'est acceptable pour le Canada, l'entrepreneur convient de consentir à la résiliation du contrat et de payer tous les coûts directs identifiables engagés par le Canada pour la migration et le stockage des données du Canada ainsi que pour le renouvellement des services de remplacement.

B14. Services

B14.1 Services de la solution

- (a) **Logiciel-service.** L'entrepreneur fournira tous les services dont le Canada a besoin pour accéder à la solution et l'utiliser, tel que précisé l'Appendice D – Énoncé des travaux et Annexe A à l'Appendice D – Énoncé des exigences
- (b) **Autorité.** L'entrepreneur déclare et garantit qu'il possède ou qu'il a obtenu et conservera pendant toute la durée du contrat tous les pouvoirs nécessaires, notamment les droits de propriété intellectuelle requis pour fournir les services conformément aux modalités du présent contrat.
- (c) **Indemnisation.** L'entrepreneur convient d'indemniser le Canada de toutes les pertes et 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) **Accessibilité :** L'entrepreneur doit fournir un accès Web à la solution qui n'entrave pas la conformité aux normes d'accessibilité, tel que spécifié par la Norme sur l'accessibilité des sites Web : <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601>.



- (e) **Octroi des droits d'utilisation.** L'entrepreneur accorde au Canada le droit d'accéder à la solution et de l'utiliser sur une base non exclusive et incessible, à partir d'un nombre illimité d'emplacements, d'appareils et d'environnements d'exploitation, au moyen d'une connexion sécurisée, sans fil, mobile ou autre, au moyen d'un navigateur Web ou d'une autre technologie de connexion qui pourrait devenir disponible.
- (f) **Inclus:** L'entrepreneur déclare et garantit que les services comprennent
- i. hébergement et maintenance de la solution,
 - ii. la fourniture de tous les services d'infrastructure de technologie de l'information accessoires et additionnels nécessaires,
 - iii. une infrastructure technique conforme à toutes les normes de sécurité requises, permettant au Canada d'utiliser la solution pour traiter les données du client conformément à ses normes de sécurité exprimées, et
 - iv. accès et utilisation sans entraves, quelle que soit la quantité de données créée, traitée ou stockée par la solution.
- Le tout est inclus dans le prix.
- (g) **Droits d'utilisation restreints.** Le Canada reconnaît qu'en fournissant les services, l'entrepreneur ne délivre aucun droit de propriété sur un produit logiciel, une composante de la solution ou une infrastructure utilisés par l'entrepreneur pour fournir les services, sauf dans les cas expressément prévus dans une autorisation de tâches. Le Canada ne fera sciemment pas les choses suivantes :
- a. distribuer, octroyer une licence, prêter ou vendre la solution;
 - b. porter atteinte aux mécanismes de sécurité de la solution ou les contourner;
 - c. 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.
- (h) **Modalités applicables.** L'entrepreneur a indiqué, et le Canada reconnaît, que l'entrepreneur peut modifier unilatéralement, sans préavis à ses clients, y compris le Canada, les modalités commerciales selon lesquelles il offre sa solution. L'entrepreneur déclare et garantit qu'une telle modification n'entraînera pas des conditions moins favorables, notamment en ce qui concerne le prix, les niveaux de service et les recours, sans égard à tout avis contraire.
- (i) **Modalités additionnelles.** Les parties conviennent que les modalités, y compris les avis par « clic » ou « fenêtre contextuelle », qui s'appliquent à l'offre commerciale de la solution par l'entrepreneur, y compris les outils de tiers ou l'infrastructure accessoire, ne s'appliquent pas à l'utilisation de la solution par le Canada si ces modalités sont en conflit avec les modalités expresses du présent contrat. Les modalités des outils tiers non spécifiés en tant que service ou solution dans l'Appendice D ne sont pas assujetties à cette section.
- (j) **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 que cela soit explicitement désigné 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.
- (k) **Récupération de données :** L'entrepreneur convient de rendre les données du Canada disponible pendant au moins 90 jours après la fin du contrat afin de laisser au client suffisamment de temps pour migrer ses données vers un nouvel environnement, sans frais supplémentaires pour le Canada.



(l) **Interface de programmation d'application (API) :**

L'entrepreneur doit :

- i. Fournir des services qui utilisent des interfaces de programmation d'applications (API) ouvertes, publiées, prises en charge et documentées, afin de prendre en charge l'interopérabilité entre les composants et de faciliter la migration des applications.
- ii. Fournir un moyen via l'API pour les applications de fournir des services et d'extraire des données de reporting, de facturation et financière relatives aux services cloud consommés par le client.
- iii. Prendre des mesures raisonnables pour protéger les API internes et externes au moyen de méthodes d'authentification sécurisées. Cela implique de s'assurer que toutes les requêtes d'API exposées en externe nécessitent une authentification réussie avant de pouvoir être appelées et permettre au GC de répondre aux normes du GC sur l'API.
<https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/normes-gouvernement-canada-api.html>

B15. Niveau de Service

L'Appendice J, Accords sur les niveaux de service,(fournis par l'entrepreneur) contient les renseignements précis qui définissent les niveaux et les normes relatifs aux processus et aux attentes en matière de rendement pour les services devant être fournis en vertu du contrat, et doit être lue conjointement avec la section suivante.

B15.1 Disponibilité. L'entrepreneur mettra le service à la disposition du Canada en stricte conformité avec la documentation sur la solution et l'Appendice J, Accords sur les niveaux de service.

B15.2 Crédits de service. L'entrepreneur accordera au Canada les crédits de service applicables s'il n'atteint pas les niveaux de disponibilité de la solution de temps de disponibilité définis à l'Appendice J, Accords sur les niveaux de service.

B15.3 Exclusions. L'entrepreneur précisera expressément toute exclusion des niveaux de disponibilité de la solution indiqués à l'Appendice J, Accords sur les niveaux de service.

B15.4 Services de soutien. L'entrepreneur fournira un soutien technique en stricte conformité avec l'Appendice J, Accords sur les niveaux de service.

B15.5 Acheminement au palier hiérarchique approprié. L'entrepreneur peut prévoir un processus de recours hiérarchique pour le règlement des différends, qui est décrit à l'Appendice J, Accords sur les niveaux de service.

B15.6 Pas d'infraction. L'entrepreneur garantit que rien dans la solution, ou dans l'utilisation de la solution par le Canada, ne constituera une appropriation illicite de la propriété intellectuelle ou des autres droits d'un tiers ni ne les enfreindra.

B16. Accords sur les niveaux de service (ANS)

B16.1 Les accords sur les niveaux de service (ANS) publiés est au l'Appendice J. Les engagements en matière de niveau de service (précisés dans l'Appendice J) doivent offrir aux clients commerciaux un soutien qui comprend, au minimum, le soutien offert sur le marché et rendu public (c.-à-d. la garantie et les services de maintenance et de soutien) généralement fourni aux clients des Solutions de logiciels-services.

B16.2 Les thèmes pouvant être traités dans les Accords sur les niveaux de service (ANS) de la Solution de logiciels-services doivent inclure:

- A. la période durant laquelle le fournisseur offrira du soutien aux Clients;



- B. les coordonnées et les renseignements concernant la procédure pour accéder aux services de soutien;
- C. les procédures de résolution de problèmes;
- D. les temps de réponse;
- E. les procédures sur la façon et le moment de répondre à toutes les communications par téléphone, télécopieur ou courriel;
- F. la disponibilité du site Web de soutien pour les clients (par exemple: jour et nuit, 365 jours par an, 99.9 % du temps); et
- G. droits de maintenance (par exemple des correctifs, mises à jour majeures/mineures de presse, etc)

B16.3 Notifications nécessaires pour le niveau 1 (Protégé A) et le niveau 2 (Protégé B).

L'entrepreneur doit fournir les éléments suivants :

- a) une notification de toute interruption qui peut avoir une incidence sur la disponibilité et le rendement du service, comme convenu entre les parties et indiqué dans l'entente sur les niveaux de service (ENS);
- b) des bilans réguliers au sujet des procédures de restauration des services à un état opérationnel selon les ENS et les exigences en matière de disponibilité du système convenues, sous forme d'alertes transmises avant et après la mise en œuvre;
- c) une notification des services qui seront mis hors service et qui ont une incidence sur le service à la clientèle;
- d) des alertes, des avis et des directives de sécurité liés au système d'information, par courriel, pour les vulnérabilités qui constituent une menace pour les services.

Toutes les modalités contenues à l'appendice J qui visent à interpréter le contrat, qui traitent du même sujet ou d'un sujet semblable, ou qui sont liées aux modalités contenues dans le contrat, sont réputées être annulées et inopérantes.

B17. Documentation

B17.1 Documentation sur la solution. L'entrepreneur doit fournir au Canada, au moment de l'attribution du contrat, l'accès à la documentation sur la solution commercialement disponible. L'entrepreneur doit mettre à jour la documentation sur la solution à des conditions commercialement raisonnables.

B17.2 Autres documents. L'entrepreneur doit fournir toute documentation nécessaire à l'exécution des travaux, ou y donner accès.

B17.3 Droits de traduction. L'entrepreneur convient que le Canada peut traduire tout produit livrable écrit, y compris la documentation sur la solution ou les documents de formation, en anglais ou en français. L'entrepreneur reconnaît que toutes les traductions appartiennent au Canada et ce dernier n'a aucune obligation de les remettre à l'entrepreneur. Tous les documents qui sont traduits par le Canada incluront l'avis de droit d'auteur ou de droit de propriété qui faisait partie du document original. L'entrepreneur ne peut être tenu responsable des erreurs techniques qui se produisent en raison d'une traduction faite par le Canada.

B17.4 Droits moraux. À la demande du Canada, l'entrepreneur peut fournir une renonciation écrite permanente aux droits moraux, sous une forme acceptable pour le Canada, de la part de chaque auteur qui a contribué à la réalisation du produit écrit. Si l'entrepreneur n'est pas capable ou pas disposé à obtenir les renoncements demandés, l'entrepreneur convient d'indemniser le Canada de toutes les pertes et dépenses (y compris les frais juridiques) découlant de toute réclamation pour violation de droits moraux par un tiers fondée sur l'utilisation de la solution par le Canada.

B17.5 Documentation défectueuse. Si, au cours de la période de garantie, le Canada avise l'entrepreneur d'un défaut ou d'une non-conformité dans une partie quelconque des documents fournis avec les travaux, l'entrepreneur doit corriger le défaut ou la non-conformité dès que possible et à ses propres frais. Le



Canada peut fournir à l'entrepreneur des renseignements sur les défauts ou la non-conformité dans d'autres documents, y compris la documentation sur la solution, à titre d'information seulement.

B18. Travaux

B18.1 Services professionnels

- (a) **Services professionnels.** L'entrepreneur doit exécuter et fournir au Canada les services professionnels (les « travaux ») décrits dans une autorisation de tâches (AT).

B18.2 Recours

- (a) **Travaux.** Si à tout moment pendant la période de garantie, les travaux ne respectent pas les obligations de garantie, l'entrepreneur doit le plus tôt possible, à la demande du Canada, corriger à ses propres frais toute erreur ou tout défaut et apporter les modifications nécessaires aux travaux.
- (b) **Droit du Canada à un recours.** Si l'entrepreneur ne s'acquitte pas d'une obligation prévue dans le présent contrat dans un délai raisonnable après avoir reçu un avis, le Canada aura le droit de remédier ou de faire remédier aux travaux défectueux ou non conformes aux frais de l'entrepreneur. Si le Canada ne souhaite pas corriger ou remplacer les travaux défectueux ou non conformes, le prix contractuel sera réduit de façon équitable.

B18.3 Retard justifiable

La sous-section A11 Retard justifiable de CIC-GC-001 – 2020-12-02 Conditions générales – contrats de biens et services de complexité moyenne / élevée, est modifiée comme suit :

Insérer :

Droit de résiliation

Si un tel événement empêche l'exécution du contrat pendant plus de 30 jours civils, l'autorité contractante peut alors choisir de résilier l'AT ou une partie ou la totalité du présent contrat sans qu'il y ait faute, ce qui signifie qu'aucune des parties ne sera responsable envers l'autre relativement au retard justifiable ou à la résiliation subséquente, et le Canada ne sera responsable que du paiement des services reçus à la date effective de la résiliation.

B18.4 Services Professionnels : Services de transition

- (a) **Migration.** L'entrepreneur convient qu'en raison de la nature des services stipulés au contrat, le Canada peut exiger qu'ils soient fournis sans interruption. Avant la transition vers le nouvel entrepreneur ou au Canada, l'entrepreneur devra fournir toute l'information et la documentation opérationnelle, techniques, conceptuelles et de configuration nécessaires à la transition, dans la mesure où il ne s'agit pas de renseignements confidentiels de l'entrepreneur. L'entrepreneur déclare et garantit qu'il n'entravera pas, directement ou indirectement, l'accès du Canada aux données du Canada ou leur transfert.
- (b) **Services de migration et de transition.** L'entrepreneur convient que, si le Canada demande des services de migration ou de transition pendant la période précédant la fin de la durée du contrat, il aidera diligemment le Canada à faire la transition entre le présent contrat et le nouveau contrat ou à faire migrer les données du Canada à l'environnement du nouveau fournisseur. Il convient que les services décrits ci-dessous ne donneront lieu à aucuns frais autres que ceux qui sont prévus dans la base de paiement.

B18.5 Inspection et acceptation des travaux

La sous-section A12 Inspection et acceptation des travaux de CIC-GC-001 – 2020-12-02 Conditions générales – contrats de biens et services de complexité moyenne / élevée, est modifiée comme suit :



Insérer :

- (a) **Procédures d'acceptation** : Sauf disposition contraire du contrat, les procédures d'acceptation sont les suivantes :
- i. Une fois les travaux sont terminés, l'entrepreneur doit en aviser l'autorité technique par écrit, avec copie à l'autorité contractante, en se référant à la présente disposition du contrat et en demandant l'acceptation des travaux;
 - ii. Le Canada disposera de 30 jours à compter de la réception de l'avis pour effectuer son inspection (la « période d'acceptation »).
- (b) **Défauts et soumission à nouveau des produits livrables** : Si le Canada découvre un défaut durant la période d'acceptation, l'entrepreneur devra le régler le plus tôt possible et aviser le Canada par écrit une fois les travaux terminés, après quoi le Canada aura le droit d'inspecter à nouveau les travaux avant leur acceptation, et la période d'acceptation recommencera. Si le Canada détermine qu'un produit livrable est incomplet ou déficient, il Page 11 de - of 50 n'est pas tenu de désigner tous les articles manquants ou tous les défauts avant de rejeter le produit livrable.
- (c) **Accès aux lieux** : L'entrepreneur doit permettre aux représentants du Canada, en tout temps durant les heures de travail, d'accéder à tous les lieux où toute partie des travaux est exécutée. Les représentants du Canada peuvent procéder à leur gré à des examens et à des vérifications. L'entrepreneur doit fournir toute l'aide, les locaux, tous les échantillons, pièces d'essai et documents que les représentants du Canada peuvent raisonnablement exiger pour l'exécution de l'inspection. L'entrepreneur doit expédier lesdits échantillons et pièces d'essai à la personne ou à l'endroit indiqué par le Canada.
- (d) **Inspection de la qualité par l'entrepreneur** : L'entrepreneur doit inspecter et approuver toute partie des travaux avant de le soumettre pour acceptation ou livraison au Canada. Tous les produits livrables soumis par l'entrepreneur doivent être d'une qualité professionnelle, exempts d'erreurs typographiques et autres erreurs, et conformes aux normes les plus élevées de l'industrie.
- (e) **Registre des inspections** : L'entrepreneur doit tenir un registre des inspections à la fois précis et complet qu'il doit mettre à la disposition du Canada, sur demande. Les représentants du Canada peuvent tirer des copies et des extraits des registres pendant l'exécution du contrat et pendant une période maximale de trois ans après la fin du contrat.
- (f) **Rétroaction informelle** : À la demande de l'entrepreneur, le Canada peut fournir une rétroaction informelle avant que tout produit livrable ne soit officiellement soumis pour acceptation. Toutefois, cela ne doit pas être utilisé comme une forme de contrôle de la qualité des travaux de l'entrepreneur. Le Canada n'est pas tenu de fournir une rétroaction informelle.

B19. Base de Paiement

B19.1 Abonnement. En ce qui concerne les services, y compris l'accès à la solution et son utilisation, la documentation sur la solution, les services de soutien et les services d'infrastructure de technologie de l'information accessoires et additionnels requis (tous les services décrits dans le présent contrat qui ne sont pas des travaux), le Canada doit payer les prix détaillés à l'Appendice E – Base de paiement.

B19.2 Services professionnels fournis dans le cadre d'une autorisation de tâches. En ce qui concerne les services professionnels demandés par le Canada, conformément à une autorisation de tâches attribuée de façon officielle, le Canada paiera à l'entrepreneur, à terme échu, jusqu'à concurrence du prix maximum pour l'AT, les heures réellement travaillées ainsi que tout produit livrable subséquent / prix ferme énoncé dans l'autorisation de tâches, aux taux quotidiens fermes tout compris indiqués à l'Appendice E – Base de paiement ou dans la soumission de l'entrepreneur, le cas échéant, les taxes sont extra.



B19.3 Frais de soutien sur place. Si le Canada l'approuve à l'avance, l'entrepreneur recevra les taux de main-d'œuvre horaires ou quotidiens précisés dans le contrat, ainsi que les frais de déplacement et de subsistance raisonnables et appropriés engagés par l'entrepreneur dans le cadre des services sur place. Les frais de déplacement et de subsistance ne seront remboursés que conformément aux indemnités de repas et de véhicule particulier prévues dans la [Directive sur les voyages du Conseil national mixte](#), telle que modifiée de temps à autre. Tous ces frais pré-approuvés devront être facturés au Canada comme frais distincts.

B19.4 Stabilité du financement

L'entrepreneur reconnaît qu'il est important pour le Canada de pouvoir continuer d'accéder aux produits et logiciels-services Énoncé des travaux après la durée du contrat. Par conséquent, l'entrepreneur offre de continuer à fournir les produits et logiciel-services à des taux raisonnables et selon toutes les autres modalités énoncées dans le présent contrat, sous réserve de la signature par les parties d'un ou de plusieurs contrats officiels à cet égard. Pour chacune des deux (2) années suivant la durée du contrat, l'entrepreneur propose par les présentes les tarifs annuels les plus bas parmi les suivants :

- (a) les taux publiés en vigueur à ce moment-là;
- (b) les taux faisant l'objet de contrats antérieurs et rajustés selon l'écart en pourcentage par rapport à l'indice des prix à la consommation (IPC) de Statistique Canada pour la période de douze (12) mois précédant la date à laquelle le changement de prix doit prendre effet;
- (c) 3 % de plus que les taux annuels offerts au Canada l'année précédente en vertu du présent contrat ou de toute prorogation conclue en vertu du présent article;

et les obligations de l'entrepreneur en vertu du présent article survivront à la résiliation ou à l'expiration du présent contrat.

B19.5 Certification des Prix. L'entrepreneur atteste que le prix indiqué ne dépasse pas le prix le plus bas facturé à quiconque, y compris le client le plus favorisé de l'entrepreneur, pour la même qualité et la même quantité de biens, de services ou les deux.

B19.6 Vérification discrétionnaire des comptes

L'attestation de l'entrepreneur à l'effet que le prix ou taux indiqué n'est pas supérieur au plus bas prix ou taux demandé à toute personne, y compris au meilleur client de l'entrepreneur, pour des biens, services ou les deux de qualité et de quantité semblables, peut faire l'objet d'une vérification des comptes par le gouvernement, à la discrétion du Canada, avant ou après que l'entrepreneur n'ait été payé.

Si la vérification des comptes démontre que l'attestation est erronée après que le paiement ait été versé à l'entrepreneur, ce dernier doit, à la discrétion du Canada, rembourser au Canada le montant qui est supérieur au plus bas prix ou taux ou autoriser le Canada à retenir le montant en le déduisant de toute somme payable à l'entrepreneur en vertu du contrat.

Si la vérification des comptes démontre que l'attestation est erronée avant que le paiement ne soit effectué, l'entrepreneur convient que le Canada ajustera les factures en suspens, en fonction des résultats de la vérification. En outre, il est entendu que si le contrat est toujours en vigueur au moment de la vérification, le prix ou taux sera réduit en fonction des résultats de la vérification des comptes.

B20. Paiement

B20.1 Factures

La sous-section A13 Présentation des factures de CIC-GC-001 – 2020-12-02 Conditions générales – contrats de biens et services de complexité moyenne / élevée, est modifiée comme suit :



Insérer :

Retenue pour les non-résidents. Le Canada doit retenir 15 % du montant à payer à l'entrepreneur pour des services rendus au Canada si l'entrepreneur n'est pas un résident du Canada, à moins que ce dernier obtienne une exonération valide de l'Agence du revenu du Canada. Le montant retenu sera conservé dans un compte pour l'entrepreneur à l'égard de toute dette fiscale exigible par le Canada.

B20.2 Mode de paiement

- (a) Le Canada paiera l'entrepreneur pour les services soit à l'avance, soit à terme échu, conformément à l'Appendice C, Modalité de paiement. Lorsque le paiement est effectué à l'avance, la période de paiement anticipé ne dépasse pas 12 mois. Le paiement anticipé n'empêche pas le Canada d'exercer un recours à l'égard de ce paiement ou de la prestation des services.
- (b) Si le Canada conteste une facture pour quelque raison que ce soit, il réglera 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. Dans le cas des factures contestées, elles ne seront réputées reçues aux fins de la section A18 de CIC-GC-001 – (2020-12-02) Conditions générales – contrats de biens et services de complexité moyenne/élevée, sous-section 3 qu'une fois le litige réglé.

B20.3 Limite des dépenses. Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.

B20.4 Paiement électronique des factures. L'entrepreneur accepte d'être payé à l'aide des instruments de paiement électronique suivants :

- (a) carte d'achat Visa;
- (b) carte d'achat MasterCard;
- (c) dépôt direct (national et international);
- (d) échange de données informatisé;
- (e) virement télégraphique (international seulement);
- (f) système de transfert de paiements de grande valeur (plus de 25 millions de dollars).

