SERVICES PARTAGÉS CANADA

Sollicitation par défis (SPD) – Préqualification

IaaS – PaaS Native

No de Sollicitation	CS-IAAS-2024	Date	19 Avril 2024
Bureau responsable	Services partagés Canada 400 rue Cooper, 6e étage Ottawa, Ontario K2P 2H8		
Autorité contractante (L'autorité contractante est la personne désignée dans le cadre de la sollicitation ou par une notification au soumissionnaire qui agit en tant que « contact » représentant Canada dans tous les aspects de cette sollicitation.)	Équipe des services infonuagiques Gestionnaire : Nadia Kelly Chef d'équipe : Khady Sy		
	Adresse courriel : PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca		
Préqualification Date et heure de clôture	13 mai 2024, 14 : 00 HAE		

Tables des matières

INTRODUCTION

Note au lecteur :

Suite à la publication de la sollicitation par défi initiale (SPD) sur AchatsCanada, le Canada a reçu des commentaires de la part des fournisseurs et les a pris en compte lors de la mise à jour de la SPD.

Cette SPD vise à préqualifier les soumissionnaires.

Seule la procédure de préqualification est détaillée dans ce document.

Sommaire exécutif

Comme décrit au point 1.4 – Étapes de la sollicitation par défis, l'étape 1 est la première étape et elle comprend la publication de l'avis de projet de marché et des documents provisoires pour démarrer officiellement la sollicitation par défis. Les principaux objectifs sont d'informer l'industrie des exigences et de la stratégie d'approvisionnement, tout en sollicitant des commentaires et des réactions afin de les peaufiner.

Webinaire d'information

Les soumissionnaires sont invités à participer à un webinaire d'information sur la Sollicitation par défis pour la préqualification. Les soumissionnaires doivent s'inscrire en communiquant avec l'autorité contractante avant la date du webinaire.

Le webinaire d'information se tiendra aux dates et heures suivantes :

a) Le webinaire en français aura lieu le 24 avril 2024 à 10 : 00 HAE

b) Le webinaire en anglais aura lieu le 24 avril 2024 à 13 : 00 HAE

Conflit d'intérêts et avantage indu

Conformément aux Instructions uniformisées 2003, une soumission peut être rejetée en raison d'un conflit d'intérêts réel ou apparent ou d'un avantage indu. À cet égard, le Canada informe qu'il a fait appel aux services de plusieurs consultants/entrepreneurs du secteur privé dans l'élaboration des stratégies et des documents liés à ce processus d'approvisionnement, notamment les suivants :

- Adirondack (Sous-traitant : CloudWise Consulting Ltd.)
- Agilipro (9421-5340 Québec inc.)
- Lightning Tree (Sous-traitants : Spring2Innovation to Gestion UniVision Management Inc.)
- Maplestream Inc., Cofomo Inc. IN JOINT VENTURE (Sous-traitant : Partners in Procurement)
- TekSystems (Sous-traitant : Robert Hilborn Consulting Inc.)
- The Lansdowne Consulting Group Inc.

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Exigences

La présente sollicitation par défis vise à établir un ou des contrats à autorisations de tâches pour la prestation de services d'infrastructure en tant que service (IaaS)[1]* et de plateforme en tant que service (PaaS*) native au gouvernement du Canada.

Consulter l'annexe B – Énoncé des défis pour avoir une description détaillée de l'exigence.

1.2 Structure de la sollicitation par défis

La sollicitation est divisée en six parties, plus les pièces jointes et les annexes.

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 sollicitation par défis.

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 ; décris 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 – comprends les attestations et les renseignements supplémentaires à fournir.

Partie 6 : Clauses du contrat subséquent ; contiens les clauses et les conditions qui s'appliqueront à tout contrat subséquent.

1.3 Processus de sollicitation

Contrairement à l'approvisionnement traditionnel, la sollicitation par défis repose sur le concept selon lequel le Canada peut mieux élaborer les mécanismes de l'approvisionnement s'il présente l'exigence comme un besoin (énoncé du ou des problèmes) et laisse à l'industrie la liberté de proposer des solutions novatrices qui répondent au besoin. Les sollicitations par défis sont accompagnées de détails décrivant ces activités et attentes, y compris, mais sans s'y limiter, la participation ou l'engagement de l'industrie et les méthodes d'évaluation. Les solutions prennent généralement la forme d'une « preuve de concept » ou d'une démonstration, et les évaluations permettent de déterminer dans quelle mesure elles répondent au besoin.

Tout au long de l'invitation à peaufiner (IàP), les soumissionnaires sont invités à fournir des commentaires sur l'énoncé du ou des problèmes en participant à des vidéoconférences, en répondant à des sondages et en prenant part à d'autres types d'activités organisées par le Canada, afin d'aider ce dernier à finaliser la sollicitation par

[1] *À défaut d'avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

défi. Acceptation de la Pièce jointe 2 – Règles d'engagement sera requise pour participer à l'IàP.

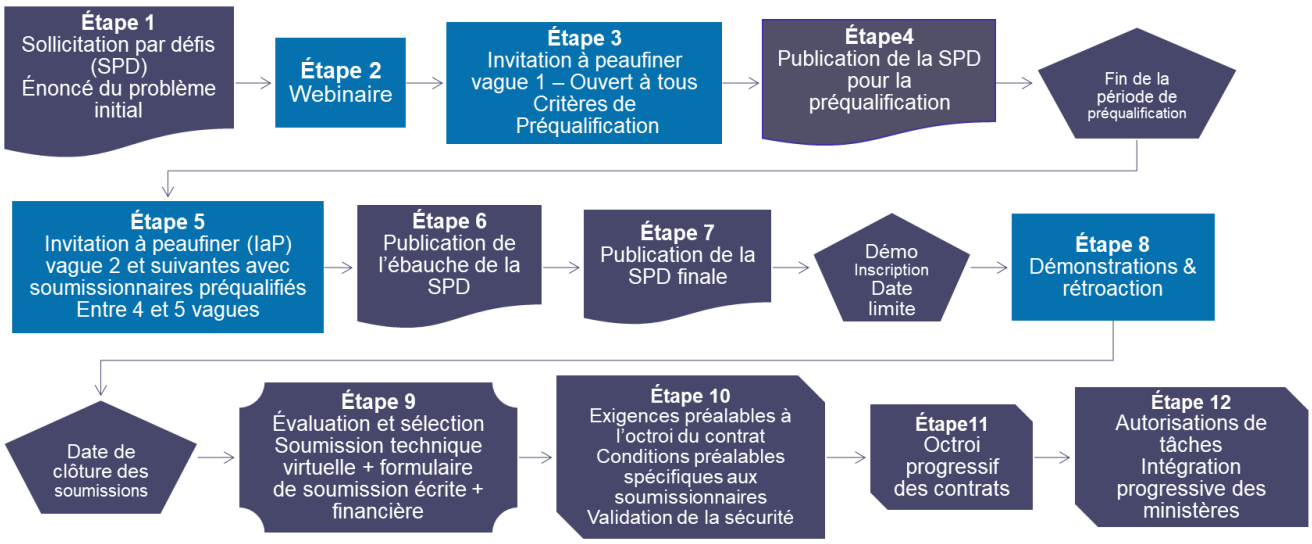
Document de sollicitation évolutif

Le document de sollicitation évoluera au cours de la période de sollicitation. Voici les différentes formes qu'il prendra ci-dessous :

1. Sollicitation par défis (SPD) – Initiale
2. SPD pour la présélection (DOCUMENT ACTUEL)
3. Ébauche de la SPD finale
4. SPD finale

1.4 Étapes de la sollicitation par défis

Tableau 1 – Sollicitation par défis pour IaaS[2]* et PaaS* Native



Étape 1 : Sollicitation par défis – Initiale

L'Avis de projet de marché (APM) et la sollicitation par défis (SPD) initiale sont publiés sur www.achatscanada.canada.ca.

Étape 2 : Webinaire d'information

Les soumissionnaires sont invités à participer à un webinaire d'information. Au cours du Webinaire d'information, le Canada donnera un aperçu de l'approche, expliquera les

[2] *À défaut d'avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

« vagues » de l'Invitation à peaufiner (IàP) et recueillera les commentaires de l'industrie sur le processus de sollicitation et le cadre d'évaluation proposée.

Étape 3 : Invitation à peaufiner – Vague 1

Au cours de la première vague, les soumissionnaires sont invités à donner leur avis sur l'énoncé du problème et les critères de présélection et à communiquer leurs points de vue en participant à diverses activités interactives (vidéoconférences, interactions de groupe, sondages et présentations des soumissionnaires) animées par le Canada, en présence de tous les soumissionnaires. Les commentaires et les présentations des soumissionnaires ne seront pas comptabilisés ni pris en compte pour le processus d'évaluation de la sollicitation ; les questions et les réponses de l'IàP seront documentées et fournies à tous les soumissionnaires. L'objectif de IàP (vague 1) est d'aider le Canada à finaliser la sollicitation par défis pour la présélection.

Étape 4. Publication de la sollicitation par défis pour la préqualification

Sur la base des conclusions de l'IàP – Vague 1, le Canada invitera les soumissionnaires à se qualifier. L'objectif de la phase de préqualification est de constituer un bassin de soumissionnaires qualifiés qui ont démontré leur capacité à résoudre l'énoncé du ou des problèmes et sont considérés comme étant les plus qualifiés conformément aux exigences de cette sollicitation.

Veuillez vous référer à la section 3 – Instructions pour la préparation des propositions pour avoir des informations sur le processus de soumission.

Le Canada sélectionnera les cinq soumissionnaires les plus qualifiés pour la formation du bassin, conformément à la section 4.1 Procédures d'évaluation - Préqualification. Le Canada informera les soumissionnaires non sélectionnés pour former le bassin de leur exclusion de toute participation ultérieure à ce processus de sollicitation.

À partir de ce stade du processus, toutes les communications relatives à la sollicitation se feront entre le Canada et les soumissionnaires préqualifiés. Il n'y aura plus d'autres publications sur AchatsCanada jusqu'à l'octroi du ou des contrats.

Étape 5 : Invitation à peaufiner (IàP) – Vague 2 et vagues suivantes avec les fournisseurs préqualifiés

Pendant la période de la vague 2 et des vagues suivantes, les soumissionnaires préqualifiés sont invités à fournir des commentaires supplémentaires sur l'énoncé du ou des problèmes et à communiquer leurs points de vue en participant à des activités interactives supplémentaires organisées par le Canada (en présence de tous les soumissionnaires préqualifiés ou « en tête-à-tête »). Les commentaires et les présentations des soumissionnaires ne seront pas notés ni pris en compte dans le processus d'évaluation de la sollicitation ; les questions et les réponses de l'IàP seront documentées et fournies à tous les soumissionnaires. L'objectif de l'IàP (vague 2 et vagues suivantes) est d'aider le Canada à finaliser la sollicitation par défis. L'ordre et le contenu des vagues peuvent être modifiés selon les besoins, et une ou plusieurs vagues peuvent se dérouler simultanément.

Invitation à peaufiner – Description des vagues

Vague 1	Critères de présélection, énoncé du problème, défis et exigences minimales viables (EMV) (complété)
Vague 2	Sécurité et protection de la vie privée
Vague 3	Énoncé des défis
Vague 4	Conditions générales, capacité des soumissionnaires à satisfaire aux exigences écologiques, aux exigences en matière d'accessibilité et aux exigences de la *Loi sur les langues officielles (LLO)*
Vague 5	Procédure de répartition des tâches
Vague 6	Suivi des prix et évaluation financière
Vague 7	Cadre d'évaluation des soumissions
Vague 8	Considérations socio-économiques
Vague 9	Soutien aux petits ministères et autres niveaux de gouvernement (ONG)

Au fur et à mesure de l'évolution de la sollicitation, des vagues d'IàP peuvent être ajoutées ou supprimées, au besoin.

Étape 6 : Publication de l'ébauche de la sollicitation par défis finale

À l'étape 6, en fonction des observations faites lors des activités de l'IàP, le Canada peaufinera et publiera une ébauche de la sollicitation par défis finale. Les soumissionnaires préqualifiés auront une dernière chance de partager leur rétroaction sur la sollicitation.

Vague 10	Ébauche finale de la SPD

Étape 7 : Publication de la sollicitation par défis finale

À l'étape 7, sur la base de la rétroaction reçue à l'étape 6, le Canada peaufinera et publiera la sollicitation par défis finale aux soumissionnaires préqualifiés.

Étape 8 : Démonstration et rétroaction

Au cours de l'étape 8, le Canada invitera les soumissionnaires préqualifiés inscrits à faire leur démonstration.

Les soumissionnaires préqualifiés auront jusqu'à la date d'inscription à la démonstration pour s'y inscrire. La démonstration est obligatoire pour pouvoir soumissionner.

Les démonstrations seront gérées conformément aux instructions de la partie 4.

Étape 9 : Évaluation et sélection

Au cours de l'étape 9, le Canada évaluera les soumissions.

Les soumissionnaires préqualifiés les mieux classés à l'issue des procédures d'évaluation et méthode de sélection (partie 4) seront avisés *(avis de sélection*) de l'intention du Canada d'octroyer plusieurs contrats.

Étape 10 : Exigences préalables à l'octroi du contrat

Au cours de l'étape préalable à l'octroi du contrat, les soumissionnaires dont la sélection a fait l'objet d'un avis à l'étape 9 vont :

- Soumettre leur soumission technique écrite qui sera jointe au contrat.
  (Note aux soumissionnaires : Les soumissions techniques écrites des soumissionnaires ne doivent pas être fournies à la clôture de la sollicitation par défis.)
- Le cas échéant, finaliser la négociation des termes et conditions spécifiques des soumissionnaires qui seront inclus dans le contrat final en tant que dernier élément de l'ordre de priorité des documents.
- Validation de la cote de sécurité requise.
- Validation de la conformité avec les attestations.

Étape 11 : Octroi progressif des contrats

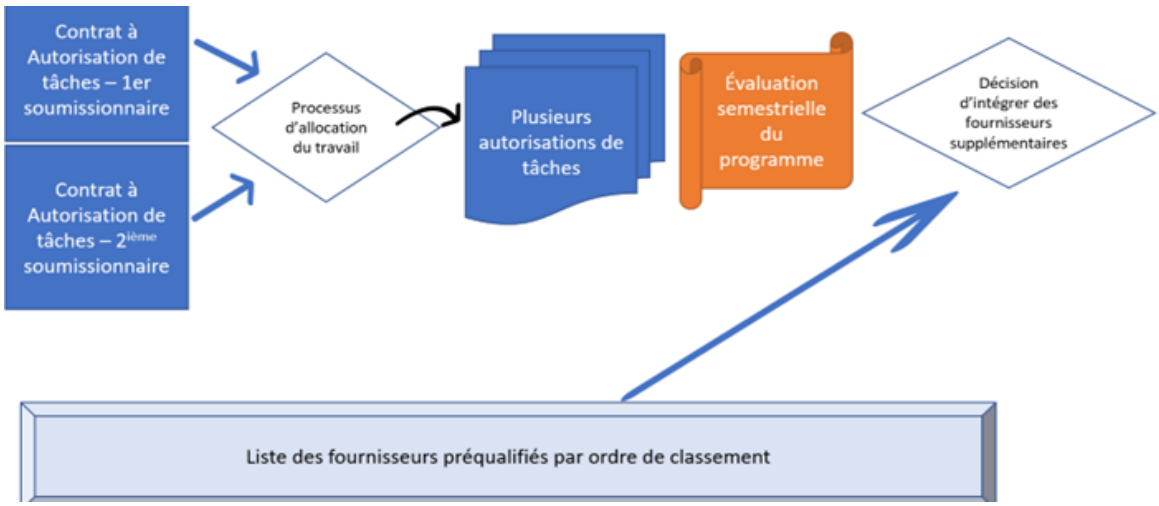
Le Canada prévoit d'attribuer plusieurs contrats d'autorisations de tâches.

Le Canada n'attendra pas que toutes les activités liées à l'étape préalable à l'octroi du contrat soient terminées pour commencer à attribuer les contrats. Dès qu'un des soumissionnaires sélectionnés aura rempli ses obligations et que le Canada aura terminé ses vérifications, le Canada pourra octroyer le contrat. Les contrats ne seront peut-être pas tous octroyés en même temps ; chacun d'entre eux sera octroyé lorsque l'un des soumissionnaires retenus satisfera à toutes les exigences préalables à l'octroi du contrat.

Étape 12 : Autorisation de tâches

Cette infographie est une représentation visuelle du processus d'autorisation de tâches de l'énoncé des défis.

Tableau 2 – Attribution des autorisations de tâches



La présente sollicitation aura les résultats suivants :

1) **Contrats :** Jusqu'à deux entrepreneurs seront invités à signer un contrat d'autorisations de tâches. Les signataires des contrats d'autorisations de tâches seront habilités à signer des autorisations de tâches conformément à la partie 6 – Clauses du contrat subséquent.

2) **Une liste d'entrepreneurs préqualifiés** qui répondent à toutes les exigences de la SPD finale, mais qui n'ont pas été sélectionnés parmi les deux soumissions les mieux classées et qui pourraient être intégrés dans l'écosystème d'approvisionnement au cours des années à venir. Deux fois par an, Services partagés Canada (SPC) évaluera la performance des fournisseurs, les besoins des ministères, l'évolution de la technologie ou tout autre élément et pourra décider d'intégrer un ou plusieurs entrepreneurs figurant sur la liste des entrepreneurs préqualifiés.

1.5 Contrat à autorisations de tâches

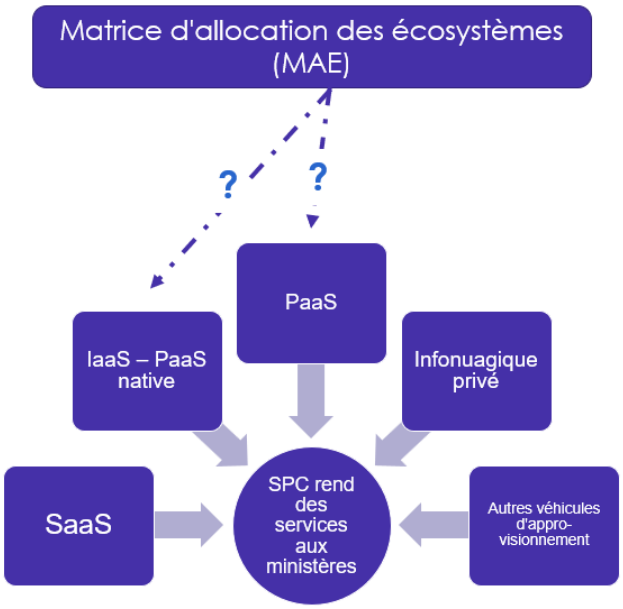
Le Canada a l'intention de structurer l'entente contractuelle sous la forme d'un contrat d'autorisation de tâches. Des autorisations de tâches (AT) individuelles seront émises dans le cadre de ce contrat pour les services infonuagiques. Un contrat d'autorisations de tâches est une méthode de prestation de services en vertu de laquelle tous les travaux ou une partie des travaux seront effectués « sur demande » dans des conditions prédéterminées, y compris un processus administratif comprenant des autorisations de tâches.

1.6 Écosystème d'approvisionnement (EA)

- SPC peut sélectionner un ou plusieurs mécanismes d'approvisionnement pour fournir des services aux ministères.
- La décision de sélectionner un ou plusieurs mécanismes d'approvisionnement (MA) sera fondée par une matrice d'allocation de l'écosystème (MAE), illustrée ci-dessous.
- SPC peut mettre en concurrence des services provenant de différents mécanismes d'approvisionnement (p. ex., concurrence du PaaS[3]* : concurrence des services IaaS* – PaaS* native et mécanisme d'approvisionnement PaaS*).
- La matrice d'allocation de l'écosystème (MAE) sera divulguée dans chaque sollicitation par défis menant à l'établissement des mécanismes d'approvisionnement.
- La MAE peut être révisée chaque année en consultation avec les entrepreneurs sélectionnés dans le cadre de l'écosystème d'approvisionnement.

[3] *À défaut d'avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

Tableau 3 – Écosystème des approvisionnements



(Note aux soumissionnaires ; le modèle d'écosystème d'approvisionnement est encore en discussion et peut évoluer)

PARTIE 2 – INSTRUCTIONS AUX SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

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

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

2.2 Instructions uniformisées

Les instructions uniformisées 2003 (2023-06-08) Biens ou services - besoins concurrentiels du Guide des CCUA est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante. Il est modifié comme suit :

a) Section 03 : Instructions, clauses et conditions uniformisées

Supprimer : « Conformément à la *Loi sur le ministère des Travaux publics et des Services gouvernementaux* (LC 1996, ch. 16) »

b) Section 04 : Définition du soumissionnaire

Supprimer : dans son intégralité

Insérer : « Soumissionnaire » désigne la personne ou l'entité (ou, dans le cas d'une coentreprise, les personnes ou entités) qui est l'initiateur du service de nuage public dans son intégralité soumettant une soumission pour exécuter un contrat de biens, de services ou les deux. Cela n'inclut pas la maison mère, les filiales ou autres affiliés du soumissionnaire, ni ses sous-traitants, ni ses revendeurs.

c) Section 05 : Présentation des soumissions, paragraphe 4

Supprimer : « Les soumissions seront valables pendant au moins 60 jours à compter de la date de clôture de la demande de soumissions, à moins d'avis contraire dans la demande de soumissions. »

Insérer : « Les soumissions seront valables pendant au moins 180 jours à compter de la date de clôture de la sollicitation, à moins d'avis contraire dans la sollicitation. »

d) Section 08 : Transmission par télécopieur ou par le service Connexion de la Société canadienne des postes (SCP) :

Supprimer dans son intégralité.

e) Section 09 : Dédouanement :

Supprimer dans son intégralité.

f) Section 13 : Communications en période de soumission :

Supprimer : « Afin d'assurer l'intégrité du processus d'appel à la concurrence, toutes les demandes de renseignements, et autres communications ayant trait à la demande de soumissions doivent être adressées uniquement à l'autorité contractante dont le nom est indiqué dans la demande de soumissions. Le défaut de se conformer à cette exigence pourrait avoir pour conséquence que la soumission soit déclarée non recevable ».

Insérer : « Afin d'assurer l'intégrité du processus de sollicitation, toutes les demandes de renseignements concernant cette sollicitation doivent être adressées uniquement à l'autorité contractante identifiée dans la sollicitation.

L'intégrité du processus de sollicitation ne peut être garantie lorsque les soumissionnaires cherchent à soulever des questions avec d'autres représentants du ministère, ce qui pourrait avoir une incidence sur le résultat de la sollicitation en cours. Par conséquent, les soumissionnaires ne doivent pas s'adresser un représentant ministériel autre que l'autorité contractante pour soulever des questions au sujet de cette sollicitation. Cela permettra de s'assurer que les questions seront soulevées et traitées par écrit, puis diffusées à tous les soumissionnaires.

Bien que les fonctionnaires (qui peuvent ou non être impliqués dans la présente demande de sollicitations) puissent participer à des échanges dans d'autres forums, tels que les médias sociaux, les soumissionnaires qui se fient sur des renseignements "trouvés" le font à leurs propres risques.

La non-conformité à la Section 13 : *Communications en période de soumission* pourrait avoir pour conséquence que la soumission soit déclarée non recevable. »

2.3 Conditions générales de la sollicitation par défis

Conditions générales de Services partagés Canada (SPC)

L'acceptation par les soumissionnaires des CLAUSES DU CONTRAT SUBSÉQUENT (partie 6) de SPC, y compris l'annexe A – Conditions générales des services infonuagiques, est une exigence obligatoire de la présente demande de sollicitation.

Aucune modification dans les CLAUSES DU CONTRAT SUBSÉQUENT (partie 6) incluses dans l'offre du soumissionnaire ne s'appliquera au contrat subséquent, même si l'offre fait partie du contrat subséquent.

Les soumissionnaires qui présentent une soumission contenant des énoncés qui laissent entendre que leur soumission est conditionnelle à une modification des présentes conditions contractuelles (y compris tous les documents incorporés au contrat par référence) ou contenant des conditions qui visent à remplacer les présentes conditions contractuelles seront considérées comme non recevables. Par conséquent, les soumissionnaires qui ont des préoccupations au sujet des termes et conditions du contrat doivent les soulever conformément à la clause « Demandes de renseignements – sollicitation par défis ».

Aucune condition alternative pour les services d'informatique en nuage proposés dans la soumission du soumissionnaire ni aucune condition dans la soumission du soumissionnaire en ce qui concerne les limites de responsabilité ni aucun terme et condition intégrée par référence dans la soumission du soumissionnaire ne s'appliqueront au contrat subséquent, même si la soumission peut faire partie du contrat subséquent.

Conditions supplémentaires du soumissionnaire relatives aux services infonuagiques

La procédure que doit suivre un soumissionnaire pour proposer des conditions supplémentaires relatives aux services infonuagiques est la suivante :

a) Le soumissionnaire peut, dans le cadre de l'appel de présélection, soumettre des conditions supplémentaires relatives aux services d'infonuagerie qui n'est pas abordée dans la PARTIE 6 – CLAUSES DU CONTRAT SUBSÉQUENT, y compris l'annexe A – Conditions générales des services infonuagiques, pour les services offerts par le soumissionnaire. Les conditions supplémentaires proposées ne doivent pas contredire les conditions incluses dans la PARTIE 6 – CLAUSES DU CONTRAT SUBSÉQUENT et à l'annexe A – Conditions générales des services infonuagiques, et doivent refléter les conditions identiques ou meilleures actuellement offertes aux clients commerciaux du soumissionnaire pour les services offerts.

b) Les soumissionnaires ne doivent pas présenter l'ensemble de leurs termes et conditions de services infonuagiques standards. Si le soumissionnaire présente l'intégralité de ses termes et conditions standards, le Canada exigera qu'il les retire et qu'il soumette seulement celles qui ne sont pas déjà abordées dans les clauses du contrat subséquent et que le soumissionnaire aimerait que le Canada prenne en considération.

c) Si le soumissionnaire est l'un des soumissionnaires les mieux classés invités à signer un contrat d'autorisation de tâches, le Canada déterminera **si les conditions supplémentaires relatives aux services infonuagiques du soumissionnaire sont acceptables**.

d) **Si les conditions supplémentaires relatives aux services infonuagiques du soumissionnaire sont acceptables**, ces conditions supplémentaires seront incluses en tant qu'annexe à tout contrat d'autorisation de tâches subséquent, en tant que dernier élément de l'article intitulé « **Priorité des documents** »

e) Si le Canada détermine que l'une des clauses de services infonuagiques proposées est inacceptable pour le Canada, il en avisera le soumissionnaire par écrit et lui donnera l'occasion de la retirer de sa soumission ou de proposer un autre libellé pour examen par le Canada. Le Canada peut fixer un délai pour la réponse du soumissionnaire.

f) À moins que les clauses supplémentaires relatives aux services infonuagiques proposés par le soumissionnaire soient incluses dans une annexe distincte du contrat subséquent, elles ne seront pas considérées comme faisant partie du contrat subséquent (même si elles font partie de la soumission qui est incorporée par référence dans le contrat subséquent). Le fait que certaines conditions supplémentaires aient été incluses dans la soumission ne signifie pas que ces conditions s'appliqueront à tout contrat subséquent, que le Canada s'y soit opposé ou non au titre des procédures décrites ci-dessus.

2.4 Demandes de renseignements – Sollicitation

Les questions et les commentaires au sujet de la présente sollicitation peuvent être présentés conformément à la section 13 *Communications en période de soumission* des instructions uniformisées 2003 (2023-06-08) du Guide des CCUA – biens ou services – besoins concurrentiels. Il y aura des périodes de questions, comme suit.

Période de questions – préqualification :

Toutes les demandes de renseignements doivent être soumises par écrit à l'autorité contractante au plus tard 5 jours civils avant la date de clôture de la préqualification. Les demandes de renseignements reçues qui ne satisfont pas à cette condition pourraient ne pas recevoir de réponse avant la date de clôture de la préqualification. Les demandes reçues après la date de clôture ne recevront pas de réponse.

Les soumissionnaires doivent faire référence aussi précisément que possible au numéro de l'élément de la sollicitation auquel se rapporte leur demande de renseignements. Ils doivent veiller à expliquer chaque question en donnant suffisamment de détails pour permettre au Canada de fournir une réponse précise. Les demandes de renseignements techniques de nature exclusive doivent être clairement mentionnées comme « exclusive » à chaque élément pertinent. Les éléments identifiés comme « exclusifs » seront traités comme tels, sauf dans les cas où le Canada considère que la demande de renseignements n'est pas de nature exclusive. Le Canada peut modifier la ou les questions ou peut demander aux soumissionnaires que la nature exclusive de la ou des questions soit éliminée, afin de pouvoir fournir la réponse à toutes les soumissionnaires. Les demandes de renseignements qui ne sont pas soumises dans une forme pouvant être communiquée à tous les soumissionnaires pourraient ne pas être répondues par le Canada.

2.5 Autorité contractante

L'autorité contractante est la personne désignée par ce titre dans la sollicitation, ou par avis aux soumissionnaires, pour agir à titre d'« autorité contractante » du Canada pour toutes les demandes de renseignements concernant le processus de sollicitation.

Nadia Kelly

Gestionnaire, Équipe des services infonuagiques

Services partagés Canada

400 rue Cooper, 6e étage

Ottawa, Ontario K2P 2H8

Adresse courriel : PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca

2.6 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur au Canada et la province de l'Ontario, et les relations entre les parties seront déterminées par ces lois.

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

2.7 Accords commerciaux

La présente sollicitation est assujettie aux dispositions des accords commerciaux suivants :

- Accord de libre-échange canadien (ALEC)
- Accord de libre-échange Canada-Chili
- Accord de Partenariat transpacifique global et progressiste (PTPGP)
- Accord de libre-échange Canada-Colombie
- Canada et l'Union européenne Accord économique et commercial global (AECG)
- Accord de libre-échange Canada-Honduras
- Accord de libre-échange Canada – Corée
- Accord de libre-échange entre le Canada et le Panama
- Accord de libre-échange Canada-Ukraine
- Accord de continuité commerciale Canada–Royaume-Uni (ACC Canada–Royaume-Uni) – Accord de continuité commerciale
- Accord sur les marchés public de l'Organisation mondiale du commerce (OMC-AMP)

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES PROPOSITIONS

3.1 Soumission des documents de préqualification écrits par les soumissionnaires

Avant la date et à l'heure de clôture de la préqualification indiquées sur la page couverture de la demande de la sollicitation par défis, les soumissionnaires doivent soumettre :

a) le Document de soumission 1 – Formulaire de soumission de préqualification, qui comprend ce qui suit :

   i) Attestations incluant l'acceptation des règles d'engagement (pièce jointe 2) ;

   ii) Soumission de préqualification qui justifie les critères d'évaluation détaillés dans le document de Pièce jointe 1 - Grille d'évaluation de préqualification.

   Les soumissionnaires sont invités à télécharger et enregistrer le Formulaire de soumission de préqualification. Il est important d'utiliser Adobe Reader pour ouvrir le formulaire, car le fait de l'ouvrir directement via un navigateur internet ou avec un autre lecteur PDF pourrait entraîner des problèmes de compatibilité ou des erreurs.

b) Conditions supplémentaires du soumissionnaire relatives aux services d'infonuagerie, le cas échéant.

3.2 Processus de vérification de conformité à la soumission *(OPTIONNEL)*

a) **Les soumissionnaires sont invités à soumettre une présoumission** : Le Canada invite les soumissionnaires à soumettre ce qui suit :

   i) Document de soumission 1 - Formulaire de soumission de préqualification - réponses provisoires aux exigences obligatoires.

   Ceci est appelé une « Pré-soumission ». La soumission d'une présoumission par n'importe quel soumissionnaire est facultative et ne constitue pas une condition préalable à la présentation d'une offre à la date de clôture. Le Canada ne retournera pas les présoumissions aux soumissionnaires, mais les traitera de la même manière qu'il traite les offres, conformément aux Instructions générales 2003.

b) **Comment soumettre une présoumission :** un soumissionnaire peut soumettre une présoumission

   par courriel à l'autorité contractante en écrivant à l'adresse suivante PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca. Lorsqu'une présoumission est reçue par courriel, l'autorité contractante enverra un accusé de réception par courriel au soumissionnaire. Si le soumissionnaire ne reçoit pas d'accusé de réception par courriel, il est encouragé à faire un suivi par téléphone auprès de l'autorité contractante ; ou

c) **une soumission préalable ne sera examinée que si elle est soumise avant la date limite de dépôt des soumissions préalables** : Le Canada examinera uniquement les soumissions préalables soumises au plus tard à 23h59 [insérer la date] (la **« date limite**

de soumission des soumissions préalables »). Le Canada examinera une seule soumission préalable de chaque soumissionnaire (c'est-à-dire qu'après réception des commentaires, le soumissionnaire ne peut pas soumettre une nouvelle version de sa soumission préalable pour examen).

d) **Le Canada fournira des commentaires sur les soumissions préalables** : l'autorité contractante fournira des commentaires confidentiels, appelés Avis d'évaluation préliminaire (AEP), à chaque soumissionnaire ayant soumis une soumission préalable avant la date limite de soumission des soumissions préalables. Le Canada fournira normalement ces commentaires par courrier électronique et le soumissionnaire est réputé avoir reçu les commentaires du Canada au moment de leur envoi par le Canada. Le Canada n'est pas responsable des retards techniques dans la réception des commentaires par le soumissionnaire.

e) **Nature des commentaires du Canada en cas d'absence de déficiences identifiées** : Si le Canada ne note aucune déficience lors de son examen d'une soumission préalable, le Canada fournira au soumissionnaire concerné une réponse « nulle ».

f) **Nature des commentaires du Canada en cas de déficiences identifiées** : Si le Canada note des déficiences lors de son examen d'une soumission préalable, le Canada fournira des commentaires écrits au soumissionnaire indiquant les exigences obligatoires que le Canada a relevées :

i) n'ont pas du tout été abordés.

ii) n'ont pas suffisamment traités ; et

iii) sont traités de telle manière que la présoumission serait déclarée non conforme si elle était soumise à la date de clôture.

Bien que le Canada précise la raison pour laquelle la présoumission est insuffisante, le Canada n'indiquera pas au soumissionnaire comment remédier à la lacune.

Une fois que le Canada a indiqué qu'une exigence obligatoire spécifique n'a pas été satisfaite, il n'est pas nécessaire de détailler chaque manière dont le soumissionnaire a échoué à satisfaire à l'exigence obligatoire. Le Canada ne répondra pas non plus aux questions concernant les commentaires. Si le Canada détermine qu'une présoumission est sensiblement insuffisante (c'est-à-dire qu'il y a plus de [5] lacunes identifiées), le Canada se réserve le droit de ne pas effectuer un examen complet, auquel cas le Canada ne signalera au soumissionnaire que les lacunes notées par le Canada avant la cessation de son examen. Lorsqu'il répond aux commentaires du Canada, le soumissionnaire doit veiller à ce que les éléments de la soumission restent cohérents après toute modification apportée.

g) **Délai pour fournir des commentaires** : Le délai pour que le Canada fournisse des commentaires dépendra du nombre de présoumissions reçues et de leur qualité. Le Canada ne s'engage pas à fournir ses commentaires dans un délai précis. Si le Canada n'a pas fourni de commentaires concernant les présoumissions au moins 5 jours civils avant la date de clôture prévue, la date de clôture sera reportée de manière à ce que tous les soumissionnaires disposent de 5 jours civils complets (le jour de réception des

commentaires n'est pas compté) pour finaliser leurs soumissions avant la date de clôture. Par exemple, le Canada envoie les commentaires aux soumissionnaires le lundi à 10h. En supposant qu'il n'y ait pas de jours fériés pendant cette période, le soumissionnaire disposera de mardi, mercredi, jeudi, vendredi et le lundi suivant pour peaufiner sa soumission. La date de clôture ne sera pas antérieure au mardi suivant.

h) **Soumissionnaire seul responsable de la soumission d'une offre conforme à la clôture de la présoumission de préqualification** : Même si le Canada fournit des commentaires concernant une présoumission, le soumissionnaire est seul responsable de s'assurer que son offre soumise à la date de clôture est précise, cohérente, complète et entièrement conforme. Le Canada ne garantit pas qu'il identifiera chaque lacune lors de son examen de la présoumission. En soumettant une présoumission, le soumissionnaire accepte que l'examen du Canada ne soit qu'une étape préliminaire et que le Canada ne soit en aucun cas responsable de ne pas identifier d'omission, de lacune ou de non-conformité lors de son examen de la pré soumission.

3.3 Transmission électronique des soumissions

Tous les soumissionnaires doivent transmettre leur soumission par courriel à PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca avant la date de clôture de la sollicitation par défis de préqualification.

a) Les soumissionnaires qui ont l'intention de soumettre une soumission sont encouragés à envoyer une notification par courriel à l'autorité contractante indiquant leur intention de soumettre en envoyant un courriel à PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca.

b) **Taille des fichiers par courriel** : Les soumissionnaires doivent s'assurer de soumettre leur soumission en plusieurs courriels si un seul courriel, y compris les pièces jointes, dépasse 10 Mo. Les courriels doivent être reçus à l'adresse courriel indiquée ci-dessus, avant la date de clôture de la préqualification, afin d'être prise en compte dans la soumission.

c) **Objet du courriel** : Les soumissionnaires sont priés d'inclure le numéro de la demande de sollicitation, tel qu'identifié sur la page de couverture de ce document, dans la ligne « objet » de chaque courriel faisant partie de leur soumission.

d) **Soumission de l'offre :** Les soumissionnaires doivent envoyer leur soumission par courriel en tant que pièce jointe à l'adresse courriel suivante PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca avant la date de clôture de la préqualification indiquée sur la page de couverture. Il est de la responsabilité des soumissionnaires de s'assurer que les soumissions par courriel soient reçues par SPC. SPC décline toute responsabilité concernant les soumissions qui n'ont pu être distribuées.

e) **Responsabilité des problèmes techniques** : En présentant une soumission, le soumissionnaire confirme qu'il convient que le Canada n'est pas responsable de ce qui suit :

i) les problèmes techniques vécus par le soumissionnaire pendant la présentation de sa soumission ou des pièces jointes qui sont rejetées ou mises en quarantaine parce qu'elles contiennent des maliciels ou d'autres codes qui sont filtrés par SPC pour des raisons de sécurité ;

ii) les problèmes techniques qui empêchent SPC d'ouvrir les pièces jointes. Par exemple, si une pièce jointe est corrompue ou ne peut être ouverte ou lue, elle sera évaluée en conséquence sans cette partie de la soumission. Les soumissionnaires ne pourront pas soumettre des pièces jointes de rechange pour remplacer celles qui sont corrompues ou vides ou qui ont été soumises dans un format n'ayant pas été approuvé.

3.4 Éligibilité – soumissionnaires préqualifiés

Seuls les soumissionnaires qualifiés à l'étape 4 - Préqualification et qui restent qualifiée à la date et à l'heure de clôture finale des soumissions seront éligible pour soumettre une soumission à l'étape finale de la SPD. Le Canada se réserve le droit de réévaluer tout aspect de la qualification de tout soumissionnaire à tout moment pendant le processus de sollicitation.

3.5 Présentation d'une seule soumission

Chaque répondant qualifié à l'issue de la phase d'invitation à se qualifier de ce processus d'approvisionnement est considéré comme un soumissionnaire. Il est interdit à tout soumissionnaire de présenter plus d'une soumission en réponse à la présente demande de soumissions. Si un soumissionnaire présente plus d'une soumission, le Canada lui demandera de retirer toutes ses soumissions sauf une. Si le soumissionnaire ne le fait pas, le Canada peut choisir à sa discrétion la soumission à évaluer.

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

Les soumissions seront évaluées en fonction de toutes les exigences de la sollicitation, ainsi que des critères d'évaluation techniques et financiers.

Le processus d'évaluation comporte plusieurs étapes, décrites dans les présentes. Même si l'évaluation et la sélection se divisent en étapes, le Canada pourra passer à une étape ultérieure du processus sans que cela signifie que le soumissionnaire a réussi toutes les étapes antérieures. Le Canada peut mener les étapes de l'évaluation en parallèle.

Une équipe d'évaluation constituée de représentants du Canada évaluera les soumissions. Les membres de l'équipe d'évaluation ne participeront pas nécessairement tous à l'ensemble des éléments de l'évaluation.

4.1 Procédures d'évaluation – Préqualification (étape 4 – ÉTAPE ACTUELLE)

Les renseignements présentés dans le Document d'appel d'offres 1 – Formulaire de présélection seront évalués conformément à Pièce jointe 1 – Grilles d'évaluation.

4.1.1 Base de sélection de la préqualification

a) Pour être déclarée recevable pour la préqualification, une soumission doit satisfaire à tous les critères obligatoires de la partie A de la grille d'évaluation de préqualification ;

b) Les soumissions qui ne satisfont pas à tous les critères obligatoires seront exclues de la suite de la procédure de sollicitation.

4.1.2 Sélection des soumissionnaires préqualifiés

c) Conformément à 4.1.1 Base de sélection pour la préqualification, le Canada sélectionnera les 5 soumissionnaires les mieux classés pour la formation d'un bassin.

d) S'il y a moins de 5 soumissionnaires qualifiés, tous seront sélectionnés pour la formation du bassin (étape 4). Le score obtenu conformément à l'annexe 1 - Grille d'évaluation de la préqualification sera prise en compte dans le cadre du processus de sélection finale (étape 9) pour la SPD finale.

e) Si plusieurs soumissionnaires obtiennent le même rang en raison de scores identiques, alors les points obtenus pour le critère noté C4 de la grille d'évaluation de la préqualification seront utilisés pour classer les soumissions ex aequo suivantes, du score le plus élevé au score le plus bas. En cas de deuxième égalité, le soumissionnaire ayant obtenu le plus grand nombre d'éléments classés de 1 à 9 sera classé premier.

4.2 Procédures d'évaluation – Sélection (étape 9)

Note aux soumissionnaires : Cette section sera affinée davantage après la préqualification. Le cadre d'évaluation finale de la SPF sera discuté avec les soumissionnaires préqualifiés et pourra être modifié.

Si, à l'issue de l'étape 4, il y a 5 soumissionnaires qualifiés ou moins, le Canada peut décider de supprimer l'étape 8 : Démonstration et rétroaction, et de procéder à la sélection en se basant sur la conformité aux exigences procédurales et une proposition de prix.

4.3 Nombre de contrats et liste permanente de fournisseurs qualifiés

4.3.1 **Contrats :** Les 2 ou 3 soumissions les mieux classés et répondant aux critères (score total) seront recommandés pour l'attribution du contrat, à condition que la deuxième soumission la mieux classée et répondant aux critères ne se situe pas dans la marge de (+/- 1%) par rapport à la première soumission la mieux classée et répondant aux critères. Si la deuxième soumission la mieux classée et répondant aux critères se situe dans la marge de (+/- 1%) par rapport à la première soumission la mieux classée et répondant aux critères, ces soumissions seront classées par ordre décroissant comme suit : Les points obtenus lors de l'évaluation de l'offre technique seront utilisés pour classer les offres suivantes qui sont à égalité de score, du score le plus élevé au score le plus bas.

4.3.2 **Liste permanente des fournisseurs qualifiés :**

Les soumissions répondant aux critères, mais non recommandées pour l'attribution du contrat seront placées sur une liste permanente de fournisseurs qualifiés, selon leur classement.

Pendant la durée du contrat, le Canada peut recommander un ou plusieurs fournisseurs qualifiés pour l'attribution du contrat.

4.4 Attribution du contrat

Les attributions de contrats sont assujetties aux processus d'approbation internes du Canada, incluant une exigence d'approbation du financement au montant de tout contrat proposé. Bien qu'un soumissionnaire puisse avoir été recommandé pour l'attribution d'un contrat, un contrat sera attribué uniquement si l'approbation interne est obtenue conformément aux politiques internes du Canada. En l'absence de l'approbation, aucun contrat ne sera attribué.

Le Canada n'attribuera les contrats qu'une fois qu'un accord final aura été conclu à propos **des conditions supplémentaires relatives aux services infonuagiques du soumissionnaire**, le cas échéant. Pour cette raison, les contrats ne peuvent pas être attribués en même temps.

4.5 Annonces aux médias

Le soumissionnaire s'engage à ne pas faire d'annonces dans les médias concernant l'attribution d'un contrat sans le consentement écrit de l'autorité contractante.

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

5.1 Exigences d’attestation

Note aux soumissionnaires : Cette section ne s’applique pas à la préqualification.

PARTIE 6 – CLAUSES DES CONTRATS SUBSÉQUENTS

Remarque à l'intention des soumissionnaires : les termes et conditions contractuelles sont destinées à servir de fondement à tout contrat découlant de la présente sollicitation par défis. Sauf indication contraire dans les termes et conditions contractuelles, l'acceptation par les soumissionnaires de l'ensemble des termes et conditions est obligatoire de la présente sollicitation.

Aucune modification des termes et conditions contractuelles figurant dans la soumission ne s'appliquera au contrat final, même si la soumission fait partie du contrat final.

Articles de convention

(Remarque à l'intention des soumissionnaires : ces articles de convention seront peaufinés pendant la ou les invitations à peaufiner [IàP] et seront finalisés avant la délivrance de la demande de sollicitation par défis finale.)

Série de contrats

L'entrepreneur reconnaît que ce contrat fait partie d'une série de deux *[Remarque à l'intention des soumissionnaires : ce nombre peut être revu à la baisse au besoin au moment de l'attribution]* contrats attribués à la suite de la sollicitation par défis lancée par Services partagés Canada le [insérer la date] sous le numéro [insérer le numéro]. Ces contrats sont inclus dans le mécanisme d'acquisition des services d'IaaS[4]* et de PaaS* native.

Écosystème des mécanismes d'approvisionnement

L'entrepreneur reconnaît que ce mécanisme d'approvisionnement pour les IaaS* et les PaaS* natives est l'un des nombreux mécanismes d'approvisionnement pour l'écosystème contractuel de l'hébergement.

L'entrepreneur reconnaît ce qui suit :

- SPC peut sélectionner un ou plusieurs mécanismes d'approvisionnement (MA) pour fournir des services aux ministères.
- La décision de sélectionner un ou plusieurs MA sera fondée sur la MAE.
- SPC peut lancer un concours entre des produits provenant de différents mécanismes d'approvisionnement (p. ex., concurrence des PaaS* : concurrence des services d'IaaS* et de PaaS* native et du mécanisme d'approvisionnement de la PaaS*).
- La MAE sera divulguée dans chacune des sollicitations menant à l'établissement des MA.
- La MAE peut être révisée chaque année en consultation avec les entrepreneurs qualifiés dans le cadre de la MA.

Évolution de l'écosystème

Pendant la durée du contrat, dans les cas où le contexte technologique rendra disponibles des services novateurs susceptibles d'aider le Canada à mieux résoudre le problème cerné dans

[4] *À défaut d'avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

l'énoncé de défis, l'entrepreneur mettra ces services à disposition sur son catalogue au prix public moins les rabais du gouvernement du Canada.

Dans les cas où l'amélioration serait apportée par une tierce partie (autre que l'entrepreneur), le Canada peut prendre l'une des mesures suivantes :

(1) inviter le fournisseur le mieux classé sur la liste permanente des fournisseurs qualifiés à signer un contrat d'autorisation de tâches et à être inclus dans le mécanisme d'acquisition des services d'IaaS[5]* et de PaaS* native ;

(2) lancer une nouvelle demande de soumissions pour qualifier de nouveaux entrepreneurs pouvant aider le Canada à résoudre ses problèmes et à mieux relever les défis auxquels il est confronté.

Environnement collaboratif

Bien que le Canada reconnaisse que les entrepreneurs ayant obtenu cette série de contrats sont en concurrence les uns avec les autres, l'entrepreneur convient de ce qui suit :

(1) à l'exception des divulgations exigées par la loi, il ne fera pas de déclarations dans les médias ou d'autres déclarations publiques concernant des services rendus ou des produits livrés dans le cadre de cette série de contrats par un autre entrepreneur sans l'accord préalable de l'autorité contractante ;

(2) il participera activement aux discussions de groupe organisées par le Canada, étant entendu qu'aucun entrepreneur n'est censé communiquer sa propriété intellectuelle, ses renseignements confidentiels ou ses renseignements confidentiels au cours de ces séances.

6.1 Exigences

6.1.1 ***[Nom du fournisseur de services infonuagiques]*** (« L'**entrepreneur** ») s'engage à fournir les services infonuagiques décrits dans l'**énoncé de défis** et à se tenir prêt à fournir aux clients les services décrits dans les autorisations de tâches individuelles délivrées par le Canada, conformément aux prix établis dans le présent contrat d'autorisation de tâches (« **CAT** ») ainsi que dans l'autorisation de tâches (« AT ») pertinente, qui seront les prix établis dans la liste de prix publiée par l'entrepreneur, moins les rabais consentis.

6.1.2 **Client :** Dans le cadre de ce CAT, Services partagés Canada (« **SPC** ») est à la fois l'autorité contractante (« **AC du CAT** ») et l'autorité technique. SPC utilisera ce CAT pour fournir des services aux « **utilisateurs finaux** », y compris SPC, les institutions gouvernementales pour qui ses services sont obligatoires à tout moment pendant la durée du CAT ou toute période de l'AT individuelle et les autres organismes pour lesquels les services de SPC sont facultatifs à tout moment pendant l'une ou l'autre période et qui choisissent d'utiliser ces services occasionnellement. SPC peut choisir d'utiliser ce CAT pour l'ensemble ou une partie de ses clients et peut utiliser d'autres moyens afin de fournir des services identiques ou similaires.