B21. Responsabilité

L'entrepreneur est responsable de tout dommage causé par l'entrepreneur, ses employés, ses sous-traitants ou ses agents à l'égard du Canada ou de tout tiers. Le Canada est responsable de tout dommage causé par lui-même, ses employés ou ses agents à l'égard de l'entrepreneur ou de tout tiers. Les parties conviennent qu'aucune disposition relative à la limitation de la responsabilité ou à des indemnités ne s'applique au dommage, à moins d'être reproduite entièrement dans les articles de convention. Les dommages signifie les blessures causées à des personnes (y compris les blessures entraînant le décès) ou la perte ou l'endommagement de biens (y compris les biens immobiliers) causés à la suite du contrat ou durant son exécution.

B22. Disposition générales

La sous-section A28 Modification et renonciations de CIC-GC-001 – 2020-12-02 Conditions générales – contrats de biens et services de complexité moyenne / élevée, est modifiée comme suit :

Insérer :

Renonciation. Le défaut ou la négligence par une partie d'appliquer les droits en vertu du présent contrat ne sera pas considéré comme une renonciation à ses droits.



APPENDICE C – MODALITÉS DE PAIEMENT AUTORISATIONS DE TÂCHES

C1. Base de Paiement

À condition de remplir de façon satisfaisante toutes ses obligations en vertu du contrat, l'entrepreneur sera payé des prix unitaires fermes, comme il est précisé à l'Appendice E Base de paiement de _____\$, (à *déterminer au moment de l'attribution du contrat*). Les droits de douane sont inclus et les taxes applicables sont en sus.

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

C2. Autorisation de tâches

L'ensemble des travaux du contrat ou une partie de ceux-ci seront réalisés « sur demande », au moyen d'une autorisation de tâches. Les travaux décrits dans cette autorisation de tâches doivent être conformes à la portée du contrat.

C2.1 Processus d'autorisation de tâches

1. Le responsable technique fournira à l'entrepreneur une description des tâches au moyen du Formulaire d'autorisation de tâches de l'Appendice I.
2. L'autorisation de tâches contiendra les détails des activités à réaliser, une description des livrables et un calendrier indiquant les dates d'achèvement des principales activités et les dates de présentation des livrables. Elle comprendra aussi les bases et les modes de paiement applicables prévus au contrat.
3. Dans les 2 jours ouvrables suivant la réception de l'autorisation de tâches, l'entrepreneur doit fournir le responsable technique le coût total estimatif proposé pour l'exécution des tâches et une ventilation de ce coût, établis conformément à la base de paiement du contrat.
4. L'entrepreneur ne doit pas commencer le travail avant d'avoir reçu une autorisation de tâches approuvée par l'autorité contractante. L'entrepreneur convient que toute tâche effectuée avant la réception d'une autorisation de tâches le sera à ses propres risques.

C2.2 Obligation du Canada – Portion des travaux réalisée au moyen d'autorisations de tâches

L'obligation du Canada à l'égard de la portion des travaux qui est réalisée en vertu du contrat au moyen d'autorisations de tâches est limitée au montant total des tâches effectivement réalisées par l'entrepreneur.

C2.3 Rapports d'utilisation périodiques – Contrats avec autorisation de tâches

L'entrepreneur doit compiler et tenir à jour des données sur les services fournis au gouvernement fédéral, conformément à l'autorisation de tâches approuvée émise dans le cadre du contrat.

L'entrepreneur doit fournir ces données conformément aux exigences en matière d'établissement de rapports précisées ci-dessous ou à l'Appendice N. Si certaines données ne sont pas disponibles, la raison doit en être indiquée. Si aucun service n'a été fourni pendant une période donnée, l'entrepreneur doit soumettre un rapport portant la mention « néant ».

Les données doivent être présentées tous les trimestres à l'autorité contractante.

Voici la répartition des trimestres :

- Premier trimestre : du 1^{er} avril au 30 juin;
- Deuxième trimestre : du 1^{er} juillet au 30 septembre;
- Troisième trimestre : du 1^{er} octobre au 31 décembre;
- Quatrième trimestre : du 1^{er} janvier au 31 mars.

Les données doivent être présentées à l'autorité contractante dans les 10 jours civils suivant la fin de la période de référence.



Exigence en matière de rapport – Explications

Il faut tenir à jour un dossier détaillé de toutes les tâches approuvées pour chaque contrat avec autorisations de tâches. Le dossier peut comprendre

Pour chaque tâche autorisée :

- ii. le numéro de l'autorisation de tâches ou le numéro de la modification de l'autorisation de tâches;
- iii. le nom, ou une brève description, de chaque autorisation de tâches;
- iii. le coût estimatif total de chaque tâche, comme il est indiqué dans l'autorisation de tâches, les taxes applicables sont en sus;
- iv. le montant total dépensé jusqu'à maintenant pour chacune des tâches autorisées, excluant les taxes applicables;
- v. la date de début et d'achèvement de chaque tâche autorisée;
- vi. l'état actuel de chaque tâche autorisée, le cas échéant.

Pour l'ensemble des tâches autorisées :

- i. le montant (les taxes applicables sont en sus) précisé dans le contrat (selon la dernière modification, s'il y a lieu) de la responsabilité totale du Canada envers l'entrepreneur pour toutes les autorisations de tâches approuvées;
- ii. le montant total (les taxes sont en sus) dépensé jusqu'à présent pour toutes les autorisations de tâches approuvées.

C3. Base de paiement – Tâches autorisées

Pour les services professionnels demandés par le Canada, conformément à une autorisation de tâches approuvée, le Canada paiera à l'entrepreneur, de façon rétroactive, jusqu'à concurrence du prix maximum de l'autorisation de tâches, pour les heures réellement travaillées, conformément aux tarifs journaliers fermes tout compris établis à l'Appendice E – Base de paiement, les taxes applicables sont en sus. Les périodes de travail de moins d'une journée seront calculées au prorata du nombre d'heures réellement travaillées, une journée normale de travail étant de 7,5 heures.

C3.1 Limitation des dépenses

1. La responsabilité totale du Canada envers l'entrepreneur en vertu du contrat ne doit pas dépasser la somme de _____ \$. Les droits de douane sont inclus et les taxes applicables sont en sus.
2. Aucune augmentation de la responsabilité totale du Canada ou du prix des travaux découlant de tout changement de conception, de toute modification ou de toute interprétation des travaux, ne sera autorisée ou payée à l'entrepreneur, à moins que ces changements de conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux. L'entrepreneur ne doit pas exécuter des travaux ni fournir des services qui entraîneraient une augmentation de la responsabilité totale du Canada, à moins que l'augmentation n'ait été autorisée par écrit par l'autorité contractante. L'entrepreneur doit informer par écrit l'autorité contractante concernant la suffisance de cette somme selon la première de ces conditions à se présenter :
 - a. lorsque 75 % de la somme est engagée;
 - b. quatre (4) mois avant la date d'expiration du contrat;
 - c. dès que l'entrepreneur juge que les fonds du contrat sont insuffisants pour l'achèvement des travaux.
3. Lorsqu'il informe l'autorité contractante que les fonds du contrat sont insuffisants, l'entrepreneur doit lui fournir par écrit une estimation des fonds additionnels requis. La présentation de cette information par l'entrepreneur n'augmente pas la responsabilité du Canada à son égard.

C4. Mode de paiement

C4.1 Frais d'intégration (frais unique)

Le Canada paiera l'entrepreneur lorsque des unités auront été terminées et livrées conformément aux dispositions de paiement du contrat si :



- a) une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis conformément aux instructions de facturation prévues au contrat;
- b) tous ces documents ont été vérifiés par le Canada;
- c) les travaux livrés ont été acceptés par le Canada.

C4.2 Fais d'abonnement mensuels et services professionnels

Le Canada paiera l'entrepreneur chaque mois pour les travaux complétés pendant le mois visé par la facture conformément aux dispositions de paiement du contrat si :

- a. une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis conformément aux instructions de facturation prévues au contrat;
- b. tous ces documents ont été vérifiés par le Canada;
- c. les travaux livrés ont été acceptés par le Canada.

Le Canada paiera l'entrepreneur pour les services soit à l'avance, soit à terme échu, conformément à L'Appendice J, Accords sur les niveaux de service applicable. Lorsque le paiement est effectué à l'avance, la période de paiement anticipé ne dépasse pas 12 mois. Le paiement anticipé n'empêche pas le Canada d'exercer un recours à l'égard de ce paiement ou de la prestation des services.

Si le Canada conteste une facture pour quelque raison que ce soit, il réglera 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. Dans le cas des factures contestées, elles ne seront réputées reçues aux fins de la section A18 Intérêt sur les comptes en souffrance qu'une fois le litige réglé.

Pour chaque autorisation de tâches émise en vertu du contrat et prévoyant un prix maximum :

- a. le Canada paiera l'entrepreneur pas plus d'une fois par mois, selon la base de paiement. L'entrepreneur doit présenter des feuilles de temps pour chaque ressource, affichant le nombre de jours et d'heures de travail effectué afin de justifier les montants réclamés sur la facture;
- b. une fois que le Canada a payé le prix maximum, il n'a plus à verser d'autres montants, mais l'entrepreneur doit achever les travaux décrits dans l'autorisation de tâches et correspondant au prix maximum. Si les travaux décrits dans l'autorisation de tâches sont terminés plus tôt que prévu, et que leur durée (confirmée par les feuilles de temps) aux taux énoncés dans le contrat représente moins que le prix maximum, le Canada n'est tenu de payer que pour le temps passé à la réalisation des travaux liés à l'autorisation de tâches ou au contrat.

C5. Taxes applicables

Les taxes applicables ne sont pas comprises dans les montants indiqués dans la base de paiement. Les taxes applicables, qui sont évaluées à _____ \$ (*à déterminer au moment de l'attribution du contrat*), sont comprises dans le montant total du contrat. Dans la mesure où elles s'appliquent, les taxes doivent être indiquées séparément dans toutes les factures et demandes d'acompte et seront acquittées par le Canada. L'entrepreneur accepte de remettre aux autorités fiscales appropriées les sommes acquittées ou exigibles au titre de taxes applicables.

C6. Instructions relatives à la facturation

1. L'entrepreneur doit soumettre ses factures conformément à l'article intitulé « Présentation des factures » des conditions générales. Les factures ne doivent pas être soumises avant que tous les travaux identifiés sur la facture soient terminés.

Chaque facture doit être appuyée par :

- a. une copie des feuilles de présence pour corroborer le temps de travail réclamé;
 - b. une copie du document de sortie et de tout autre document précisé au contrat;
2. Les factures doivent être distribuées ainsi :



L'original et un (1) exemplaire doivent être envoyés à l'adresse qui apparaît à la page 1 du contrat et un exemplaire doit être envoyé à l'autorité contractante identifié à la section Responsables du contrat pour attestation et paiement.

C7. Frais de déplacement et de subsistance

Le Canada n'accepte aucuns frais de déplacement et de subsistance pour :

- a) les travaux réalisés à l'intérieur de la région de la capitale nationale (RCN). La RCN est définie dans la [Loi sur la capitale nationale](#), L.R. 1985, ch. N-4 1985, art. 2, laquelle peut être consultée sur le site Web du ministère de la Justice;
- b) tout déplacement entre l'établissement de l'entrepreneur et la RCN;
- c) toute réinstallation de personnel exigée pour répondre aux conditions du contrat.

Ces frais sont inclus dans le prix ferme pour les honoraires professionnels précisés ci-dessus. »

C8. Sous-traitance

L'entrepreneur sera remboursé pour les dépenses de sous-traitance qu'il a raisonnablement et convenablement engagées dans l'exécution des travaux. Ces dépenses seront payées au coût réel, sans majoration, sur présentation d'une copie de la facture (accompagnée des reçus appropriés, s'il y a lieu) qui a été remise à l'entrepreneur par le sous-traitant.

Coût estimatif : _____ \$



APPENDICE D – ÉNONCÉ DES TRAVAUX

D1. Titre

Système de gestion de l'apprentissage (SGA) organisationnel infonuagique pour utilisation à l'échelle du ministère Immigration, Réfugiés et Citoyenneté Canada (IRCC).

D2. Objectif

IRCC est à la recherche d'un entrepreneur offrant une application de type logiciel en tant que service (modèle SaaS) pour héberger une solution pouvant être configurée de manière à répondre aux exigences particulières d'IRCC et qui permet la gestion, la prestation, le suivi et l'évaluation de tous les contenus de formation et d'apprentissage, de même que la production de rapports connexes.

L'état final sera un système infonuagique accessible par navigateur et reposant sur la technologie, disponible pour 12 000 employés ministériels. Ce système permettra aux employés d'accéder à du contenu d'apprentissage tout en conservant et en suivant leur progrès. L'application ou le système infonuagique doit offrir une expérience d'apprentissage simplifiée et améliorée de bout en bout et permettre un contrôle efficace, complet et global de la gestion, de l'analyse, de l'administration et de la communication du contenu pédagogique auprès des apprenants, des fournisseurs de services d'apprentissage et des décideurs.

D3. Contexte

La Direction générale des ressources humaines (DGRH) détient l'autorité fonctionnelle de l'apprentissage au sein d'IRCC. Elle cherche à mettre en place un système de gestion de l'apprentissage (désigné ci-après par SGA ou la Solution) à l'échelle du ministère afin de normaliser l'apprentissage ministériel. La croissance au sein du ministère étant constante, la demande de formation est considérable. Actuellement, une importante part de la prestation de la formation au sein d'IRCC est gérée par la division de l'apprentissage et du perfectionnement (DAP) à l'intérieur de la DGRH.

La haute direction a souligné la nécessité du signalement en temps opportun, du suivi et de la conformité des activités d'apprentissage au sein du Ministère. Afin de faire en sorte que la Division de l'apprentissage et du perfectionnement ait l'accès et le contrôle nécessaires pour se conformer aux nouvelles priorités d'apprentissage approuvées à IRCC de manière normalisée, la solution proposée est un SGA mandaté à l'échelle du ministère.

Un SGA offrira à IRCC une expérience d'apprentissage de bout en bout rationalisée et améliorée. Ce système permettra d'exercer une surveillance efficace, complète et globale sur la gestion, l'administration et la communication des contenus d'apprentissage auprès des apprenants, des fournisseurs de services d'apprentissage et des décideurs. Il s'agit également d'un outil puissant qui peut aider IRCC à faire correspondre l'apprentissage aux besoins organisationnels. Un SGA offrira un système unique d'enregistrement des données d'apprentissage couplé avec des contrôles et un suivi comptables afin de permettre une compréhension exhaustive de l'investissement d'apprentissage d'IRCC et de faciliter l'évaluation de la valeur et de l'effet de l'apprentissage sur le rendement individuel et organisationnel. Des analyses approfondies offertes par un SGA permettront à IRCC de mesurer et de documenter entièrement tout l'apprentissage géré au sein du ministère.

D4. Étendue des travaux

L'entrepreneur doit fournir un SGA qui fournira à IRCC un système organisationnel de gestion de bout en bout de l'apprentissage des employés ainsi qu'un soutien intégré de la gestion du contenu, de la prestation, de l'analyse et de la présentation de rapports en conformité avec les exigences ministérielles.

La portée des travaux comprendra l'acquisition, la configuration et la mise en œuvre d'un système qui offrira à IRCC ces fonctionnalités et éléments généraux :

- a. un référentiel commun des renseignements opérationnels pour le SGA qui couvre :



- i. l'apprenant, le produit d'apprentissage et le catalogue des objets d'apprentissage et l'information sur l'inscription;
 - ii. l'information d'apprentissage historique de l'apprenant;
 - iii. l'information concernant le curriculum et la certification;
 - iv. l'enregistrement des apprenants aux programmes ou aux produits d'apprentissage au moyen d'une inscription en ligne et un enregistrement par un ou plusieurs rôles centraux.
- b. un référentiel commun pour les produits d'apprentissage et les objets d'apprentissage
- c. un référentiel commun pour les renseignements logistiques, y compris :
- i. les salles de classe;
 - ii. l'équipement;
 - iii. le matériel de cours ou d'offres.
- d. une source d'information faisant autorité ou un référentiel commun à partir duquel les rapports seront générés pour les administrateurs et les gestionnaires ministériels
- e. un accès à distance pour les apprenants, les administrateurs et les gestionnaires d'IRCC, au sein de la région de la capitale nationale (RCN) de même que pour toutes les régions au Canada et, au besoin, aux employés d'IRCC travaillant à l'étranger.
- f. une méthode pour qu'IRCC prenne en charge tous les rôles administratifs.

D4.1 Éléments clés du travail

L'acquisition, la configuration et l'opération d'un système de gestion de l'apprentissage (SGA) basé en nuage sont les objectifs clés et la portée de ce travail.

Les composantes clés du travail comprendront :

- a. la livraison d'un SGA de modèle SaaS infonuagique entièrement fonctionnel, hébergé et commercial, comme décrit dans l'énoncé des besoins (annexe A à appendice D) et à l'article D4.2. Les coûts associés doivent comprendre toutes les licences d'inscription pour que le SGA soit opérationnel, entièrement fonctionnel et sécurisé au sein du centre de données offert par le fournisseur, tout en adhérant à l'hébergement infonuagique sécuritaire et aux exigences de propriété intellectuelle identifiées par IRCC. L'application doit respecter toutes les précisions de sécurité requises, comme énoncées dans l'article D7 — Limites et contraintes.
- b. La préparation, l'installation et la configuration ainsi que le transfert du SGA à IRCC. Le travail de préparation comprend également les ressources de consultation techniques et commerciales requises pour effectuer la configuration.
- c. Un SGA doit respecter les exigences du Profil des mesures de sécurité pour les services du GC fondés sur l'infonuagique. Les lignes directrices sont disponibles ici : <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html>.

D4.2 Exigences



La Solution doit comprendre les exigences fonctionnelles énumérées dans le tableau A de l'annexe A à l'appendice D — Énoncé des exigences du SGA d'IRCC et **doit** aussi comprendre les fonctionnalités supplémentaires obligatoires suivantes :

- a. Un système infonuagique qui est une plateforme indépendante de l'appareil, accessible à tous les utilisateurs, y compris les administrateurs système, sans qu'il soit nécessaire d'installer un logiciel supplémentaire;
- b. Toutes les mises à niveau, y compris les mises à jour réglementaires, sont fournies sans frais supplémentaires;
- c. La Solution doit s'étendre à au moins 25 000 utilisateurs autorisés et permettre l'extensibilité pendant toute la durée du contrat;
- d. Un soutien d'intégration de l'authentification unique;
- e. Des environnements multiples SaaS (élaboration, essai et production) hébergés dans un centre de données sécurisé situé au Canada;
- f. Des configurations multilocataires avec accès granulaire, marque distinctive individuelle et sécurité;
- g. Doit permettre à IRCC de configurer et d'entretenir la Solution au besoin;
- h. Toutes les données traitées, entreposées et maintenues dans la Solution, y compris tout l'entreposage en ligne de même que les sauvegardes de données et les données archivées doivent demeurer au Canada.
- i. Feuille de route et libérations du produit — Selon les libérations du produit antérieures, l'entrepreneur doit démontrer sa volonté d'investir dans le produit de façon continue en lançant un minimum de deux mises à jour du produit chaque année.
 - i. L'entrepreneur doit démontrer la disponibilité d'une feuille de route du produit;
 - ii. L'entrepreneur doit démontrer l'existence d'un processus qui définit la façon dont la communauté des utilisateurs peut proposer des améliorations et de nouvelles fonctionnalités ainsi que comment et quand celles-ci font l'objet d'une décision, leur ordre de priorité, leur élaboration et leur lancement.

D4.3 Livraison

Le contracteur doit être livré, programmé et configuré le SGA infonuagique au Canada, et il doit être installé et configuré de manière que toutes les données, y compris les sauvegardes de données demeurent au Canada. Le SGA devra être accessible par les utilisateurs finaux, à la fois les apprenants et les administrateurs, au Canada et ailleurs dans le monde par Internet.

D5. Tâches et produits livrables

L'entrepreneur doit être en mesure de respecter les exigences suivantes et d'offrir les éléments suivants au responsable technique du client :

D5.1 Solution entièrement fonctionnelle

- a. La mise en œuvre réussie nécessitera une approche disciplinée qui comprend des services de gestion de projet, de configuration de conception de système, de déploiement, de documentation, de mise à l'essai, de formation et de soutien aux utilisateurs finaux. IRCC exige une solution entièrement fonctionnelle pour laquelle l'entrepreneur doit prévoir et fournir un soutien continu, notamment :
 - i. offrir des consultations approfondies, sur demande, au sujet des pratiques exemplaires et de l'efficacité des processus, et assurer une intégration réussie avec les processus et les procédures d'IRCC;
 - ii. fournir de la formation et du matériel de formation aux utilisateurs finaux et aux administrateurs, sur demande;
 - iii. fournir un soutien pour veiller à ce qu'IRCC optimise à la fois l'utilisation et la rentabilité de la Solution.



- b. Pour assurer le succès de la mise en œuvre de la Solution, celle-ci doit inclure, au minimum, les livrables de mise en œuvre suivants. L'entrepreneur doit créer chaque produit livrable et doit les présenter officiellement à IRCC pour examen et acceptation. Dans les cas où il y a des jalons avec plusieurs étapes ou des jalons avec des étapes qui sont requises comme conditions préalables à la ou aux étapes suivantes, les étapes doivent être entièrement détaillées pour contenir chaque livrable (sauf indication contraire).

L'entrepreneur doit fournir les livrables de mise en œuvre présentés ci-dessous.

- a. Un (1) SGA de modèle SaaS infonuagique hébergé et entièrement fonctionnel avec la capacité de soutenir l'apprentissage et le perfectionnement numériques des employés d'IRCC, comprenant :
- i. une moyenne de 5000 utilisateurs actifs chaque mois à l'échelle du pays;
 - ii. tous les droits d'utilisation de la Solution accordés, la documentation du logiciel, la garantie, l'hébergement, et le soutien (excluant la formation), les renonciations, les ententes de confidentialité ou autres lancements au Canada.
- b. Un plan de projet détaillé, qui comprend les éléments suivants.
- i. Plan de mise en œuvre du projet :
 - Liste détaillée des étapes, des tâches et des sous-tâches pour l'ensemble du projet, y compris les dates de début et de fin, les rôles et leurs responsabilités correspondantes ainsi que les prédécesseurs. Les tâches comprennent, mais sans s'y limiter, toutes les activités de mise en œuvre, les échéances, les jalons, les produits livrables provisoires, les périodes d'examen, les produits livrables finaux et les approbations.
 - ii. Plan de communication :
 - Processus détaillés de la manière dont les communications et l'engagement se produiront efficacement entre IRCC et le fournisseur, y compris les descriptions des points de contact, la fréquence et les méthodes.
 - iii. Plan de gestion et d'atténuation des risques et des problèmes :
 - Processus détaillé qui fournit les explications sur la manière dont tout risque ou problème prédéterminé ou futur sera déterminé et déposé par le fournisseur ou IRCC tout au long du cycle de vie du projet.
 - iv. Rapports continus sur la communication, la coordination et l'avancement du projet :
 - Rapports créés et livrés sur demande.
 - v. Plan de conception de l'infrastructure technique et de la mise en œuvre :
 - Conception d'environnements hébergés proposés par l'entrepreneur, comprenant au minimum des informations sur les éléments suivants.
 - A. La méthodologie, les outils, les procédures, les activités et les services;
 - B. L'infrastructure et les services de sécurité (identification, protection, surveillance/détection et intervention/récupération);
 - C. La réseautique et la connectivité;
 - D. Les caractéristiques de rendement;
 - E. Les exigences relatives à la disponibilité et à la souplesse.
 - vi. Modèle cible de la conception du système
- c. Un produit de travail qui définit à la fois les décisions relatives aux processus opérationnels et les décisions relatives à la configuration du système pour tous les processus opérationnels et les caractéristiques visées.
- i. Configuration, migration et intégration du système
 - 1. Configuration;
 - 2. Migration des données (au besoin);
 - 3. Mise en œuvre et élaboration des rapports (au besoin);



4. Intégration de l'application.
- ii. Essai
 1. Plans de mise à l'essai et scripts (au besoin);
 2. Essai d'acceptation par l'utilisateur;
 3. Essais de sécurité de préproduction.
- iii. Formation
 1. Formation des utilisateurs finaux qui accéderont à la Solution et l'administreront.
- iv. Documentation et formation sur l'administration du système : manuel système complet et aide-mémoire sur l'utilisation du système configuré.
- v. Plan de soutien
 - Plan de soutien en appui à la tenue à jour continue pour toute la durée du contrat.
- vi. Plan de mise en œuvre
 - Ensemble complet d'activités requises pour l'entrée en service, y compris le soutien avant et après la mise en service.

D5.2 Services professionnels

L'entrepreneur doit fournir des services professionnels sur demande, conformément au processus d'autorisation du travail. Les services professionnels visent la planification préliminaire et le lancement requis pour mettre en fonction le SGA, de même que pour la formation et la période après l'attribution du contrat en lien avec le SGA pour son utilisation par IRCC. Les autorisations de travail seront utilisées par le responsable technique pour tout objectif à l'intérieur de la portée ou du contexte de cet énoncé des travaux (EDT) jusqu'à la valeur maximale précisée par le responsable technique.

Les ressources professionnelles suivantes seront nécessaires pour soutenir la configuration, la migration, la gestion des changements, etc. du nouveau SGA d'IRCC. La liste d'activités ci-dessous est sujette à changement après l'attribution du contrat une fois que les diverses activités sont en cours.

L'entrepreneur doit fournir les catégories de ressources suivantes au fur et à mesure des besoins. Les tâches comprennent, mais sans s'y limiter, les activités suivantes :

Liste des services professionnels		
ID	Titre du rôle	Description des rôles
P1	Gestionnaire de projet	<p>IRCC exige un gestionnaire de projet pour gérer la configuration et aider à l'entièreté de l'exercice de migration. Cela comprend le travail pour assurer que l'installation se passe bien et le travail quotidien avec les intervenants sur la migration.</p> <ol style="list-style-type: none"> a. Organiser et gérer le projet, y compris l'établissement des normes, l'élaboration d'un plan de projet efficace pour l'installation, la configuration et le lancement du SGA, la gestion de tout changement qui pourrait avoir une influence sur le projet et la gestion des tâches relatives au projet; b. Mettre en application les processus et les pratiques de gestion de projet; c. Fournir une aide dans le repérage et la résolution des problèmes; d. Veiller à ce que le projet atteigne les objectifs fixés; e. Faire des rapports sur la consommation de ressources du projet; f. Veiller à ce que les produits livrables soient livrés en conformité avec le calendrier et le budget et qu'ils satisfassent aux besoins en matière de qualité; g. Élaborer et mettre en œuvre une stratégie de gestion des changements;



		h. Élaborer et mettre en œuvre une stratégie de gestion des risques;
P2	Analyste fonctionnel	<p>Un analyste fonctionnel est nécessaire pour développer et mettre en œuvre les processus réels. Bien que les processus opérationnels soient fixes, IRCC a besoin de documenter les processus en des termes que le personnel d'IRCC connaît. Ce rôle comprend le travail avec le chef de projet et l'équipe de projet d'IRCC sur les plans de migration des processus actuels vers la solution SGA.</p> <ol style="list-style-type: none"> Définir les processus commerciaux et recommander des changements à l'architecture du système, aux configurations du système et aux stratégies de migration du point de vue de l'aspect technique; Travailler avec le gestionnaire de projet afin d'élaborer, de gérer le plan de projet et d'en évaluer les coûts; Cerner les jalons essentiels et veiller à ce qu'ils soient inclus dans le plan global; Élaborer et réviser les processus et la documentation d'apprentissage afin d'en assurer l'efficacité et la qualité; Préparer les plans des processus et de la migration des données; Aider à déterminer et à mettre en œuvre les exigences en matière de sécurité; Travailler en collaboration avec les équipes chargées des essais et de la formation concernant les problèmes et les besoins relatifs aux aspects technique et organisationnel, aux données ainsi que sur le plan des délais.
P3	Architecte de l'information	<p>Ce rôle comprend deux responsabilités :</p> <ol style="list-style-type: none"> Travailler avec les intervenants sur la migration initiale (p. ex. assembler et formater les données pour la migration); Travailler avec les intervenants sur les exigences et les processus pour l'intégration du SGA et des données PeopleSoft. <p>Ce rôle vise à soutenir l'apprenant et la transcription des données et du contenu.</p> <ol style="list-style-type: none"> Définir les processus d'intégration des relations entre le SGA et les autres systèmes de l'entreprise (p. ex. PeopleSoft); Définir les stratégies de migration des données; Préparer les plans techniques et les plans de conversion des données; Travailler avec le gestionnaire de projet afin d'élaborer, de gérer les aspects concernant les données du plan de projet et d'en évaluer les coûts; Consigner les conceptions du modèle de données et les changements qui y sont apportés; Contribuer au développement de prototypes; Contribuer aux processus d'essai; Mener des examens opérationnels de vérification et de validation de l'assurance de la qualité du modèle de données.
P4	Gestionnaire du changement	<p>Cette ressource doit aider IRCC à gérer la mise en œuvre, l'adoption et l'utilisation du nouveau système SGA infonuagique.</p> <ol style="list-style-type: none"> Gérer le processus de mise en œuvre des changements importants rendus nécessaires dans le cadre du projet afin d'atténuer les risques, de réduire les coûts du changement et d'optimiser les avantages ; Fournir le leadership et l'orientation nécessaires à la réussite du projet; Planifier et adopter une stratégie pour le projet afin de surmonter la résistance au changement.Ce concentré sur les questions de gestion



		<p>de la résistance et de l'inconfort des apprenants au sein d'IRCC qui sont touchés par le projet du SGA.</p> <p>d. Administrer les changements rendus nécessaires en raison du projet :</p> <p>e. Utiliser des méthodes et des techniques éprouvées afin d'éviter que de nouvelles erreurs se produisent et de minimiser les conséquences des changements;</p> <p>f. Instaurer un ensemble complet de processus afin de veiller à ce que les changements soient mis en œuvre de manière transparente, contrôlée et ordonnée;</p> <p>g. S'efforcer de traiter de manière systématique les conséquences du projet sur les changements organisationnels;</p> <p>h. Définir et instaurer de nouvelles valeurs, des normes, une attitude et un comportement positifs dans le contexte du projet et de son incidence sur l'organisation afin d'adopter de nouvelles manières de travailler et de surmonter la résistance au changement;</p> <p>i. Obtenir un consensus de la part des apprenants et des intervenants à l'égard des changements particuliers qui sont conçus pour répondre plus adéquatement à leurs besoins;</p> <p>j. Planifier, tester et mettre en œuvre tous les aspects de la transition découlant du projet au sein de l'organisation.</p>
P5	Formateur (bilingue)	<p>L'entrepreneur doit proposer du personnel de formation bilingue qualifié pour les apprenants et les administrateurs pour:</p> <p>a. Élaborer et mettre en œuvre une stratégie et une approche de formation, en consultation avec le responsable technique ou son remplaçant désigné;</p> <p>b. Assurer le suivi des besoins de formation et les évaluer;</p> <p>c. Élaborer des méthodes et créer et tenir à jour les trousseaux de formation;</p> <p>d. Fournir la formation;</p> <p>e. Évaluer continuellement l'efficacité de la formation;</p> <p>f. Consigner les stratégies, les méthodes et les trousseaux de formation;</p> <p>g. Travailler avec le responsable pour élaborer, estimer et gérer les aspects de la formation du SGA;</p> <p>h. Conseiller le responsable technique ou son remplaçant autorisé.</p> <p>i. Le formateur doit effectuer les tâches ci-dessus en français ou en anglais, tel que déterminé par le responsable technique et précisé dans l'autorisation du travail.</p>

Les ressources proposées par l'entrepreneur doivent répondre aux exigences suivantes:

- P1. Gestionnaire du changement de niveau intermédiaire** — Doit détenir un minimum de quatre ans d'expérience obtenue au cours des dix dernières années dans un rôle de gestionnaire du changement;
- P2. Analyste fonctionnel de niveau intermédiaire** – Doit détenir un minimum de deux ans d'expérience en tant qu'analyste fonctionnel dans un environnement de technologie de l'information, et idéalement avec les applications de type SGA, obtenue au cours des cinq dernières années;
- P3. Architecte de l'information de niveau intermédiaire** — Doit détenir un minimum de deux ans d'expérience en architecture de SGA obtenue au cours des cinq dernières années;



- P4. Gestionnaire de projet de niveau intermédiaire** — Doit détenir un minimum de quatre ans d'expérience au cours des 10 dernières années, y compris deux ans d'expérience en gestion de projets de type SGA;
- P5. Formateur de niveau intermédiaire** — Doit avoir donné au moins soixante (60) jours de formation au cours des trois dernières années comme animateur de formation. Si l'animation de la formation en ligne est exigée dans la demande, le formateur doit avoir donné au moins 60 heures de formation au cours des trois dernières années à titre d'animateur de formation en ligne.

L'entrepreneur doit s'assurer que les ressources disponibles pour fournir le soutien des services professionnels, au besoin, et que les ressources affectées satisfont aux qualités identifiées ci-dessus, telles qu'évaluées par IRCC. Le tableau suivant donne un aperçu du niveau d'effort estimé en jours nécessaire pour chacune des catégories de ressources identifiées. IRCC a le droit de modifier le nombre total d'heures pour chaque catégorie après l'attribution du contrat et au fur et à mesure que la mise en œuvre avance selon les échéanciers des divers produits livrables du projet.

EXIGENCES DE SERVICES PROFESSIONNELS ESTIMÉS POUR LE SGA ¹²						
	Exercice 2021- 22	Exercice 2022- 23	Exercice 2023- 24	Exercice 2024- 25	Exercice 2025- 26	Exercice 2026- 27
Ressources de consultation du SGA³	Jours	Jours	Jours	Jours	Jours	Jours
Formateur intermédiaire	70	60	15	15	10	10
Gestionnaire de projet intermédiaire	110	100	50	50	50	50
Architecte de l'information de niveau intermédiaire	130	80	20	20	20	20
Analyste des activités de niveau intermédiaire	110	55	50	50	40	40
Gestionnaire du changement de niveau intermédiaire	115	50	15	10	10	10
TOTAUX :	535	345	150	145	130	130

D 5.3 Dates de livraison

Le tableau suivant présente les dates de livraison estimées pour certaines des activités clés en lien avec l'installation, la configuration, la mise à l'essai et la livraison de la solution SGA à IRCC. Des échéanciers particuliers seront élaborés et acceptés par IRCC et l'entrepreneur suivant l'attribution du contrat.

Livrable	Description	Date de livraison prévue
Réunion de lancement	Plan de projet détaillé; Plan de communication;	Une semaine après l'attribution du contrat
Planification et conception	Plan de conception et de mise en œuvre de l'infrastructure technique; Plan de formation, document de validation des exigences, modèle cible de conception du système	16 semaines après la réunion de lancement

¹ Les jours de services professionnels indiqués correspondent aux nombres de jours maximum alloués par l'exercice. Aucun nombre minimum de jours n'est requis.

² L'utilisation des services professionnels dans le contrat pour tous les exercices est optionnelle.

³ Le nombre de ressources utilisées pour fournir les produits livrables est à la discrétion de l'entrepreneur tant que le nombre total de jours n'est pas dépassé.



Livrable	Description	Date de livraison prévue
Intégration des données et du contenu	Plan(s) de mise à l'essai; Plan de gestion et d'atténuation des risques	22 semaines après l'attribution du contrat
Assurance de la qualité Tests et formation	Rapports d'assurance de la qualité et de mise à l'essai; Soumission d'un manuel de l'utilisateur complet du système	26 semaines après l'attribution du contrat
Mise en œuvre et soutien	Plan de soutien	26 semaines à partir de l'attribution du contrat
Transfert	Autonomie d'IRCC	28 semaines à partir de l'attribution du contrat
Acceptation et Clôture et soutien continu	Plan de clôture du projet; Plan de mise en œuvre; Plan de gestion du changement;	30 semaines à partir de l'attribution du contrat

D6. Limites et contraintes

L'entrepreneur doit respecter les exigences de sécurité énoncées dans 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-contrôle-sécurité-services-ti-fondés-information-nuage.htm) (<https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-contrôle-sécurité-services-ti-fondés-information-nuage.htm>), qui est un ensemble complet de lignes directrices et de mesures fondées sur le guide ITSG-33. La solution de l'entrepreneur doit respecter le *Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage* en offrant l'un de ces éléments :

- Rapport SOC-2 ou SOC-3 valide (ISAE-3402);
- Certification ISO 27001;
- Conformité avec la Publication 800-53 de l'U.S. National Institute of Standards and Technology (NIST);
- Preuve de l'acceptation de la demande d'accord d'approvisionnement de la [Méthode d'approvisionnement de logiciels-services \(Infonuagiques GC\) \(EN578-191593/F\)](https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-EEM-003-35660) (<https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-EEM-003-35660>)

D7. Langues officielles

La solution doit être disponible et entièrement fonctionnelle dans les deux langues officielles du Canada (anglais et français). Toute la documentation et le soutien requis doivent également être disponibles et fournis sur demande dans les deux langues officielles du Canada (anglais et français).

D8. Déplacements

Le lieu de travail est l'installation de l'entrepreneur. Aucun déplacement n'est prévu. Si l'entrepreneur ou ses ressources doivent se déplacer en personne dans les installations d'IRCC, toutes les dépenses seront l'entière responsabilité de l'entrepreneur.

D9. Disponibilité du personnel

L'entrepreneur atteste que lui-même, ses employés et ses sous-traitants seront prêts à commencer l'exécution des travaux à compter de la date d'attribution du contrat et qu'ils demeureront disponibles pour mener à bien les travaux conformément aux exigences contractuelles.

D10. Diversité

IRCC s'engage à rendre notre ministère inclusif pour tout le monde et à favoriser une culture organisationnelle équitable qui valorise la diversité et qui crée un environnement accueillant et gratifiant pour tous. Nous encourageons les entreprises qui travaillent avec nous à refléter ces valeurs. De plus amples renseignements



sont disponibles à : <https://www.canada.ca/fr/gouvernement/fonctionpublique/mieux-etre-inclusion-diversite-fonction-publique/diversite-equite-matiere-emploi2.html>.



ANNEXE A à APPENDICE D –Énoncé des exigences de SGA IRCC (voir ci-joint)



APPENDICE E – BASE DE PAIEMENT

Durant la période du contrat, l'entrepreneur sera payé tel qu'il est précisé ci-dessous pour les travaux exécutés en vertu du contrat.

Tous les livrables sont franco à bord (FAB) destination, droits de douane canadiens compris et les taxes applicables sont en sus.

Aux fins de l'évaluation des soumissions et de la sélection de l'entrepreneur ou des entrepreneurs seulement, le prix évalué d'une soumission sera déterminé conformément à l'Appendice E – Base de paiement.

La responsabilité totale du Canada envers l'entrepreneur, en vertu du présent contrat, ne doit pas dépasser la somme de _____ \$ (*à déterminer lors de l'attribution du contrat*), y compris toutes les options, les dépenses de déplacements et les taxes applicables.

Le soumissionnaire doit remplir ce barème de prix et l'inclure dans sa soumission financière. Le soumissionnaire doit uniquement remplir les sections requises dans le tableau de prix ci-dessous; il ne doit effectuer aucune autre modification ou substitution. Si cette directive n'est pas respectée, la réponse du soumissionnaire sera jugée non conforme et sera éliminée du processus concurrentiel.

1. Le soumissionnaire doit remplir le barème de prix et le joindre à sa soumission financière. Au minimum, il doit donner suite à ce barème en indiquant dans sa soumission financière, pour chacune des périodes précisées ci-dessous, les taux journaliers fermes tout compris qu'il offre (en dollars canadiens) pour chacune des catégories de consultants précisées.
2. Les prix ou les taux indiqués ci-dessous, lorsque soumis par le soumissionnaire, comprennent les dépenses énumérées ci-après qui peuvent devoir être engagées pour respecter les conditions de tout contrat conclu à la suite de la soumission :
 - a) tous les frais de déplacement et de subsistance pour des travaux exécutés à l'intérieur de la région de la capitale nationale (RCN). La région de la capitale nationale est définie dans la [Loi sur la capitale nationale](#), L.R. 1985, ch N-4 1985, art. 2, qui peut être consultée sur le site Web du ministère de la Justice;
 - b) tous les frais relatifs aux déplacements entre l'établissement de l'entrepreneur et la RCN.
 - c) tous les frais de déplacement et subsistance pour réinstaller des membres du personnel afin de répondre aux conditions de tout contrat subséquent. Ces frais ne peuvent pas être imputés directement et séparément des honoraires professionnels à tout contrat subséquent qui pourrait découler de la demande de soumissions.
3. Les données volumétriques comprises dans le barème de prix de l'Appendice E – Base de paiement sont fournies uniquement à des fins de détermination du prix évalué de la soumission. Elles ne doivent pas être considérées comme une garantie contractuelle.



BARÈME DE PRIX

La rémunération de l'entrepreneur sera établie selon le **taux unitaire ferme**, tout compris, ci-dessous pour les travaux exécutés au titre de ce contrat. Les tarifs doivent comprendre tous les frais liés à l'exécution du contrat. Toutes les taxes applicables sont en sus.

Pour l'Environnement unique mise en place, le tarif unitaire ferme, tout compris inclus y compris la configuration, l'aide à l'intégration et l'installation du système de gestion de l'apprentissage (SGA), jusqu'à l'achèvement réussi de l'acceptation du système conformément au plan approuvé. Il comprend également la fourniture de toute documentation utilisateur associée

Pour les services d'abonnement, le tarif unitaire tout compris inclus la documentation du logiciel les services de maintenance et de soutien du logiciel, ainsi que les services d'hébergement sur l'infrastructure de base proposée, relié au Système de Gestion Apprentissage et décrit dans L'Annexe A à l'Appendice D – Énoncé des travaux, l'entrepreneur sera payé annuellement et à l'avance les prix annuels fermes précisés dans les tableaux 1 et 3.

TABLEAU 1 – LISTE DES PRODUITS INITIAUX

Tableau 1 – Liste des produits initiaux											
Période initiale: Attribution du contrat jusqu'au 31 octobre 2024											
A	B	C	D	E	F	G	H	I	J	K	L
No. d'article	Exigence	Numéro d'article	Nom du produit logiciel-Services	Nom de l'éditeur Logiciel-services	Nom de fournisseur de service d'infonuagiques	Unité de mesure	Langue (AN/FR)	Quantité estimatif	No de mois	Tarif unitaire ferme tous compris (CAD\$)	Prix prolongée I x J x K
Année 1: Attribution du contrat jusqu'au 31 octobre 2022											
T1.1	Environnement unique mis en place							1	n/a	\$	\$
T1.2	Services d'abonnement					Par utilisateur		12,000	12	\$	\$
T1.3	Sous-total pour la période initiale: ANNÉE 1										\$
Année 2: 1 novembre 2022 jusqu'au 31 octobre 2023											
T1.4	Services d'abonnement					Par utilisateur		12,000	12	\$	\$
T1.5	Sous-total pour la période initiale : ANNÉE 2										\$
Année 3: 1 novembre 2023 jusqu'au 31 octobre 2024											
T1.6	Services d'abonnement					Par utilisateur		12,000	12	\$	\$
T1.7	Sous-total pour la période initiale : ANNÉE 3										\$
T1.8	Sous-totale (Année 1 + Année 2 + Année 3):										\$

TABLEAU 2 – Liste services professionnels “sur demande” pendant la période initiale

Pour les services professionnels requis par le Canada, conformément à une autorisation de tâche (AT) approuvée, le Canada paiera l'entrepreneur, rétroactivement, jusqu'au prix maximum de l'AT, pour les heures réelles travaillées, aux taux quotidiens fermes tout compris établis dans les tableaux 2 et 4 TPS, TVH ou TVQ en sus, s'il y a lieu. Les périodes de travail de moins d'une journée seront calculées au prorata, une journée normale de travail étant de 7,5 heures.

Pour les sessions de formations, le tarif unitaire ferme tous compris comprend la fourniture de tout le matériel de formation.