[5] *À défaut d'avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

6.1.3 **Réorganisation du client :** Le changement de nom, la restructuration, le réaménagement ou le remaniement du client n'aura aucune incidence sur l'obligation de l'entrepreneur en ce qui a trait à l'exécution des travaux (et ne donnera pas lieu non plus au paiement d'honoraires supplémentaires). La restructuration, le réaménagement et le remaniement du client comprennent la privatisation de tout client, sa fusion avec une autre entité ou sa dissolution, lorsque cette dissolution est suivie de la création d'une autre entité ou d'autres entités ayant des mandats similaires à ceux du client initial. Dans le cadre de toute forme de réorganisation, le Canada peut désigner un autre ministère ou organisme gouvernemental comme AC ou autorité technique, en fonction des nouveaux rôles et responsabilités liés à la réorganisation.

6.1.4 **Autres administrations :** Le Canada se réserve le droit d'autoriser d'autres administrations canadiennes à utiliser le contrat pour les exigences en matière de services infonuagiques.

6.1.5 **Termes définis :** Les mots et expressions utilisés dans le présent CAT sont définis à l'annexe E.

6.2 Autorisation de tâches (AT)

La totalité ou une partie des services infonuagiques prévus dans le contrat seront réalisés sur demande en utilisant le processus d'autorisation de tâches (PAT) qui sera défini ultérieurement.

6.3 Durée du contrat et période d'autorisation de tâches

6.3.1 La « **durée du contrat** » est la période entière pendant laquelle l'entrepreneur est tenu de fournir des services infonuagiques aux termes du contrat, qui commence à la date d'attribution du contrat et se termine lorsque le Canada cesse d'utiliser le contrat. Il s'agit de la période pendant laquelle le Canada peut délivrer des AT.

6.3.2 La « **période d'autorisation de tâches (AT)** » est la période entière pendant laquelle l'entrepreneur est tenu de fournir des services infonuagiques. Cela comprend :

a) La « **période initiale de l'AT** », qui commence à la date de délivrance de l'AT et se termine lorsque l'entrepreneur a fourni les services infonuagiques conformément aux exigences de l'AT ;

b) toute période pendant laquelle l'AT est prolongé par le Canada.

6.3.3 Option de prolongation de l'AT

L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée de l'AT aux mêmes conditions, sous réserve de la disponibilité des mêmes services infonuagiques, au moyen d'une modification de l'AT délivrée par l'autorité contractante. L'entrepreneur consent que, pendant la période prolongée de l'AT, il sera payé selon les conditions applicables énoncées dans la base de paiement.

6.4 Processus d'autorisation de tâches

6.4.1 Étant donné que plus d'un contrat a été attribué pour ce besoin, l'un des deux entrepreneurs sera invité à signer une AT conformément à la procédure de répartition des tâches (PRT) décrite à la section 6.5.

6.4.2 L'entrepreneur indiqué par la PRT recevra une demande d'exécution d'une tâche. S'il confirme par écrit qu'il n'est pas en mesure d'exécuter la tâche, la demande d'exécution d'une tâche sera alors transmise à l'entrepreneur classé deuxième. Si aucun entrepreneur ne peut exécuter la tâche, le Canada se réserve le droit de combler ce besoin par d'autres moyens. Un entrepreneur peut informer par écrit l'autorité technique et l'autorité contractante qu'il n'est pas en mesure d'exécuter des tâches supplémentaires en raison d'engagements antérieurs au titre d'une AT, et aucune demande d'exécution d'une tâche ne lui sera envoyée tant qu'il n'aura pas informé par écrit l'autorité technique et l'autorité contractante qu'il est disponible pour exécuter des tâches supplémentaires.

a) L'autorité technique fournira à l'entrepreneur une description de la tâche au moyen du formulaire d'AT figurant à l'annexe 1.

b) L'autorisation de tâches (AT) qui en découle contient les détails des activités à réaliser ou des services à rendre et une description des livrables. L'AT comprendra également la ou les bases applicables et les méthodes de paiement précisées dans le contrat.

c) L'entrepreneur ne doit pas commencer les travaux avant d'avoir reçu une AT autorisée par l'autorité contractante. L'entrepreneur reconnaît que toute tâche effectuée avant la réception de l'AT le sera à ses propres risques.

6.5 Procédure de répartition des tâches

(Remarque à l'intention des soumissionnaires : La procédure sera élaborée au cours de l'IàP.)

6.6 Émission d'autorisation de tâches multiples

6.6.1 L'entrepreneur reconnaît ce qui suit :

a) Plusieurs **autorisations de tâches** seront attribuées par le Canada pour des services infonuagiques.

b) Le CAT a été attribué suite à un processus concurrentiel.

c) Si le Canada respecte le processus d'attribution des autorisations de tâches décrit ci-dessous, l'entrepreneur n'a aucun droit contre le Canada en ce qui concerne la façon dont il administre les contrats avec les autres entrepreneurs. Par exemple, l'entrepreneur n'a pas le droit de déposer une plainte contre le Canada après que celui-ci a choisi d'accorder des prolongations à un entrepreneur ou choisi de ne pas exercer les droits ou les recours auxquels il pourrait avoir droit pour un autre contrat de cette série de contrats. Si une autorisation de tâches met en jeu des travaux fournis par plusieurs entrepreneurs, l'interaction entre ces entrepreneurs ou avec un entrepreneur tiers sera traitée dans l'autorisation de tâches.

6.6.2 Réponse aux autorisations de tâches : Bien que l'entrepreneur n'ait pas à répondre aux autorisations de tâches, celui-ci consent à participer activement à l'examen des demandes d'autorisation de tâches et à donner suite aux demandes comportant des tâches qu'il est en mesure de mener à bien.

6.7 Base de paiement

L'entrepreneur sera payé pour l'exigence précisée dans l'AT autorisée, conformément à la base de paiement.

La responsabilité du Canada à l'égard de l'entrepreneur au titre de l'AT autorisée ne doit pas dépasser la **limite de dépenses** qui y est précisée. Les taxes applicables sont en sus.

6.7.1 Pour les services infonuagiques publics commercialement disponibles fournis dans le cadre d'AT individuels, l'entrepreneur doit être payé aux prix fermes applicables aux services infonuagiques sélectionnés (p. ex. services sur demande, abonnement, prépayé, etc.) conformément au catalogue commercial de l'entrepreneur, moins tout rabais applicable du gouvernement du Canada.

a) Les frais des services infonuagiques ne doivent pas dépasser les prix publiés en ligne par l'entrepreneur pour les services infonuagiques publics commercialement disponibles. L'entrepreneur doit faire bénéficier le Canada de remises tarifaires échelonnées et de rabais de volume, le cas échéant.

i. En cas de diminution du prix d'un service infonuagique déjà fourni, l'entrepreneur doit appliquer cette diminution de prix.

ii. Le nouveau prix réduit des services infonuagiques doit être appliqué automatiquement au prochain paiement dû par le client et sera maintenu pour la durée restante de l'AT, à moins qu'un nouveau prix réduit ne devienne disponible.

6.7.2 Le Canada doit indiquer les conditions de paiement dans l'AT.

6.7.3 **Crédits de service :** Si le service infonuagique n'atteint pas le niveau de disponibilité minimal au cours d'un mois donné, le Canada aura le droit de réclamer des crédits conformément à l'entente de niveau de service et au processus de crédit de service publié par l'entrepreneur et disponible sur le contrat.

6.7.4 **Devise :** Tous les services infonuagiques natifs disponibles sur le marché doivent être payés en dollars canadiens. Dans les cas où les prix des services non natifs disponibles en ligne dans le contrat sont exprimés en dollars américains, le fournisseur de services infonuagiques doit prévoir une fonctionnalité permettant de convertir les prix en dollars canadiens. Le taux de conversion doit être aussi favorable que celui proposé aux clients commerciaux du fournisseur.

6.7.5 **Refus du renouvellement automatique :** Par les présentes, le Canada informe l'entrepreneur que, sauf indication contraire dans une AT, il refuse tout renouvellement automatique des services infonuagiques disponibles sur le marché.

6.8 Modes de paiement

6.8.1 **Mode de paiement pour les services sur demande :** Le Canada paiera en arrérages pour les services infonuagiques qu'il demande, conformément à l'AT,

services ayant été demandés et reçus par le Canada, taxes applicables en sus. Le Canada ne paiera pas l'entrepreneur plus d'une fois par mois, conformément aux clauses prévues à la section Base de paiement. L'entrepreneur doit soumettre une facture pour chaque AT active sur laquelle figurent tous les détails de l'utilisation à l'appui des frais demandés dans la facture.

6.8.2 **Mode de paiement pour les services fondés sur l'abonnement :** Le Canada paiera à l'avance pour les services infonuagiques par abonnement qu'il demande, conformément à l'AT, les taxes applicables en sus. Le Canada fera un paiement anticipé à l'entrepreneur pour les services par abonnement (à la fois mensuellement et annuellement) dans les 30 jours suivant la réception d'une facture complète (et tout document à l'appui requis), ou dans les 30 jours suivant toute date précisée dans l'AT pour le versement du paiement anticipé, la date la plus tardive étant retenue.

a) Si le Canada conteste une facture pour une raison ou une autre, il paiera à l'entrepreneur la partie non contestée de la facture, à la condition que les articles non contestés soient indiqués séparément sur la facture et que leur paiement soit exigible. Dans le cas de factures contestées, la facture ne sera considérée comme ayant été reçue que pour le calcul des « intérêts à facturer sur les comptes en souffrance » une fois que le différend aura été résolu.

b) L'entrepreneur reconnaît qu'il s'agit d'un paiement anticipé et reconnaît que ce dernier n'empêche pas le Canada d'exercer un recours à l'égard de ce paiement ou de tout service infonuagique, si ce service n'a pas été fourni conformément à l'AT.

6.8.3 **Mode de paiement pour une AT prépayé avec un prix maximum :** Le Canada paiera à l'avance un montant forfaitaire duquel l'entrepreneur déduira, par versements mensuels par arrérages, le coût des services infonuagiques utilisés, taxes applicables en sus.

a) La durée du paiement anticipé sera d'une période de service maximale d'un (1) an.

b) Lorsque les modalités du paiement anticipé sont un paiement périodique sur une période maximale d'un (1) an, le Canada indiquera dans l'AT la période visée par les paiements mensuels, trimestriels ou semi-annuels.

c) Les paiements en arrérages seront effectués sur une base mensuelle ou trimestrielle.

6.8.4 Pour chaque AT validement émis au titre du contrat qui contient un prix maximum :

a) Le Canada ne paiera pas l'entrepreneur plus d'une fois par mois, conformément aux clauses prévues à la section Base de paiement.

b) L'entrepreneur doit soumettre une facture pour chaque AT active qui montre tous les détails de l'utilisation et/ou de l'abonnement/du paiement anticipé à l'appui des frais demandés dans la facture.

c) L'entrepreneur peut soumettre une ou plusieurs factures supplémentaires pour l'utilisation qui dépasse le prix payé d'avance, à condition qu'il rende des outils accessibles aux clients pour la surveillance de l'utilisation et qu'il

permette à ceux-ci d'établir des seuils et des alertes pour l'utilisation des services infonuagiques.

d) Lorsque les services sont acceptés ou résiliés en dehors du cycle de facturation régulier (p. ex. cycle mensuel), l'entrepreneur doit facturer les services conformément à son processus publié disponible sur le marché.

6.9 Divulgation des renseignements liés aux émissions de gaz à effet de serre et établissement des cibles de réduction.

Le Canada s'est engagé à atteindre l'objectif de zéro émission nette de gaz à effet de serre (GES) d'ici 2050 dans le but de positionner le Canada pour réussir dans une économie verte et d'atténuer les impacts des changements climatiques. Par conséquent, la sollicitation finale peut inclure les exigences suivantes :

i) Critères d'évaluation ou autres instructions dans la demande d'offre ou les documents contractuels concernant la mesure et la divulgation des émissions de GES de votre entreprise ;

ii) Il est demandé ou exigé de participer à l'une des initiatives suivantes afin de soumettre une offre ou en cas d'attribution d'un contrat :

A) le Défi carboneutre du gouvernement du Canada ;

B) l'Objectif zéro des Nations unies ;

C) l'Initiative des cibles fondées sur des connaissances scientifiques ;

D) le projet de divulgation du carbone ;

E) l'Organisation internationale de normalisation ;

iii) Il est demandé de fournir d'autres preuves de l'engagement et des actions de votre entreprise en vue d'atteindre les objectifs de carboneutralité d'ici 2050.

6.10 Interaction avec des fonctionnaires

6.10.1 L'entrepreneur consent à ne pas envoyer à des fonctionnaires fédéraux des courriels non sollicités ou d'autres documents pour les inciter ou les encourager à lui confier plus de travaux, ou portant sur l'administration du présent contrat ou d'une AT qui s'y rattache, sauf avec le consentement écrit de l'autorité contractante.

6.10.2 L'entrepreneur ne doit pas discuter des produits de tiers, qui comprennent les autres entrepreneurs faisant partie de cette série de contrats, durant ses interactions avec les fonctionnaires, sauf si cela est prévu dans l'autorisation de tâches.

6.11 Responsables

a) Autorité contractante

L'autorité contractante dans le cadre du contrat est :

Nom : _____
Titre : _____
Téléphone : _____
Adresse électronique : _____

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

b) Responsable technique

Le responsable technique pour le contrat est (la personne sera identifiée après l'octroi du contrat) :

Nom : _____
Titre : _____
Organisation : _____
Téléphone : _____
Adresse électronique : _____

Le responsable technique [représente le ministère ou l'organisme pour lequel les travaux sont exécutés en vertu du contrat, et 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 responsable technique ; cependant, celui-ci ne peut pas autoriser les changements touchant la portée des travaux. De telles modifications ne peuvent être effectuées que par l'entremise d'une modification au contrat émise par l'autorité contractante.

c) **Représentant de l'entrepreneur -** (la personne sera identifiée l après l'octroi du contrat) :

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____
Téléphone : _____
Adresse électronique : _____

6.12 Code de conduite pour l'approvisionnement – contrat

L'entrepreneur accepte de se conformer au Code de conduite pour l'approvisionnement et de s'y soumettre pour la durée du contrat.

6.13 Priorité des documents pour ce contrat

En cas de divergence entre les libellés des documents figurant sur la liste suivante, le libellé du document figurant en premier sur la liste prévaut sur le libellé de tout document figurant plus loin sur la liste :

a) les articles du présent contrat d'autorisation de tâches (CAT)

b) Annexe A – Conditions générales des services infonuagiques, Obligations en matière de sécurité, Obligations en matière de protection des renseignements personnels

c) Clauses de l'AT qui en découle

d) Annexe B – Énoncé de défis

e) Annexe C – Liste de vérification des exigences relatives à la sécurité (LVERS)

f) Annexe D – Guide de classification de la LVERS

g) Annexe E – Définitions

h) Annexe F – Proposition de l'entrepreneur datée du ***[date]***, en réponse au processus de sollicitation nº xxxxxx, ne comprenant aucune disposition dans l'offre concernant les limitations de responsabilité, et ne comprenant aucune condition incorporée par référence (y compris par l'intermédiaire d'un lien Internet) dans la soumission.

i) Annexe G – Les conditions de services infonuagiques supplémentaires du soumissionnaire approuvées par le Canada

LISTE DES ANNEXES

Les annexes qui s'appliqueront au contrat résultant :

Annexe A	**Conditions générales des services infonuagiques**
	Appendice 1 - Obligations en matière de sécurité
	Appendice 2 - Obligations en matière de protection de la vie privée
Annexe B	**Énoncé des défis**
Annexe C	**Liste de vérification des exigences relatives à la sécurité (LVERS)**
Annexe D	**Guide de classification de la LVERS**
Annexe E	**Définitions**
Annexe F	**Les modalités de services infonuagiques supplémentaires du soumissionnaire approuvées par le Canada**

Documents de préqualification :

Document de soumission 1	**Formulaire de préqualification**
Pièce jointe 1	**Grilles d'évaluation de la préqualification**
Pièce jointe 2	**Règles d'engagement**

**Note aux soumissionnaires : Certains documents et annexes ne sont pas inclus dans l'étape 4 - Publication de la SPD de préqualification. Ces documents sont en cours d'élaboration et seront disponibles ultérieurement.

Annexe A – Conditions générales des services infonuagiques

Table des Matières

1.1 Limitation de responsabilité

1.1.1 Sauf disposition contraire de l'article 1.1.2, l'entrepreneur est responsable envers le Canada de tous les dommages directs qu'il cause en exécutant ou en omettant d'exécuter le Contrat en relation avec :

(1) les actes ou omissions de l'entrepreneur en vertu du Contrat résultant d'une négligence grave, d'une faute intentionnelle et de fraude liée à la violation des obligations en vertu du Contrat d'autorisation de tâche (CAT) et à la violation des droits de propriété intellectuelle, et ;

(2) la violation par l'entrepreneur des obligations de confidentialité en vertu du Contrat, mais cette limitation ne s'applique pas à la divulgation par l'entrepreneur des secrets commerciaux du Canada ou d'un tiers liés à la technologie de l'information.

Cependant, l'entrepreneur n'est pas responsable envers le Canada pour les dommages indirects, spéciaux ou consécutifs causés par les éléments 1 et 2 ci-dessus.

1.1.2 En ce qui concerne tous les dommages directs non énumérés ci-dessus, la responsabilité maximale de l'entrepreneur envers le Canada est le coût total estimé du Contrat (c'est-à-dire le montant en dollars indiqué sur la première page de l'Autorisation de tâche dans le bloc intitulé « Coût total estimé »). Dans cette limite, tous les dommages directs non énumérés ci-dessus sont soumis à un maximum du montant total payé pour l'Autorisation de tâche au cours des 12 mois précédant l'événement de responsabilité.

1.1.3 Si les dossiers ou données du Canada sont endommagés en raison de la négligence ou de l'acte intentionnel de l' entrepreneur, la seule responsabilité de l' entrepreneur est, à ses propres frais, de restaurer les dossiers et données du Canada à l'aide de la sauvegarde la plus récente conservée par le Canada. Le Canada est responsable de maintenir une sauvegarde adéquate de ses dossiers et données.

Aucune des limitations ci-dessus ne s'applique aux dommages résultant de pertes de vie ou de blessures ni aux réclamations basées sur la violation de la propriété intellectuelle.

1.2 Résiliation pour raison de commodité

1.2.1 Le Canada peut résilier le CAT et toute AT pour raison de commodité après notification écrite à l'entrepreneur ou en utilisant la fonction de résiliation ou d'annulation fournie par le portail en ligne de l'entrepreneur. Si le Contrat est résilié en partie seulement, l'entrepreneur doit continuer à fournir les services infonuagiques qui ne sont pas affectés par l'avis de résiliation.

1.2.2 Si le Canada résilie le CAT et toute AT pour raison de commodité, l'entrepreneur aura droit au paiement du solde dû pour tout service infonuagique fourni conformément à une ou plusieurs AT (moins tout crédit applicable appliqué et auquel il a droit de recevoir).

1.2.3 Le total des montants auxquels l'entrepreneur a le droit d'être payé en vertu de cette section, ainsi que tout montant payé, dû ou devenant dû aux Contracteurs, ne doit pas dépasser le Prix de l'AT. L'entrepreneur n'aura aucune réclamation pour dommages, compensation, perte de profit, allocation découlant de tout avis de résiliation donné par le Canada en vertu de cette section, sauf dans la mesure où cette section le prévoit expressément. L'entrepreneur accepte de rembourser immédiatement au Canada la portion de tout paiement anticipé qui n'est pas liquidée à la date de la résiliation.

1.2.4 La résiliation du CAT pour raison de commodité ne met pas fin à une AT individuelle pour commodité. Toute AT individuelle serait résiliée séparément pour commodité. La résiliation du CAT n'affectera pas ou ne mettra pas fin à une AT individuelle conclue avant la date de résiliation du CAT, à moins que l'événement donnant lieu à la résiliation du CAT ne résulte directement d'une violation des obligations du Contracteur ou du Canada en vertu de cette AT, auquel cas cette AT sera résiliée conformément à ses termes.

1.3 Résiliation pour manquement

L'Autorité contractante peut résilier le CAT avec effet immédiat en envoyant un avis de résiliation au Contracteur, dans les circonstances suivantes :

L'entrepreneur ne satisfait pas aux exigences de qualification continues décrites dans ce CAT ;

1.3.1 L'entrepreneur a enfreint l'une des conditions spécifiques détaillées dans ce CAT ou dans une AT individuelle ; ou

1.3.2 L'entrepreneur devient en faillite ou insolvable.

1.4 Récupération des données du Canada suite à une résiliation

À tout moment pendant la Période du CAT, le Canada doit avoir la possibilité d'accéder et d'extraire toutes les Données du Canada stockées dans le Service. À la résiliation complète du CAT ou d'une ou plusieurs AT, l'entrepreneur doit conserver les Données du Canada stockées dans le Service pendant un minimum de 90 jours civils et fournir au Canada un compte à fonctionnalités limitées, similaire au compte principal du Gouvernement du Canada (GC), qui permet au Canada d'extraire ses données pendant cette période. Le Canada doit avoir la possibilité d'extraire ses données de manière sécurisée et dans un format lisible par machine et utilisable, acceptable pour le Canada, sans frais supplémentaires en cas de résiliation pour défaut. Après la fin de la période de conservation, l'entrepreneur doit, sur demande du Canada, désactiver le compte du Canada.

1.5 Exigences de qualification continue et attestations

1.5.1 L'entrepreneur doit continuer de satisfaire aux exigences de qualification et se conformer à ses attestations dans sa soumission en tant que condition du CAT, soumises à vérification par le Canada pendant toute la période du CAT et chaque période d'AT. Si l'entrepreneur cesse de rester qualifié, ne se conforme pas à une certification ou s'il est déterminé que toute certification faite par l'entrepreneur dans

son offre est inexacte, que cela soit fait délibérément ou involontairement, le Canada a le droit, en vertu de la disposition de défaut du CAT, de résilier le CAT et une ou plusieurs AT pour défaut.

1.5.2 L'entrepreneur doit fournir toute information demandée par le Canada concernant le maintien ou non des exigences de qualification continues dans un délai raisonnable demandé par le Canada, n'excédant pas 15 jours ouvrables ou tel qu'il en est autrement convenu mutuellement.

1.6 Exigences de sécurité et de confidentialité pour les entrepreneurs

Les exigences de sécurité et de confidentialité énoncées dans ce Contrat d'Autorisation de Tâche s'appliquent au CAT et à chaque AT et doivent être maintenues en tout temps pendant la Période du CAT et chaque Période d'AT.

1.7 Processus continu d'intégrité de la chaîne d'approvisionnement

1.7.1 Les Parties reconnaissent que la sécurité est une considération essentielle pour le Canada en ce qui concerne ce CAT et qu'une évaluation continue de l'ISCA sera nécessaire à l'égard des AT individuelles tout au long de la Période du CAT.

1.7.2 Les parties reconnaissent que le Canada se réserve le droit de revoir les services Infonuagique natifs et les services de marché de tiers de tout Contracteur en tout ou en partie à tout moment pour des raisons d'intégrité de la chaîne d'approvisionnement. Cette reconnaissance n'oblige pas l'entrepreneur à soutenir l'examen de l'ISCA.

1.7.3 Tout au long de la Période du CAT et de toute Période d'AT, l'entrepreneur doit fournir au Canada des informations relatives à toute violation de données du réseau du Contracteur dont il a connaissance, qui résulte soit (a) de tout accès illégal au contenu du Canada stocké sur l'équipement ou les installations du Contracteur, soit (b) de tout accès non autorisé à ces équipements ou installations lorsque dans l'un ou l'autre cas un tel accès entraîne la perte, la divulgation ou l'altération du contenu du Canada en relation avec le changement de propriétés, aux services infonuagiques en vertu de ce CAT, et à toute AT individuelle ce qui compromettrait l'intégrité, la confidentialité, les contrôles d'accès, la disponibilité, la cohérence ou le mécanisme d'audit du système ou des données et des applications du Canada.

1.8 Sous-processeurs

1.8.1 L'entrepreneur doit fournir une liste des sous-processeurs qui pourraient être utilisés pour effectuer une partie quelconque des services infonuagiques dans le cadre de la fourniture des Services au Canada. La liste doit inclure les informations suivantes : (i) le nom du sous-processeur ; (ii) l'identification des activités qui seraient effectuées par le sous-processeur ; et (iii) le pays (ou les pays) où le sous-processeur effectuerait les activités nécessaires pour soutenir les services infonuagiques.

1.8.2 L'entrepreneur doit fournir une liste des sous-processeurs dans les dix jours suivant la date d'attribution du Contrat d'Autorisation de Tâche. L'entrepreneur doit informer le Canada (en mettant à jour le site Web et en fournissant au client un mécanisme pour obtenir un avis de cette mise à jour) de tout nouveau sous-processeur au moins

14 jours avant de fournir à ce sous-processeur un accès aux données du client ou aux données personnelles.