Tableau 2 - Liste services professionnels “sur demande”				
Période Initiale: Attribution du contrat jusqu’au 31 octobre 2024				
A	B	C	D	E
No. d'article	Nom du produit	Niveau d'effort estimé	Taux journalier ferme ou taux unitaire ferme tous compris (CAD\$)	Prix prolongée à des fins d'évaluation E = C x D
ANNÉE 1: Attribution du contrat jusqu’au 31 octobre 2022				
T2.1	Formateur intermédiaire	40 jours	\$	\$
T2.2	Gestionnaire de projet intermédiaire	220 jours	\$	\$
T2.3	Architecte d'information intermédiaire	130 jours	\$	\$
T2.4	Analyste des activités intermédiaire	10 jours	\$	\$
T2.5	Gestionnaire de changement intermédiaire	89 jours	\$	\$
T2.6	Formation – en ligne	1 session	\$	\$
T2.7	Formation – en personne/en classe	1 session	\$	\$
T2.8	Sous-total pour la période initiale: ANNÉE 1			\$
Année 2: 1 novembre 2022 jusqu’au 31 octobre 2023				
T2.9	Formateur intermédiaire	60 jours	\$	\$
T2.10	Gestionnaire de projet intermédiaire	100 jours	\$	\$
T2.11	Architecte d'information intermédiaire	50 jours	\$	\$
T2.12	Analyste des activités intermédiaire	36 jours	\$	\$
T2.13	Gestionnaire de changement intermédiaire	25 jours	\$	\$
T2.14	Formation – en ligne	1 session	\$	\$
T2.15	Formation – en personne/en classe	1 session	\$	\$
T2.16	Sous-total pour la période initiale: ANNÉE 2			\$
Année 3: 1 novembre 2023 jusqu’au 31 octobre 2024				
T2.17	Formateur intermédiaire	15 jours	\$	\$
T2.18	Gestionnaire de projet intermédiaire	50 jours	\$	\$
T2.19	Architecte d'information intermédiaire	20 jours	\$	\$
T2.20	Analyste des activités intermédiaire	50 jours	\$	\$
T2.21	Gestionnaire de changement intermédiaire	15 jours	\$	\$
T2.22	Formation – en ligne	1 session	\$	\$
T2.23	Formation – en personne/en classe	1 session	\$	\$
T2.24	Sous-total pour la période initiale: ANNÉE 3			\$
T2.25	Sous-totale (Année 1 + Année 2 + Année 3):			\$



Définition d'une journée/calcul au prorata

Aux fins du présent contrat, la journée de travail comprend 7,5 heures, à l'exclusion des pauses-repas. Les paiements sont effectués pour les journées travaillées; il n'y a aucune disposition concernant les congés annuels, les congés fériés et les congés de maladie. Une journée de travail correspond à sept heures et demie; le travail effectué en plus ou moins d'une journée sera payé au prorata en fonction du nombre d'heures réellement travaillées, selon la formule suivante :

$$\frac{\text{Heures travaillées} \times \text{taux journalier ferme applicable}}{7,5 \text{ heures}}$$

1. Tous les membres du personnel proposés doivent être en mesure de travailler en dehors des heures normales pendant la durée du contrat.
2. Aucuns frais d'heures supplémentaires ne seront autorisés dans le cadre du contrat. Les heures travaillées seront rémunérées conformément au paragraphe ci-dessus.

TABLEAU 3 – LISTE DE LIVRABLES – ANNÉES D'OPTION

Tableau 3 – Liste de livrables - Années d'option											
A	B	C	D	E	F	G	H	I	J	K	L
No. d'article	Exigence	Numéro d'article	Nom du produit logiciel-Services	Nom du l'éditeur Logiciel-services	Nom de fournisseur de service d'infonuagiques	Unité de mesure	Langue (AN/FR)	Quantité estimatif	No. de mois	Tarif unitaire ferme tous compris (CAD\$)	Prix prolongée L = I x J x K
Année d'option 1: 1 novembre 2024 jusqu'au 31 octobre 2025											
T3.1	Services d'abonnement					Par utilisateur		12,000	12	\$	\$
T3.2	Sous-total pour l'année d'option 1										\$
Année d'option 2: 1 novembre 2025 jusqu'au 31 octobre 2026											
T3.3	Services d'abonnement					Par utilisateur		12,000	12	\$	\$
T3.4	Sous-total pour l'année d'option 2										\$
Année d'option 3: 1 novembre 2026 jusqu'au 31 octobre 2027											
T3.5	Services d'abonnement					Par utilisateur		12,000	12	\$	\$
T3.6	Sous-total pour l'année d'option 3 :										\$
T3.7	Sous-Total (Année d'option 1 + Année d'option 2 + Année d'option 3):										\$

TABLEAU 4 – LISTE DES SERVICES PROFESSIONNELS “SUR DEMANDE” – ANNÉES D'OPTION

Tableau 4 – Liste de services professionnels “sur demande” - Années d'option				
A	B	C	D	E
No. d'article	Nom du produit	Niveau d'effort estimé (jours)	Taux journalier ferme ou taux unitaire ferme tous compris (CAD\$)	Prix prolongée à des fins d'évaluation E = C x D
Année d'option 1: 1 novembre 2024 jusqu'au 31 octobre 2025				
T4.1	Formateur intermédiaire	10	\$	\$



T4.2	Gestionnaire de projet intermédiaire	50	\$	\$
T4.3	Architecte d'information intermédiaire	20	\$	\$
T4.4	Analyste des activités intermédiaire	40	\$	\$
T4.5	Gestionnaire de changement intermédiaire	10	\$	\$
T4.6	Formation – en ligne	1	\$	\$
T4.7	Formation – en personne/en classe	1	\$	\$
T4.8	Sous-total pour l'année d'option 1			\$
Année d'option 2: 1 novembre 2025 jusqu'au 31 octobre 2026				
T4.9	Formateur intermédiaire	10	\$	\$
T4.10	Gestionnaire de projet intermédiaire	50	\$	\$
T4.11	Architecte d'information intermédiaire	20	\$	\$
T4.12	Analyste des activités intermédiaire	40	\$	\$
T4.13	Gestionnaire de changement intermédiaire	10	\$	\$
T4.14	Formation – en ligne	1	\$	\$
T4.15	Formation – en personne/en classe	1	\$	\$
T4.16	Sous-total pour l'année d'option 2			\$
Année d'option 3: 1 novembre 2026 jusqu'au 31 octobre 2027				
T4.17	Formateur intermédiaire	15	\$	\$
T4.18	Gestionnaire de projet intermédiaire	50	\$	\$
T4.19	Architecte d'information intermédiaire	20	\$	\$
T4.20	Analyste des activités intermédiaire	50	\$	\$
T4.21	Gestionnaire de changement intermédiaire	10	\$	\$
T4.22	Formation – en ligne	1	\$	\$
T4.23	Formation – en personne/en classe	1	\$	\$
T4.24	Sous-total pour l'année d'option 3			\$
T4.25	Sous-Total (Année d'option 1 + Année d'option 2 + Année d'option 3)			\$

TABLEAU 5 – LISTE D'ACCES POUR LES UTILISATEURS SUPPLÉMENTAIRES (FACULTATIF)

Accès pour les utilisateurs supplémentaires ne sera pas considéré lors de l'évaluation financière. Toutefois, si l'on exerce l'achat des articles durant la période initiale et optionnelle, les prix de ceux-ci ne peuvent pas excéder au-delà de 3% par année. Les soumissionnaires doivent remplir les colonnes E et F du tableau 5.

TABLEAU 5 : ACCES POUR LES UTILISATEURS SUPPLEMENTAIRE					
(A)	(B)	(C)	(D)	(E)	(F)
No. d'article	Description	Nombre d'utilisateur aux fins d'évaluation	Nombre de mois	Prix ferme par utilisateur (CAD\$)	Prix évalué aux fins d'évaluations F = C x D x E
T5.1	Accès pour les utilisateurs supplémentaires – période initiale – Année 1	1,000	12	\$	\$



T5.2	Accès pour les utilisateurs supplémentaires – période initiale – Année 2	1,000	12	\$	\$
T5.3	Accès pour les utilisateurs supplémentaires – période initiale – Année 3	1,000	12	\$	\$
T5.4	Sous-total pour la période initiale (T5.1 + T5.2 + T5.3)				\$
T5.5	Accès pour les utilisateurs supplémentaires - Année d'option 1	1,000	12	\$	\$
T5.6	Accès pour les utilisateurs supplémentaires - Année d'option 2	1,000	12	\$	\$
T5.7	Accès pour les utilisateurs supplémentaires - Année d'option 3	1,000	12	\$	\$
T5.8	Sous-total pour les périodes d'options (T5.5 + T5.6 + T5.7) :				\$
T5.9	Sous-total pour Tableau 5 :				\$

TABLEAU 6 – PRIX TOTAL ÉVALUÉ AUX FINS D'ÉVALUATION

Tableau 6 : Prix total estimatif aux fins de calcul			
(A)	(B)	(C)	(D)
No. D'article	Description	Calcul du prix	Prix calculé
T1	Produits initiaux – période initiale	Total du tableau 1	\$
T2	Services professionnels – période initiale	Total du tableau 2	\$
T3	Produits initiaux – années d'option	Total du tableau 3	\$
T4	Services professionnels – années d'option	Total du tableau 4	\$
PRIX TOTAL ÉVALUÉ aux fins d'évaluations (T1 + T2 + T3 + T4):			\$



APPENDICE F – LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat PR#152202
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 Immigration Refugee and Citizenship Canada	2. Branch or Directorate / Direction générale ou Direction Learning Academy / HRSB		
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant		
4. Brief Description of Work - Brève description du travail Cloud Based Software as a Solution (SaaS) Learning Management System			
5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> 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? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> 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.) <input type="checkbox"/> No / Non <input checked="" type="checkbox"/> 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. <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> 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 commerciales sans entreposage de nuit? <input checked="" type="checkbox"/> No / Non <input type="checkbox"/> 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 <input checked="" type="checkbox"/>	NATO / OTAN <input type="checkbox"/>	Foreign / Étranger <input type="checkbox"/>	
7. b) Release restrictions / Restrictions relatives à la diffusion			
No release restrictions Aucune restriction relative à la diffusion <input checked="" type="checkbox"/>	All NATO countries Tous les pays de l'OTAN <input type="checkbox"/>	No release restrictions Aucune restriction relative à la diffusion <input type="checkbox"/>	
Not releasable À ne pas diffuser <input type="checkbox"/>	Restricted to: / Limité à: <input type="checkbox"/>	Restricted to: / Limité à: <input type="checkbox"/>	
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 <input checked="" type="checkbox"/>	NATO UNCLASSIFIED NATO NON CLASSIFIÉ <input type="checkbox"/>	PROTECTED A PROTÉGÉ A <input type="checkbox"/>	
PROTECTED B PROTÉGÉ B <input type="checkbox"/>	NATO RESTRICTED NATO DIFFUSION RESTREINTE <input type="checkbox"/>	PROTECTED B PROTÉGÉ B <input type="checkbox"/>	
PROTECTED C PROTÉGÉ C <input type="checkbox"/>	NATO CONFIDENTIAL NATO CONFIDENTIEL <input type="checkbox"/>	PROTECTED C PROTÉGÉ C <input type="checkbox"/>	
CONFIDENTIAL CONFIDENTIEL <input type="checkbox"/>	NATO SECRET NATO SECRET <input type="checkbox"/>	CONFIDENTIAL CONFIDENTIEL <input type="checkbox"/>	
SECRET SECRET <input type="checkbox"/>	COSMIC TOP SECRET COSMIC TRÈS SECRET <input type="checkbox"/>	SECRET SECRET <input type="checkbox"/>	
TOP SECRET TRÈS SECRET <input type="checkbox"/>		TOP SECRET TRÈS SECRET <input type="checkbox"/>	
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) <input type="checkbox"/>		TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) <input type="checkbox"/>	

Security Classification / Classification de sécurité unclassified

TBS/SCT 350-103 (2004/12)





Contract Number / Numéro du contrat PR#152202
Security Classification / Classification de sécurité unclassified

PART A (continued) / PARTIE A (suite)

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity.
Dans l'affirmative, indiquer le niveau de sensibilité :

No / Non Yes / Oui

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

No / Non Yes / Oui

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

<input checked="" type="checkbox"/> RELIABILITY STATUS COTE DE FIABILITÉ	<input type="checkbox"/> CONFIDENTIAL CONFIDENTIEL	<input checked="" type="checkbox"/> SECRET SECRET	<input type="checkbox"/> TOP SECRET TRÈS SECRET
<input type="checkbox"/> TOP SECRET - SIGINT TRÈS SECRET - SIGINT	<input type="checkbox"/> NATO CONFIDENTIAL NATO CONFIDENTIEL	<input type="checkbox"/> NATO SECRET NATO SECRET	<input type="checkbox"/> COSMIC TOP SECRET COSMIC TRÈS SECRET
<input type="checkbox"/> SITE ACCESS ACCÈS AUX EMBLEMES			

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?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

No / Non Yes / Oui

If Yes, will unscreened personnel be escorted?
Dans l'affirmative, le personnel en question sera-t-il escorté?

No / Non Yes / Oui

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

No / Non Yes / Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

No / Non Yes / Oui

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

No / Non Yes / Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

No / Non Yes / Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

No / Non Yes / Oui

Security Classification / Classification de sécurité unclassified
--





Contract Number / Numéro du contrat PR#152202
Security Classification / Classification de sécurité unclassified

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 CLASSIFIÉE			NATO				COMSEC					
	A	B	C	Confidential Confidentiel	Secret	Top Secret Très Secret	NATO Restricted NATO Diffusion Restreinte	NATO Confidential	NATO Secret	COSMIC Top Secret COSMIC Très Secret	Protected Protégé			Confidential Confidentiel	Secret	Top Secret Très Secret
											A	B	C			
Information / Assets Renseignements / Biens	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Production	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IT Media Support TI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IT Link Lien électronique	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée.

12. b) Will the document 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, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquez qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Security Classification / Classification de sécurité unclassified
--



ANNEXE A à APPENDICE F

SÉCURITÉ DES CONTRATS – EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN (Centre de données)

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ A, délivrées par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC).
2. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITE, comme requis par le guide de sécurité, approuvée par la PSC de TPSGC.
3. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données et(ou) de production au niveau PROTÉGÉ jusqu'à ce que l'autorisation écrite a été émise par l'autorité en matière de sécurité pour le ministère ou agence du client. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau PROTÉGÉ A.
4. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de la PSC de TPSGC.
5. L'entrepreneur ou l'offrant doit se conformer aux dispositions des documents suivants :
 - a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité, reproduite ci-joint à l'Appendice F;
 - b) le *Manuel de la sécurité des contrats* (dernière édition);
 - c) Site Web du PSC : Exigences de sécurité des contrats du gouvernement du Canada, veuillez visitez <https://www.tpsgc-pwgsc.gc.ca/esc-src>

SÉCURITÉ INDUSTRIELLE INTERNATIONALE – EXIGENCES EN MATIÈRE DE SÉCURITÉ POUR LES FOURNISSEURS ÉTRANGÈRES

No DE DOSSIER DE TPSGC : 152202_FOR, DEMANDE DE PROPOSITION, COTE DE FIABILITÉ, ACCÈS ET SÉCURITÉ AUX RENSEIGNEMENTS AU NIVEAU CANADA PROTÉGÉS A, UTILISATION DE TI, (INFONUAGE)

L'Autorité désignée en matière de sécurité pour le Canada (ADS canadien) pour les questions industrielles au Canada est la Direction de la sécurité industrielle internationale (DSII), Secteur de la sécurité industrielle (SSI), Travaux publics et Services gouvernementaux Canada (TPSGC). L'ADS canadien est chargée d'évaluer la conformité des soumissionnaires aux exigences en matière de sécurité pour les **fournisseurs étrangers**. Les exigences de sécurité suivantes s'appliquent à l'**entrepreneur étranger** destinataire constituée ou autorisé à faire des affaires dans une administration autre que le Canada et la prestation ou l'exécution à l'extérieur du Canada les travaux décrits dans le nuage de solutions, en plus des exigences en matière de sécurité et de protection. Ces exigences en matière de sécurité sont en plus des exigences énoncées dans la section intitulée Protection et sécurité des données stockées dans des bases de données.

1. **L'entrepreneur/Le sous-traitant** étranger destinataire doit être dans un pays de l'Union européenne, dans un pays de l'organisation du traité de l'Atlantique Nord (OTAN) ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité et un protocole d'entente bilatérale ou multinationale. Le programme de sécurité a des ententes en matière de sécurité et protocole d'entente bilatérale ou multinationale avec les pays mentionnés au site de TPSGC suivant: <http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html>.



2. **L'entrepreneur/Le sous-traitant** étranger destinataire doit en tout temps, au cours de la durée du **contrat/sous-traitance**, être inscrits auprès de l'autorité nationale de supervision de la protection des renseignements personnels appropriée des pays dans lesquels ils sont incorporés ou autorisé à exercer des activités commerciales. **L'entrepreneur/le sous-traitant** étranger destinataire doit fournir une preuve de son enregistrement avec l'autorité de supervision applicables à l'autorité contractante et l'autorité contractante en matière de sécurité et de cerner les renseignements personnels pertinents à l'échelle nationale. Pour **les entrepreneurs/sous-traitants** européens, ce sera l'autorité de protection des données nationales (APDN).
3. **L'entrepreneur/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution du **contrat**, tenir une équivalence à une vérification d'organisation désignée (VOD), délivrée par l'ADS canadien comme suit :
 - i. **L'entrepreneur/Le sous-traitant** étranger destinataire doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence.
 - ii. **L'entrepreneur/Le sous-traitant** étranger destinataire ne doit pas entreprendre les travaux, fournir les services ou assurer toute autre prestation tant que l'Administration désignée en matière de sécurité au Canada (ADS canadien) n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le **contrat**. L'ADS canadien donne cette confirmation par écrit à **l'entrepreneur/au sous-traitant** étranger destinataire. Un Formulaire d'attestation remis par l'ADS canadien à **l'entrepreneur/au sous-traitant** étranger destinataire permettra de confirmer la conformité et l'autorisation de fournir les services prévus.
 - iii. **L'entrepreneur/Le sous-traitant** étranger destinataire proposé doit identifier l'agent de sécurité du contrat (ASC) autorisé et un agent remplaçant de sécurité d'entreprise (ARSE) (le cas échéant) qui sera responsable du contrôle des exigences de sécurité, telles qu'elles sont définies dans le **contrat**. Cette personne sera désignée par le président-directeur général ou par un cadre supérieur clé de l'entreprise étrangère destinataire proposée. Les cadres supérieurs clés comprennent les propriétaires, les agents, les directeurs, les cadres et les partenaires occupant un poste qui leur permettrait d'avoir une influence sur les politiques ou les pratiques de l'organisation durant l'exécution du **contrat/sous-traitance**.
 - iv. **L'entrepreneur/Le sous-traitant** étranger destinataire n'autorisera pas l'accès à des renseignements/biens de niveau **CANADA PROTÉGÉ A**, sauf à son personnel, sous réserve des conditions suivantes :
 - a. Le personnel a un besoin de savoir pour l'exécution du **contrat**;
 - b. Le personnel a fait l'objet d'une vérification du casier judiciaire valide, avec des résultats favorables, d'une agence gouvernementale reconnue ou d'une organisation du secteur privé dans **leur pays**, ainsi qu'une vérification d'antécédents, validé par l'ADS canadien;
 - c. **L'entrepreneur/Le sous-traitant** étranger destinataire doit s'assurer que le personnel consente à la divulgation du casier judiciaire et antécédents à l'ADS canadien et d'autres fonctionnaires du gouvernement canadien, si demandé; et
 - d. Le Gouvernement du Canada se réserve le droit de refuser l'accès aux renseignements/ biens de niveau **CANADA PROTÉGÉ A** à **l'entrepreneur/au sous-traitant** étranger destinataire pour cause.
4. Les renseignements/biens de niveau **CANADA PROTÉGÉ** fournis ou produits dans le cadre du **contrat** ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants :



- a. L'ADS canadien atteste par écrit que le sous-traitant étranger destinataire a obtenu l'accès aux renseignements/biens de niveau **CANADA PROTÉGÉ** par l'intermédiaire de l'ADS canadien;
 - b. L'ADS canadien donne son autorisation écrite lorsque l'autre sous-traitant étranger destinataire est situé dans un autre pays.
5. **L'entrepreneur/Le sous-traitant** étranger destinataire NE DOIT PAS emporter de renseignements/biens de niveau **CANADA PROTÉGÉ** hors des établissements de travail visés, et **l'entrepreneur/ sous-traitant** étranger destinataire doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.
 6. **L'entrepreneur/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements/biens de niveau **CANADA PROTÉGÉ** pour répondre à des besoins distincts de l'exécution du **contrat** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS canadien.
 7. **L'entrepreneur/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution du **contrat** tenir une équivalence à une autorisation de détenir des renseignements (ADR) de **CANADA PROTÉGÉ A**.

Tous les renseignements/biens de niveau **CANADA PROTÉGÉ** fournis à **l'entrepreneur/au sous-traitant** étranger destinataire ou produits par ce dernier doivent être aussi protégés comme suit:

8. **L'entrepreneur/Le sous-traitant** étranger destinataire doit signaler immédiatement à l'ADS canadien tous les cas dans lesquels il est connu où il a lieu de soupçonner que les renseignements/biens de niveau **CANADA PROTÉGÉ** obtenus dans le cadre du **contrat** ont été com prom is.

OU

9. **L'entrepreneur/Le sous-traitant** étranger destinataire doit signaler immédiatement à l'ADS canadien tous les cas dans lesquels il sait où il a lieu de croire que des renseignements/biens de niveau **CANADA PROTÉGÉ** fournis ou produits par **l'entrepreneur/le sous-traitant** étranger destinataire conformément au **contrat** ont été perdus ou divulgués à des personnes non autorisées.
10. **L'entrepreneur/Le sous-traitant** étranger destinataire ne doit pas divulguer les renseignements/biens de niveau **CANADA PROTÉGÉ** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'ADS canadien.
11. **L'entrepreneur/Le sous-traitant** étranger destinataire assurera une protection des renseignements/biens de niveau **CANADA PROTÉGÉ** aussi stricte que celle mise en œuvre par le gouvernement du Canada, conformément aux politiques, aux lois et aux règlements nationaux en matière de sécurité nationale, et comme prévu par l'ADS canadien.
12. À la fin des travaux, **l'entrepreneur/le sous-traitant** destinataire doit restituer au gouvernement du Canada tous les renseignements/biens de niveau **CANADA PROTÉGÉ** qu'il aura reçus ou produits en vertu du **contrat**, y compris tous les renseignements/biens de niveau **CANADA PROTÉGÉ** remis à ses sous-traitants ou produits par eux.
13. **L'entrepreneur/Le sous-traitant** étranger destinataire exigeant aux renseignements/biens de niveau **CANADA PROTÉGÉ** ou aux sites à accès restreint en vertu du **contrat**, doit présenter une demande pour l'accès au site à l'agent de sécurité ministériel du ministère d'**Immigration, Réfugiés et Citoyenneté Canada**.



14. **L'entrepreneur/Le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker dans un système informatique des renseignements de niveau **CANADA PROTÉGÉ A** avant que l'ADS canadien lui en donne le droit.
15. **L'entrepreneur/Le sous-traitant** étranger destinataire doivent s'assurer que toutes les bases de données y compris les bases de données de sauvegarde utilisées par les organisations pour offrir les services décrits à l'énoncé de travaux contenant des renseignements de niveau **CANADA PROTÉGÉ** liés aux travaux se trouvent dans le Canada.
16. Les sous-traitances comportant des exigences relatives à la sécurité NE doivent PAS être attribuées sans l'autorisation écrite préalable de l'ADS canadien.
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/Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'Appendice F.
20. Le Canada a le droit de rejeter toute demande visant l'accès électronique, le traitement, la production ou l'entreposage de renseignements/biens de niveau **CANADA PROTÉGÉ** liés aux travaux dans un autre pays s'il y a des raisons de croire que leur sécurité, leur confidentialité ou leur intégrité pourrait être menacée.

Protection et sécurité des données stockées dans des bases de données

1. **L'entrepreneur/Le sous-traitant** étranger destinataire doit s'assurer que toutes les bases de données (utilisés par les organisations pour fournir les services décrits à l'Appendice D – Énoncé des travaux) contenant des renseignements personnels, liées au travail, se trouvent au Canada.
2. **L'entrepreneur/Le sous-traitant** étranger destinataire doit contrôler l'accès à toutes les bases de données dans lesquelles sont stockées des données liées au **contrat**, afin que seules les personnes qui ont la cote de sécurité appropriée puissent avoir accès à la base de données, soit au moyen d'un mot de passe ou d'un autre moyen d'accès (comme des mesures de contrôle biométrique).
3. **L'entrepreneur/Le sous-traitant** étranger destinataire doit s'assurer que toutes les bases de données contenant des données relatives au **contrat** sont physiquement et logiquement indépendantes (ce qui signifie qu'il n'y a pas de connexion directe ou indirecte) avec toutes les autres bases de données.
4. **L'entrepreneur/Le sous-traitant** étranger destinataire doit s'assurer que toutes les données liées au **contrat** sont traitées uniquement au Canada ou dans un autre pays approuvé par l'autorité contractante conformément au paragraphe 1.
5. **L'entrepreneur/Le sous-traitant** étranger destinataire doit s'assurer que le trafic sur le réseau national (c'est-à-dire le trafic partant d'une partie du Canada vers une destination située dans une autre partie du Canada) s'effectue exclusivement au Canada, sauf si l'autorité contractante a approuvé au préalable, par écrit, une autre route. L'autorité contractante prendra uniquement en considération une route dans un autre pays pour la transmission de données, si ce pays respecte les exigences décrites au paragraphe 1.



6. Malgré tout article des conditions générales relatif à la sous-traitance, **l'entrepreneur/le sous-traitant** 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.

Renseignements personnels

Interprétation

Dans le **contrat**, à moins que le contexte n'indique un sens différent,

« Conditions générales » désigne les conditions générales qui font partie du **contrat/sous-traitance** ;

« Renseignement personnel » désigne tout renseignement qui concerne un individu, y compris le type de renseignements décrit à la section 3 de la *Loi sur la protection des renseignements personnels*, L.R.C. 1985, ch. P-21.

« Dossier » désigne un exemplaire papier ou des données sous forme lisible par machine comprenant des renseignements personnels.

Les mots et expressions définis dans les conditions générales et utilisés dans le présent article ont le sens qui leur est donné dans les conditions générales.

En cas de divergence entre les conditions générales et les présents articles portant sur la confidentialité des renseignements personnels, les dispositions pertinentes des présents articles l'emportent.

Propriété des renseignements personnels et des dossiers

Pour exécuter les travaux, **l'entrepreneur/le sous-traitant** étranger destinataire aura accès à des renseignements personnels de tiers et(ou) en recueillera. **L'entrepreneur/Le sous-traitant** étranger destinataire reconnaît qu'il ne détient aucun droit sur ces renseignements personnels ou ces dossiers. **L'entrepreneur/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.

Utilisation des renseignements personnels

L'entrepreneur/Le sous-traitant étranger destinataire convient de créer, de recueillir, de recevoir, de gérer, de consulter, d'utiliser, de conserver, de divulguer et de disposer des renseignements personnels et des dossiers uniquement pour exécuter les travaux conformément au contrat, et ce, conformément aux dispositions du présent **contrat**.

Cueillette des renseignements personnels

1. Si **l'entrepreneur/le sous-traitant** étranger destinataire doit obtenir des renseignements personnels d'un tiers dans le cadre des travaux, il ne doit recueillir que les renseignements personnels lui permettant d'exécuter les travaux. **L'entrepreneur/Le sous-traitant** étranger destinataire doit recueillir les renseignements personnels auprès de l'individu concerné et l'informer (au moment de la cueillette ou préalablement) de ce qui suit :
 - a) les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;
 - b) les usages qui seront faits des renseignements personnels recueillis;
 - c) que 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;



- d) les conséquences, s'il en est, du refus de fournir les renseignements;
 - e) que l'intéressé au droit d'accéder à ses renseignements personnels et d'y apporter des corrections;
 - f) 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/au sous-traitant** étranger destinataire.
2. **L'entrepreneur**, ses sous-traitants 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 en vertu d'un contrat passé avec le Canada.
3. Si l'autorité contractante l'exige, **l'entrepreneur/le sous-traitant** étranger destinataire doit élaborer un formulaire de demande de consentement à utiliser lors de la cueillette de renseignements personnels ou un texte dans le cas de la cueillette de renseignements personnels par téléphone. **L'entrepreneur/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.
4. Si, lors de la cueillette de renseignements personnels auprès d'un individu, **l'entrepreneur/le sous-traitant** étranger destinataire sait ou soupçonne que cet individu n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, **l'entrepreneur/le sous-traitant** étranger destinataire doit demander des directives à l'autorité contractante.

Exactitude, confidentialité et intégrité des renseignements personnels

L'entrepreneur/Le sous-traitant étranger destinataire doit veiller à ce que les renseignements personnels soient les plus exacts, complets et à jour que possible. Pour ce faire, **l'entrepreneur/le sous-traitant** étranger destinataire doit, au minimum :

- a) ne pas utiliser de données d'identification personnelle (par ex., le numéro d'assurance sociale, le numéro de passeport, le numéro d'identificateur client unique) pour lier de nombreuses bases de données qui comprennent des renseignements personnels;
- b) isoler les dossiers des renseignements et des dossiers de **l'entrepreneur/du sous-traitant** étranger destinataire;
- c) ne donner l'accès aux renseignements personnels et aux dossiers qu'à ceux qui le requièrent aux fins d'exécution des travaux (par exemple, en utilisant des mots de passe ou un accès biométrique);
- d) donner de la formation à toute personne à laquelle **l'entrepreneur/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 d'exécution des travaux. **L'entrepreneur/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;
- e) 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;
- f) tenir 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);

- g) joindre une note à tout dossier qu'un individu a demandé de corriger, mais que l'**entrepreneur/le sous-traitant** étranger destinataire a décidé, pour quelque raison que ce soit, de ne pas corriger. Lorsque cela se produit, l'entrepreneur doit immédiatement informer l'autorité contractante de la correction demandée et des raisons de l'**entrepreneur/le sous-traitant** étranger destinataire de ne pas l'effectuer. Si l'autorité contractante demande que la correction soit effectuée, l'**entrepreneur/le sous-traitant** étranger destinataire a l'obligation de le faire;
- h) tenir un registre de la date et de l'auteur de la dernière mise à jour de chaque dossier;
- i) 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/le sous-traitant étranger destinataire et le Canada en tout temps;
- j) sécuriser et contrôler l'accès à tout renseignement personnel.

Protection des renseignements personnels

L'**entrepreneur/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. Pour ce faire, l'**entrepreneur/le sous-traitant** étranger destinataire doit au moins :

- a) stocker les renseignements personnels sous format électronique de manière à ce qu'un mot de passe (ou un autre mécanisme de contrôle) soit requis pour accéder au système ou à la base de données où sont stockés les renseignements personnels;
- b) s'assurer que les mots de passe ou autres moyens d'accès aux renseignements personnels ne sont fournis qu'aux individus qui le requièrent aux fins d'exécution des travaux;
- c) ne pas confier à un tiers (y compris un affilié) le stockage des renseignements personnels sans l'autorisation préalable et écrite de l'autorité contractante;
- d) protéger les bases de données ou les systèmes informatiques qui emmagasinent les
- e) renseignements personnels contre un accès externe de manière à protéger les renseignements très protégés et de nature délicate;
- f) faire une sauvegarde et une mise à jour de tous les dossiers au moins une fois par semaine;
- g) mettre en œuvre toutes les mesures de sécurité ou de protection demandées par le Canada de temps à autre;
- h) aviser immédiatement l'autorité contractante de toute infraction (p. ex. un accès, un usage ou une divulgation non autorisé de renseignements) ou de tout incident pouvant mettre en danger la sécurité ou l'intégrité des dossiers, des systèmes ou des installations ou des renseignements personnels sont conservés. Si une infraction se produit, l'entrepreneur ou le sous-traitant devra immédiatement prendre toutes les mesures raisonnables nécessaires pour limiter l'étendue des impacts possibles ou pour résoudre le problème et empêcher celui-ci de se reproduire. Le Canada peut exiger de l'entrepreneur qu'il prenne des mesures précises pour régler le problème et éviter qu'il se reproduise, et pourrait invoquer les dispositions de la présente entente en lien avec la suspension ou la résiliation du contrat pour manquement.

Nomination d'un agent de protection de la vie privée

L'**entrepreneur/Le sous-traitant** étranger destinataire doit nommer quelqu'un comme agent de protection de la vie privée, qui agira en tant que son représentant pour toutes les questions touchant les renseignements personnels et les dossiers. L'**entrepreneur/Le sous-traitant** étranger destinataire doit fournir le nom de cette personne à l'autorité contractante dans un délai de dix (10) jours suivant l'attribution du contrat.



Obligation de présenter des rapports trimestriels

Dans un délai de trente (30) jours suivant la fin de chaque trimestre (janvier-mars; avril-juin; juillet-septembre; octobre-décembre), l'**entrepreneur/le sous-traitant** étranger destinataire doit présenter à l'autorité contractante:

- a) une description de toute nouvelle mesure qu'il a prise pour protéger les renseignements personnels (par exemple, un nouveau logiciel ou de nouveaux contrôles d'accès utilisés par l'**entrepreneur/le sous-traitant** étranger destinataire);
- b) une liste des corrections apportées aux renseignements personnels à la demande d'un individu (y compris le nom de la personne, la date de la demande et la correction apportée);
- c) les détails de toute plainte reçue d'individus concernant la manière dont leurs renseignements personnels sont recueillis ou traités par l'**entrepreneur/le sous-traitant** étranger destinataire;
- d) une copie (dans un format électronique convenu par l'autorité contractante et l'**entrepreneur/le sous-traitant** étranger destinataire) de l'ensemble des renseignements personnels conservés électroniquement par l'**entrepreneur/le sous-traitant** étranger destinataire.

Évaluation des menaces et des risques

L'**entrepreneur/Le sous-traitant** étranger destinataire doit présenter à l'autorité contractante une évaluation des menaces et des risques dans un délai de quatre-vingt-dix (90) jours suivant l'attribution du **contrat**, et dans un délai de trente (30) jours civils suivant chaque date d'anniversaire du contrat s'il dure plus d'un an, qui doit comprendre :

- i. une copie de la dernière version du formulaire de demande de consentement ou du script que l'**entrepreneur/le sous-traitant** étranger destinataire utilise pour recueillir les renseignements personnels;
- ii. une liste des types de renseignements personnels utilisés par l'**entrepreneur/le sous-traitant** étranger destinataire se rapportant aux travaux;
- iii. une liste de tous les emplacements où les exemplaires papiers des renseignements personnels sont conservés;
- iv. une liste de tous les emplacements où les renseignements personnels sous forme lisible par machine sont conservés (par exemple, l'emplacement du serveur sur lequel la base de données est installée), ainsi que les sauvegardes;
- v. une liste de toutes les personnes auxquelles l'entrepreneur/le sous-traitant étranger destinataire a donné l'accès aux renseignements personnels ou aux dossiers;
- vi. une liste de toutes les mesures prises par l'entrepreneur/le sous-traitant étranger destinataire pour protéger les renseignements personnels et les dossiers;
- vii. une explication détaillée des menaces réelles ou potentielles touchant les renseignements personnels ou les dossiers, accompagnée d'une évaluation des risques créés par ces menaces et la pertinence des protections existantes visant à prévenir ces risques; et
- viii. une explication de toute nouvelle mesure que l'entrepreneur/le sous-traitant étranger destinataire considère prendre afin de protéger les renseignements personnels et les dossiers.

Vérification

Le Canada peut vérifier en tout temps la conformité de l'**entrepreneur/le sous-traitant** étranger destinataire aux articles relatifs à la protection des renseignements personnels. À la demande de l'autorité contractante,



L'entrepreneur/le sous-traitant étranger destinataire doit donner au Canada (ou à son représentant autorisé) l'accès à ses locaux et aux renseignements personnels et dossiers en tout temps jugé raisonnable. Si le Canada découvre un problème durant la vérification, **l'entrepreneur/le sous-traitant** étranger destinataire doit le corriger immédiatement à ses frais.

Obligations réglementaires

2. **L'entrepreneur/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](#), 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 /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 toute autre loi qui entre en vigueur lorsqu'il y a lieu.
3. **L'entrepreneur/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/le sous-traitant** étranger destinataire estime que l'une ou l'autre des obligations du contrat l'empêche de s'acquitter de ses obligations en vertu de ces lois, il doit immédiatement informer l'autorité contractante de la disposition du contrat et de l'obligation de la loi qu'il considère comme contradictoires.

Élimination et retour des dossiers au Canada

L'entrepreneur/Le sous-traitant étranger destinataire ne peut éliminer aucun dossier à moins que l'autorité contractante le lui demande. Sur demande de l'autorité contractante, ou lorsque les travaux liés aux renseignements personnels sont achevés, le contrat est achevé ou lorsque le contrat est résilié, selon ce qui se produit en premier, **l'entrepreneur/le sous-traitant** étranger destinataire doit retourner tous les dossiers (y compris les copies) à l'autorité contractante.

Obligation juridique de divulguer les renseignements personnels

Avant de divulguer tout renseignement personnel conformément à toute loi, à tout règlement ou toute ordonnance rendue par une cour de justice, un tribunal ou une entité administrative compétente, **l'entrepreneur/le sous-traitant** étranger destinataire doit immédiatement informer l'autorité contractante afin de lui permettre de participer aux procédures pertinentes.

Plaintes ou demandes d'accès

Le Canada et **l'entrepreneur/le sous-traitant** étranger destinataire conviennent de s'informer immédiatement et mutuellement de la réception d'une plainte en vertu de la *Loi sur l'accès à l'information*, 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 et mutuellement de son dénouement.

Exception

Les obligations énoncées dans ces articles 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/le sous-traitant** étranger destinataire ou de tout sous-traitant, agent ou représentant de l'entrepreneur ou de leurs employés.



EXIGENCES EN MATIÈRE DE SÉCURITÉ POUR UN DDP

SECRET

L'entrepreneur et les sous-traitants doivent être dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational, ou qui posséderont un tel instrument avec le Canada avant la fin de la période de soumission. Le programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d'entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de SPAC: <http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html>.

1. Tous les renseignements et les biens de niveau **CANADA PROTÉGÉ** fournis à l'entrepreneur / à l'offrant / au sous-traitant étranger destinataire doivent être protégés comme suit :
2. L'entrepreneur/L'offrant/Le sous-traitant étranger destinataire doit, en tout temps durant l'exécution du contrat/du contrat de sous-traitance, détenir une Attestation de sécurité d'installation valide, délivrée par l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) **du pays du fournisseur** d'un niveau équivalent à **SECRET**.
3. Dans l'éventualité du retrait de la partie destinataire ou à la fin du **contrat /du contrat de sous-traitance**, tous les renseignements et les biens de niveau **CANADA PROTÉGÉ** fournis ou produits en vertu du **contrat/contrat de sous-traitance** continueront d'être protégés, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.
4. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire assurera une protection des renseignements et des biens de niveau **CANADA PROTÉGÉ** aussi stricte que celle mise en œuvre par le gouvernement du Canada, conformément aux politiques, aux lois et aux règlements nationaux en matière de sécurité nationale, et comme prévu par l'Autorité nationale de sécurité (ANS) ou par l'Autorité désignée en matière de sécurité (ADS) de **du pays du fournisseur**.
5. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire doit attribuer à tous les renseignements et biens de niveau **CANADA PROTÉGÉ** qui lui sont fournis par le gouvernement du Canada en vertu du **contrat/du contrat de sous-traitance** la cote de sécurité équivalente utilisée par **Le pays du fournisseur**, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur**.
5. L'entrepreneur/L'offrant/Le sous-traitant étranger destinataire doit, en tout temps durant l'exécution du **contrat/du contrat de sous-traitance** veiller à ce que le transfert des renseignements et des biens de niveau **CANADA PROTÉGÉ** soit effectué conformément aux législations, règlements, et politiques nationales **du pays du fournisseur** et aux dispositions du Protocole d'entente bilatérale sur la sécurité industrielle signé **du pays du fournisseur** et le Canada.
6. À la fin des travaux, **l'entrepreneur/l'offrant/le sous-traitant** étranger destinataire doit restituer au gouvernement du Canada, par l'entremise des circuits officiels, tous les renseignements et les biens de niveau **CANADA PROTÉGÉ** qu'il aura reçu ou produit en vertu **du contrat/du contrat de sous-traitance**, y compris tous les renseignements et les biens de niveau **CANADA PROTÉGÉ** remis à ses sous-traitants ou produits par eux **sauf autrement autorisé au préalable écrite par l'ADS du Canada**.
7. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de l'Autorité nationale de la sécurité (ANS) ou l'Autorité



désignée en matière de sécurité (ADS) concernée, conformément aux législations, règlements, et politiques nationales **du pays du fournisseur / l'ADS du Canada.**

8. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou conserver dans un système informatique des renseignements/biens de niveau **CANADA PROTÉGÉ** avant que l'Autorité nationale de la sécurité (ANS) ou l'Autorité désignée en matière de sécurité (ADS) **du pays du fournisseur** lui en donne le droit. Une fois que **l'entrepreneur / l'offrant / le sous-traitant** étranger destinataire a reçu cette approbation écrite, il peut effectuer ces tâches jusqu'au niveau **PROTÉGÉ A.**
9. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements /biens de niveau **CANADA PROTÉGÉ** pour répondre à des besoins distincts de l'exécution **du contrat/ du contrat de sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS du Canada.
10. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire visitant des sites gouvernementaux ou industriels canadiens dans le cadre du contrat doit soumettre pour approbation une demande de visite à l'administration désignée en matière de sécurité (ADS) du Canada, par l'entremise de son Autorité nationale de la sécurité (ANS) ou son Autorité désignée en matière de sécurité (ADS).
11. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire doit signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait où il a lieu de croire que des renseignements/biens de niveau **CANADA PROTÉGÉ** obtenus dans le cadre **du contrat / du contrat de sous-traitance** ont été compromis.
12. **L'entrepreneur/L'offrant/Le sous-traitant** étranger destinataire ne doit pas divulguer les renseignements/biens de niveau **CANADA PROTÉGÉ** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'intermédiaire de l'Autorité nationale de la sécurité (ANS) ou de l'Autorité désignée en matière de sécurité (ADS) du destinataire / ADS du Canada.
13. **L'entrepreneur / L'offrant / Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'Appendice F.

Installations ou locaux proposés par le soumissionnaire nécessitant des mesures de sauvegarde

Tel qu'indiqué à la Partie 6 Exigences relatives à la sécurité, le soumissionnaire doit fournir l'adresse complète de ses installations ou de ses locaux et celles des individus proposés, pour lesquelles des mesures de sauvegarde sont nécessaires à la réalisation des travaux :

N° civique / nom de la rue, unité / N° de bureau / d'appartement
Ville, province, territoire / État
Code postal / code zip
Pays



ANNEXE B à APPENDICE F – GUIDE DE CLASSIFICATION DE SÉCURITÉ

N°	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
1.	Tout membre du personnel de l'entrepreneur ayant un accès physique aux centres de données de l'entrepreneur	<ul style="list-style-type: none"> • Matériel physique • Installations de centres de données • Données telles qu'elles sont stockées sur des supports de sauvegarde locaux de l'entrepreneur 	Canada	Fiabilité	Cela concerne le personnel de l'entrepreneur, notamment les ressources chargées de la gestion des installations qui ont physiquement accès au matériel lié aux services infonuagiques dans les centres de données de l'entrepreneur.
2.	Tout membre du personnel de l'entrepreneur ayant un accès logique limité aux services de l'entrepreneur	<ul style="list-style-type: none"> • Toutes les données opérationnelles • Données telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur 	Les deux	Fiabilité	Cela concerne le personnel de l'entrepreneur qui a un accès logique aux données du GC hébergées dans les centres de données de l'entrepreneur et à tout système sensible de même qu'aux données sur les incidents de sécurité. Il peut s'agir de ressources de niveau 1 de type bureau de service.
3.	Tout membre du personnel de l'entrepreneur qui a des rôles privilégiés et un accès logique non restreint à des biens du GC dans les services de l'entrepreneur	<ul style="list-style-type: none"> • Toutes les données opérationnelles • Données du GC telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur • Biens, dont les données et les justificatifs du GC 	Les deux	Secret	Cela concerne le personnel de l'entrepreneur qui a des privilèges élevés assortis d'un accès logique sans restriction aux données du GC hébergées dans les centres de données de l'entrepreneur, à tout système sensible, de même qu'aux données sur les incidents de sécurité. Cela comprend l'accès autorisé par l'intermédiaire d'un processus établi comme les demandes juridiques.