1.9 Changement de Contrôle

1.9.1 Si le Canada détermine à sa seule discrétion qu'un changement de contrôle affectant l'entrepreneur (soit l'entrepreneur lui-même, soit l'une de ses sociétés mères, jusqu'au propriétaire ultime) peut nuire à la sécurité nationale, le Canada peut résilier le CAT sur une base « sans faute » en envoyant un avis au Contracteur dans les 90 jours civils suivant la réception de l'avis de l'entrepreneur concernant le changement de contrôle. Le Canada ne sera pas tenu de fournir ses raisons de résilier le CAT en relation avec le changement de contrôle, si le Canada détermine à sa discrétion que la divulgation de ces raisons pourrait elle-même être préjudiciable à la sécurité nationale.

1.9.2 Si le Canada détermine à sa seule discrétion qu'un changement de contrôle affectant un sous-traitant (soit le sous-traitant lui-même, soit l'une ou l'autre de ses sociétés mères, jusqu'au propriétaire ultime) peut nuire à la sécurité nationale, le Canada avisera l'entrepreneur par écrit de sa détermination. Le Canada ne sera pas tenu de fournir les raisons de sa détermination, si le Canada détermine à sa discrétion que la divulgation de ces raisons pourrait elle-même être préjudiciable à la sécurité nationale. L'entrepreneur doit, dans les 30 jours civils suivant la réception de la détermination du Canada, organiser qu'un autre sous-traitant, acceptable pour le Canada, assure la livraison de la partie des services infonuagiques assurée par le sous-traitant existant (ou l'entrepreneur doit assurer cette partie des services infonuagiques lui-même). Si l'entrepreneur ne le fait pas dans ce délai, le Canada aura le droit de résilier le CAT sur une base « sans faute » en envoyant un avis au Contracteur dans les 120 jours civils suivant la réception de l'avis initial du Contracteur concernant le changement de contrôle.

1.9.3 Dans le présent article, la résiliation sur une base « sans faute » signifie qu'aucune des parties ne sera responsable envers l'autre du changement de contrôle et de la résiliation qui en résulte, et que le Canada ne sera responsable que du paiement des services reçus jusqu'à la date d'effet de la résiliation.

1.9.4 Malgré ce qui précède, le droit du Canada de résilier sur une base « sans faute » ne s'appliquera pas aux circonstances dans lesquelles il y a une réorganisation interne qui n'affecte pas la propriété de la société mère ou de la société mère du Contracteur ou du sous-traitant, selon le cas ; c'est-à-dire que le Canada n'a pas le droit de résilier le CAT en vertu du présent article lorsque l'entrepreneur ou le sous-traitant continue, en tout temps, d'être contrôlé, directement ou indirectement, par le même propriétaire ultime.

1.10 Exigences en matière d'assurance

L'entrepreneur est responsable de décider s'il doit s'assurer pour remplir ses obligations en vertu du CAT ou de toute AT individuelle 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.

1.11 Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur au Canada et dans la province de l'Ontario et les relations entre les parties seront déterminées par ces lois.

1.12 Instructions de facturation

1.12.1 L'entrepreneur doit soumettre des factures pour chaque AT émises en vertu du CAT. Tous les prix et paiements de factures doivent être en dollars canadiens.

1.12.2 La facture de l'entrepreneur doit indiquer les services infonuagiques et la quantité pour laquelle il facture, avec les prix unitaires correspondants, conformément aux Conditions de Paiement, ainsi que l'extension des totaux des services fournis. Les factures doivent également inclure la date, le numéro d'AT, le numéro d'entreprise de l'approvisionnement et le ou les codes financiers.

1.12.3 En soumettant des factures (à l'exception des éléments faisant l'objet d'un paiement anticipé), l'entrepreneur certifie que les services infonuagiques ont été fournis et que les frais ont été calculés conformément à l'AT.

1.12.4 L'entrepreneur doit appliquer tout crédit de service applicable dû au Canada après la soumission d'une réclamation valide conformément au processus publié commercialement de l'entrepreneur, à la facture d'AT qui suit le mois après que les crédits de service ont été accumulés en vertu de cette AT.

1.12.5 Les Taxes applicables doivent être spécifiées sur toutes les factures en tant qu'élément distinct, ainsi que les numéros d'enregistrement correspondants des autorités fiscales.

1.12.6 L'entrepreneur doit fournir l'original de chaque facture à l'Utilisateur final. Sur demande, l'entrepreneur doit fournir une copie de toutes les factures demandées par l'Autorité contractante.

1.13 Intérêts sur les paiements en retard

Le délai de paiement standard du Canada est de 30 jours. Le Canada versera à l'entrepreneur des intérêts simples au taux moyen (la moyenne arithmétique simple des taux bancaires en vigueur à 16 h, heure de l'Est, chaque jour pendant le mois calendaire précédant celui dans lequel le paiement est effectué) majoré de 3 pour cent par an, sur tout montant impayé, à compter de la date à laquelle ce montant devient impayé jusqu'à la veille de la date du paiement, inclusivement, à condition que le Canada soit responsable du retard dans le paiement à l'entrepreneur.

1.14 Ressortissants étrangers

L'entrepreneur doit se conformer aux exigences canadiennes en matière d'immigration relatives aux ressortissants étrangers qui doivent séjourner temporairement au Canada pour exécuter le contrat. Si l'entrepreneur souhaite embaucher un ressortissant étranger pour travailler au Canada, pour exécuter le contrat, il devrait communiquer immédiatement avec le bureau régional de Service Canada le plus près, pour obtenir des renseignements sur les exigences de Citoyenneté et Immigration Canada en ce qui concerne la délivrance d'un permis de travail temporaire à un ressortissant étranger.

L'entrepreneur doit acquitter tous les frais occasionnés par suite de la non-conformité aux exigences en matière d'immigration.

1.15 Limite des dépenses

1.15.1 La responsabilité totale du Canada envers l'entrepreneur en vertu de chaque AT autorisée émise par l'autorité contractante ne doit pas dépasser le montant indiqué dans l'AT, taxes applicables incluses, y compris toute révision émise par l'autorité contractante.

1.15.2 Aucune augmentation de la responsabilité totale du Canada ne sera autorisée ou payée à l'entrepreneur, à moins qu'une augmentation ait été approuvée, par écrit, par l'autorité contractante.

1.15.3 L'entrepreneur doit fournir des capacités de produire des rapports dans la cadre de son service permettant à l'Utilisateur final d'évaluer l'adéquation de cette somme et de déterminer s'il doit réduire l'utilisation ou augmenter le financement afin de permettre la fourniture des services infonuagiques dans les limites du budget.

Obligations en matière de sécurité

Au stade de la passation du contrat, l'entrepreneur devra satisfaire pleinement aux exigences de sécurité jusqu'au niveau et incluant Protégé B / actif de grande valeur, telle que définie dans le guide du Centre Canadian pour la cybersécurité (CCCS), sauf indication contraire. La formulation et la liste complète des exigences seront davantage affinées au cours d'un des étapes d'invitation à peaufiner (étape 5).

Annexe A – Appendice 1 –Obligations en matière de sécurité pour les services d'informatique en nuage commerciaux (jusqu'au niveau Protégé B inclusivement –recouvrement des actifs de valeur)

1. Généralités

1.1 Objet

Le présent appendice a pour objet d'énoncer les obligations de l'entrepreneur en matière de bonne gestion des données du Canada, y compris la protection contre les modifications, les exfiltrations et les accès non autorisés, conformément à l'entente, au présent appendice et aux mesures de sécurité de l'entrepreneur (collectivement, les « **obligations en matière de sécurité** »).

1.2 *Transfert des obligations en matière de sécurité*

Les obligations de l'entrepreneur contenues dans les présentes obligations en matière de sécurité doivent être transférées par l'entrepreneur à ses sous-traitants dans la mesure où elles s'appliquent à ces derniers.

1.3 *Gestion du changement*

(1) L'entrepreneur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir les obligations en matière de sécurité afin de se conformer aux pratiques de sécurité des normes de l'industrie énoncées dans le présent appendice.

(2) L'entrepreneur doit informer le Canada de tous les changements qui nuisent ou qui pourraient nuire sensiblement aux services d'informatique en nuage offerts dans le cadre du présent contrat, y compris les changements ou les améliorations de nature technologique, administrative ou autre. L'entrepreneur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier, sans supplément pour le Canada.

2. Reconnaissance

Les parties reconnaissent ce qui suit :

(1) Les données du Canada sont assujetties aux présentes obligations en matière de sécurité.

(2) Nonobstant toute autre disposition du présent appendice, les parties partagent la responsabilité de l'élaboration et du maintien des politiques, des procédures et des mesures de sécurité relatifs aux données du Canada.

(3) L'entrepreneur ne doit pas avoir en sa possession ou tenter d'avoir en sa possession des données du Canada ni permettre à aucun membre du personnel des services d'informatique en nuage d'y avoir accès avant que ne soient instaurées les obligations en matière de sécurité prévues au présent appendice, au plus tard à la date d'attribution du contrat.

(4) Les obligations en matière de sécurité s'appliquent aux **services d'informatique en nuage commerciaux** (jusqu'au et incluant niveau Protégé B / actifs de valeur, tel que définit dans l'orientation du Centre canadien pour la cybersécurité (CCCS), sauf indication contraire.

3. Protection des données du Canada

(1) L'entrepreneur doit protéger les données du Canada contre toute modification, toute exfiltration et tout accès non autorisé. Cela comprend la mise en œuvre et le maintien de mesures de sécurité techniques et organisationnelles adaptées, notamment des politiques, procédures et mesures de sécurité de l'information, afin de préserver la confidentialité, l'intégrité et la disponibilité des données du Canada.

4. Rôles et responsabilités liés à la sécurité

(1) L'entrepreneur doit clairement définir les rôles et responsabilités relatifs aux mesures et aux fonctions de sécurité des services d'informatique en nuage prévue 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.

(2) L'entrepreneur doit fournir au Canada un document à jour qui définit les rôles et les responsabilités : i) au moment de l'attribution du contrat; ii) chaque année; iii) lorsque des changements importants sont apportés à ces rôles et responsabilités à la suite d'une modification des services d'informatique en nuage; ou iv) à la demande du Canada.

5. Programme de la cybersécurité

(1) L'entrepreneur doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information qui comprennent les services de l'entrepreneur et les sous-traitants qui traitent et stockent les données du Canada.

(2) Le programme de cybersécurité doit être fondé sur l'évaluation des risques effectuée par l'entrepreneur et doit être conçu pour assurer les fonctions essentielles de cybersécurité suivantes :

(a) établir et évaluer les risques internes et externes en matière de cybersécurité qui peuvent menacer la sécurité ou l'intégrité des données du Canada stockées dans les systèmes d'information de l'entrepreneur;

(b) utiliser une infrastructure défensive et la mise en œuvre de politiques et de procédures visant à protéger les systèmes d'information de l'entrepreneur, ainsi que les données du Canada stockées sur ces systèmes d'information, contre l'accès non autorisé, l'utilisation ou d'autres actes malveillants;

(c) détecter les événements liés à la cybersécurité;

(d) réagir aux événements de cybersécurité établis ou détectés afin d'en atténuer les effets négatifs;

(e) se rétablir d'événements liés à la cybersécurité et rétablir des opérations et des services normaux;

(f) remplir les obligations réglementaires applicables en matière d'établissement de rapports.

(3) l'entrepreneur doit désigner une personne qualifiée (p. ex., responsable de la sécurité de l'information, responsable de la sécurité de l'entreprise, etc.) chargée de superviser et de mettre en œuvre le programme de cybersécurité de l'entrepreneur et d'appliquer sa politique en matière de cybersécurité. Cette personne désignée doit :

(a) conserver la responsabilité du respect des obligations en matière de sécurité énumérées dans le présent document;

(b) rendre compte par écrit au Canada, au moins une fois par an, du respect des obligations en matière de sécurité;

(c) rendre compte sur les risques de cybersécurité pour l'entrepreneur et les données du Canada;

(d) rendre compte sur l'efficacité globale du programme de cybersécurité de l'entrepreneur.

(4) Toute la documentation et l'information relatives au programme de cybersécurité de l'entrepreneur doivent être mises à la disposition du Canada sur demande.

6. Politique de cybersécurité

(1) L'entrepreneur doit mettre en œuvre et tenir à jour des politiques écrites, approuvées par un haut fonctionnaire ou par le conseil d'administration de l'entrepreneur ou un organe directeur équivalent, énonçant les politiques et procédures de l'entrepreneur en matière de protection de ses systèmes d'information et des données stockées sur ces systèmes d'information. La Politique sur la cybersécurité est fondée sur une évaluation des risques organisationnels et porte sur les domaines suivants, dans la mesure où ils s'appliquent aux activités de l'entrepreneur :

(a) Sécurité de l'information
(b) Gouvernance et classification des données
(c) Inventaire des actifs et gestion des appareils
(d) Mesures de contrôle d'accès et gestion des identités
(e) Planification et ressources en matière de continuité des activités et de reprise après sinistre
(f) Opérations des systèmes et questions de disponibilité
(g) Sécurité des systèmes et des réseaux
(h) Surveillance des systèmes et des réseaux
(i) Développement de systèmes et d'applications et assurance qualité
(j) Sécurité physique et mesures de contrôle environnementales
(k) Confidentialité des données des clients
(l) Gestion des risques liés à la chaîne d'approvisionnement, y compris la gestion des fournisseurs et des prestataires de services tiers
(m) Évaluation des risques
(n) Sensibilisation et formation à la sécurité
(o) Réponse aux incidents

7. Évaluation des risques

(1) L'entrepreneur doit procéder à une évaluation périodique des risques liés aux systèmes d'information de l'entrepreneur, suffisante pour étayer la conception du programme de cybersécurité requis par la présente partie. Cette évaluation des risques doit être mise à jour si cela est raisonnablement nécessaire pour tenir compte des modifications apportées aux systèmes d'information de l'entrepreneur, tout en continuant à respecter les obligations en matière de sécurité énumérées dans le présent document. L'évaluation des risques de l'entrepreneur doit permettre la révision des mesures pour répondre aux développements technologiques et à l'évolution des menaces et doit tenir compte des risques particuliers des activités commerciales de l'entrepreneur liés à la cybersécurité, aux données du Canada recueillies ou stockées, aux systèmes d'information utilisés ainsi qu'à la disponibilité et à l'efficacité des mesures visant à protéger les données et les systèmes d'information du Canada.

(2) L'évaluation des risques doit être effectuée conformément aux politiques et procédures écrites et doit être documentée. Ces politiques et procédures doivent inclure ce qui suit :

(a) des critères d'évaluation et de catégorisation des risques ou menaces ciblés en matière de cybersécurité auxquels l'entrepreneur est confronté;

(b) les critères d'évaluation de la confidentialité, de l'intégrité, de la sécurité et de la disponibilité des systèmes d'information de l'entrepreneur et des données du Canada, y compris la capacité des mesures existantes dans le contexte des risques établis;

(c) des exigences décrivant comment les risques identifiés seront atténués ou acceptés sur la base de l'évaluation des risques et comment le programme de cybersécurité traitera les risques;

(d) une formation régulière de sensibilisation à la cybersécurité pour l'ensemble du personnel, mise à jour en fonction des risques établis par l'entrepreneur dans son évaluation des risques.

8. Assurance d'une tierce partie : Certifications et établissement de rapports

(1) L'entrepreneur doit veiller à ce que les données du Canada, l'infrastructure de l'entrepreneur (y compris les services IaaS, PaaS ou SaaS fournis au Canada) et les points de prestation des services soient protégés par des mesures de sécurité appropriées qui sont conformes aux exigences énoncées dans ses pratiques et politiques sur la sécurité.

(2) L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et rapports de vérification suivants en fournissant des rapports d'évaluation ou des certifications de tiers indépendants qui portent sur chaque couche de service (p. ex., IaaS, PaaS et SaaS) au sein de l'offre de services d'informatique en nuage, notamment :

(a) ISO/IEC 27001:2022 Sécurité des renseignements, cybersécurité et protection de la confidentialité – Systèmes de gestion de la sécurité de l'information – Certification obtenue par un organisme de certification accrédité (ou des versions subséquentes);

(b) ISO/IEC 27017:2015 Technologie de l'information – Techniques de sécurité – Code de pratique pour les mesures de sécurité de l'information fondée sur la norme ISO/IEC 27002 pour les services d'informatique en nuage, obtenue par un organisme de certification accrédité (ou des versions subséquentes);

(c) Mesures de contrôle au niveau du système et au niveau organisationnel de l'AICPA (Service Organization Control [SOC]) 2 Type II Rapport de vérification 2 de type II se rapportant aux principes des services Trust (sécurité, disponibilité, intégrité du traitement et confidentialité) – produit par un comptable public accrédité (CPA) indépendant.

(3) Chaque rapport de certification ou de vérification fourni doit : (i) mentionner le nom légal de l'entreprise de l'entrepreneur ou du sous-processeur applicable; (ii) mentionner la date de certification de l'entrepreneur ou du sous-processus et l'état de cette certification; et (iii) dresser la liste des services visés par le rapport de certification. Si la méthode déterminée est utilisée pour exclure des sous-traitants proposant des services comme l'hébergement de centres de données, le rapport d'évaluation du sous-traitant doit être inclus.

(4) Chaque vérification doit faire l'objet d'un rapport qui sera mis à la disposition du Canada. Les certifications doivent être accompagnées d'éléments de preuve à l'appui, comme le rapport d'évaluation ISO élaboré pour valider la conformité avec la certification ISO, et elles doivent clairement divulguer toutes les constatations importantes du vérificateur. L'entrepreneur doit remédier rapidement aux problèmes soulevés dans tout rapport de vérification à la satisfaction du vérificateur et fournir au Canada des preuves à l'appui des mesures correctives prises ou une confirmation du vérificateur que les problèmes ont été réglés à la satisfaction du vérificateur.

(5) Chaque rapport SOC 2 type II doit avoir été réalisés dans les 12 mois précédant le début du contrat. Une lettre de transition peut être fournie pour démontrer que l'entrepreneur attend son renouvellement, s'il y a un écart entre la date du rapport du fournisseur de services et la fin de l'exercice de l'organisation utilisatrice (année civile ou fiscale).

(6) L'entrepreneur doit conserver les certifications ISO 27001, ISO 27017 et/ou SOC 2 Type II, selon le cas, 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 documents pouvant être raisonnablement exigés pour démontrer que l'entrepreneur possède des certifications à jour.

9. Vérification de la conformité

(1) L'entrepreneur doit veiller à ce que les vérifications de confidentialité et de sécurité portant sur la sécurité des ordinateurs, de l'environnement de la TI et des centres de données physiques qu'il utilise pour traiter et protéger les données du Canada soient effectuées de la manière 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 un vérificateur tiers indépendant qui i) est qualifié selon l'AICPA, CPA Canada ou le régime de certification ISO et ii) se conforme à la norme ISO/IEC 17020 sur les systèmes de gestion de la qualité, selon le choix et aux frais de l'entrepreneur.

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

(3) À la demande du Canada, l'entrepreneur ou le sous-traitant peut fournir des preuves supplémentaires, y compris des plans de sécurité du système, des dessins ou des documents d'architecture qui donnent 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 exigées de l'industrie. Cela inclut le cas où le contractant est un fournisseur SaaS ou PaaS qui utilise des centres de données physiques fournis par un fournisseur IaaS tiers.

10. Évaluation de la sécurité de la TI du fournisseur de services d'informatique en nuage (FSIN)

(1) L'entrepreneur doit recruter une organisation tierce d'évaluation autorisée FeDRAMP qui devra participer au processus de sécurité des TI.

(2) L'entrepreneur doit démontrer, avec le soutien de l'organisation tierce, qu'il respecte les exigences de sécurité sélectionnées :

(a) Le profil moyen des mesures de sécurité de l'informatique en nuage du CCCS, aussi connu comme l'annexe B des recommandations du Profil des mesures de la sécurité de l'informatique en nuage du Centre canadien pour la cybersécurité (CCCS) – MOYEN, pour le champ d'application des services fondés sur l'informatique en nuage offert par l'entrepreneur;

(b) Recouvrement des actifs de grande valeur Protégé B du CCCS, pour le champ d'application des services d'informatique en nuage fournis et déterminés comme capable par l'entrepreneur.

(3) La conformité sera validée et vérifiée par l'entremise du Processus d'évaluation de la sécurité de la technologie de l'information (TI) du CCCS visant les FSIN. L'entrepreneur doit fournir les documents suivants pour démontrer qu'il a terminé le processus :

(a) Une copie du dernier rapport d'évaluation rempli fourni au gouvernement du Canada;

(b) Une copie du dernier rapport sommaire fourni au gouvernement du Canada.

(4) Le Canada se réserve le droit de demander des preuves de conformité aux obligations en matière de sécurité, d'évaluer la conformité et, le cas échéant, d'ordonner des mesures correctives (p. ex., renforcer les mesures de sécurité) pour l'exploitation des services de l'entrepreneur.

(5) En tout temps, il incombe à l'entrepreneur des services d'informatique en nuage proposés d'avertir le ministère contractant du GC lorsque des changements importants sont apportés à la prestation des services de sécurité de la TI associée à son offre.

(6) L'entrepreneur doit contacter le ministère du gouvernement Canada responsable de la passation de marché pour tout renseignement supplémentaire sur le processus d'évaluation de la sécurité de la TI du CCCS visant les FSI.

11. Protection des données

(1) L'entrepreneur doit :

(a) Mettre en œuvre le chiffrement des données inactives pour tous les services d'informatique en nuage qui hébergent des données du Canada lorsque le chiffrement des données inactives demeure en vigueur, ininterrompu et actif en tout temps, même en cas de panne d'équipement ou de technologie, conformément à la section 17 – Protection cryptographique.

(b) Transmettre les données du Canada de façon sécuritaire, y compris la capacité, pour le GC, de mettre en œuvre le chiffrement des données en cours de transfert pour toutes les transmissions de données du Canada, conformément à la section 17 – Protection cryptographique et à la section 25 – Sécurité des réseaux et des communications.

(2) L'entrepreneur doit :

(a) Mettre en place des mesures de sécurité qui restreignent l'accès administratif aux données et aux systèmes du Canada par l'entrepreneur et qui permettent d'exiger l'approbation écrite du gouvernement du Canada avant que l'entrepreneur puisse accéder aux données du Canada pour effectuer des activités de soutien, d'entretien ou d'exploitation;

(b) Prendre des mesures raisonnables afin de veiller à ce que le personnel de l'entrepreneur n'ait pas de droits d'accès permanents ou continuels aux données du Canada, et que l'accès soit limité au personnel de l'entrepreneur ayant un besoin de savoir, y compris les ressources qui fournissent un soutien technique ou à la clientèle, en fonction de l'approbation du gouvernement du Canada.

(c) Mettre en œuvre des mesures de sécurité qui limitent l'utilisation des outils d'intelligence artificielle non autorisés donnant l'accès aux données du Canada.

(3) L'entrepreneur ne doit pas faire de copies des bases de données ou de parties de ces bases de données contenant des données du Canada à l'extérieur des capacités de résilience des services réguliers et dans les lieux ou zones régionaux approuvés au Canada.

(4) L'entrepreneur ne doit pas déplacer ou transmettre des copies approuvées à l'extérieur des régions de service convenues, sauf lorsque l'approbation écrite est obtenue du Canada.

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

12. Séparation des données

(1) L'entrepreneur doit mettre en place des mesures visant à assurer une séparation appropriée des ressources, afin que les données du gouvernement du Canada ne se retrouvent pas mêlées à celles d'autres locataires pendant l'utilisation, le stockage ou le transfert, et dans tous les aspects des fonctions et de l'administration du système des services d'informatique en nuage et de l'infrastructure de l'entrepreneur. Cela comprend la mise en œuvre de mesures de contrôle d'accès et la mise en place d'une séparation logique ou physique appropriée pour favoriser :

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

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

(c) (IaaS) la capacité du gouvernement du Canada (GC) de prendre en charge l'isolement dans un environnement à locataires géré par le GC.

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

13. Emplacement des données

(1) L'entrepreneur doit être en mesure de stocker et de protéger les données du Canada inactives, y compris les données sauvegardées ou conservées aux fins de redondance. Cela comprend la capacité d'isoler les données au Canada dans des centres de données approuvés. Un centre de données approuvé possède les caractéristiques suivantes :

(a) Il répond à toutes les exigences et certifications de sécurité exposées dans la section 33 concernant la sécurité physique (centre de données/installations).

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

(c) Il emploie le chiffrement afin de veiller à ce qu'aucune donnée ne soit écrite sur disque sous une forme non chiffrée, conformément à la section 17 – Protection cryptographique.