N°	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
4.	Tout le personnel de l'entrepreneur ayant un accès physique ou logique aux documents de conception détaillés.	<ul style="list-style-type: none">Documents de conception détaillés de la solution de GSTI, notamment les détails de l'application logique et physique, les architectures de la solution d'infrastructure technologique, les contrôles et l'architecture de sécurité, les détails des diagrammes des composantes, le code source, les détails des cas d'utilisation et des schémas des processus d'activités, les détails de l'application, les flux de données et les modèles de données, les conceptions des bases de données, les interfaces de systèmes, les contrôles internes, les plans des essais et les résultats des essais.	Les deux	Fiabilité	Cela concerne surtout l'accès aux documents relatifs à l'architecture et à la conception détaillée.
5.	Personnel du centre des opérations de sécurité (COS) de l'entrepreneur	<ul style="list-style-type: none">Données telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneurDonnées de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur	Les deux	Fiabilité	Il s'agit du personnel du COS de l'entreprise.



N°	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
6.	Soutien de 4 ^e niveau du fabricant d'origine	<ul style="list-style-type: none">• Matériel physique• Installations de centres de données• Données telles qu'elles sont stockées sur des supports de sauvegarde locaux de l'entrepreneur	Canada	S. O.	L'entrepreneur aura recours à des sous-traitants pour certains de ses services liés aux opérations du centre de données. L'entrepreneur doit retenir les services de ses sous-traitants comme il se doit en concluant un contrat et en définissant clairement les travaux. Ces ressources n'auront pas un accès physique direct aux données du gouvernement du Canada. Elles peuvent toutefois participer à la résolution de problèmes liés à leur niveau d'expertise avec des ressources de l'entrepreneur qui possèdent les autorisations de sécurité requises et qui ont accès aux données. Si la ressource de soutien de 4 ^e niveau du fabricant d'origine se trouve aux centres de données de l'entrepreneur, elles seront accompagnées par les opérateurs de l'entrepreneur détenteurs d'une attestation de sécurité appropriée. Par exemple : Assistance avec l'équipement réseau, assistance avec le CVC.



APPENDICE G – Obligations en matière de sécurité et protection de la vie privée

Annexe 1 – Obligations en matière de sécurité

Objet

La présente annexe a pour objet d'énoncer les obligations du fournisseur en ce qui concerne la configuration et la gestion appropriées des actifs et des actifs informationnels, afin de protéger ces actifs et ces actifs contre toute modification, accès ou exfiltration non autorisés, le tout conformément au contrat, la présente annexe, les mesures de sécurité spécifiques du fournisseur et les politiques canadiennes en matière de sécurité et de confidentialité (collectivement appelées «obligations de sécurité et de confidentialité»).

Exécution des obligations en matière de protection de la vie privée

Les obligations du fournisseur contenues dans les présentes obligations de sécurité et confidentialité doivent être transférées par le fournisseur aux sous-processeurs du fournisseur, dans la mesure où elles s'appliquent à chaque sous-processeur du fournisseur, étant donné la nature des services fournis au fournisseur.

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 annexe.

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.

1. Reconnaissance

Les parties reconnaissent que:

- a) Tous les biens et les actifs informationnels sont assujettis à ces obligations en matière de sécurité et de confidentialité.
- b) Nonobstant toute autre disposition de la présente annexe, les parties partagent la responsabilité d'élaboration et du maintien des politiques, des procédures et des contrôles de sécurité relatifs aux biens et aux actifs informationnels.
- c) Le fournisseur ne doit pas avoir ou tenter d'obtenir la garde d'un actif d'information, ni permettre à un membre du personnel des services à accéder à un actif information avant la mise en œuvre des obligations de sécurité et de confidentialité requises, comme l'exige la présente annexe, au plus tard à l'attribution du marché.
- d) Les obligations de sécurité s'appliquent au Palier 1 (jusqu'à la protection A / blessures faibles) et au Palier 2 (jusqu'à la protection B / blessures moyennes), sauf indication contraire.



2. Protection des données du Canada

L'entrepreneur doit protéger les données du Canada contre tout accès, modification ou exfiltration non autorisés. Cela 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.

3. Rôles et responsabilités liés à la sécurité

- a. 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. Cela 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.
- b. 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.

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

- a. L'entrepreneur doit s'assurer que les données du Canada, l'infrastructure de l'entrepreneur (y compris tout service IaaS, PaaS ou SaaS fourni au Canada) et les emplacements de service sont protégés par des mesures de sécurité appropriées et qui respectent les exigences établies dans les pratiques et politiques en matière de sécurité de l'entrepreneur.
- b. 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. IaaS, PaaS, SaaS) au sein des services infonuagiques, y compris :
 - i. 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;
 - ii. ISO/IEC 27017:2015 Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27 002 pour les services du nuage;
 - iii. 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. 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 des exclusions sont précisées, ou s'il faut séparer des organismes de sous-services, comme l'hébergement du centre de données, le rapport d'évaluation de l'organisme de sous-services doit être fourni.
- d. 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.

- e. 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).
- f. L'entrepreneur doit conserver les certifications ISO 27001, ISO 27017 et SOC 2 Type II 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.

5. Vérification de la conformité

- a. L'entrepreneur doit effectuer 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 comme suit :
 - i. 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;
 - ii. 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;
 - iii. 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.
- b. 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.
- c. 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.

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

- a. Pendant la durée du contrat, l'entrepreneur doit respecter les exigences de sécurité sélectionnées dans le Profil de contrôle de sécurité pour les services de TI du gouvernement du Canada (GC) fondés sur l'infonuagique pour les renseignements classés « PBMM » (<https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html>) selon la portée des services infonuagiques offerts 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.

- b La conformité sera évaluée et validée par l'entremise du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (FSI) (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, 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 de la lettre de confirmation stipulant qu'il a intégré le programme;
- (ii) Une copie du rapport d'évaluation le plus récent fourni par le CCC;
- (iii) Une copie du rapport sommaire le plus récent fourni par le CCC.

L'entrepreneur devrait communiquer avec le service à la clientèle du CCC, comme il est indiqué à l'appendice L, Programme d'évaluation de la sécurité des TI de SaaS, pour obtenir tout renseignement supplémentaire concernant le Programme d'évaluation de la sécurité des technologies de l'information (STI) s'appliquant aux FSI.

L'entrepreneur des services infonuagiques proposés a l'obligation continue d'aviser le CCC lorsqu'il y a d'importants changements à la prestation des services de sécurité des TI à l'appui des services offerts par l'entrepreneur.

Les certifications sont présentées ci-dessous et validées au moyen d'évaluations de tiers indépendants.

- c Dans les cas où l'entrepreneur est un fournisseur de SaaS utilisant un fournisseur d'aaS approuvé par le GC qui se conforme déjà aux exigences de l'article 4 – Assurance d'une tierce partie et des sous-sections (1) et (2) de l'article 6 – Programme d'évaluation de la sécurité des TI des fournisseurs de services infonuagiques, le fournisseur de SaaS 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 final concernant l'évaluation. Pour toute question, il est possible de communiquer avec le CCC par courriel à l'adresse contact@cyber.gc.ca.

7. Protection des données

- a L'entrepreneur doit :
- i. 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.
 - ii. transmettre les données du Canada de 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.



- iii. 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 du Canada avant que l'entrepreneur puisse avoir accès aux données du Canada pour effectuer des activités opérationnelles, de soutien ou de maintenance.
 - iv. 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 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.
- b. 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.
 - c. L'entrepreneur doit s'assurer que tout traitement effectué à l'extérieur du Canada, y compris le déplacement ou la transmission de copies approuvées de données, a lieu à l'intérieur de la région de service convenue.
 - d. 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.

8. Isolement des données

- a. L'entrepreneur doit mettre en place des contrôles afin d'assurer un isolement approprié des ressources, afin 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. Cela nécessite la mise en œuvre de contrôles d'accès et la mise en place d'une séparation logique ou physique appropriée pour soutenir :
 - i. la séparation entre l'administration interne de l'entrepreneur et les ressources utilisées par ses clients;
 - ii. 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;
 - iii. la capacité du GC de soutenir l'isolation dans un environnement à locataires géré par le GC.
- b. À la demande du Canada, l'entrepreneur doit fournir au Canada un document qui décrit l'approche permettant d'assurer l'isolation 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.

9. Emplacement des données

- a. L'entrepreneur doit stocker et protéger les données du Canada, au repos, y compris les données sauvegardées ou conservées à des fins de redondance. Cela comprend la capacité d'isoler les données au Canada dans des centres de données approuvés. Un centre de données approuvé est défini comme suit :
 - i. Un centre de données qui répond à toutes les exigences et certifications de sécurité identifiées à l'article 30 pour la sécurité physique (centre de données ou installations);



- ii. Garantit l'impossibilité de trouver les données d'un client en particulier sur des supports physiques;
 - iii. 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.
- b. Le fournisseur doit attester que la prestation et l'approvisionnement des services en vertu du présent marché proviennent de pays membres de l'Organisation du traité de l'Atlantique Nord (OTAN) (https://www.nato.int/cps/fr/natohq/nato_countries.htm) ou de l'Union européenne (UE) (https://europa.eu/european-union/about-eu/countries_fr) ou de pays avec lesquels le Canada a un accord international ou bilatéral en matière de sécurité industrielle. Dans le cadre du Programme de sécurité des contrats, des accords internationaux bilatéraux en matière de sécurité industrielle ont été conclus avec les pays énumérés sur le site Web <https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html> de SPAC. La liste est mise à jour périodiquement.
- c. L'entrepreneur doit avoir la capacité pour le Canada d'isoler les données du Canada hébergées par les services infonuagiques des centres de données situés géographiquement au Canada.
- d. À la demande du Canada, l'entrepreneur doit :
 - i. Fournir au GC une liste à jour des emplacements physiques, y compris la ville, qui peuvent contenir des données du Canada;
 - ii. Identifier 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.
- e. L'entrepreneur des services infonuagiques proposés a l'obligation continue d'aviser le Canada lorsqu'il y a des mises à jour de la liste des emplacements physiques qui peuvent stocker des données du Canada au repos.

10. 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, pseudodirectes et hors ligne, y compris, sans toutefois s'y limiter, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activités infonuagiques, les codes source 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://www.bac-lac.gc.ca/fra/services/gestionressources-documentaires-gouvernement/lignes-directrices/Pages/lignes-directrices-formatsfichier-transferers-ressources-documentaires.aspx>).



11. Disposition des dossiers et remise des dossiers au Canada

- a. L'entrepreneur doit éliminer ou réutiliser en toute sécurité les ressources (p. ex. l'équipement, le stockage des données, les fichiers et la mémoire) qui contiennent des données du Canada et s'assurer que les données précédemment stockées ne peuvent être traitées par d'autres clients après leur diffusion. Cela touche 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.
- b. L'entrepreneur doit fournir au Canada une confirmation 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.

12. 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 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 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-pourinformation-non-classifie-protege-et-protege-b>);
- 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 (PVMC) (<https://www.cse-cst.gc.ca/fr/groupe/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.



13. Gestion des clés

L'entrepreneur doit s'assurer qu'un service de gestion des clés peut être utilisé et qu'il fournit des capacités, y compris, mais sans s'y limiter :

- a. la création ou la génération et la suppression des clés de cryptage par le GC;
- 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 par l'entrepreneur 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;
- e. la capacité d'importer de façon sécuritaire les clés générées par le GC à partir d'un module matériel de sécurité, géré sur place par le GC, et ce, sans exposition du texte en clair des clés pendant le processus d'importation;
- f. la capacité d'empêcher le fournisseur de services infonuagiques de récupérer des copies en texte clair des clés générées par le GC;
- g. la capacité de déléguer les privilèges liés à l'utilisation des clés pour leur usage par les services infonuagiques utilisés pour les services gérés par le GC.

14. 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 maliciels, les attaques et les abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide to General Server Security [guide relatif à la sécurité générale des serveurs]), des points de référence du Center for Internet Security (CIS) ou d'une norme équivalente approuvée par écrit par le Canada.

15. 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 (OWASP) (p. ex. Application Security Verification Standard [ASVS]) 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.

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

- a. L'entrepreneur doit avoir la capacité pour le Canada de soutenir un accès sécurisé aux services, y compris la capacité de configurer :
 - i. l'authentification multifacteur conformément à la norme ITSP.30.031 V3 du CST (ou à ses versions ultérieures) (<https://cyber.gc.ca/fr/orientation/guide-sur->



[l'authentification-des-utilisateurs-dans-les-systemes-de-technologie-de](#)) au moyen de justificatifs approuvés par le GC;

- ii. un accès en fonction du rôle;
 - iii. les contrôles d'accès aux objets entreposés;
 - iv. les politiques d'autorisation granulaire pour permettre ou limiter l'accès.
- b. L'entrepreneur doit être en mesure d'établir des paramètres par défaut pour l'ensemble de l'organisme pour la gestion des politiques des locataires.

17. Fédération

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 (SAML) 2.0 et l'OpenID Connect 1.0, ou ses versions ultérieures, où les justificatifs et authenticateurs 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.

18. Gestion des accès privilégiés

(1) L'entrepreneur doit :

- a. 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;
- b. 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;
- c. appliquer et vérifier les autorisations d'accès aux services infonuagiques et aux données du Canada;
- d. 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;
- e. 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 consignnant 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 CST (<https://cyber.gc.ca/fr/orientation/guide-sur-l'authentification-des-utilisateurs-dans-les-systemes-de-technologie-de>);
- 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 consignnant 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 CST (<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 multifacteur pour authentifier les utilisateurs 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>);
 - 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.

19. Gestion à distance

- a. 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 :
 - i. mettre en place des mécanismes d'authentification multifacteur pour authentifier les utilisateurs d'accès à distance, 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>);
 - ii. employer des mécanismes cryptographiques pour protéger la confidentialité des séances d'accès à distance, conformément à l'article 13 (Protection cryptographique);
 - iii. acheminer tout l'accès à distance par des points de contrôle des accès gérés, surveillés et vérifiés.



- iv. déconnecter ou désactiver rapidement les connexions non autorisées de gestion à distance ou d'accès à distance;
 - v. autoriser l'exécution à distance des commandes privilégiées et l'accès à distance aux informations relatives à la sécurité.
- b. 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.

20. Sécurité des réseaux et des communications

L'entrepreneur doit :

- a. appliquer 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://cyber.gc.ca/fr/orientation/conseils-sur-laconfiguration-securisee-des-protocoles-reseau-itsp40062>) et ITSP.40.111 (<https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-nonclassifie-protege-et-protege-b>);
- c. utiliser des certificats correctement configurés dans les connexions TLS conformément aux directives du CST.
- d. permettre au Canada de mettre en œuvre des contrôles d'accès au réseau et des règles de sécurité qui permettent ou refusent le trafic réseau vers les ressources canadiennes.

21. Journalisation et vérification

- a. 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.
- b. 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 [CEF], Syslog et autres formats communs) ainsi que d'interfaces de programmation d'application (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.
- c. L'entrepreneur doit permettre au Canada d'examiner et d'analyser de manière centralisée les dossiers de vérification de multiples composants des services infonuagiques utilisés par l'entrepreneur. Ceci comprend de fournir des interfaces API qui permettent d'inspecter et d'interroger les données au repos dans les applications SaaS, notamment d'évaluer les événements tels que l'accès et les comportements des utilisateurs et des administrateurs ainsi que les changements relatifs à l'accès des tiers aux interfaces API stockés dans les journaux des applications SaaS.



22. Surveillance continue

- a. 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 :
- i. 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;
 - ii. faire de son mieux pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le refus de service;
 - iii. faire de son mieux pour détecter les attaques, les incidents de sécurité et autres événements anormaux;
 - iv. détecter l'utilisation et l'accès non autorisés à tous les services infonuagiques, données et composants pertinents aux services infonuagiques IaaS, PaaS ou SaaS du Canada;
 - v. 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;
 - vi. répondre aux menaces et aux attaques contre les services infonuagiques du fournisseur, les contenir et veiller à la récupération;
 - vii. au besoin, prendre des contre-mesures proactives, y compris, des mesures préventives et d'intervention permettant d'atténuer les menaces.
- b. Les services infonuagiques de l'entrepreneur doivent permettre de copier les données des applications du GC dans les services infonuagiques hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du gouvernement).

23. Gestion des incidents de sécurité

- (a) Le processus d'intervention en cas d'incident de sécurité de l'entrepreneur pour les services infonuagiques doit comprendre un processus de gestion des incidents de sécurité des TI ainsi que des pratiques de soutien des activités de préparation, de détection, d'analyse, de confinement et de récupération. Il s'agira notamment de :
- i. 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.



- ii. des processus et procédures documentés indiquant comment l'entrepreneur relèvera les incidents de sécurité, y donnera suite et y remédiera, dressera un rapport à leur sujet et les signalera au Canada, y compris : (i) la portée des incidents de sécurité de l'information que l'entrepreneur doit signaler au Canada; (ii) le degré de divulgation des incidents de sécurité de l'information détectés et les réponses connexes; (iii) le délai cible de signalement des incidents de sécurité de l'information; (iv) la procédure de signalement et d'acheminement en cas d'incidents de sécurité; (v) les coordonnées des personnes-ressources pour le traitement des enjeux relatifs aux incidents de sécurité de l'information; (vi) tout recours applicable à certains incidents de sécurité de l'information.
 - iii. 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.
 - iv. Cela permet uniquement aux représentants désignés du client autorisés (comme le Centre des opérations de sécurité de SPC) par le responsable technique :
 - a. de demander et de recevoir un accès et de l'information 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;
 - b. d'effectuer le suivi d'un événement signalé lié à la sécurité de l'information.
 - v. Des procédures de réponse aux demandes de preuves numériques potentielles ou d'autres renseignements se trouvant dans l'environnement des services infonuagiques, y compris des procédures judiciaires et des mesures de protection pour la tenue d'une chaîne de possession;
- (b) À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit le processus d'intervention en cas d'incident de sécurité de l'entrepreneur.

L'entrepreneur doit :

- a. collaborer avec le Centre des opérations de sécurité du Canada (p. ex. CCC, SOC ministériel) en ce qui concerne le confinement, l'élimination et la reprise en cas d'incident de sécurité, conformément au processus d'intervention en cas d'incident de sécurité.
 - b. tenir un registre des violations de la sécurité comprenant une description de la violation de la sécurité, la durée, les conséquences de la violation, le nom de la personne ayant signalé la violation, et la personne à qui la violation a été signalée, et la procédure pour récupérer les données ou le service;
 - 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.
- (c) Le Canada pourrait exiger des preuves judiciaires de la part de l'entrepreneur pour contribuer à une enquête du GC. L'entrepreneur consent à fournir de l'aide au GC dans la mesure du possible.



24. Intervention en cas d'incident de sécurité

- a. L'entrepreneur doit alerter et aviser promptement le client (par téléphone ou par courriel) 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.
- b. Si l'entrepreneur prend connaissance de toute compromission ou toute violation et qu'il relève une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée des données ou l'accès accidentel ou illégal aux données du client ou des données personnelles du client 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 des renseignements détaillés sur cet incident de sécurité; (iii) prendre les mesures raisonnables pour remédier aux causes et atténuer les dommages découlant de l'incident de sécurité.

25. Fuite d'information

- a. L'entrepreneur doit avoir un processus documenté qui énonce son approche en cas d'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 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 :
 - i. un processus d'identification des éléments de données précis utilisés dans la contamination d'un système;
 - ii. un processus visant à isoler et à éradiquer un système contaminé;
 - iii. 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.

26. Essais de sécurité et validation

- a. L'entrepreneur doit disposer d'un processus qui permet au Canada d'effectuer une analyse de vulnérabilité ou un essai de pénétration non perturbateur et non destructif visant la partie canadienne des composantes du service infonuagique dans l'environnement de l'entrepreneur.

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



27. Filtrage de sécurité du personnel

- a. L'entrepreneur doit veiller à la mise en place de mesures de sécurité qui accordent et maintiennent le niveau de filtrage de sécurité requis pour le personnel de l'entrepreneur impliqué dans la prestation des services infonuagiques et pour le personnel du sous-traitant, en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées.
- b. 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.gc.ca/pol/doc-fra.aspx?id=28115>), ou utiliser un équivalent acceptable convenu par le Canada.
- c. 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 :
 - i. 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;
 - ii. 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;
 - iii. 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;
 - iv. 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;
 - v. l'approche de détection des initiés malveillants potentiels et les contrôles 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.

28. Sécurité matérielle (centre des données et installations)

- a. L'entrepreneur doit veiller à la mise en place de mesures de sécurité matérielle qui assurent la protection des installations de TI et des actifs du système d'information dans lesquels les données du Canada sont stockées et protégées contre toute forme de manipulation, de perte, de dommages et de saisie. Des mesures de protection physique visant toutes les installations qui abritent des données du Canada 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 à l'appendice C de la Directive sur la gestion de la sécurité du Conseil du Trésor : Procédures obligatoires relatives aux mesures de sécurité matérielle (<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611>) 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.
- b. À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit les mesures de sécurité matérielle de l'entrepreneur.
 - c. 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.

29. Gestion des risques de la chaîne d'approvisionnement

- a. L'entrepreneur doit veiller à ce que des mesures de sécurité soient prises 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 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.
- b. 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.
- c. 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.
- d. Dans les cas où l'entrepreneur est un fournisseur de SaaS utilisant un fournisseur d'IaaS 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 SaaS utilisant un fournisseur d'IaaS 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 IaaS approuvé par le GC pour un examen de l'intégrité de la chaîne d'approvisionnement (ICA).
Cet examen de l'ICA sera effectué au plus tôt tous les trois ans.