(2) L'entrepreneur doit certifier que la prestation et l'approvisionnement des services d'informatique en nuage en vertu du présent contrat proviennent de pays de l'Organisation du traité de l'Atlantique Nord (OTAN) (https://www.nato.int/cps/fr/natohq/nato_countries.htm), de pays membres de l'Union européenne (UE) (https://european-union.europa.eu/principles-countries-history/country-profiles_fr) ou de pays avec lesquels le Canada dispose d'un dispositif bilatéral de sécurité industrielle internationale. Le Canada dispose d'un dispositif bilatéral de sécurité industrielle internationale. 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, tel qu'il est mis à jour de temps à autre.

(3) L'entrepreneur doit veiller à ce que les données concernant le Canada ou les citoyens ou résidents du Canada – données classées au niveau de sensibilité Protégé B – soient collectées, traitées et/ou stockées à l'intérieur des frontières géographiques du Canada.

(4) Avant de transférer des données concernant le Canada ou les citoyens ou résidents du Canada à l'étranger à des fins de traitement précises (p. ex., détection d'une activité anormale, analyse des menaces), l'entrepreneur doit d'abord :

(a) Obtenir l'accord du Canada, à la suite duquel l'entrepreneur doit traiter les données de manière appropriée et appliquer des mesures de protection comparables pour atteindre un niveau de protection similaire à celui stipulé dans le présent document.

(b) Certifier que la prestation et l'approvisionnement des services d'informatique en nuage dans le cadre du présent contrat 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://european-union.europa.eu/principles-countries-history/country-profiles_fr) ou de pays avec lesquels le Canada a conclu un instrument bilatéral international en matière de sécurité industrielle. Dans le cadre du Programme de sécurité des contrats (PSC), des accords internationaux bilatéraux en matière de sécurité industrielle ont été conclus avec les pays indiqués sur le site Web (https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html) du PSC, mis à jour ponctuellement.

(c) Le Canada doit avoir la possibilité de refuser d'utiliser un service offert par l'entrepreneur et fourni à partir de l'étranger et, dans ce cas, se voir offrir un service similaire fourni à partir du Canada lorsqu'il en fait la demande.

(d) Le contractant ne doit pas stocker les données en dehors du Canada.

(5) L'entrepreneur ne doit pas utiliser ou divulguer les renseignements à d'autres fins. Ainsi, un transfert de données en vue d'un traitement doit être effectué dans un but pour lequel les renseignements ont été collectés à l'origine et pour lequel le Canada a donné son accord.

(6) L'entrepreneur doit avoir la capacité pour le Canada d'isoler les données du Canada hébergé dans des services d'informatique en nuage dans des centres de données géographiquement situés au Canada.

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

(a) Fournir au GC une liste à jour des emplacements physiques, y compris la ville, qui peut contenir des données du Canada pour chaque centre de données qui sera utilisé pour fournir les services d'informatique en nuage.

(b) Indiquer les parties des services d'informatique en nuage qui sont fournis depuis l'étranger, y compris tous les endroits où les données sont stockées et traitées et d'où l'entrepreneur gère le service.

(8) L'entrepreneur des services d'informatique en nuage proposés a l'obligation permanente d'avertir le Canada par écrit lorsque des mises à jour sont apportées à la liste des emplacements physiques où peuvent se trouver des données du Canada.

14. Transfert et récupération des données

(1) L'entrepreneur doit fournir au Canada la capacité suivante, notamment des outils et des services :

(a) Extraire toutes les données du Canada en ligne, pseudodirect 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 d'informatique en nuage, 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 connexes, dans un format lisible et utilisable par machine (y compris le format CSV) et conformément aux Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires de Bibliothèque et Archives Canada (https ://bibliotheque-archives.canada.ca/fra/services/gouvernement-canada/information-disposition/lignes-directrices-information/Pages/lignes-directrices-formats-fichier-ressources-documentaires.aspx).

15. Conservation des données

(1) L'entrepreneur doit conserver les données pendant toute la durée du contrat sur la base de la période de conservation approuvée par le GC et conformément aux outils d'évaluation générale de la Bibliothèque et des Archives (https://library-archives.canada.ca/eng/services/government-canada/information-disposition/generic-valuation-tools/Pages/generic-valuation-tools.aspx). Il s'agit des données du Canada sous forme structurée et non structurée.

(2) L'entrepreneur doit éliminer les données du Canada conformément à la *section 16 – Élimination des données et retour des documents au Canada* lorsqu'elles atteignent la fin de la période de conservation.

16. Élimination des données et renvoi des dossiers au Canada

(1) L'entrepreneur doit effacer, purger, éliminer ou détruire en toute sécurité les ressources (par exemple, équipement, stockage de données, fichiers et mémoire) ou les dispositifs susceptibles de contenir des données du Canada et veiller à ce que les données précédemment stockées ne puissent pas être réintroduites dans le système ou les dispositifs.

(2) L'entrepreneur doit éliminer ou réutiliser en toute sécurité les ressources (p. ex., l'équipement, les unités de stockage, les fichiers et la mémoire) qui contiennent des données du Canada et veiller à ce que les données précédemment stockées ne puissent pas être consultées par d'autres clients après leur diffusion. Cette mesure concerne 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'une des pratiques exemplaires suivantes :
i) National Industrial Security Program Operating Manual (DoD 5220.22-M6); ii) Guidelines for Media Sanitization (NIST SP 800-88); ou iii) Centre de la sécurité des télécommunications (CST) – Nettoyage des supports de la TI (ITSP.40.006) (https://www.cyber.gc.ca/fr/orientation/nettoyage-des-supports-de-ti-itsp40006). À la demande du Canada, l'entrepreneur doit produire un document qui décrit son processus d'élimination ou de réutilisation des ressources.

(3) L'entrepreneur doit présenter au Canada la confirmation écrite démontrant qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de tout système, de toute capacité (logiciel ou processus), de toute donnée ou de toute information retirées ou détruites une fois que le Canada a cessé d'utiliser les services d'informatique en nuage.

17. Protection cryptographique

L'entrepreneur doit :

(1) 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 clé 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 approuvées par le CST, comme indiquées dans le guide intitulé « Algorithmes cryptographiques pour l'information NON CLASSIFIÉE, PROTÉGÉ A et PROTÉGÉ B » (ITSP.40.111) (https ://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111) et le guide intitulé « Conseils sur la configuration sécurisée des protocoles réseau » (ITSP.40.062) (https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062), et rester cohérent avec toute version ultérieure publiée sur https://cyber.gc.ca/.

(2) Utiliser des algorithmes cryptographiques approuvés par le CST qui ont été validés par le Cryptographic Algorithm Validation Program (en anglais seulement)

(https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program), avec des paramètres et des tailles de clés de chiffrement appropriées, comme indiqué dans le guide intitulé « Algorithmes cryptographiques pour l'information NON CLASSIFIÉE, PROTÉGÉ A et PROTÉGÉ B » (ITSP.40.111) (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111), et rester cohérent avec toute version ultérieure publiée sur https://cyber.gc.ca/.

(3) Veiller à ce que l'utilisation d'algorithmes cryptographiques, les paramètres et tailles de clés de chiffrement et les périodes de validité des clés soient configurables et puissent être mis à jour dans les protocoles, les applications et les services conformément aux directives relatives à la transition, comme indiqué dans le guide intitulé « Algorithmes cryptographiques pour l'information NON CLASSIFIÉE, PROTÉGÉ A et PROTÉGÉ B » (ITSP.40.111) (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111) et le guide intitulé « Conseils sur la configuration sécurisée des protocoles réseau » (ITSP.40.062) (https ://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062), et rester cohérent avec toute version ultérieure publiée sur https://cyber.gc.ca/. L'entrepreneur doit prendre en charge la transition vers la cryptographie post-quantique, conformément aux directives figurant dans l'ITSP.40.111 et l'ITSP.40.062 et toute version ultérieure.

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

(5) Veiller à ce que tout module cryptographique utilisé possède une certification PVMC active, à jour et valide. Les produits validés par le PVMC se verront attribuer des numéros de certificat, lesquels figurent sur la liste des modules validés par le PVMC (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules).

(6) Les modules cryptographiques doivent être configurés et exploités dans un mode approuvé ou autorisé conformément à la Politique sur la sécurité publiée par le PVMC.

(7) Appuyer l'agilité cryptographique afin que la protection des données en transit ou au repos puisse rester conforme aux recommandations du CST/CCCS en matière de protection cryptographique, y compris l'utilisation de nouvelles normes pour atténuer la menace de l'informatique quantique.

18. Gestion des clés

(1) L'entrepreneur doit veiller à ce que la clé principale de la DSIC ou les clés racines utilisées pour dériver d'autres clés soient générées et gérées selon des processus sécurisés et approuvés, validés par la norme FIPS 140, pour la génération, la distribution, le stockage et la gestion du cycle de vie des clés.

(2) L'entrepreneur doit fournir au Canada un service de gestion des clés conforme au Guide sur le chiffrement des services d'informatique en nuage (ITSP.50.106) du CCC (https://cyber.gc.ca/fr/orientation/guide-sur-le-chiffrement-des-services-infonuagiques-itsp50106) et à leurs versions subséquentes publiées sur https://cyber.gc.ca, qui inclut :

(a) La capacité d'importer en toute sécurité des clés de chiffrement générées par le GC à partir d'un module de sécurité matériel (MSM) sur place gérée par le GC, sans exposition du texte en clair de la clé au cours du processus d'importation, et de les stocker dans un MSM spécialisé géré par l'entrepreneur pour le Canada.

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

(c) La protection de l'accès au matériel relatif aux clés, y compris la prévention de l'accès 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'empêcher le fournisseur de services d'informatique en nuage de récupérer des copies en texte clair des clés générées par le GC.

(f) La capacité de déléguer les privilèges liés à l'utilisation des clés pour leur usage par les services d'informatique en nuage utilisés pour les services gérés par le GC.

(3) L'entrepreneur doit fournir une capacité de gestion des clés qui permet l'interopérabilité et l'accès aux clés de chiffrement contrôlées par le GC et stockées dans une infrastructure MSM sur place gérée par le GC.

19. Protection des points terminaux

(1) L'entrepreneur doit mettre en œuvre, gérer et surveiller les points d'accès sécurisés à l'aide de protections hébergées actives afin de prévenir les maliciels, les attaques et les abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide 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.

(2) L'entrepreneur doit veiller à ce que les supports contenant des données de l'organisation sur des supports numériques et non numériques soient protégés par un mécanisme cryptographique afin de préserver la confidentialité et l'intégrité de ces informations.

20. Sécurisé dès la conception et développement

(1) L'entrepreneur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes dans le cadre d'une approche sécurisée dès la conception 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, SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, (ii) ISO/IEC 27034-1:2011 - Information technology — Security techniques — Application security — Part 1: Overview and concepts, (iii) CCCS Annex 2 - Information system security risk management activities (ITSG-33), (iv) SAFECode, (v) CISA Principles and Approaches for Security by Design, or (vi) Open Web Application Security Project (OWASP) (p. ex., Application Security Verification Standard [ASVS]) ou une norme équivalente approuvée par le Canada par écrit.

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

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

(1) L'entrepreneur doit mettre en œuvre la capacité pour le Canada de prendre en charge un accès sécurisé aux services d'informatique en nuage, y compris la capacité de configurer :

(a) une authentification à facteurs multiples résistante à l'hameçonnage conformément au document ITSP.30.031 V3 (ou une version subséquente) du CST (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de) au moyen de justificatifs approuvés par le GC;

(b) un accès basé sur les rôles;

(c) des mesures de l'accès aux objets stockés;

(d) des politiques d'autorisation granulaire pour autoriser ou limiter l'accès.

(2) L'entrepreneur doit avoir la capacité d'établir des paramètres par défaut à l'échelle de l'organisation pour gérer les politiques applicables à l'ensemble des locataires.

22. Fédération

(1) L'entrepreneur doit mettre en œuvre la capacité pour le Canada de prendre en charge l'intégration fédérée de l'identité, y compris :

(a) Prendre en charge des normes ouvertes pour les protocoles d'authentification comme le langage SAML (Security Assertion Markup Language) 2.0 (ou versions ultérieures) et OpenID Connect 1.0 (ou versions ultérieures), selon lesquelles les identifiants de l'utilisateur final et l'authentification aux services d'informatique en nuage relèvent exclusivement du Canada.

(b) Être en mesure 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'informatique en nuage correspondants.

23. Gestion de l'accès privilégié

(1) L'entrepreneur doit :

(a) mettre en œuvre des politiques et procédures de contrôle de l'accès qui prennent en compte l'intégration, la désinstallation, la transition entre les rôles, des examens réguliers de l'accès pour déterminer les privilèges excessifs, les limites et le contrôle de l'utilisation des privilèges d'administrateur;

(b) gérer et surveiller l'accès privilégié aux services d'informatique en nuage afin de veiller à ce que toutes les interfaces de service dans un environnement à locataires multiples soient protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC;

(c) restreindre et réduire au minimum l'accès aux services d'informatique en nuage et aux données du Canada seulement aux appareils autorisés et aux utilisateurs finaux ayant explicitement besoin de cet accès;

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

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

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

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

(h) mettre en place des mécanismes de contrôle 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, ainsi que 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 d'informatique en nuage et aux données du Canada;

(k) utiliser des terminaux à sécurité renforcée (p. ex., ordinateurs, dispositifs d'utilisateurs finaux, serveurs intermédiaires) configurés de façon à offrir une fonctionnalité minimale (p. ex., terminal spécialisé qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) afin d'assurer la prise en charge et l'administration des services d'informatique en nuage 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 identifiants d'accès associés à tout membre du personnel de services.

(2) À la demande du Canada, l'entrepreneur doit produire un document qui décrit l'approche et le processus de l'entrepreneur pour la gestion et la surveillance des accès privilégiés aux services d'informatique en nuage.

24. Gestion à distance

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

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

(b) Employer des mécanismes et des algorithmes cryptographiques pour protéger la confidentialité des séances d'accès à distance, conformément à la section 13 – Protection cryptographique.

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

(d) Effectuer rapidement une déconnexion ou une désactivation en cas de gestion à distance ou d'accès à distance non autorisés.

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

(2) À la demande du Canada, l'entrepreneur doit produire un document qui décrit l'approche et le processus de l'entrepreneur pour la gestion et la surveillance de l'administration à distance des services d'informatique en nuage.

25. Sécurité des réseaux et des communications

(1) L'entrepreneur doit :

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

(b) Utiliser des protocoles ainsi que des algorithmes et des certificats cryptographiques pris en charge et à jour, comme le décrivent les normes ITSP.40.062 (https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062) du CCC et ITSP.40.111 (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111).

(c) Utiliser des certificats correctement configurés dans les connexions TLS conformément aux Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) du CCC (https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062).

(d) Permettre au Canada de mettre en œuvre des mesures de contrôle d'accès au réseau et des règles de sécurité qui restreignent l'accès aux seuls dispositifs et emplacements du réseau autorisés aux ressources du Canada.

(e) Permettre au Canada de mettre en œuvre des connexions dédiées ou privées vers ses centres de données et appuyer les charges de travail sensibles qui peuvent l'exiger.

(f) Fournir des outils et des capacités pour évaluer l'efficacité des mesures de sécurité et fournir une visibilité sur l'application des mesures de sécurité sur l'ensemble du chemin de transition des données en utilisant des technologies telles que les journaux d'activité et les rapports.

(g) Valider la posture de sécurité, identifier de manière unique et authentifier les demandes avant d'établir une connexion réseau avec le locataire ou les ressources en matière d'informatique en nuage de l'organisation cliente.

(h) Concevoir et mettre en œuvre des mesures opérationnelles pour garantir que les logiciels, le matériel et les systèmes de communication en réseau prennent en charge des services redondants et résilients afin de résister aux perturbations, aux pannes de matériel et aux événements cyberdestructeurs.

26. Accès et vérification

(1) L'entrepreneur doit mettre en œuvre des pratiques et des mesures de contrôle de création et de gestion des journaux pour toutes les composantes des services d'informatique en nuage qui stockent ou traitent les données du Canada, et qui sont conformes aux normes et aux pratiques exemplaires de l'industrie, comme celles énoncées dans le document 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 produire un document décrivant ses pratiques et mesures de contrôle de création et de gestion des journaux.

(2) L'entrepreneur doit permettre au Canada de gérer et de configurer de façon centralisée le contenu à saisir dans les enregistrements de vérification à partir de composantes multiples (p. ex., réseau, données, stockage, calcul, etc.) à partir des services d'informatique en nuage utilisés par le Canada, afin de permettre au Canada d'effectuer la surveillance de la sécurité, l'établissement de rapports, des analyses, des enquêtes et la mise en œuvre de mesures correctives, au besoin. Ceci comprend la capacité du Canada :

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

(b) de veiller à ce que les événements de vérification réduisent au minimum l'exposition de données sensibles telles que les renseignements personnels à l'aide de techniques et de mesures de protection de la confidentialité appropriées, conformément à la section 17 – Protection cryptographique;

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

(d) de fournir en temps réel des alertes d'échec de vérification aux membres du personnel ayant le pouvoir de remédier aux échecs de vérification;

(e) de repérer des incidents de sécurité et des journaux de bord distincts pour les différents comptes du Canada afin de permettre au GC de surveiller et de gérer les événements à l'intérieur de ses frontières qui ont une incidence sur l'instance d'un service d'informatique en nuage IaaS, PaaS ou SaaS qui lui est rendu par le fournisseur ou un sous-traitant.

(3) L'entrepreneur doit donner au Canada la capacité d'exporter des journaux des événements de sécurité à l'aide d'interfaces de rapport, de protocoles et de formats de données normalisés (p. ex., Common Event Format [CEF], journal d'exploitation [syslog] ou autres formats de journal communs) et d'API qui prennent en charge l'extraction à distance des données des journaux (p. ex., au moyen d'une interface de base de données utilisant SQL), pour les services d'informatique en nuage qu'il utilise, pour appuyer les activités du GC, y compris la surveillance des services d'informatique en nuage et la divulgation électronique et les mises en suspens pour des raisons juridiques.

(4) Pour les services SaaS, l'entrepreneur doit fournir des interfaces de programmation d'applications (IPA) qui permettent :

(a) d'inspecter et interroger les données inactives dans les applications SaaS;

(b) d'exporter les journaux des événements de sécurité pour les solutions;

(c) d'évaluer les événements comme les accès et les comportements des utilisateurs, les accès et les comportements des administrateurs, et les changements apportés aux accès aux API par des tiers, stockés dans les registres des applications SaaS.

27. Surveillance continue

(1) L'entrepreneur doit continuellement gérer, surveiller et maintenir la posture de sécurité de l'infrastructure et des points de prestation des services de l'entrepreneur qui hébergent les données du Canada pendant toute la durée du contrat, et veiller à ce que les services d'informatique en nuage fournis au Canada soient conformes aux présentes obligations en matière de sécurité. Dans le cadre de cette obligation, l'entrepreneur doit :

(a) surveiller activement et continuellement les menaces et les vulnérabilités pesant sur l'infrastructure de l'entrepreneur, les points de prestation des services ou les données du Canada;

(b) Mettre en œuvre des politiques, des procédures et des mesures fondées sur les risques, conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès ou l'utilisation non autorisés, ou la falsification, des données du Canada par ces utilisateurs autorisés;

(c) effectuer régulièrement des analyses de vulnérabilité et des tests de pénétration sur l'infrastructure et les points de prestation des services de l'entrepreneur dans le but d'identifier les lacunes et les mesures correctives afin de prévenir les accès non autorisés à des renseignements sensibles, le contournement des mesures de contrôle d'accès et de l'escalade des privilèges et l'exploitation de vulnérabilités pour accéder aux systèmes ou aux renseignements;

(d) tout mettre en œuvre pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le déni de service;

(e) tout mettre en œuvre pour détecter les attaques, les incidents de sécurité et autres événements anormaux;

(f) détecter l'utilisation et l'accès non autorisé à tous les services d'informatique en nuage, données et composants afférents aux services d'informatique en nuage IaaS, PaaS ou SaaS du Canada;

(g) gérer et appliquer les rustines et les mises à jour liées à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de corriger tout problème signalé publiquement dans les services d'informatique en nuage ou les bibliothèques que les services d'informatique en nuage utilisent, et donner des préavis de rustine conformément aux engagements convenus relatifs au niveau de service;

(h) répondre aux menaces et aux attaques contre les services d'informatique en nuage de l'entrepreneur, les contenir et veiller à la récupération;

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

(2) Les services d'informatique en nuage de l'entrepreneur doivent permettre de copier les données des applications (IaaS, PaaS et SaaS) et l'achalandage réseau (IaaS et PaaS) du gouvernement du Canada dans les services d'informatique en nuage hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du gouvernement).

(3) Pour les services SaaS, les services d'informatique en nuage de l'entrepreneur doivent permettre au Canada de déployer et d'utiliser des logiciels de sécurité pour assurer la surveillance avancée et l'atténuation des cybermenaces pour les services d'informatique en nuage du Canada pour les composants gérés par le Canada seulement.

28. Gestion des incidents de sécurité

(1) L'entrepreneur doit :

(a) Mettre en place et maintenir un centre d'opérations de sécurité (COS) qui fonctionne dans le cadre de la durée d'activité et du modèle de service définit par l'organisation, p. ex., une couverture de 24 heures sur 24 et 7 jours sur 7.

(b) Mettre en place et maintenir une équipe d'intervention en cas de cyberincident qui peut être déployée par la DSIC dans le cadre des objectifs de service prévus par l'organisation.

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

(a) Un processus d'intervention en cas d'incident de sécurité publié et documenté en vue de l'examen par le Canada, conforme à l'une des normes suivantes : i) ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management; ii) NIST SP 800-61 Rev.2, Computer Security Incident Handling Guide; 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); file:///C:/Users/UberigA/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/BTN5ATL4/(https:/cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b)duCST;ou iv) autres pratiques exemplaires des normes de l'industrie, si le Canada détermine, à sa discrétion, qu'elles répondent à ses exigences relatives à la sécurité.

(b) Des processus et procédures documentés décrivant comment l'entrepreneur détectera, gérera et corrigera les incidents de sécurité et les signalera et les soumettra au Canada, notamment : i) la portée des incidents liés à la sécurité de l'information que l'entrepreneur signalera au Canada; ii) le niveau de divulgation de la détection des incidents liés à la sécurité de l'information et les interventions connexes; iii) le délai cible de notification des incidents liés à la sécurité de l'information; iv) la procédure de notification des incidents liés à la sécurité de l'information; v) les coordonnées des personnes-ressources pour le traitement des problèmes relatifs aux incidents liés à la sécurité de l'information, conformément aux procédures d'établissement de rapports décrits dans le PGEC GC (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html); et vi) tous les recours qui s'appliquent si certaines mesures de sécurité de l'information sont prises.

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

(d) Autorise uniquement les représentants désignés et autorisés du client (p. ex., le CCC ou d'autres organismes approuvés par le GC) qui sont autorisés par le responsable technique :

(i) à demander et à recevoir un accès et de l'information confidentiels associés 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 de pare-feu, etc.) dans un format non chiffré, aux fins d'enquête;
(ii) à effectuer le suivi d'un événement signalé lié à la sécurité de l'information.

(e) Procédures pour répondre aux demandes de preuves numériques potentielles ou d'autres renseignements provenant de l'environnement des services d'informatique en nuage et conformes aux normes et aux pratiques exemplaires de l'industrie, y compris la norme ISO 22095:2020 Chaîne de contrôle – Terminologie générale et modèles (https://www.iso.org/fr/standard/72532.html), y compris les procédures judiciaires et les mesures de protection appropriées pour :

(i) la gestion d'une chaîne de possession de l'information relative à la vérification;
(ii) la collecte, la conservation et la présentation de preuves de l'intégrité des données.

(3) Dans les dix jours suivant la date d'entrée en vigueur du contrat, l'entrepreneur doit fournir un document décrivant son processus de réponse aux incidents de sécurité, y compris les coordonnées des personnes-ressources. Ce processus, y compris les coordonnées des personnes-ressources, doit être tenu à jour et, au minimum, être validé annuellement et approuvé par le Canada.

(4) L'entrepreneur doit :

(a) Collaborer avec le ou les centres des opérations de sécurité du Canada (p. ex., SOC du GC, équipes de sécurité de la TI du ministère) et les principaux intervenants du PGEC GC (c.-à-d. le CCC et le Secrétariat du Conseil du Trésor du Canada [SCT]) en matière de confinement, d'éradication et de reprise en cas d'incidents de sécurité, conformément au processus d'intervention en cas d'incident de de sécurité, et au PGEC GC (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html).

(b) Tenir un registre des atteintes à la sécurité comprenant une description de l'atteinte, sa durée, ses conséquences, le nom de la personne qui l'a signalée et celui de la personne à qui elle a été signalée, et la procédure pour récupérer les données ou le service, ainsi que des registres des activités liées à la gestion de l'incident de sécurité, y compris les communications internes et externes (p. ex., dans le cas d'un événement de type rançongiciel, toutes les communications, y compris les demandes de rançon, etc.). Ces renseignements doivent être fournis au Canada sur demande.

(c) Suivre ou permettre au Canada de suivre les divulgations de données du Canada, y compris le type de données divulguées, les personnes y ayant eu accès et le moment où l'incident s'est produit.

(5) À l'appui des enquêtes de sécurité, le Canada peut exiger des preuves judiciaires de la part de l'entrepreneur pour faciliter une enquête du GC. L'entrepreneur doit :

(a) conserver les rapports d'enquête liés à une enquête de sécurité pendant une période de deux (2) ans suivant la fin de l'enquête ou les remettre au Canada aux fins de conservation;

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

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

(d) appuyer la divulgation électronique;

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

(6) Si l'entrepreneur fait appel à une entreprise externe dans le cadre de ses activités d'intervention en cas d'incident, il doit veiller à ce que les dispositions de la présente *section 28 – Gestion des incidents de sécurité* et la *section 29 – Intervention en cas d'incident de sécurité* s'appliquent également à l'équipe externe d'intervention en cas d'incident et soient documentées dans le processus d'intervention en cas d'incident de sécurité de l'entrepreneur.

29. Intervention en cas d'incident de sécurité

(1) L'entrepreneur doit alerter et aviser promptement le Canada (par téléphone ou par courriel), conformément aux procédures d'établissement de rapports de la *section 28 – Gestion des incidents de sécurité*, de toute compromission, de toute violation ou de toute preuve comme :
i) un incident de sécurité;
ii) une défectuosité liée à la sécurité d'un actif;
iii) l'accès irrégulier ou non autorisé à un actif;
iv) la copie à grande échelle d'un actif d'information ou
v) toute autre activité illégale recensée par l'entrepreneur, portant ce dernier à croire de manière raisonnable que le risque de compromission, d'atteinte à la sécurité ou à la vie privée est ou pourrait être imminent, ou si les mesures de protection existantes ont cessé de fonctionner, au cours de la période suivante (tous les jours, 24 heures par jour, 365 jours par année), et sans tarder, dans tous les cas, dans les 72 heures, et conformément aux engagements convenus relatifs au niveau de service.

(2) Si l'entrepreneur prend connaissance de toute compromission 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'agent contractuel (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 nécessaires pour remédier aux causes et atténuer les dommages découlant de l'incident de sécurité.

iv) coopérer avec le Canada dans le cadre de l'enquête sur l'événement, y compris en mettant à disposition tous les enregistrements, journaux, fichiers, rapports de données et autres documents relatifs aux données du Canada requis pour se conformer à la législation applicable ou à toute autre exigence du Canada;

v) identifier toutes les données du Canada touchées ou risquant d'être touchées;

vi) informer le Canada des mesures qu'il prend ou qu'il prendra immédiatement pour réduire le risque de perte supplémentaire pour le Canada;

vii) exécuter ou prendre toute autre mesure nécessaire pour se conformer à la loi applicable à la suite de l'événement;

viii) restaurer toute donnée perdue, corrompue ou autrement compromise, de la manière et selon le calendrier établi par le Canada, sans frais pour ce dernier;

ix) fournir au Canada, dans les 10 jours ouvrables ou dès que possible (à condition qu'un plan préliminaire ait été fourni au Canada dans les 10 jours ouvrables), un plan détaillé de l'incident décrivant les mesures que l'entrepreneur prendra pour éviter qu'un tel incident ne se reproduise;

x) coopérer avec le Canada pour participer à l'enquête sur la violation et pour exercer un contrôle sur le signalement de l'accès non autorisé ou de la divulgation des données du Canada, dans la mesure permise par la loi et dans la mesure où les registres de vérification des activités des applications des locataires du Canada sont pertinents à l'événement et à l'enquête, et sous réserve des obligations de l'entrepreneur et des mesures de confidentialité prévues au contrat et des certifications industrielles applicables, y compris, mais sans s'y limiter, celles précisées à la section 8 (Assurance d'une tierce partie).

(3) L'entrepreneur doit signaler au Canada les atteintes intentionnelles ou accidentelles des mécanismes de protection des données et de cryptographie, en fournissant des documents et des preuves sur les mesures prévues ou prises pour remédier à la situation.
(4) Les entrepreneurs doivent signaler les incidents majeurs aux services de police compétents à la demande du Canada.

30. Fuite d'information

(1) L'entrepreneur doit disposer d'un processus documenté décrivant son approche en cas d'incident de fuite d'information. Ce 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. Sans égard à ce qui précède, le processus d'intervention en cas de fuite d'information de l'entrepreneur doit comprendre, à tout le moins :

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

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

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

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

31. Test de sécurité et validation

(1) L'entrepreneur doit disposer d'un processus qui permet d'effectuer une analyse des vulnérabilités ou un test d'intrusion non perturbateur et non destructif des services d'informatique en nuage qui hébergent les données du Canada. Cela comprend la capacité de réaliser des analyses internes et externes périodiques liées à l'emplacement où se trouvent les données du GC et, si des changements importants sont apportés à la plateforme principale, de détecter toute vulnérabilité potentielle du système liée à l'emplacement où se trouvent les données du GC grâce à :
(i) des analyses des vulnérabilités;
(ii) des analyses des applications Web;
(iii) des tests d'intrusion.

(2) L'entrepreneur doit établir un plan d'action avec des étapes clés documentant toute mesure corrective prévue pour corriger les faiblesses ou les lacunes au niveau de la plateforme principale en vue de réduire ou d'éliminer les vulnérabilités connues du système, ou des vulnérabilités liées aux services d'informatique en nuage hébergeant les données du Canada et au fonctionnement de l'emplacement où se trouvent les données du GC.

(3) 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 des services d'informatique en nuage dans l'environnement de l'entrepreneur.

(4) L'entrepreneur doit fournir la capacité d'activer un outil libre-service de vérification de l'état de sécurité ou de notation qui mesure la posture de sécurité des services d'informatique en nuage configurés par le Canada.

32. Filtrage de sécurité du personnel

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

(2) Les mesures de filtrage 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-https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115sct.gc.ca/pol/doc-eng.aspx?id=28115), ou utiliser un équivalent acceptable convenu par le Canada.

(3) Des accords de non-divulgation doivent être mis en place pour le personnel de l'entrepreneur ayant accès aux données du Canada.

(4) À la demande du Canada, l'entrepreneur doit produire un document qui décrit son processus de filtrage de sécurité du personnel. Ce processus doit contenir, au minimum :

(a) Une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux données du Canada ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services d'informatique en nuage.

(b) Une description des activités et pratiques du processus 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 provoquent des doutes ou des préoccupations.

(c) Une description de la sensibilisation et de la formation à la sécurité dans le cadre de l'intégration dans l'emploi, lorsque les rôles des employés et des sous-traitants changent, et de façon continue, afin de veiller à ce que les employés et les sous-traitants comprennent, connaissent et assument leurs responsabilités en matière de sécurité des renseignements.

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

(e) L'approche de détection, de contrôle et d'atténuation des menaces internes potentielles et des mesures de sécurité mis en œuvre pour atténuer le risque d'accès aux données du GC ou d'incidence sur la fiabilité des services d'informatique en nuage hébergeant les données du Canada.

33. Sécurité physique (centre de données/installations)

(1) L'entrepreneur doit mettre en place des mesures de sécurité qui assurent la protection des installations de la 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.

(2) L'entrepreneur doit veiller à ce que les installations du centre de données qui abritent des données du Canada utilisent une approche fondée sur les risques et reposant sur la prévention, la détection, l'intervention et la récupération, conformément aux mesures et aux pratiques en matière de sécurité physique figurant dans la Directive sur la gestion de la sécurité du Conseil du Trésor (https://www.tbs-sct.canada.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 et entre les installations de l'entrepreneur, qui sont notamment suffisamment disparates sur le plan géographique pour que la perte d'une installation n'empêche pas la récupération des données du Canada conformément aux engagements de niveau de service prescrits;

(ii) l'utilisation adéquate des supports de la 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 périphériques 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 points de prestation des services au personnel des services d'informatique en nuage autorisé en fonction du poste ou du rôle et du principe du besoin d'accès, validé par deux formes d'identification;

(vi) l'accompagnement 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 prestation des services 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 vidéosurveillance dans toutes les zones fragiles, ainsi que de mécanismes de détection des intrusions;

(ix) effectuer des vérifications de sécurité continues aux limites des points de service et des installations pour détecter l'exfiltration non autorisée d'information ou de composants de système.

(3) À la demande du Canada, l'entrepreneur doit produire un document qui décrit ses mesures de sécurité physique.

(4) Si des changements apportés aux mesures de sécurité physique sont susceptibles de compromettre considérablement la sécurité physique, l'entrepreneur doit en informer le Canada.

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

(1) L'entrepreneur doit s'engager à fournir les renseignements nécessaires au Canada pour effectuer une évaluation de la sécurité de la chaîne d'approvisionnement, y compris les renseignements sur la structure de propriété, l'enregistrement de l'entreprise, les investisseurs et les dirigeants, les fournisseurs, les sous-traitants, les relations avec les tiers et tout autre renseignement nécessaire à une telle évaluation.

(2) L'entrepreneur doit appuyer l'évaluation de la sécurité de la chaîne d'approvisionnement en fournissant des informations sur les équipements, les microprogrammes, les logiciels ou tout autre système, selon les besoins.

(3) L'entrepreneur doit prendre et maintenir des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de la TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de la TI servant à offrir les services d'informatique en nuage. Cela comprend, sans s'y limiter, la protection tout au long du cycle de développement des systèmes par la conception et la mise en œuvre de mesures visant à atténuer et à contenir les risques liés à la sécurité des données au moyen d'une séparation appropriée des tâches, d'un accès fondé sur les rôles et d'un accès selon le moindre privilège pour tout le personnel de la chaîne d'approvisionnement; la sensibilisation aux menaces, la formation de l'effectif responsable des acquisitions sur les menaces, les risques et les mesures de sécurité requis; et l'obligation pour les entités de la chaîne d'approvisionnement de mettre en œuvre les mesures de protection nécessaires.

(4) L'entrepreneur doit disposer d'une approche de la gestion des risques liés à la chaîne d'approvisionnement (GRCA), y compris un plan de gestion des risques liés à la chaîne d'approvisionnement orienté en fonction de l'une des pratiques exemplaires suivantes :

a. ISO/IEC 27036 Technologie de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4).

b. NIST Special Publication 800-161 — Supply Chain Risk Management Practices for Federal Information Systems and Organizations (pratiques de gestion des risques liés à la chaîne d'approvisionnement pour les organisations et les systèmes d'information fédéraux).

c. Mesure de sécurité ITSG-33 pour SA-12 lorsque les garanties de sécurité définies sont documentées dans un plan de GRCA.

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

(5) Présenter une preuve selon laquelle 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.

(6) L'entrepreneur doit fournir au Canada une copie du plan de GRCA tous les ans ou sur demande.

(7) Si l'entrepreneur est un fournisseur SaaS qui utilise un fournisseur IaaS approuvé par le GC qui se conforme déjà aux exigences de la section 34 – Gestion des risques de la chaîne d'approvisionnement, dans les 90 jours suivant l'attribution du contrat, le fournisseur SaaS qui utilise un fournisseur IaaS approuvé par le GC doit fournir une liste des produits de technologie de l'information et des communications (TIC) décrivant l'équipement des TIC qui est déployée dans l'environnement du fournisseur IaaS approuvé par le GC aux fins d'un examen de l'intégrité de la chaîne d'approvisionnement (ICA). Cet examen de l'intégrité de la chaîne d'approvisionnement sera effectué au plus tôt tous les trois ans.

35. Sous-traitants

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

(2) L'entrepreneur doit fournir une liste des sous-traitants dans les dix jours suivant la date d'entrée en vigueur du contrat. Le fournisseur doit 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.

(3) L'entrepreneur doit mettre en œuvre des politiques et des procédures écrites conçues pour assurer la sécurité des systèmes d'information et des données du Canada qui sont destinées à des sous-traitants, ou qui sont détenues par ceux-ci. Ces politiques et procédures doivent porter, dans la mesure du possible, sur les points suivants :

(a) l'identification et l'évaluation des risques des sous-traitants;

(b) les pratiques minimales en matière de cybersécurité auxquelles ces sous-traitants doivent se conformer pour pouvoir faire affaire avec l'entrepreneur;

(c) la confirmation du respect des obligations en matière de sécurité;

(d) les processus de diligence raisonnable utilisés pour évaluer l'adéquation des pratiques de cybersécurité de ces sous-traitants et/ou sous-traitants;

(e) l'évaluation périodique de ces sous-traitants en fonction du risque qu'ils présentent et du maintien de l'adéquation de leurs pratiques en matière de cybersécurité.

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

(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, avec des mesures approuvées de protection des documents au niveau PROTÉGÉ B, délivrée par le Programme de sécurité des contrats (PSC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

(2) CHAQUE membre du personnel de l'entrepreneur ou de l'offrant qui nécessite un accès à des renseignements, des biens ou des lieux de travail PROTÉGÉS doit détenir une attestation de sécurité valide au niveau SECRET ou
COTE DE FIABILITÉ, selon les exigences du guide de sécurité, accordée ou approuvée par le PSC de TPSGC.

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

(4) Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE DOIVENT PAS être attribués sans l'autorisation écrite préalable du PSC de TPSGC.

(5) L'entrepreneur ou l'offrant doit respecter les dispositions suivantes :

(a) de la Liste de vérification des exigences relatives à la sécurité et de la Directive sur la sécurité (s'il y a lieu), reproduite ci-joint à l'annexe B et à l'annexe C;

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

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

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

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

L'administration désignée en matière de sécurité canadienne (ADS canadienne) pour les questions de sécurité industrielle au Canada est le Secteur de la sécurité industrielle (SSI), Services publics et Approvisionnement Canada (SPAC), administrée par la Direction de la sécurité industrielle internationale (DSII), SPAC. L'ADS canadienne est chargée d'évaluer la conformité des entrepreneurs et sous-traitants aux exigences en matière de sécurité pour les fournisseurs étrangers. Les exigences suivantes en matière de sécurité s'appliquent aux entrepreneurs et sous-traitants destinataires étrangers constitués en société ou autorisés à faire des affaires ailleurs qu'au Canada et qui fournissent ou exécutent à l'extérieur du Canada les services d'informatique en nuage décrit dans les solutions d'informatique en nuage, en plus des exigences en matière de confidentialité et de sécurité. Ces exigences en matière de sécurité

s'ajoutent aux exigences figurant dans la section intitulée « Protection et sécurité des données stockées dans des bases de données ».

(1) **L'entrepreneur ou le sous-traitant** atteste que la prestation et l'approvisionnement des services d'informatique en nuage en vertu des modalités du présent contrat seront exécutés dans un pays de l'Organisation du Traité de l'Atlantique Nord (OTAN), un pays de l'Union européenne (UE) ou un pays avec lequel le Canada dispose d'un dispositif bilatéral de sécurité internationale. Dans le cadre du Programme de sécurité des contrats (PSC), des accords internationaux bilatéraux en matière de sécurité ont été conclus avec les pays énumérés sur le site Web de SPAC : https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html), tel qu'il est mis à jour de temps à autre.

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

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

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

(5) L'entrepreneur ou le sous-traitant destinataire étranger doit désigner un agent de sécurité des contrats (ASC) autorisé et un agent remplaçant de sécurité des contrats (ARSC), au besoin, qui sera responsable du contrôle des exigences relatives à la sécurité, telles qu'elles sont définies dans le présent contrat. Cette personne sera désignée par le président-directeur général ou par un cadre supérieur clé désigné de l'entrepreneur ou du sous-traitant destinataire étranger proposant. Les cadres supérieurs clés comprennent les propriétaires, les mandataires, les directeurs, les cadres et les partenaires occupant un poste qui leur permettrait de porter atteinte aux politiques ou aux pratiques de l'organisation durant l'exécution du contrat.

(6) **L'entrepreneur ou le sous-traitant** ne doit pas accorder l'accès aux renseignements et aux biens **PROTÉGÉ B du CANADA**, sauf aux employés ayant un besoin de savoir dans le cadre de l'exécution du **contrat** et qui ont fait l'objet d'une vérification de sécurité conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115), ou doit utiliser des mesures équivalentes acceptables convenues par le Canada.

(7) Les renseignements ou biens de niveau PROTÉGÉ AU CANADA qui sont fournis à l'entrepreneur ou au sous-traitant destinataire étranger ou produits par celui-ci doivent respecter les conditions suivantes :

(a) Ne doivent pas être divulgués à un autre gouvernement, à une autre personne ou à une autre entreprise ou à un représentant de l'un ou de

l'autre qui ne soit pas directement lié à l'exécution du **contrat**, sans l'autorisation écrite préalable du Canada. Cette autorisation doit être obtenue auprès de l'ADS canadienne en collaboration avec l'autorité contractante.

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

(8) **L'entrepreneur ou le sous-traitant** destinataire étranger NE DOIT PAS emporter de renseignements ou d'actifs **PROTÉGÉS DU CANADA** hors des lieux de travail visés, et **l'entrepreneur ou le sous-traitant** destinataire étranger doit veiller à ce que son personnel soit au courant de cette restriction et qu'il la respecte.

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

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

(11) L'entrepreneur étranger destinataire devra signaler immédiatement à l'ADS canadienne tous les cas pour lesquels il sait où a lieu de croire que des renseignements ou des biens PROTÉGÉS AU CANADA relatif à l'exécution du contrat ou contrat de sous-traitance ont été compromis.

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

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

(14) Dans le cadre du présent contrat, l'entrepreneur destinataire étranger qui doit avoir accès à des renseignements ou à des biens PROTÉGÉS DU CANADA ou à des sites canadiens à accès restreint doit présenter une demande d'accès au site au dirigeant principal de la sécurité de nom du ministère ou de l'organisation du Canada.

(15) L'entrepreneur destinataire étranger NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker dans un système de la TI (et transférer au moyen d'un lien électronique) des renseignements de niveau PROTÉGÉ B AU CANADA avant que l'ADS canadienne lui en donne le droit.

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

(17) Tous les contrats de sous-traitance attribués à un destinataire étranger tiers 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 destinataire étranger tiers NE DOIVENT PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne afin de confirmer les exigences en matière de sécurité qui seront imposées aux sous-traitants.

(19) **L'entrepreneur ou le sous-traitant** destinataire étranger doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'annexe B et C.

(20) Nonobstant toute disposition des conditions générales concernant la sous-traitance, l'entrepreneur destinataire étranger ne doit pas sous-traiter (y compris à une société affiliée) une fonction qui consiste à fournir à un sous-traitant l'accès à des données relatives au contrat, à moins que l'autorité contractante (en collaboration avec l'ADS canadienne) n'y consente au préalable par écrit.

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

38. Transport et transmission physiques de l'information

(1) L'entrepreneur doit mettre en place des mesures pour protéger l'information du Canada sous sa forme physique, y compris les biens à l'arrêt (p. ex., utilisés ou entreposés), les biens en transit (p. ex., transportés ou transmis) et ceux qui sont détruits au moyen d'une méthode appropriée. Cela comprend notamment :

(a) Veiller à ce que les dispositifs portatifs de stockage de données soient adéquatement sécurisés en tout temps, selon le niveau de classification de sécurité le plus élevé de l'information qui y est entreposée, dans un contenant de sécurité approprié tel que défini dans le chapitre 6 du manuel de sécurité des contrats du CSPP :

Traitement et protection de l'information et des actifs - Manuel de sécurité des contrats - Exigences de sécurité pour les contrats avec le gouvernement du Canada - Filtrage de sécurité - Sécurité nationale - Sécurité nationale et défense - canada.ca (tpsgc-pwgsc.gc.ca) et annexe C :

(b) Lignes directrices pour la sauvegarde des informations et des actifs.

(c) Chiffrer toute l'information du Canada stockée sur des dispositifs portatifs de stockage de données à l'aide d'un module de chiffrement certifié par le Programme de validation des modules cryptographiques et conformément à la section 17 – Protection cryptographique, y compris l'utilisation de produits accrédités par le Programme canadien lié aux Critères communs.

(d) Avant de connecter le dispositif au réseau de la TI du Canada aux fins du transfert unidirectionnel de renseignements des réseaux de la TI du Canada vers le dispositif, veiller à ce que le dispositif soit balayé pour détecter la présence de maliciels chaque fois qu'il est connecté à l'infrastructure de la TI du Canada.

(e) Veiller à ce que tous les dispositifs portatifs utilisés pour transporter l'information du Canada soient supprimés du dispositif afin d'empêcher la récupération de l'information, conformément aux exigences de nettoyage des supports énoncées à la section 16 (1) – Élimination des données et remise des documents au Canada.

(2) Les renseignements protégés sont considérés comme « en cours de transmission » jusqu'à ce qu'ils soient arrivés au centre de données de l'entrepreneur ou sortis de l'enveloppe. S'ils sont sortis de l'enveloppe, les renseignements doivent être protégés, conformément à la section 33 – *Sécurité physique*, et au chapitre 6 du manuel de sécurité des contrats du PSPC : Traitement et protection de l'information et des actifs - Manuel de sécurité des contrats - Exigences de sécurité pour les contrats avec le gouvernement du Canada - Filtrage de sécurité - Sécurité nationale - Sécurité nationale et défense – canada.ca (tpsgc-pwgsc.gc.ca) et annexe C : Lignes directrices pour la sauvegarde des informations et des actifs.

(3) Le contractant doit signaler toute perte ou vol réel ou suspecté de dispositifs de stockage de données portables, conformément à l'article 29 - Réponse aux incidents de sécurité, et au chapitre 6 du manuel de sécurité des contrats du CPS :
Traitement et protection de l'information et des actifs - Manuel de sécurité des contrats – Exigences de sécurité pour les contrats avec le gouvernement du Canada - Filtrage de sécurité - Sécurité nationale – Sécurité nationale et défense – canada.ca (tpsgc-pwgsc.gc.ca) et annexe C :

Lignes directrices pour la sauvegarde des informations et des actifs.

Annexe A – Appendice 2 – Obligations en matière de protection des renseignements personnels pour les services commerciaux d'informatique en nuage (jusqu'au niveau Protégé B inclusivement)

1. Généralités

1.1 *Objet*

Le présent appendice a pour objet d'énoncer les obligations de l'entrepreneur en matière de protection de la vie privée en ce qui a trait à l'utilisation, au recueil, au traitement, à la transmission, au stockage ou à l'élimination des données du Canada contenant des renseignements personnels. Tous les renseignements personnels qui sont stockés dans les systèmes de l'entrepreneur ou que l'entrepreneur est tenu de traiter (recueillir, conserver, utiliser, divulguer et éliminer) doivent être protégés en tout temps. Cela suppose la mise en place des mesures de protection administratives, physiques et techniques nécessaires pour garantir la protection des renseignements personnels en fonction du préjudice qui pourrait être subi en cas d'atteinte à la vie privée et conformément à l'accord de traitement des données de l'entrepreneur, au présent appendice et aux mesures spécifiques de protection de la vie privée de l'entrepreneur (collectivement, les « **obligations en matière de protection de la vie privée** »).

1.2 *Transfert des obligations en matière de protection des renseignements personnels*

Les obligations de l'entrepreneur contenues dans les présentes obligations en matière de protection des renseignements personnels doivent être transférées par l'entrepreneur à ses sous-traitants dans la mesure où elles s'appliquent à eux.

1.3 *Gestion du changement*

L'entrepreneur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir à jour les obligations en matière de protection des renseignements personnels afin de se conformer aux pratiques de sécurité des normes de l'industrie.

L'entrepreneur doit informer le Canada de tous les changements qui nuisent ou qui pourraient nuire aux services infonuagiques offerts dans le cadre du présent contrat, y compris les changements ou les améliorations de nature technologique, administrative ou autre qui sont apportés et qui pourraient avoir une incidence sur le recueil, l'utilisation, la divulgation et l'élimination actuels des données contenant 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.

2. Reconnaissance

Les parties reconnaissent ce qui suit :

(a) Toutes les données du Canada contenant des renseignements personnels sont soumises à ces obligations en matière de protection de la vie privée.

(b) Nonobstant toute autre disposition du présent appendice, 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 en sa possession ou tenter d'avoir en sa possession des données du Canada ni permettre à aucun membre de son personnel d'y avoir accès avant que ne soient instaurées les obligations en matière de protection des renseignements personnels prévues par le présent appendice, au plus tard à la date d'attribution du contrat.

3. Propriété des données

(1) Le Canada demeurera en tout temps le responsable des renseignements personnels traités par l'entrepreneur dans le cadre du contrat. Le Canada est chargé d'assurer le respect des obligations en matière de protection de la vie privée à titre de responsable du traitement en vertu des lois applicables en matière de protection des données, en particulier en ce qui concerne la justification de toute transmission de renseignements personnels à l'entrepreneur (y compris la fourniture de tous les avis requis et l'obtention de tous les consentements et/ou autorisations nécessaires, ou l'obtention de tout autre fondement juridique approprié en vertu de la loi applicable sur la protection des données), et des décisions et des mesures du Canada concernant le traitement de ces données personnelles.