30. Sous-traitants

- a. 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.
- b. 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 aviser 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) au sujet 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.



Annexe 2 – Obligations en matière de confidentialité

Généralités

Objet

La présente annexe 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 annexe et aux mesures particulières de l'entrepreneur en matière de confidentialité (collectivement, les « **obligations en matière de confidentialité** »).

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.

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 obligations en matière de confidentialité afin de se conformer aux pratiques de sécurité des normes de l'industrie.

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, susceptibles d'avoir une incidence sur la collecte, l'utilisation, la divulgation ou l'élimination des données qui contiennent des renseignements personnels. 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.

1. Remerciements

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 annexe, 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 annexe, au plus tard à la date de l'attribution du contrat.

2. 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 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 [LPRPDE])
- (3) L'entrepreneur doit s'abstenir d'utiliser ou 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 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.

3. 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).
- (2) Dans les 30 jours suivant l'attribution du contrat, l'entrepreneur doit fournir un document qui décrit de quelle manière il aidera le Canada à traiter les demandes d'accès, y compris la manière dont il attestera la réception d'une demande d'accès et fournira les renseignements demandés.

4. Assurance tierce : Attestations

- (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 IaaS, PaaS ou SaaS 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. IaaS, PaaS, SaaS) 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 (PII) dans l'informatique en nuage public agissant comme processeur de PII – Certification obtenue par un organisme de certification accrédité.
- (3) Chaque certification présentée 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.
- (5) L'entrepreneur doit conserver les certifications ISO 27018, ISO 27017 et SOC 2 Type II 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.

5. Conformité aux exigences en matière de confidentialité

- (1) L'entrepreneur doit démontrer, au moyen de rapports d'évaluation et de rapports d'audit 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.

6. Vérification de la conformité

- (1) Si le Canada doit effectuer des vérifications, inspections de sécurité et de confidentialité ou examiner d'autres renseignements (documents, flux des données, description de la protection de données, architecture de données et descriptions de sécurité), les deux parties conviennent de négocier de bonne foi pour trouver une solution et de tenir compte à la fois de la justification de la demande du Canada et des processus et protocoles de l'entrepreneur.
- (2) L'entrepreneur doit effectuer les vérifications de confidentialité et de sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter les données du Canada qui contiennent des renseignements personnels de la façon suivante :
 - (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 des vérificateurs de sécurité qualifiés, indépendants et reliés à une tierce partie qui (i) sont qualifiés selon l'AICPA, CPA Canada ou le régime de certification ISO, et (ii) sont conformes à la norme ISO/CEI 17 020 sur les systèmes de gestion de la qualité à la sélection et aux frais de l'entrepreneur.
- (3) 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.

- (4) À la demande du Canada, l'entrepreneur ou un sous-traitant peut fournir des preuves supplémentaires, y compris des plans de sécurité et de confidentialité du système, des conceptions ou des documents d'architecture qui fournissent une description complète du système qui comprend tous les éléments de données contenant des renseignements personnels, 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.

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 l'annexe 1 – Obligations en matière de sécurité, article 16 (développement sécurisé).

8. Agent de protection de la confidentialité

L'entrepreneur doit, dans les 10 jours suivant la date d'entrée en vigueur du présent contrat, fournir au Canada les renseignements permettant d'identifier une personne à titre d'agent de protection de la confidentialité pour agir à titre de représentant de l'entrepreneur pour toutes les questions liées aux renseignements personnels et aux dossiers. L'entrepreneur doit fournir le nom et les coordonnées de cette personne, y compris son titre commercial, son adresse courriel et son numéro de téléphone.

9. Aide dans la prestation d'une évaluation des facteurs relatifs à la confidentialité du Canada

L'entrepreneur doit aider le Canada à créer une évaluation des facteurs relatifs à la vie privée (EFVP) conformément à la Directive sur l'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor (<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308>) en aidant le Canada à produire la documentation à l'appui, y compris une EFVP de base pour le Canada fournie par l'entrepreneur. L'entrepreneur convient de fournir ce soutien dans les cinq à dix jours ouvrables suivant une demande ou dans un délai convenu d'un commun accord, selon la complexité de la demande par le Canada.

10. 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 l'annexe 1 – Obligations en matière de sécurité.
- (2) L'entrepreneur doit :
 - (a) tenir un registre des atteintes à la sécurité avec une description de l'atteinte, la période, les conséquences de l'atteinte, le nom du déclarant et de la personne à qui l'atteinte a été signalée, ainsi que la procédure de récupération des données;
 - (b) 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.

11. 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.

11.1 Propriété des renseignements personnels et des dossiers

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.

11.2 Utilisation des renseignements personnels

- (1) **L'entrepreneur ou le sous-traitant** étranger destinataire convient de créer, recueillir, recevoir, gérer, utiliser et 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**.

Collecte de renseignements personnels

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 cueillette ou préalablement) de ce qui suit :

- (a) les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;
 - (b) les usages qui seront faits des renseignements personnels recueillis;
 - (c) 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;
 - (d) les conséquences, le cas échéant, du refus de fournir les renseignements;
 - (e) l'intéressé a le droit d'accéder à ses renseignements personnels et d'y apporter des corrections;
 - (f) les renseignements personnels feront partie d'un répertoire particulier (au sens de la Loi sur la protection des renseignements personnels), et le demandeur est informé de l'institution fédérale qui gère le répertoire de renseignements personnels, si l'autorité contractante a fourni ces renseignements à **l'entrepreneur ou au sous-traitant** étranger destinataire.
- (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.



- (3) Si l'autorité contractante l'exige, **l'entrepreneur ou le sous-traitant** destinataire étranger doit élaborer un formulaire de demande de consentement à utiliser lors de la cueillette de renseignements personnels ou un texte dans le cas de la cueillette 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.
- (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.

11.3 Exactitude, confidentialité et intégrité des renseignements personnels

- (1) **L'entrepreneur ou le sous-traitant** étranger destinataire doit veiller à ce que les renseignements personnels soient les plus 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 :
 - (a) 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;
 - (b) isoler tous les dossiers des renseignements et des dossiers de **l'entrepreneur ou du sous-traitant** étranger destinataire;
 - (c) 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).
 - (d) 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;
 - (e) 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;
 - (f) 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);
 - (g) 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 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;



- (h) tenir un registre de la date et de l'auteur de la dernière mise à jour de chaque dossier;
- (i) maintenir un journal de vérification électronique qui enregistre tous les accès et toutes 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;
- (j) sécuriser et contrôler l'accès à tout exemplaire papier des dossiers.

11.4 Protection des renseignements personnels

- (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 l'annexe 1 – Obligations en matière de sécurité.

11.5 Obligations législatives

- (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 du Canada*, 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 toute autre loi qui entre en vigueur lorsqu'il y a lieu.
- (2) L'**entrepreneur ou le sous-traitant** destinataire étranger reconnaît que les obligations dont il doit s'acquitter en vertu du contrat/du contrat de sous-traitance 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, l'**entrepreneur ou le sous-traitant** étranger destinataire 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.

11.6 Obligation juridique de divulguer les renseignements personnels

- (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).
- (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.

11.7 Plaintes

Le Canada et l'**entrepreneur ou le sous-traitant** étranger destinataire conviennent de s'informer immédiatement et mutuellement de la réception d'une plainte en vertu de la *Loi sur l'accès à l'information*, 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 et mutuellement de son dénouement.



11.8 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.



APPENDICE H – PROCESSUS D'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

Processus d'intégrité de la chaîne d'approvisionnement

1. Exigences Obligatoire

1.1 Exigences relatives à la présentation des soumissions (obligatoires à la date de clôture de la demande de soumissions). Les soumissionnaires doivent joindre à leur soumission, au plus tard à la date de clôture de la demande de soumissions, l'ISCA suivante :

1.1.1 Liste des produits informatiques: Les fournisseurs doivent identifier les solutions logiciel-service sur lesquelles les données du Canada seraient transmises et / ou stockées, qui seront utilisées et / ou installées pour exécuter toute partie des travaux et / ou des services décrits dans le contrat subséquent, en ce qui concerne la solution logiciel-service, en complétant le modèle de soumission du formulaire 3-SCI fourni dans la DDP, qui comprend les informations suivantes:

- a. **Nom OEM:** Entrez le nom du fabricant de l'équipement d'origine (OEM) du produit commandé
- b. **Numéro OEM DUNS:** Entrez le numéro DUNS du fabricant OEM. Le système de numérotation universelle des données (DUNS) est un numéro unique à neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme mondiale utilisée pour déterminer le pointage de crédit d'une entreprise. Si la société ne possède pas de numéro DUNS ou si vous ne parvenez pas à vous en procurer un, veuillez compléter les informations demandées sous «C - Informations sur la propriété». Les informations sur la propriété comprennent les 5 premiers, en pourcentage, les investisseurs et les propriétaires de l'entreprise. Les noms fournis aux investisseurs et aux propriétaires doivent être ceux qui figurent dans les documents d'investissement ou de propriété de la société en question.
- c. **Nom du produit:** entrez le nom du fabricant OEM pour le produit.
- d. **Numéro de modèle:** Entrez le modèle OEM et / ou le numéro de version du produit.
- e. **URL du produit:** entrez l'URL de la page Web du fabricant pour le produit.
- f. **Informations sur la vulnérabilité:** Saisissez les informations concernant les 5 derniers problèmes de sécurité signalés concernant le produit. Si le fabricant OEM publie ces informations sur le site Web CVE, indiquez les numéros CVE séparés par des points-virgules (;). Si le fabricant OEM ne publie pas ces informations sur le site Web de CVE, vous devrez lui demander directement des informations sur les failles de sécurité et les fournir au Centre canadien de la cybersécurité. Si tel est le cas pour un produit particulier, entrez "voir les informations jointes" dans le champ Informations sur la vulnérabilité et incluez le ou les noms de fichier dans la colonne d'informations supplémentaires fournissant les informations de vulnérabilité requises

1.1.2 Informations sur la propriété: les entrepreneurs doivent identifier le fabricant d'origine du (des) produit (s) ou service (s) commandé (s), ainsi que le nom de tout entrepreneur (c.-à-d. Sous-traitants (particuliers ou entreprises), entrepreneurs de sous-traitants (particuliers ou entreprises) tout au long de la chaîne, revendeurs, distributeurs, sous-traitants, etc.) du ou des produits ou services commandés. Cette liste doit identifier tous les tiers pouvant exécuter toute partie des travaux, qu'il s'agisse de soustraitants pour le entrepreneur ou de sous-traitants pour sous-traitants du entrepreneur tout au long de la chaîne. Tout sous-traitant pouvant accéder aux données du Canada doit être identifié. Aux fins de cette exigence, un tiers qui est simplement un entrepreneur de biens pour le entrepreneur, mais qui n'exécute aucune partie des travaux, n'est pas considéré comme un sous-traitant. Les sous-traitants incluent, par exemple, des techniciens qui pourraient être déployés ou assurer la maintenance de la solution du entrepreneur. Si le entrepreneur ne prévoit pas faire appel à



des sous-traitants pour exécuter une partie quelconque des travaux, il est demandé au entrepreneur de l'indiquer dans sa réponse.

Les entrepreneurs sont priés de fournir leurs informations sur le formulaire 3. Il est demandé aux entrepreneurs d'indiquer leur nom légal sur chaque page, d'insérer un numéro de page ainsi que le nombre total de pages. Les entrepreneurs sont également invités à insérer une ligne distincte pour chaque sous-traitant et des lignes supplémentaires, le cas échéant.

Pour chacune des entités répertoriées, indiquez **Numéro OEM DUNS**: Entrez le numéro DUNS du fabricant OEM. Le système de numérotation universelle des données (DUNS) est un numéro unique à neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme mondiale utilisée pour déterminer le pointage de crédit d'une entreprise. Si la société ne possède pas de numéro DUNS ou si vous ne parvenez pas à vous en procurer un, renseignez les informations demandées sous «C - Informations sur la propriété». Les informations sur la propriété comprennent les 5 premiers, en pourcentage, les investisseurs et les propriétaires de l'entreprise. Les noms fournis aux investisseurs et aux propriétaires doivent être ceux qui figurent dans les documents d'investissement ou de propriété de la société en question.

- c. **Pays / Nationalité**: le pays dans lequel une personne répertoriée a sa nationalité principale ou le pays dans lequel une personne morale est enregistrée.
- d. **Lien vers le site Web d'entreprise**: pour chaque nom OEM ou nom de entrepreneur, propriété, investisseurs et dirigeants énumérés ci-dessus, indiquez un URI / URL aux informations prenant en charge les revendications répertoriées dans chacun des champs

1.1.3 **Diagrammes de réseau** : Un ou plusieurs diagrammes de réseau conceptuels montrant la totalité du réseau proposé pour la réalisation des travaux décrits dans la présente Énoncé des travaux. Les diagrammes de réseau doivent uniquement comprendre les portions du réseau du soumissionnaire (et de ceux de ses sous-traitants) sur lesquelles les données du Canada seraient transmises dans le cadre de l'exécution de tout contrat subséquent. À tout le moins, le diagramme doit illustrer ce qui suit :

- i. les principaux nœuds suivants servant à la prestation de services dans le cadre de tout contrat subséquent :
 1. les points de service;
 2. le réseau de base;
 3. le ou les réseaux de sous-traitants (préciser le nom du sous-traitant qui figure sur la liste des sous-traitants);
- ii. les interconnexions entre les nœuds, s'il y a lieu;
- iii. toute interconnexion entre les nœuds et Internet;
- iv. pour chaque nœud, un renvoi au produit qui sera déployé dans ce nœud, à l'aide du numéro d'article de la liste des produits de TI.

1.1.4 **Liste des sous-traitants** : Le soumissionnaire doit remettre une liste de tous les sous-traitants qui pourraient participer à l'exécution d'une partie des travaux (cela comprend les sous-traitants qui lui sont affiliés ou liés) dans le cadre de tout marché attribué. Au minimum, la liste doit inclure ce qui suit :

- i. le nom du sous-traitant;
- ii. l'adresse du siège social du sous-traitant;
- iii. la partie des travaux que réaliserait le sous-traitant;
- iv. le ou les lieux où le sous-traitant réaliserait les travaux.



2. Évaluation de l'information sur la sécurité de la chaîne d'approvisionnement :

- 2.1. Le Canada déterminera si, à son avis, les informations sur la sécurité de la chaîne logistique créent la possibilité que la solution de l'entrepreneur puisse compromettre ou être utilisée pour compromettre la sécurité des équipements, micrologiciels, logiciels, systèmes ou informations du Canada.
- 2.2. Dans le cadre de son évaluation:
 - a. Le Canada peut demander au entrepreneur toute information supplémentaire dont il a besoin pour effectuer une évaluation de sécurité complète des informations de sécurité de la chaîne logistique. Le entrepreneur disposera de 2 jours ouvrables (ou d'une période plus longue, si l'autorité de sécurité de la chaîne d'approvisionnement le spécifie par écrit) pour fournir les informations nécessaires au Canada. Si ce délai n'est pas respecté, la réponse sera disqualifiée.
 - b. Le Canada peut utiliser les ressources du gouvernement ou les consultants pour effectuer l'évaluation et peut contacter des tiers pour obtenir des informations complémentaires. Le Canada peut utiliser n'importe quel renseignement, qu'il soit inclus dans la réponse ou provenant d'une autre source, qu'il juge souhaitable de mener une évaluation complète des renseignements sur la sécurité de la chaîne logistique.
- 2.3. Si, de l'avis du Canada, un aspect quelconque de l'Information sur la sécurité de la chaîne logistique, s'il est utilisé dans une solution, risque de compromettre ou d'être utilisé comme compromettant la sécurité des équipements, micrologiciels, logiciels, systèmes ou informations du Canada:
 - a. Le Canada informera le entrepreneur par écrit (par courrier électronique) et identifiera le ou les aspects de l'information sur la sécurité de la chaîne d'approvisionnement qui sont sujets à préoccupation ou qui ne peuvent pas être évalués (par exemple, les futures versions proposées des produits ne peuvent pas être traitées). évalué). Toute information supplémentaire que le Canada pourrait être en mesure de fournir au entrepreneur au sujet de ses préoccupations sera déterminée en fonction de la nature des préoccupations. Dans certaines situations, pour des raisons de sécurité nationale, le Canada pourrait ne pas être en mesure de fournir des informations supplémentaires au entrepreneur; Par conséquent, dans certaines circonstances, le entrepreneur ne connaîtra pas les raisons sous-jacentes des préoccupations du Canada en ce qui concerne un produit, un sous-traitant ou un autre aspect de ses informations sur la sécurité de la chaîne d'approvisionnement.
 - b. L'avis donnera au entrepreneur une occasion de soumettre des informations révisées sur la sécurité de la chaîne logistique dans les 10 jours civils suivant le jour où la notification écrite du Canada est envoyée au entrepreneur (ou sur une période plus longue spécifiée par écrit par la chaîne logistique. Autorité de sécurité).
 - c. Si le entrepreneur soumet les informations révisées sur la sécurité de la chaîne d'approvisionnement dans le délai imparti, le Canada procédera à une deuxième évaluation. Si le Canada détermine que certains aspects des informations de sécurité de la chaîne d'approvisionnement révisées du entrepreneur pourraient compromettre ou servir à compromettre la sécurité de l'équipement, des micrologiciels, des logiciels, des systèmes ou des informations du Canada, aucune autre possibilité de révision des informations de sécurité de la chaîne d'approvisionnement ne sera fournie. la réponse sera disqualifiée.
- 2.4. En participant à ce processus, le entrepreneur reconnaît que la nature de la technologie de l'information est telle que de nouvelles vulnérabilités, y compris des failles de sécurité, sont constamment identifiées. En outre, le entrepreneur reconnaît que l'évaluation de la sécurité effectuée par le Canada n'entraîne pas l'évaluation de la solution proposée. Par conséquent:
 - a. une qualification en vertu de la présente DDP ne constitue pas une approbation du fait que les produits ou autres informations inclus dans les informations de sécurité de la chaîne logistique satisfont aux exigences de la demande de soumissions ultérieure ou de tout contrat



subséquent ou autre instrument pouvant être attribué en tant que résultat de toute demande de soumissions ultérieure;

b. la qualification en vertu de la présente DDP ne signifie pas que des informations identiques ou similaires sur la sécurité de la chaîne d'approvisionnement seront évaluées de la même manière pour les besoins futurs; (c) à tout moment au cours du processus de demande de soumissions subséquent, le Canada peut informer un entrepreneur que certains aspects de ses informations sur la sécurité de la chaîne d'approvisionnement font désormais l'objet de préoccupations en matière de sécurité. À ce stade, le Canada en informera le défendeur et donnera au entrepreneur l'occasion de réviser ses informations sur la sécurité de la chaîne d'approvisionnement, en utilisant le même processus que celui décrit ci-dessus.

c. au cours de l'exécution d'un contrat ultérieur, si le Canada a des préoccupations concernant certains produits, conceptions ou sous-traitants initialement inclus dans les informations sur la sécurité de la chaîne logistique, les conditions de ce contrat régiront le processus de traitement de ces préoccupations.

- 2.5 Tous les entrepreneurs seront informés par écrit s'ils sont ou non qualifiés en vertu de la présente DDP pour passer à la prochaine étape du processus d'approvisionnement.
- 2.6 Tout entrepreneur qualifié en vertu de la présente DDP sera tenu de proposer une solution cohérente avec la version finale de l'information sur la sécurité de la chaîne d'approvisionnement qu'il a soumise avec sa réponse à la présente DDP (révision seulement conformément au paragraphe ci-dessous). Sauf en vertu du paragraphe ci-dessous, aucun produit alternatif ou supplémentaire ni aucun sous-traitant ne peuvent être proposés dans la solution du entrepreneur. Ceci est une exigence obligatoire de ce processus de sollicitation. La solution proposée lors de toute demande de soumissions ultérieure ne doit pas nécessairement contenir tous les produits dans les informations finales sur la sécurité de la chaîne d'approvisionnement.
- 2.7 Une fois qu'un entrepreneur a été qualifié en réponse à la présente DDP, aucune modification n'est autorisée dans les informations sur la sécurité de la chaîne logistique, sauf dans des circonstances exceptionnelles déterminées par le Canada. Étant donné qu'on ne peut pas prévoir toutes les circonstances exceptionnelles, on peut déterminer si des changements peuvent être apportés et le processus régissant ces changements sera déterminé par le Canada au cas par cas.

APPENDICE I – FORMULAIRE D’AUTORISATION DE TÂCHES

DEMANDE D’AUTORISATION DE TÂCHES			
1.0 Renseignements administratifs			
Entrepreneur :			
Numéro de BC :	Numéro de contrat :	Date :	
N° de l’autorisation de tâches :	Numéro d’ordre d’achat :	Réponse requis :	
2.0 Description des travaux à exécuter			
Renseignements généraux :			
But général et portée :			
Tâches et responsabilités :			
Livrables :			
3.0 Période de services	De :		à :
4.0 Emplacement des travaux			
5.0 Exigences en matière de déplacements			
6.0 Autorisation de sécurité requise	<input type="checkbox"/> Fiabilité <input type="checkbox"/> Confidentiel <input type="checkbox"/> Secret <input type="checkbox"/> Sans objet		
7.0 Équipement et matériel fournis par le gouvernement			
8.0 Autorités			
Chargé de projet de IRCC		Autorité contractante de IRCC	
9.0 Base de paiement pour l’autorisation de tâches			
Type de catégorie de personnel	Taux de salaire journalier fixe tout compris	Niveau d’effort estimé	Prix total (\$)
Total partiel - Personnel			
Frais de déplacement			
Autres coûts			
Total partiel - Tout			
Taxes applicables			
TOTAL			
Base de paiement utilisée			
Limitation des dépenses			
Mode de paiement utilisé			
Mensuel			
Soumissions des factures			
APPROBATION DE L’AUTORISATION DE TÂCHES			



10.0 Autorité contractante de CIC - Autorisation de procéder à l'autorisation de tâches	
Signature :	Date :
11.0 Chargé de projet de CIC – La proposition relative à l'autorisation de tâches de l'entrepreneur est acceptée.	
Signature :	Date :
12.0 Entrepreneur - Autorisation des dépenses	
Signature :	Date :
Vous devez vendre au Canada, conformément aux conditions énoncées dans le contrat n° _____ d'IRCC et aux conditions énoncées dans le présent document, mentionnées par renvoi ou jointes à celui-ci, les services énumérés dans la présente autorisation de tâches au prix indiqué.	



APPENDICE J – ACCORDS SUR LES NIVEAUX DE SERVICE (ANS)

Uniquement les modalités de l'ANS, détaillées à la section 1 du paragraphe 3.2 : La présentation technique, (c)(vi), relative aux niveaux de service et à la prestation des services fera partie du Contrat.

En présentant une soumission, l'entrepreneur reconnaît et convient que toutes les modalités contenues à l'Appendice J – Accords sur les niveaux de service de la solution ANS 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'Appendice J – Accords sur les niveaux de service du ANS qui comprend des renseignements sur les prix, comme (sans s'y limiter) ceux 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.



APPENDICE K – ENTENTE DE NON-DIVULGATION DE SPAC RELATIF A L'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

Note aux fournisseurs: Veuillez noter que cet accord de non-divulgence couvre uniquement les exigences de SCI en vertu de l'article 3.6, Section IV: Exigences relatives à l'intégrité de la chaîne d'approvisionnement. Les fournisseurs seront invités à conclure un accord de confidentialité bilatéral (NDA) avec la CCCS une fois qu'ils auront intégré le programme d'évaluation de la sécurité des TI des logiciels-services

Entente de non-divulgence

En présentant une réponse, l'entrepreneur doit accepter les modalités de l'entente de non-divulgence cidessous (l'« Entente de non-divulgence ») :

1. L'entrepreneur accepte d'assurer la confidentialité de toute information qu'il reçoit du Canada au sujet de l'évaluation qu'a faite ce dernier de l'information sur la sécurité de la chaîne d'approvisionnement fournie par l'entrepreneur (l'« information sensible »), y compris, sans toutefois s'y limiter, les aspects de l'information sur la sécurité de la chaîne d'approvisionnement qui soulèvent des préoccupations, et les raisons qui ont mené aux interrogations du Canada à cet égard.

L'information sensible comprend, mais pas exclusivement, les documents, instructions, directives, données, éléments matériels, avis ou autres, qu'ils aient été reçus verbalement, sous forme imprimée ou d'une autre façon ou qu'ils soient ou non considérés comme classifiés, exclusifs ou sensibles.

2. L'entrepreneur convient de ne pas reproduire, copier, divulguer, publier ou communiquer, en tout ou en partie, de quelque façon que ce soit, de l'information sensible à une autre personne qu'un employé d'entrepreneur détenant une habilitation de sécurité correspondant à la sensibilité de l'information consultée, sans le consentement écrit préalable de l'autorité de la sécurité de la chaîne d'approvisionnement. L'entrepreneur accepte d'aviser immédiatement l'autorité de la sécurité de la chaîne d'approvisionnement dès qu'une personne, autre que celles autorisées en vertu du présent article, accède à de l'information sensible.

3. Toute l'information sensible demeure la propriété du Canada et doit être retournée à l'autorité de sécurité de la chaîne d'approvisionnement ou détruite à la demande de cette dernière dans les 30 jours suivant cette demande.

4. L'entrepreneur, est conscient qu'un manquement à cette entente de non-divulgence peut entraîner sa disqualification à l'étape de l'arrangement en matière d'approvisionnement (AMA), ou une résiliation immédiate du contrat subséquent. L'entrepreneur reconnaît également que toute violation de cette entente de non-divulgence peut entraîner un examen de sa cote de sécurité ainsi qu'un examen de son statut en tant que soumissionnaire admissible pour d'autres besoins.

5. La présente entente de non-divulgence demeure en vigueur indéfiniment.



APPENDICE L – PROGRAMME D'ÉVALUATION DE LA SÉCURITÉ DES TI DES LOGICIELS-SERVICES : PROCESSUS D'INTEGRATION

- 1. Présenter une soumission au Programme d'évaluation de la sécurité des TI des logiciels-services**
 - a. Pour présenter une soumission au Programme, le soumissionnaire doit suivre les étapes suivantes
 - b. Communiquer avec le Centre d'appel du CCC à l'adresse contact@cyber.gc.ca, au 613-949- 7048 ou au 1-833-CYBER-88.
 - c. Se préparer à conclure une entente de non-divulgence bilatérale avec le CCC.
 - d. Fournir tous les documents nécessaires à l'évaluation au Centre de contact du CCC. Lorsqu'il fournit des documents, il devrait utiliser les identifiants du programme de cryptage PGP (Pretty Good Privacy) pour chiffrer les documents. Voir la section 2, Clé PGP, pour obtenir une copie de ladite clé.

- 2. Clé PGP**
 - a. Envoyer un courriel ou téléphoner au Centre de contact du CCC pour demander la clé publique requise pour la clé PGP du CCC. Utiliser cette clé pour chiffrer les documents sensibles à soumettre dans le cadre du Programme d'évaluation de la sécurité des TI du PSC.

- 3. Personnes-ressources et assistance**
 - a. Le centre d'appel du CCC est le point de contact pour toutes les soumissions de documents liés au programme d'évaluation de la sécurité des TI des logiciels-services. Le responsable de l'équipe d'évaluation des logiciels-services, ou un délégué autorisé, a accès à cette boîte de réception. Tous les documents d'évaluation de la sécurité des TI du PSC seront gérés et protégés au moyen du chiffrement PGP pendant leur transmission (voir la section 2 pour obtenir une copie de la clé PGP). Tous les documents seront également traités et gérés conformément aux politiques de gestion de l'information du CCC.

Centre d'appel du CCC
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

APPENDICE M – EXIGENCES RELATIFS A LA SÉCURITÉ NIVEAU 1

Exigences relatives à la sécurité pour logiciel-service

Exigences de qualification

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

1. Palier 1 (Renseignements classés jusqu'au niveau Protégé A, inclusivement)

ID de l'exigence obligatoire	Sous-catégorie	Besoins	Obligation de démontrer la conformité au niveau 1
O1	Rôles et responsabilités en matières de sécurité	Le fournisseur doit définir clairement les rôles et les responsabilités en ce qui concerne les contrôles de sécurité et les fonctionnalités des services entre le fournisseur (toutsous-processeur du fournisseur, le cas échéant) et le Canada	Dans le document, le fournisseur doit inclure, au minimum, les rôles et responsabilités des parties en ce qui concerne: (i) la gestion des comptes; (ii) la protection des frontières; (iii) la sauvegarde des actifs et du système d'information; (iv) la gestion des incidents; (v) la surveillance du système; et (vi) la gestion des vulnérabilités.



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O2	Protection des données	<p>Les emplacements physiques du logiciel-service public commercial (qui peut contenir des données du Canada) doivent être situés à l'un ou l'autre de ces endroits :</p> <ul style="list-style-type: none"> a. un pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN); b. un pays membre de l'Union européenne (UE); ou c. un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité industrielle. <p>Les fournisseurs sont priés de noter ce qui suit :</p> <p>De plus amples renseignements sur les pays de l'OTAN sont accessibles à l'adresse suivante :</p> <p>https://www.nato.int/cps/fr/natohq/nato_countries.htm.</p> <p>De plus amples renseignements sur les pays de l'UE sont accessibles à l'adresse suivante :</p> <p>https://europa.eu/europeanunion/about-eu/countries_fr.</p> <p>Dans le cadre du Programme de sécurité des contrats, des accords internationaux bilatéraux en matière de sécurité industrielle ont été conclus avec les pays énumérés sur le site Web https://www.tpsgc-pwgsc.gc.ca/esc-src/internationalfra.html de SPAC, tel qu'il est mis à jour de temps à autre.</p>	<p>Le fournisseur doit présenter une documentation démontrant la façon dont le logiciel-service public commercial proposé satisfait aux exigences obligatoires de l'Exigences relatives à la protection des données.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> a. 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. <p>L'Exigences relatives à la 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. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O3	Installations des centres de données	<p>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 actifs 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.</p> <p>Cette description doit inclure, à tout le moins, les éléments qui suivent :</p> <ul style="list-style-type: none"> a. des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont 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'ENS prescrite; 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. a restriction de l'accès physique aux actifs des systèmes d'information aux employés autorisés et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, et valider l'accès au moyen f. l'accompagnement des visiteurs et la surveillance de leur activité; g. la tenue des 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); et 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. 	<p>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 de la section XX, Exigences relatives aux installations du centre de données. Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> 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 actifs 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. <p>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. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O4	Sécurité du personnel	<p>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 actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées.</p> <p>Les mesures en matière de filtrage de sécurité seront 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/docfra.aspx?id=28115), ou à une norme équivalente approuvée par le Canada. Cette description doit inclure, à tout le moins, les éléments qui suivent :</p> <ul style="list-style-type: none"> 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; et e. approche de détection des initiés malveillants potentiels et des contrôles mis en oeuvre pour atténuer le risque d'accès aux données du GC ou d'incidence sur la fiabilité du logiciel-service hébergeant les actifs et les données du gouvernement du Canada. 	<p>Le fournisseur doit présenter une documentation démontrant la façon dont le fournisseur du logiciel-service public commercial respecte les exigences de la relatives à la sécurité du personnel.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> 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 actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. b. 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. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
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 oeuvre de politiques, de procédures et de contrôles de sécurité de l'information	<p>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.</p> <p>Le fournisseur doit présenter les certifications suivantes de l'industrie afin de démontrer la conformité du service proposé :</p> <ol style="list-style-type: none"> 1. l'une des certification suivantes : <ol style="list-style-type: none"> i. ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences, ii. contrôle de l'organisation des services (SOC) de l'AICPA – rapports des SOC 2 de type II; 2. autoévaluation de ses services par rapport à la version 3.01 (ou une version ultérieure) de la matrice des contrôles infonuagiques (MC) de la Cloud Security Alliance (CSA). <p>Chaque rapport de certification et d'évaluation fourni doit :</p> <ol style="list-style-type: none"> a. être valide à la date de clôture de la soumission. b. indiquer la dénomination sociale du fournisseur proposé et du soustraitant 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 soustraitante doit être inclus, et 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. <p>Remarque :</p> <ul style="list-style-type: none"> • Les certifications doivent être fournies pour toutes les parties du service proposé. • Les certifications doivent être accompagnées de rapports d'évaluation. <p>Les certifications doivent être valides et avoir été émises dans les 12 mois précédant le début du contrat.</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O6	Gestion de la chaîne d'approvisionnement	<p>Le fournisseur doit présenter une liste de fournisseurs tiers contenant des renseignements à leur sujet (filiales, sous-traitants, y compris les fournisseurs de services infonuagiques, etc.) qui fourniraient au Canada le logiciel-service public commercial.</p> <p>Aux fins de cette exigence, une entreprise qui n'est qu'un fournisseur de biens du fournisseur du logiciel-service public commercial proposé, mais qui n'exécute aucune partie de la chaîne d'approvisionnement qui pourrait fournir au Canada le logiciel-service public commercial, n'est pas considérée comme un tiers</p> <p>Parmi les exemples de tiers, mentionnons les techniciens qui pourraient être déployés ou qui seraient affectés à la maintenance du logiciel-service public commercial du fournisseur du logiciel-service qui ont été proposés par le fournisseur.</p> <p>Remarque :</p> <p>Les fournisseurs sont avisés que les étapes fournisseur avise régulièrement le Canada en cas de mise à jour de la liste des fournisseurs tiers.</p>	<p>Le fournisseur doit fournir une liste de documentation des sous-processeurs pouvant être utilisés pour exécuter une partie quelconque des services en fournissant les services au Canada. La liste doit inclure les informations suivantes (i) le nom du sous-processeur; (ii) l'identification des activités de périmètre qui seraient réalisées par le sous-processeur; et (iii) le ou les emplacements où le sous-processeur effectuerait les activités requises pour prendre en charge les services.</p> <p>1) Pour le SaaS, le contractant doit démontrer que l'laaS/PaaS est mis à profit par ces services:</p> <ul style="list-style-type: none">a) Les sous-processeurs des fournisseurs ont été évalués conformément par le programme CCCS; etb) Le fournisseur respecte les obligations de sécurité des sous-processeurs et/ou des sous-traitants énoncés dans les exigences pendant toute la durée du contrat. <p>Si le fournisseur du logiciel-service commercial proposé n'utilise pas de tiers pour effectuer une partie de la chaîne d'approvisionnement susceptible de fournir au Canada le logiciel-service public disponible dans le commerce proposé, il est demandé au fournisseur de l'indiquer leur réponse à cette exigence.</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O7	Gestion des risques de la chaîne d'approvisionnement	Le fournisseur du logiciel-service public commercial proposé doit mettre en oeuvre 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 oeuvre 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	<p>Le fournisseur doit démontrer la façon dont le fournisseur du logiciel-service public commercial respecte les exigences, comme le précise le programme du logiciel-service.</p> <p>Pour être jugée conforme, la documentation fournie doit démontrer la conformité du fournisseur à l'une des trois normes suivantes :</p> <ol style="list-style-type: none"> 1. ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4); <p>Ou</p> <ol style="list-style-type: none"> 2. publication spéciale 800-161 du NIST – <i>Supply Chain Risk Management Practices for Federal Information Systems and Organizations</i> (pratiques de gestion des risques de la chaîne d'approvisionnement pour les systèmes d'information et organisations du fédéral); <p>Ou</p> <ol style="list-style-type: none"> 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.



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O8	Gestion de l'accès privilégié	<p>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 :</p> <ol style="list-style-type: none"> a. 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 gouvernement du Canada; b. restreindre et minimiser l'accès aux services et aux renseignements du Canada 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 renseignements; d. restreindre tout l'accès aux interfaces de service qui hébergent des données et des renseignements aux utilisateurs finaux, aux appareils et aux processus (ou services) ayant un identifiant, une authentification et une autorisation uniques; e. mettre en oeuvre 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 : <ol style="list-style-type: none"> 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://cyber.gc.ca/fr/node/1842/html/26717); f. mettre en oeuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux (niveau 2 seulement) ayant un accès privilégié, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://cyber.gc.ca/fr/node/1842/html/26717); g. mettre en place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux données et aux renseignements du GC; h. définir et mettre en oeuvre 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; 	<p>Le fournisseur doit démontrer sa conformité en fournissant de la documentation décrivant la capacité du logiciel-service commercial à répondre aux exigences relatives à la sécurité liées aux exigences en matière de gestion de l'accès privilégié :</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ol style="list-style-type: none"> a. les documents sur le système ou un livre blanc décrivant les politiques, les processus et les procédures utilisés pour gérer la gestion de l'accès privilégié. <p>La justification requise pour la gestion de l'accès privilégié ne peut simplement reprendre l'exigence obligatoire. Le répondant doit présenter des explications et une démonstration et indiquer où se trouvent les documents de référence dans la réponse. Pour ce faire, il doit fournir le titre du document et les numéros de page et de paragraphe et préciser la façon dont le fournisseur du logiciel-service commercial proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
		<ul style="list-style-type: none">i. adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services 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; etm. révoquer, en cas de cessation d'emploi, les authentificateurs et les justificatifs d'accès associés au personnel de service.	



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O9	Fédération de l'identité	<p>Fédération de l'identité</p> <p>Le fournisseur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment :</p> <ol style="list-style-type: none"> mettre en oeuvre 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://cyber.gc.ca/fr/node/1842/html/26717); prendre en charge le Security Assertion Markup Language (SAML) 2.0 et OpenID Connect 1.0, où les justificatifs et authentificateurs des utilisateurs finaux pour les services d'infonuagique sont contrôlés uniquement par le Canada; 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 d'infonuagique correspondants. 	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fédération de l'identité.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ol style="list-style-type: none"> les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en oeuvre pour la protection de la fédération de l'identité. <p>Pour les sections Fédération de l'identité, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p>
O10	Protection des points d'extrémité	<p>Protection des points d'extrémité</p> <p>Le fournisseur doit mettre en oeuvre, 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 (CIS) ou d'une norme équivalente approuvée par écrit par le Canada.</p>	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection des points d'extrémité.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ol style="list-style-type: none"> les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en oeuvre pour la protection de la fédération de l'identité. <p>Pour les sections Protection des points d'extrémité, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O11	Développement sécurisé	<p>Développement sécurisé</p> <p>Le fournisseur doit mettre en oeuvre 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 (OWASP) (p. ex. Application Security Verification Standard [ASVS]) ou une norme équivalente approuvée par le Canada par écrit.</p>	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Développement sécurisé.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> a. les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en oeuvre pour la protection de la fédération de l'identité. <p>Pour les sections Développement sécurisé, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p>
O12	Gestion à distance du fournisseur	<p>Gestion à distance des fournisseurs</p> <p>Le fournisseur doit gérer et surveiller l'administration à distance du service du fournisseur utilisé pour héberger les services du GC et prendre des mesures raisonnables pour:</p> <ul style="list-style-type: none"> a. Mettre en oeuvre des mécanismes d'authentification multifacteurs pour authentifier les utilisateurs d'accès distant, conformément au ITSP.30.031 V2 du CST (ou versions ultérieures) (https://www.cse-cst.gc.ca/fr/node/1842/html/26717); b. Employer un algorithme cryptographique approuvé par le CSTC pour protéger la confidentialité des sessions d'accès à distance; c. acheminez tous les accès à distance via des points de contrôle d'accès contrôlés, surveillés et vérifiés; d. déconnecter ou désactiver rapidement les connexions de gestion à distance ou d'accès à distance non autorisées; e. Autoriser l'exécution à distance de commandes privilégiées et l'accès à distance aux informations relatives à la sécurité 	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Gestion à distance du fournisseur.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> a. les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en oeuvre pour la protection de la fédération de l'identité. <p>Pour les sections de la Gestion à distance du fournisseur, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O13	Fuite d'information	<p>Fuite d'information</p> <ol style="list-style-type: none"> 1. 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 du fournisseur doit être harmonisé <ol style="list-style-type: none"> 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 approuvée par écrit par le Canada. Nonobstant ce qui précède, le processus d'intervention en cas de fuite d'information du fournisseur doit comprendre, à tout le moins : <ol style="list-style-type: none"> a. un processus d'identification du renseignement précis impliqué dans la contamination d'un actif ou d'un système; b. un processus visant à isoler et à éradiquer un renseignement ou un système contaminé; c. un processus d'identification des renseignements ou des systèmes pouvant 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, et ce, chaque année ou après toute modification apportée au 	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fuite d'information.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ol style="list-style-type: none"> a. les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en oeuvre pour la protection de la fédération de l'identité. <p>Pour les sections Fuite d'information, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O14	Protection Cryptographique	<p>Protection cryptographique</p> <p>Le fournisseur doit fournir au Canada un document décrivant le processus suivi pour répondre à une protection cryptographique de l'information.</p> <ol style="list-style-type: none"> Configurez toute cryptographie utilisée pour mettre en oeuvre des sauvegardes de confidentialité ou d'intégrité, ou utilisée dans le cadre d'un mécanisme d'authentification (solutions VPN, TLS, modules logiciels, infrastructure à clé publique et jetons d'authentification, le cas échéant), conformément au Centre de la sécurité des communications (CST). – algorithmes cryptographiques, tailles de clés cryptographiques et périodes cryptographiques approuvés; Utilisez des algorithmes cryptographiques, des tailles de clés cryptographiques et des périodes cryptographiques validées par le programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/), et spécifiés dans ITSP.40.111 Algorithmes cryptographiques. pour les informations non classifiées, protégées A et protégées B, ou des versions ultérieures (https://cyber.gc.ca/fr/guidance/cryptographic-algorithmsunclassified-protected-and-protected-b-informationitp40111); Assurez-vous que la cryptographie validée FIPS 140 est utilisée lorsque le cryptage est requis, et qu'elle est implémentée, configurée et utilisée dans un module cryptographique, validée par le programme de validation du module cryptographique (https://www.cse-cst.gc.ca/programme-de-validation-module-crypto-module), 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 attendus de la manière attendue; et Assurez-vous que tous les modules FIPS 140-2 utilisés possèdent une certification active, à jour et valide. Les produits conformes / validés FIPS 140 auront des numéros de certificat. 	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection Cryptographique.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ol style="list-style-type: none"> les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en oeuvre pour la protection de la fédération de l'identité. <p>Pour les sections de la Protection Cryptographique, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p> <p>Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.</p>



ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O15	Séparation des données	<p>Le fournisseur doit, pour les deux pays, mettre en place des contrôles pour assurer l'isolation appropriée des ressources, de sorte que les actifs informationnels ne soient pas mélangés avec les données d'autres locataires, qu'ils soient en cours d'utilisation, de stockage ou de transit, ainsi que dans tous les aspects des fonctionnalités du service fournisseur et de l'infrastructure fournisseur et administration du système. Cela inclut la mise en oeuvre de contrôles d'accès et l'application de la séparation logique ou physique appropriée pour prendre en charge:</p> <ul style="list-style-type: none">a. la séparation entre l'administration interne du fournisseur et les ressources utilisées par ses clients; etb. La séparation des ressources du client dans des environnements multi-locataires afin d'empêcher qu'un consommateur malveillant ou compromis affecte le service ou les données d'un autre.	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences.</p>



APPENDICE N – RENSEIGNEMENTS SUR LE FOURNISSEUR ET AUTORISATION

(voir ci-joint)



APPENDICE O – RENSEIGNEMENTS SUR LE FOURNISSEUR ET AUTORISATION

Nom et adresse du fournisseur

Statut juridique (constitué en personne morale, enregistré, etc.)

- Individuelle (propriétaire unique)
 Entreprise privée
 Coentreprise incorporée ou Entité corporative
 Autre (spécifier):

Numéro d'inscription aux fins de la TPS/TVH et numéro d'entreprise (Agence du revenu du Canada)

Nom et titre de la personne qui a l'autorisation de signer au nom du fournisseur

Nom en caractère d'imprimerie _____ Titre _____

Signature _____ Date _____

Point de contact central

Le fournisseur a désigné la personne suivante à titre de point de contact central pour toutes les questions portant sur la proposition de contrat, y compris la communication de tous les renseignements demandés :

Nom et titre _____

Téléphone _____ Télécopieur _____

Courriel _____

Chaque proposition doit être accompagnée d'une copie de la présente page dûment remplie et signée.