(2) L'entrepreneur est et demeurera en tout temps un préposé au traitement en ce qui concerne les données contenant des renseignements personnels qui lui sont fournies par le Canada en vertu du contrat. L'entrepreneur est responsable de respecter ses obligations conformément à l'accord de traitement des données de l'entrepreneur et à ses obligations en tant que sous-traitant en vertu des lois applicables en matière de protection des renseignements personnels (c.-à-d. la *Loi sur la protection des renseignements personnels et les documents électroniques* [LPRPDE] et la *Loi sur la protection des renseignements personnels*).

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

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

4. Demandes d'accès aux 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 civils suivant l'attribution du contrat, l'entrepreneur doit fournir un document décrivant comment il aidera le Canada à traiter les demandes d'accès; notamment comment il accusera réception d'une demande d'accès et comment il fournira l'information demandée.

5. Assurance d'une tierce partie : Attestations

(1) L'entrepreneur doit s'assurer que, en ce qui a trait à tout renseignement personnel, y compris les données du Canada, celui-ci peut héberger, stocker ou traiter des données sur son infrastructure [y compris tout service d'infrastructure comme service (IaaS), de plateforme comme service (PaaS) ou de logiciel comme service (SaaS) fourni au Canada] et que les emplacements de ses services sont protégés par des mesures de protection de la vie privée et de sécurité appropriée qui

respectent les exigences énoncées dans les pratiques et politiques de l'entrepreneur en matière de protection de la vie privée.

(2) L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications suivantes en fournissant des rapports d'évaluation ou des certifications de tiers indépendants qui portent sur chaque couche de service (p. ex. IaaS, PaaS et SaaS) au sein de l'offre de services infonuagiques, notamment :

(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 fournie doit :

(i) indiquer la raison sociale légale de l'entrepreneur ou du sous-traitant concerné;

(ii) indiquer la date de certification de l'entrepreneur ou du sous-traitant et l'état de cette certification;

(iii) indiquer les services compris dans le champ d'application du rapport de certification. Si la méthode déterminée est utilisée pour exclure des sous-traitants proposant des services comme l'hébergement de centres de données, le rapport d'évaluation du sous-traitant doit être inclus.

(4) Chaque vérification doit faire l'objet d'un rapport qui sera mis à la disposition du Canada. Les certifications doivent être accompagnées d'éléments de preuve à l'appui, comme le rapport d'évaluation ISO élaboré pour valider la conformité avec la certification ISO, et elles doivent clairement divulguer toutes les constatations importantes du vérificateur. L'entrepreneur doit régler rapidement tout problème soulevé dans un rapport de vérification, à la satisfaction du vérificateur.

(5) L'entrepreneur est censé maintenir sa certification ISO 27018 pendant 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 documents pouvant être raisonnablement exigés pour démontrer que l'entrepreneur possède des certifications à jour.

6. Conformité en matière de protection des renseignements personnels

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

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

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

7. Vérification de la conformité

(1) Si le Canada doit procéder à des vérifications de sécurité et de protection des renseignements personnels, à des inspections ou à un examen de toute information supplémentaire (p. ex. documentation, flux de données, description de la protection des données, architecture des données et descriptions de sécurité), les deux parties conviennent de négocier une solution de bonne foi et d'examiner les motifs de la demande du Canada ainsi que les processus et protocoles de l'entrepreneur.

(2) L'entrepreneur doit effectuer les vérifications de la confidentialité et de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter les données du Canada contenant des renseignements personnels, de la manière 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 tiers qualifiés, indépendants, et qui (i) sont qualifiés selon l'American Institute of Certified Public Accountants (AICPA) ou CPA Canada (Comptables professionnels agréés du Canada) ou selon le régime de certification ISO, et (ii) respectent la norme ISO/CEI 17020 sur les systèmes de gestion de la qualité au choix 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 énoncer clairement toutes les constatations importantes faites par le vérificateur externe. 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 donnent une description complète du système, notamment 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 aux certifications requises de l'industrie.

8. Protection des renseignements personnels dès la conception

L'entrepreneur doit démontrer qu'il met en œuvre une protection de la vie privée dès la conception au cours du cycle de vie du développement de son logiciel, conformément à l'appendice 1 – Obligations en matière de sécurité, section 20 (Développement sécurisé).

9. Agent de protection de la vie privée

(1) 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 des renseignements personnels chargé d'agir à titre de représentant de l'entrepreneur pour toutes les questions liées aux

renseignements personnels et aux enregistrements. 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.

10. Aide à l'évaluation des facteurs relatifs à la vie privée du Canada

(1) L'entrepreneur doit assister le Canada pour la création d'une évaluation des facteurs relatifs à la vie privée 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 l'aidant à produire la documentation à l'appui, y compris une évaluation des facteurs relatifs à la vie privée (EFVP) de base pour le Canada fournie par l'entrepreneur. L'entrepreneur s'engage à 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 du Canada.

11. Atteinte à la vie privée

(1) L'entrepreneur, s'il soupçonne ou constate un accès ou un traitement non autorisé de renseignements personnels (« **incident** »), doit évaluer cet incident et y réagir rapidement. Dans la mesure où l'entrepreneur prend connaissance d'un incident et détermine qu'il s'agit d'une atteinte à la vie privée entraînant un détournement ou une destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès à des renseignements personnels transmis, stockés ou autrement traités dans ses systèmes ou dans l'environnement des services infonuagiques qui compromettent la sécurité, la confidentialité ou l'intégrité de ces renseignements personnels (« atteinte à la vie privée »), il informera le Canada de cette atteinte sans retard indu et conformément à la section 29 de l'appendice 1 – Obligations en matière de sécurité.

(2) L'entrepreneur doit :

(a) **En cas d'atteinte à la vie privée suspectée ou avérée, tenir un registre des atteintes et fournir au gouvernement du Canada les informations suivantes :**

i. La date de l'atteinte ou la période où l'atteinte s'est produite; et la date de sa découverte;

ii. Une description de l'atteinte, y compris le type et la cause;

iii. Le nombre de personnes touchées ou une approximation de ce nombre;

iv. Les éléments de renseignements personnels en cause;

v. Une description des mesures de protection pertinentes qui étaient en place;

vi. Toutes les mesures correctives, y compris toutes les mesures pour limiter l'atteinte et toutes les mesures d'atténuation et de prévention, qui ont été ou qui seront prises;

vii. La méthode utilisée pour aviser les personnes dont les renseignements personnels ont été touchés, ou une justification au cas où les personnes, dont les renseignements personnels, ont été touchées ne serait pas avisée;

viii. Le lieu physique ou géographique où l'atteinte s'est produite;

ix. Une liste de toutes les organisations qui ont été notifiées de l'atteinte;

x. **La procédure de récupération des données;**(b) Suivre ou permettre au Canada de suivre les divulgations de données du Canada, y compris le type de données divulguées, les personnes y ayant eu accès et le moment où l'incident s'est produit.

12. Renseignements personnels

Les sous-sections qui suivent s'appliquent aux situations où l'entrepreneur confirme qu'il a accès aux données du Canada, et qu'il en assure la garde et le contrôle.

12.1 Propriété des dossiers et renseignements personnels

(1) Pour exécuter les services infonuagiques, l'**entrepreneur ou le sous-traitant** destinataire étranger recevra ou recueillera des renseignements personnels auprès de tiers. **L'entrepreneur ou le sous-traitant** destinataire étranger reconnaît qu'il n'a aucun droit sur les dossiers et renseignements personnels et que le Canada est propriétaire des dossiers. 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.

12.2 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 fournir les services infonuagiques conformément au **contrat**.

12.3 Cueillette des renseignements personnels

(1) Si **l'entrepreneur ou le sous-traitant** étranger destinataire doit obtenir des renseignements personnels d'un tiers dans le cadre de la fourniture des services infonuagiques, il ne doit recueillir que les renseignements personnels lui permettant de fournir ces services. L'entrepreneur ou le sous-traitant étranger destinataire doit recueillir les renseignements personnels auprès de la personne concernée et l'informer (au moment de la collecte 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 lui seront décrits;

(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 seront mentionnés;

(d) Les conséquences, le cas échéant, du refus de fournir les renseignements seront énoncées;

(e) L'intéressé a le droit d'accéder à ses renseignements personnels et d'y apporter des corrections;

(f) Les renseignements personnels font partie d'un fichier de renseignements personnels particulier (au sens de la *Loi sur la protection des renseignements personnels*) et fournissent à la personne des renseignements sur l'institution fédérale qui contrôle ce fichier de renseignements personnels, si l'autorité contractante a fourni ces renseignements à l'**entrepreneur ou au sous-traitant** destinataire étranger.

(2) L'**entrepreneur ou le sous-traitant** destinataire étranger et ses employés respectifs doivent se faire connaître des personnes auprès desquelles ils recueillent des renseignements personnels et leur donner un moyen de vérifier qu'elles sont autorisées à recueillir les renseignements personnels dans le cadre d'un contrat avec le Canada.

(3) À la demande de l'autorité contractante, l'entrepreneur ou le sous-traitant destinataire étranger doit préparer un formulaire de demande de consentement à utiliser pour la collecte de renseignements personnels ou un script pour la collecte de renseignements personnels par téléphone. **L'entrepreneur ou le sous-traitant** étranger destinataire ne peut utiliser le formulaire ou le script 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 script.

(4) Si, au moment où il demande des renseignements personnels à une personne, l'**entrepreneur ou le sous-traitant** destinataire étranger doute que la personne a la capacité de consentir à la divulgation et à l'utilisation de ses renseignements personnels, il doit demander des instructions à l'autorité contractante.

12.4 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 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 :

(a) S'abstenir d'utiliser des données d'identification personnelle (p. ex. numéro d'assurance sociale) pour coupler des bases de données multiples contenant des renseignements personnels;

(b) Isoler tous les dossiers de ses propres dossiers et renseignements;

(c) Ne donner l'accès aux dossiers et renseignements personnels qu'à ceux qui en ont besoin pour assurer les services infonuagiques (p. ex. en utilisant des mots de passe ou un accès biométrique);

(d) Offrir de la formation à toute personne à qui **l'entrepreneur ou le sous-traitant** destinataire étranger donne accès aux renseignements personnels sur l'obligation d'assurer la confidentialité et de ne l'utiliser qu'aux fins d'assurer les services infonuagiques. **L'entrepreneur ou le sous-traitant** destinataire étranger 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 auxquelles **l'entrepreneur ou le sous-traitant** destinataire étranger donne 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 une personne de révision de ses renseignements personnels et de toutes les demandes de correction d'erreurs ou d'omissions concernant les renseignements personnels (que les demandes soient faites directement par une personne ou par le Canada au nom d'une personne);

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

(h) Tenir un registre de la date et de l'auteur de la dernière mise à jour de chaque dossier;

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

(j) Sécuriser et contrôler l'accès à tout exemplaire papier des dossiers.

12.5 Protection des renseignements personnels

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

12.6 Obligations réglementaires

(1) **L'entrepreneur ou le sous-traitant** destinataire étranger comprend que le Canada est tenu de traiter les dossiers et renseignements personnels conformément aux dispositions de la *Loi sur la protection des renseignements personnels*, L.R.C., 1985, ch. P-21, de la *Loi sur l'accès à l'information*, L.R.C., 1985, ch. A-1, et de la *Loi sur la Bibliothèque et les Archives du Canada*, L.C. 2004, ch. 11. **L'entrepreneur ou le sous-traitant** étranger destinataire convient de se conformer à toute exigence requise établie par l'autorité contractante pour permettre au Canada de remplir ses obligations en vertu de ces lois et de toute autre loi qui entre en vigueur.

(2) **L'entrepreneur ou le sous-traitant** étranger destinataire reconnaît que ses obligations aux termes du contrat s'ajoutent à toute obligation qu'il a en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, ou une loi semblable qui entre 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 la disposition législative avec laquelle il y a conflit selon lui.

12.7 Obligation juridique de divulguer les renseignements personnels

(1) Si l'entrepreneur reçoit une assignation à témoigner ou une ordonnance judiciaire, administrative ou arbitrale d'une agence exécutive ou administrative, d'un organisme de réglementation ou de toute autre autorité gouvernementale qui concerne le traitement des renseignements personnels (« demande de divulgation »), il doit transmettre rapidement cette demande de divulgation au Canada sans y répondre, à moins que la loi applicable ne l'exige (y compris pour fournir un accusé de réception à l'autorité qui a fait la demande de divulgation).

(2) À la demande du Canada, l'entrepreneur fournira au Canada les renseignements raisonnables en sa possession qui pourraient répondre à la demande de divulgation et toute l'aide raisonnablement requise pour que le Canada puisse répondre à la demande de divulgation en temps opportun.

12.8 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* ou de la *Loi sur la protection des renseignements personnels* ou de toute autre loi pertinente concernant les renseignements personnels. Les parties conviennent de s'échanger toute information nécessaire pour faciliter le règlement de la plainte et de s'informer immédiatement l'une l'autre de son dénouement.

12.9 Exception

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

Annexe B – Énoncés des défis

L'Énoncé des défis n'a pas été modifié depuis la publication initiale de la SPD. Des discussions auront lieu avec les fournisseurs préqualifiés.

Énoncés du problème, défis et les résultats liés à l'IaaS[6]*

Contexte

Le gouvernement du Canada (GC) a besoin d'accéder à des services infonuagiques publics commercialement disponibles (« services infonuagiques ») pour répondre à ses besoins opérationnels dans un large éventail d'organisations gouvernementales. Afin d'aider les organisations à répondre aux attentes de la population canadienne et pour fournir des services et des avantages gouvernementaux en toute simplicité et de manière sûre et efficace, le Canada souhaite obtenir l'accès à des services infonuagiques commercialement disponibles, ainsi qu'à les fournir à divers niveaux de classification des données.

Le GC doit créer un écosystème de sécurité numérique d'entreprise sécurisée et résilient pour continuer à offrir les services dont la population canadienne dépend aujourd'hui, tout en accélérant l'évolution du Canada vers des services modernes sécurisés, fiables, axés sur l'utilisateur et exempt d'obstacle tout en répondent au besoin de confidentialité et de transparence[i]. Ceci est essentiel pour maintenir la confiance à l'égard des institutions du Canada.

Portée

La portée du contrat subséquent consiste à résoudre le problème, à relever les défis et à produire les résultats. La portée restera stable pendant la durée de vie du contrat, mais la façon dont les services infonuagiques seront rendus peut évoluer.

Énoncé du problème et des défis

Énoncé du problème

Le Canada n'a pas la capacité de déployer son infrastructure numérique avec agilité et rapidité, ni d'évoluer et de tirer parti des technologies émergentes pour avancer sa prestation de services aux Canadiens.

Défis

L'environnement d'application du Canada est caractérisé par une infrastructure existante vieillissante qui limite sa capacité à faire progresser son programme numérique. Combinez cela à un grand ensemble de données de nature délicate qui auraient, si elles sont compromises, des répercussions importantes sur la sécurité et la protection des renseignements personnels de la population canadienne, du GC et des parties prenantes.

Les défis suivants limitent la capacité du Canada à résoudre le problème :

a. La complexité liée à une forte dépendance aux systèmes existants et à une infrastructure vieillissante.

[6] *À défaut d'avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

b. La difficulté à composer avec les fluctuations de la demande et à adapter les services sur site en temps opportun.
c. La complexité d'intégrer les services infonuagiques dans les services sur site et de les connecter entre eux.
d. L'application des normes strictes du GC en matière de sécurité et de protection des renseignements personnels, de même que des politiques et règlements du gouvernement.
e. La capacité limitée à prévoir et à gérer le coût des services infonuagiques en raison du manque de visibilité au niveau de l'organisation en ce qui a trait aux consommations et coûts de service détaillés.
f. Le recrutement, la conservation et la formation des professionnels qualifiés nécessaires pour mettre en œuvre des services infonuagiques en constante évolution.

Résultats escomptés du contrat

Le GC doit continuer de relever les défis de la modernisation numérique et de composer avec les risques liés à ses systèmes de TI vieillissants pour offrir des avantages à long terme à toutes les personnes et entreprises qu'il dessert, y compris les employés du GC. La capacité du gouvernement d'offrir à la fois d'importantes modernisations techniques et des améliorations itératives est essentielle pour améliorer l'expérience vécue par les Canadiens dans l'ère numérique.

Dans le cas du premier incrément, le Canada s'attend à fournir des technologies fondées sur des solutions de plateformes infonuagiques hautement évolutives qui facilitent la transformation plus rapide d'idées en valeur, une sécurité robuste et des mécanismes de conformité, de même que la prévisibilité financière.

Le GC doit continuer d'offrir un environnement de prestation de services internes interopérables, sûrs et fiables et qui respectent la confidentialité et d'applications opérationnelles hébergées dans des environnements infonuagiques. Cela permettra l'amélioration continue de la prestation de services numériques du Canada pour répondre à l'évolution de ses besoins, de son ambition et de ses engagements.

[i] Ambition numérique - Canada.ca

EMV liées à l’approvisionnement d’IaaS* et de PaaS[7] native

ÉBAUCHE DE TRAVAIL

Les EMV feront l’objet de discussion avec les fournisseurs préqualifiés.

Exigences minimales viables (EMV)

Les sections ci-dessous décrivent les capacités minimales attendues de la solution. La présente ébauche décrit ce que la solution doit être en mesure d’accomplir (exigences fonctionnelles) et la façon dont elle doit interagir avec l’environnement et les autres appareils (exigences non fonctionnelles). Les EMV sont obligatoires.

[7] *À défaut d’avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

1. Généralité

1.1. Le soumissionnaire doit offrir des services disponibles sur le marché, accompagnés de documentation accessible publiquement. Ces services doivent également venir avec un soutien complet, y compris de l'assistance technique, des accords de niveau de service (SLA) définis et des mises à jour régulières.

2. Calcul

2.1. La solution doit comporter des instances de calcul afin d'offrir des ressources informatiques permettant d'exécuter des applications et des charges de travail dans le nuage.

3. Stockage

3.1. La solution doit comprendre des capacités évolutives de stockage de blocs, d'objets et de fichiers.

4. Tableaux de bord opérationnel et de sécurité, rapports et journaux

4.1. La solution doit comprendre un tableau de bord centralisé pour accéder à l'information et aux mesures permettant de surveiller l'infrastructure et les charges de travail et de produire des rapports sur celles-ci, y compris : l'état de santé, la posture de sécurité, ainsi qu'un tableau de bord de la conformité.

5. Configurations automatisées centralisées

5.1. La solution doit pouvoir être configurée et être consommable au moyen de l'infrastructure en tant que code (IaC) que ce soit par le biais d'un système d'automatisation natif ou d'une solution fournie par une tierce partie.

5.2. La solution doit être en mesure d'être intégrée dans les services et les systèmes qui utilisent un système d'interface de programmation d'applications (API).

6. Exigences en matière de résilience

6.1. Il doit y avoir au moins deux régions géographiquement redondantes et deux centres de données par région pour permettre un basculement transparent de l'un à l'autre sans incidence importante sur les activités et la gestion de tout cela ne doit nécessiter aucune contribution opérationnelle du GC.

6.2. La solution doit comprendre des mécanismes de redondance et de basculement à divers niveaux des IaaS* et des PaaS[8], y compris au niveau du calcul, du stockage et du réseautage, afin d'atténuer les points de défaillance uniques.

7. Évolutivité

7.1. La solution doit être en mesure d'adapter les ressources horizontalement et verticalement pour répondre à la hausse de la demande sans que cela n'entraîne une dégradation des services, y compris des politiques de mise à l'échelle automatique, un équilibrage de charge élastique et une planification de la capacité.

8. Capacité du réseau

[8] *À défaut d'avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

8.1. La capacité du réseau fait référence à la quantité de ressources réseau et de bande passante disponibles dans l'environnement d'IaaS[9] qui détermine la quantité de données pouvant être transférées entre les machines virtuelles (MV), les ressources de stockage et les autres composants à l'autre au sein de l'infrastructure.

8.2. Le réseau de la solution doit se connecter conformément aux exigences du SC2G (Secure-Cloud-to-Ground) du GC.

9. Capacités en termes de pare-feu natifs et tiers

9.1. La solution doit comprendre une capacité de pare-feu natif qui peut être configurée de manière à gérer les groupes de sécurité.

9.2. La solution doit être en mesure d'utiliser des pare-feu et des appareils de sécurité tiers (p. ex., Fortinet et F5).

9.3. La solution doit comprendre un pare-feu d'applications Web (WAF) pour protéger les applications Web contre diverses menaces et attaques en ligne.

9.4. La solution doit comprendre un système de détection des intrusions (SDI) comme mécanisme de sécurité qui surveille les activités du réseau ou du système à la recherche de signes d'accès non autorisés, de violations des politiques de sécurité et de comportements suspects.

10. Étiquetage/identification des biens

10.1. La solution doit comporter un mécanisme d'étiquetage pour tous les biens et services.

11. Contrôle administratif des accès par authentification multifacteur (AMF)

11.1. La solution doit sécuriser l'accès au portail et à l'API à l'aide de l'authentification multifacteur (AMF) par le biais de son système de gestion des identités et de l'accès (IAM) natif.

12. Surveillance antimenace et évaluation de la vulnérabilité

12.1. La solution doit fournir un service de détection des menaces qui surveille continuellement la présence de menaces possibles.

12.2. La solution doit avoir un service qui évalue les instances de calcul concernant les menaces et les vulnérabilités en matière de sécurité.

13. Connectivité

13.1. La solution doit permettre aux protocoles SSL (couche de sockets sécurisés) et TLS (sécurité de la couche transport) de sécuriser la transmission de données.

13.2. La solution doit fournir un REST-API sécurisé pour l'intégration des applications et l'échange de données en ce qui a trait aux sources internes et externes à la solution.

14. Contrôles financiers

14.1. La solution doit comprendre des contrôles financiers en ce qui concerne les dépenses globales et des mécanismes qui empêchent des éléments en particulier d'être utilisés sans obtenir au préalable la permission de l'autorité de SPC qui délègue les pouvoirs.

[9] *À défaut d'avoir des termes en français pour ces abréviations, les anglicismes informatiques communément utilisés en français sont empruntés

Annexe E – Définitions

Terme	Définition
Agent	Un agent autorisé par l'entrepreneur qui peut exécuter une ou plusieurs des tâches suivantes selon les termes du CAT et de tout AT correspondant : 1) Fournir des informations sur la facturation 2) Facturer 3) Fournir des services d'information sur la consommation 4) Recevoir les paiements au nom de l'entrepreneur Un agent n'a pas accès ou ne fournit pas d'accès à Services partagés Canada (SPC) à un compte principal, pas plus qu'il n'a accès à un client locataire, aux données d'un client ou à un compte principal d'un client.
Données du Canada	Informations ou données, y compris tous les fichiers texte, son, vidéo ou image, les logiciels et les métadonnées connexes, quelle qu'est leur forme ou leur format : (A) divulguées par le personnel, les clients, les partenaires, les participants à des coentreprises, les concédants de licence, les vendeurs ou les fournisseurs du Canada par l'entremise de l'utilisation des services d'informatique en nuage; (B) divulguées par les utilisateurs finaux des services d'informatique en nuage; ou (C) recueillies, utilisées, traitées par les services d'informatique en nuage ou stockées à l'intérieur de ceux-ci; qui est directement ou indirectement divulguée à l'entrepreneur ou aux sous-traitants par le Canada ou en son nom, ou par l'utilisation des services d'informatique en nuage, y compris toute information ou donnée à laquelle, (i) l'entrepreneur ou tout sous-traitant obtient l'accès, intentionnellement ou par inadvertance; (ii) qui réside sur tout réseau, système ou matériel utilisé ou géré pour le Canada par l'entrepreneur pour les services d'informatique en nuage et les services de l'entrepreneur, y compris l'infrastructure de l'entrepreneur.

Informatique en nuage	L'informatique en nuage est un modèle qui permet un accès omniprésent, pratique et à la demande à un bassin de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement approvisionné et libéré avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de services. Définition tirée de la définition de l'informatique en nuage de l'Institute of Standards and Technology (NIST), qui figure dans le document SP 800-145, à l'adresse suivante : http://csrc.nist.gov/publications/PubsSPs.html#800-145.
Services d'informatique en nuage	Les services d'informatique en nuage sont des offres de services qui proposent un modèle d'informatique en nuage permettant un accès réseau omniprésent, pratique, et à la demande à un bassin partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peut être rapidement mises à disposition et libéré avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services.
Fournisseur de services d'informatique en nuage (FSIN)	Un fournisseur de services d'informatique en nuage est une entité (qui peut comprendre une ou plusieurs personnes physiques, des sociétés, des sociétés de personnes, des sociétés à responsabilité limitée, etc.) qui fournit le service public en nuage dans son entièreté.
Disponible sur le marché	Un service mis à la disposition du public pour être utilisé ou consommé.
Compromission	Une violation de la sécurité du gouvernement qui inclut, mais n'est pas limitée à : • l'accès non autorisé, la divulgation, la modification, l'utilisation, l'interruption, la suppression ou la destruction de renseignements ou de biens sensibles, entraînant une perte de confidentialité, d'intégrité, de disponibilité ou de valeur; • toute action, conduite, menace ou geste d'une personne à l'égard d'un employé sur le lieu de travail ou d'un individu dans les installations fédérales qui a causé un préjudice ou une blessure à cet employé ou à cet individu; • les événements entraînant une perte d'intégrité ou de disponibilité des services ou des activités du gouvernement. (Référence : Plan ministériel de gestion des événements de cybersécurité du GC.)
Entrepreneur	L'entrepreneur est l'entité (il peut s'agir d'une ou de plusieurs personnes physiques, de sociétés, de partenariats, de partenariats à responsabilité limitée, etc.) qui fournit les services d'informatique en nuage au gouvernement du Canada et à ses partenaires. Il s'agit de l'entité approuvée et désignée comme « entrepreneur » dans le contrat subséquent.

Utilisateur final	Toute personne, ou tout processus de système agissant au nom d'une personne, autorisée par le Canada à accéder aux services d'informatique en nuage.
Actif informationnel	Tout élément de données individuel de ces données du Canada.
Déversement d'informations	Il s'agit d'incidents au cours desquels un bien d'information est placé par inadvertance sur un bien ou un système qui n'est pas autorisé à le traiter (par exemple ITSG-33, IR-9).
Infrastructure sous forme de service (IaaS)	La capacité fournie au consommateur de fournir des ressources de traitement, de stockage, de réseaux et d'autres ressources informatiques fondamentales où le consommateur peut déployer et exécuter des logiciels arbitraires, y compris des systèmes d'exploitation et des applications. Le consommateur ne gère ni ne contrôle l'infrastructure en nuage sous-jacente, mais il a le contrôle des systèmes d'exploitation, du stockage, des applications déployées, et éventuellement un contrôle limité de certains composants de réseau (par exemple, les pare-feu de l'hôte).
Fournisseur de services gérés (FSG)	Un fournisseur du gouvernement du Canada qui offre des services opérationnels ou technologiques pour les programmes et les services du gouvernement du Canada. Les FSG sont souvent considérés comme l'externalisation d'un secteur d'activité sous la responsabilité du GC. Les FSG se chargent souvent de la fourniture d'un secteur d'activité ou d'une partie de la fourniture de technologie. La relation contractuelle entre le GC et un FSG est généralement régie par un accord sur les niveaux de service (ANS). Un FSG peut faire appel à un ou plusieurs fournisseurs de services d'informatique en nuage pour fournir les composants technologiques de ses services, tels que les portails en libre-service, la gestion des dossiers et l'analyse. Le GC n'a pas de relation contractuelle directe avec le FSIN, mais il tient le FSG contractuellement responsable des services du FSIN. Le GC est un consommateur des services du FSG et, à son tour, le FSG est un consommateur des services du FSIN. Autre définition – Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030) – Centre canadien de cybersécurité – Section 1.1
Compte principal	Un compte avec des privilèges de niveau racine pour générer des comptes clients ou des sous-comptes qui permettront aux départements d'accéder à des services d'informatique en nuage publics disponibles dans le marché.
Métadonnées	Informations décrivant les caractéristiques des données, y compris, par exemple, les métadonnées structurelles décrivant les structures de données (par exemple, le format, la

	syntaxe et la sémantique des données) et les métadonnées descriptives décrivant le contenu des données (par exemple, les étiquettes de sécurité de l'information). (Référence : NIST SP 800-53 Rev. 4)
PaaS native	Une PaaS native se définit comme une PaaS soutenue, gérée et exploitée par le FSIN (PaaS de la première partie du FSIN).
Renseignements personnels	Renseignements concernant une personne identifiable et enregistrés sous quelque forme que ce soit, tels que définis à l'article 3 de la *Loi sur la protection des renseignements personnels*. Les exemples incluent, sans s'y limiter, les informations relatives à la race, la nationalité, l'origine ethnique, la religion, l'âge, l'état civil, l'adresse, l'éducation ainsi que les antécédents médicaux, criminels, financiers ou professionnels d'une personne. Les renseignements personnels comprennent également tout numéro ou symbole d'identification, tel que le numéro d'assurance sociale, attribué à une personne. (Référence : https://laws-lois.justice.gc.ca/fra/lois/p-21/section-3.html)
Plateforme sous forme de service (PaaS)	La capacité fournie au consommateur est de déployer sur l'infrastructure en nuage des applications créées ou acquises par le consommateur et créées à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure en nuage sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais il contrôle les applications déployées et éventuellement les paramètres de configuration de l'environnement d'hébergement des applications.
Infrastructure PaaS	Infrastructure de la plateforme gérée par l'entrepreneur et fournie sous forme de service (par exemple, centre de données, réseau, stockage, serveurs, plateforme de virtualisation, système d'exploitation, intergiciel et temps d'exécution), y compris les systèmes, le matériel et les logiciels utilisés pour gérer, exploiter et mettre à disposition l'infrastructure PaaS.
Atteinte à la vie privée	Une atteinte à la vie privée implique la collecte, l'utilisation, la divulgation, la conservation et l'élimination inappropriées ou non autorisées de renseignements personnels.
Processeur	Désigne une personne physique ou morale, une autorité publique, une organisation ou un autre organisme qui traite des renseignements personnels au nom et selon les instructions du Canada.
Services d'informatique en nuage	Informatique en nuage publique : l'infrastructure en nuage est mise à la disposition du grand public pour une utilisation ouverte. Elle peut être détenue, gérée et exploitée par une

	entreprise, un établissement d'enseignement ou une organisation gouvernementale, ou une combinaison de ceux-ci. Il existe dans les locaux du fournisseur de services d'informatique en nuage. Les services publics d'informatique en nuage désignent un ensemble partagé de modèles de services d'informatique en nuage configurables mis à la disposition des utilisateurs en tant que libre-service rapide, à la demande et élastique sur Internet à partir des serveurs d'un fournisseur de services d'informatique en nuage, par opposition aux services fournis à partir des propres serveurs d'une entreprise sur place.
Dossier	Tout document papier ou toute donnée dans un format lisible par machine contenant des renseignements personnels
Gestion des événements	Un événement, une omission ou une situation peut être préjudiciable à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité. Les exemples d'événements liés à la cybersécurité comprennent, sans s'y limiter, la divulgation de nouvelles vulnérabilités, des renseignements indiquant qu'un acteur menaçant est en train de planifier une attaque contre un système d'information du GC – par exemple une attaque par déni de service distribué (DDOS) – et des tentatives d'intrusion dans le périmètre du réseau, etc.
Journal des événements de sécurité	Tout événement, notification ou alerte qu'un dispositif, un système ou un logiciel est techniquement capable de produire en fonction de son état, de ses fonctions et de ses activités. Les journaux d'événements de sécurité ne sont pas limités aux dispositifs de sécurité, mais s'appliquent à tous les dispositifs, systèmes et logiciels qui sont techniquement capables de produire des journaux d'événements qui peuvent être utilisés dans les enquêtes de sécurité, la vérification et la surveillance. Les systèmes pouvant produire des journaux d'événements de sécurité sont, entre autres, les suivants : pare-feu, systèmes de prévention des intrusions, routeurs, commutateurs, filtrage de contenu, journaux de flux de trafic réseau, réseau, services d'authentification, services d'annuaire, DHCP, DNS, plateformes matérielles, plateformes de virtualisation, serveurs, systèmes d'exploitation, serveurs Web, bases de données, applications, pare-feu d'application/de couche 7.
Incident de sécurité	Tout événement (ou ensemble d'événements), acte, omission ou situation ayant entraîné un compromis. Exemples d'incidents de cybersécurité : Exploitation active d'une ou plusieurs vulnérabilités identifiées, exfiltration de données,

	défaillance d'une mesure de sécurité, violation d'un service du GC hébergé ou géré dans le nuage, etc. (Référence : Plan ministériel de gestion des événements de cybersécurité du GC)
Services	a) accorder des droits d'utilisation aux services d'informatique en nuage; fournir la documentation relative aux services d'informatique en nuage; b) maintenir, améliorer et mettre à jour les services d'informatique en nuage; c) gérer les incidents et les défauts afin de garantir que les services d'informatique en nuage fonctionnent au niveau de service applicable; et d) fournir des services d'infrastructure informatique accessoires et supplémentaires nécessaires pour fournir les services d'informatique en nuage.
Gestion des événements	Tout événement, omission ou situation susceptible de nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité. Exemples d'événements liés à la cybersécurité : Divulgation d'une nouvelle vulnérabilité, renseignements indiquant qu'un acteur menaçant est en train de planifier une attaque contre un système d'information du GC (par exemple, attaque par déni de service distribué [DDOS]), tentatives de violation du périmètre du réseau, etc. (Référence : Plan ministériel de gestion des événements de cybersécurité du GC)
Accord sur les niveaux de service (ANS)	L'accord sur les niveaux de service est un contrat entre un fournisseur de services (interne ou externe) et l'utilisateur final qui définit le niveau de service attendu du fournisseur de services.
Lieu de service	Toute installation, tout site ou tout autre emplacement physique détenu, loué, fourni ou occupé de toute autre manière par le fournisseur ou tout sous-traitant du fournisseur à partir duquel le fournisseur ou tout sous-traitant du fournisseur fournit des services.
Logiciel sous forme de service (SaaS)	Le SaaS est un modèle de service dans lequel la capacité fournie au consommateur est d'utiliser les applications du fournisseur fonctionnant sur une infrastructure en nuage. Les applications sont accessibles à partir de divers dispositifs clients par l'entremise d'une interface client légère, telles qu'un navigateur Web (par exemple, une messagerie électronique basée sur le Web) ou une interface de programme. Le consommateur ne gère ni ne contrôle l'infrastructure en nuage sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même les capacités des applications individuelles, à l'exception éventuelle des paramètres d'une application limitée spécifique à l'utilisateur.

Sous-traitant	Toute personne à laquelle l'entrepreneur sous-traite l'exécution de ses services, en tout ou en partie.
Sous-processeur	Toute personne physique ou morale, autorité publique, organisation ou autre organisme qui traite des données à caractère personnel pour le compte d'un responsable du traitement ou d'un entrepreneur.
Système	Toute combinaison de matériel et de logiciel, y compris toute ligne ou réseau de communication utilisé pour faire le lien entre cette combinaison de matériel et de logiciels liés aux services.
Utilisateur	Un utilisateur est une personne ou un processus de système agissant au nom d'une personne autorisée par le Canada à accéder aux services.

Pièce jointe 1 – Grille d'évaluation de la préqualification

Partie A – Critères obligatoires

Les critères obligatoires suivants doivent être satisfaits.

	Critères	Renseignements devant être fournis par les soumissionnaires	Éléments de notation
O1	**Capacité du soumissionnaire à vendre une infrastructure en tant que service (IaaS) disponible sur le marché ET une plateforme en tant que service (PaaS).** Le soumissionnaire doit être un fournisseur de services infonuagiques (FSI) proposant des services d'IaaS disponibles sur le marché **ET** des services de PaaS native.	Le soumissionnaire devrait fournir la documentation énumérant les services d'IaaS disponibles sur le marché et les services (types d'instances) de PaaS native, pour les services suivants : 1. les services qui répondent à chaque catégorie et sous-catégorie des services d'IaaS disponibles sur le marché : a. Catégorie 1 – Instances à usage général ou standard qui peuvent être configurées de façon à équilibrer la quantité de ressources de calcul, mémoire et réseau en fonction des exigences des applications et des charges de travail. b. Catégorie 2 – Instances optimisées pour le calcul pour les applications et les charges de travail qui exigent une grande puissance de calcul utilisant des processeurs haute performance. c. Catégorie 3 – Instances à mémoire optimisée pour les applications et les charges de travail qui exigent un traitement rapide de grands ensembles de données en mémoire. d. Catégorie 4 – Instances spécialisées pour les applications et les charges de travail qui nécessitent des exigences particulières, y compris n'importe qu'elles des sous-catégories suivantes : i. Calcul de haute performance (CHP) ii. Capacités de stockage accrues iii. Processus assisté par GPU (unité centrale graphique) iv. Systèmes d'apprentissage automatique e. Catégorie 5 – Capacités évolutives de stockage de blocs, d'objets et de fichiers f. Catégorie 6 – Stockage hors-ligne pour le stockage à long terme de données archivées	Pour être conforme, le soumissionnaire doit démontrer les services suivants par le biais des hyperliens: • Un minimum de 5 services d'IaaS disponibles sur le marché pour chacune des catégories, démontrés par leur liste de produits/services publiquement visible (1a à 1g). • Un minimum de 4 services de PaaS disponibles sur le marché pour chacune des catégories, démontrés par leur liste de produits/services publiquement visible (2a à 2f). Note : Si un hyperlien fourni dans la soumission ne fonctionne pas, SPC se réserve le droit de demander des éclaircissements au soumissionnaire ; cependant, les services spécifiés doivent demeurer conformes à la soumission originale.

	Critères	Renseignements devant être fournis par les soumissionnaires	Éléments de notation
		g. Catégorie 7 – Stockage de haute performance fondé sur la technologie de disque SSD (disque statique à semiconducteurs). 2. les services (types d'instances) qui répondent collectivement à chaque catégorie des services de PaaS native suivants : a. Catégorie 8 - Services de conteneurs b. Catégorie 9 - Outils du développeur c. Catégorie 10 - Services de bases de données d. Catégorie 11 - Services réseau et de sécurité e. Catégorie 12 - Intelligence artificielle (IA) ou apprentissage automatique f. Catégorie 13 - Services d'analyse et de métadonnées	
O2	**Capacité du soumissionnaire à sécuriser les données du Canada** Le soumissionnaire doit détenir les dernières versions des certifications de l'industrie et rapports de vérification actuels et valides suivants : 1. Norme ISO/IEC 27001 : Technologie de l'information – Techniques de sécurité – systèmes de gestion de la sécurité de l'information – Exigences; 2. Norme ISO/IEC 27017 : Technologie de l'information – Techniques de sécurité – Code de pratique pour les contrôles de la sécurité de l'information fondés sur la norme ISO/IEC 2 7002 en ce qui concerne les services infonuagiques; 3. Norme Service Organization Control (SOC) 2 Type II de l'AICPA pour les principes de confiance, de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité. *Seules les certifications émises par une tierce partie indépendante admissible en vertu de l'AICPA, CPA Canada ou conformément à la norme de système de qualité ISO/IEC 17020 seront acceptées.	Le soumissionnaire devrait fournir les évidences suivantes pour chaque certification et rapport de vérification : - des copies des certifications et des rapports de vérification; - une lettre ou un énoncé de vérification de l'organisme émetteur confirmant l'état actuel et valide de la certification; - la date d'émission et d'expiration (s'il y a lieu).	Pour être conforme, le soumissionnaire doit démontrer qu'il possède les dernières versions des certifications et rapports de vérification actuels, et valides suivants : norme ISO/IEC 27001, norme ISO/IEC 27017 et norme service Organization Control (SOC) 2 Type II de l'AICPA

Partie B – Critères cotés

Les critères suivants seront cotés selon les éléments de notation définis dans le tableau.

Note totale maximale = 77 points

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
C1	**Capacité à satisfaire les exigences en matière d'hébergement (maximum 15 points)** Le soumissionnaire devrait avoir au moins un centre de données situées au Canada. Le Canada utilise le système de classification par niveaux de l'Uptime Institute pour la définition des centres de données. Aux fins de cette sollicitation, un centre de données est une infrastructure physique qui répond ou dépasse les exigences du niveau « Data Center Tier III ».	Le soumissionnaire devrait fournir l'adresse physique d'une installation de centre de données situées au Canada.	Jusqu'à 15 points seront attribués. Les points seront attribués comme suit : • Le soumissionnaire a une installation de centre de données situées au Canada = 15 points; • Le soumissionnaire n'a pas d'installation de centre de données situées au Canada = 0 point.
C2	**Capacité de la solution du soumissionnaire à protéger les données du Canada (maximum 12 points)** Le soumissionnaire devrait démontrer que la solution à la capacité de chiffrer les données en mouvement et au repos en utilisant la cryptographie approuvée par le Centre de la sécurité des télécommunications Canada (CST). *Remarque à l'intention des soumissionnaires : Cette exigence n'est pas obligatoire à l'étape de la présélection. Elle sera obligatoire aux étapes suivantes de l'approvisionnement et sera vérifiée avant l'octroi du contrat.* La cryptographie approuvée par le CST se trouve sur la page suivante : Algorithmes cryptographiques pour l'information NON CLASSIFIÉE, PROTÉGÉ A et PROTÉGÉ B - ITSP.40.111 (version 3 – 18 mars 2024) (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111)	**1. Dans le cas des données en mouvement :** Pour démontrer sa capacité, le soumissionnaire devrait fournir le mécanisme cryptographique utilisé pour empêcher la divulgation non autorisée de renseignements et pour détecter toute modification apportée aux renseignements durant la transmission et fournir des preuves des éléments suivants : a) Déterminer si la conformité des modules cryptographiques à la norme FIPS 140-3 a fait l'objet d'essais et été validée en vertu du Programme de validation des modules cryptographiques (PVMC) : Exigences de sécurité pour les modules cryptographiques (Security Requirements for Cryptographic Modules) conformément à l'article 12 de la norme ITSP 40.111 b) Déterminer quels algorithmes de chiffrement ont été mis en œuvre et confirmer qu'ils font partie de la liste d'algorithmes de chiffrement	Jusqu'à 12 points seront attribués. Les points seront attribués comme suit : **1. <u>Dans le cas des données en mouvement</u> :** a) Algorithme confirmé comme étant conforme à la norme FIPS 140-3 en vertu du CMVP = 2 points, confirmés comme étant conformes à la version précédente de la norme FIPS en vertu du CMVP = 1 point non confirmé comme étant conforme en vertu du CMVP = 0 point b) L'algorithme de chiffrement figure sur la liste des algorithmes recommandés par le CST = 2 points L'algorithme de chiffrement figure sur la liste des algorithmes suffisants produite par le CST = 1 point Tout autre algorithme = 0 point

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
		recommandés conformément aux articles 2 et 3 de la norme ITSP 40.111. c) Confirmer si les mises en œuvre d'algorithmes cryptographiques ont été soumises à des essais et validées en vertu du Programme de validation des algorithmes cryptographiques (CAVP pour Cryptographic Algorithm Validation Program), conformément à l'article 12 de la norme ITSP 40.111. **2. Dans le cas des données au repos :** Pour démontrer sa capacité, le soumissionnaire devrait fournir le mécanisme cryptographique utilisé pour empêcher la modification et la divulgation non autorisée de renseignements au repos sur les composants du système d'information stockant les données du Canada et fournir des preuves des éléments suivants : a) Déterminer si la conformité des modules cryptographiques à la norme FIPS 140-3 a fait l'objet d'essais et été validée dans le cadre du Programme de validation des modules cryptographiques (PVMC) : Exigences de sécurité pour les modules cryptographiques (Security Requirements for Cryptographic Modules) conformément à l'article 12 de la norme ITSP 40.111. b) Déterminer quels algorithmes de chiffrement ont été mis en œuvre et confirmer qu'ils font partie de la suite d'algorithmes de chiffrement recommandés conformément aux articles 2 et 3 de la norme ITSP 40.111. c) Confirmer si les mises en œuvre d'algorithmes cryptographiques ont été soumises à des essais et validées en vertu du Programme de validation des algorithmes cryptographiques (CAVP pour Cryptographic Algorithm Validation Program), conformément à l'article 12 de la norme ITSP 40.111.	c) Algorithme confirmé comme étant conforme en vertu du CAVP = 2 points Algorithme non confirmé comme étant conforme en vertu du CAVP = 0 point **2. Dans le cas des données au repos :** Les points seront attribués comme suit : a) Algorithme confirmé comme étant conforme à la norme FIPS 140-3 en vertu du CMVP = 2 points confirmés comme étant conformes à la version précédente de la norme FIPS en vertu du CMVP = 1 point non confirmé comme étant conforme en vertu du CMVP = 0 point b) L'algorithme de chiffrement figure sur la liste des algorithmes recommandés par le CST = 2 points l'algorithme de chiffrement figure sur la liste des algorithmes suffisants produite par le CST = 1 point Tout autre algorithme = 0 point c) Algorithme confirmé comme étant conforme en vertu du CAVP = 2 points Algorithme non confirmé comme étant conforme en vertu du CAVP = 0 point

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
		Pour chaque élément, les preuves suivantes pourraient être fournies : 1. La politique de protection des systèmes et des communications; 2. Les procédures relatives à la protection des renseignements au repos et en mouvement; 3. La documentation relative à la conception des systèmes d'information; 4. Les paramètres de configuration des systèmes d'information et la documentation connexe; 5. Les mécanismes cryptographiques et la documentation de configuration connexe; 6. Les dossiers de vérification des systèmes d'information; 7. Tous les autres documents ou dossiers pertinents.	
C3	**Expérience du soumissionnaire à fournir des services d'IaaS et de PaaS native à de grandes organisations (maximum 21 points)** Le soumissionnaire devrait démontrer son expérience en matière de fourniture de services d'IaaS et de PaaS native à de grandes organisations gouvernementales ou à de grandes sociétés privées externes. *« externe » fait référence aux organisations ou aux sociétés qui ne font pas partie de la propre structure d'entreprise du soumissionnaire ou de son organisation mère.* *Dans ce critère, « services uniques » désigne un élément spécifique du catalogue de services infonuagiques publics et disponibles sur le marché. Cela exclut spécifiquement les services infonuagiques non publics, y compris, mais sans s'y limiter, les services infonuagiques privés et les services d'hébergement de centre de données.*	Pour démontrer son expérience, le soumissionnaire devrait fournir une liste de trois (3) clients à qui des services d'IaaS et de PaaS native ont été offerts. Pour chaque client, les renseignements suivants devraient être fournis : 1) Le nom de l'entreprise cliente 2) La durée des services, y compris la date de début et de fins des services (mois et année) 3) Le nombre d'employés de l'entreprise cliente 4) Le nombre de services uniques fournis et utilisés par le client au cours de la durée des services.	Jusqu'à 21 points seront attribués en utilisant la moyenne des points totaux pour les trois clients. Les points seront attribués comme suit : **Durée des services fournis au client** - 7 ans ou plus = 7 points - 5 ans ou plus et moins de 7 ans = 5 points - 3 ans ou plus et moins de 5 ans = 3 points - Moins de 3 ans = 0 point **Nombre d'employés du client** - 50 000 employés ou plus = 7 points - Entre 29 999 et 50 000 employés = 5 points - Entre 9 999 et 30 000 employés = 3 points - Moins de 10 000 employés = 0 point **Services uniques fournis et utilisés** - 200 services et plus = 7 points - Entre 149 et 200 services = 5 points - Entre 99 et 150 services = 3 points - Moins de 100 services = 0 point

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
			Si plus de trois clients sont présentés, seuls les trois premiers clients inscrits dans la soumission seront évalués.
C4	**Capacité du soumissionnaire à résoudre le problème (maximum de 29 points)** Le soumissionnaire devrait démontrer sa capacité à résoudre le problème de l'énoncé des défis. *Le terme « région » se définit comme plusieurs centres de données situés à moins de 100 km les uns des autres au sein de la même région définie.*	Le soumissionnaire devrait fournir les renseignements suivants afin de démontrer sa capacité à résoudre le problème de l'énoncé des défis pour chaque élément énuméré ci-dessous : **Évaluation comparative** 1. Le nombre de régions au Canada. 2. Le nombre de régions mondialement. 3. Le nombre de centres de données (CD) au Canada. Le soumissionnaire devrait fournir la ville de chaque CD associé à la région. 4. Le nombre total de centres de données déployés et en service mondialement. 5. Le nombre de connexions réseau au Canada. Le soumissionnaire devrait fournir le nom des entreprises de chaque connexion réseau avec lequel il est associé. 6. Le nombre de points d'appairage réseau mondialement 7. La capacité de bande passante en gigabits par seconde (Gb/s) au Canada Le soumissionnaire devrait fournir les gigabits par seconde (Gb/s). 8. Le nombre total de cœurs déployés au Canada 9. Pourcentage de la capacité disponible en termes de cœurs Le soumissionnaire devrait fournir les données associées au calcul suivant : le pourcentage de la capacité disponible en termes de cœurs est calculé comme suit : [1 - (nombre de cœurs utilisés au Canada / nombre de cœurs déployés au Canada (élément 8))] *	Jusqu'à 29 points seront attribués en utilisant la somme de l'évaluation comparative et la notation directe des éléments (1 à 11). Chaque élément (1 à 11) se verra attribuer des points individuellement. **Évaluation comparative des éléments** Pour les éléments 1 à 9 : A. **Établissement du classement** : Les soumissionnaires seront classés du nombre le plus élevé au nombre le plus bas. B. **Attribution des points** : Les points seront attribués en fonction du classement du soumissionnaire dans chaque élément, du plus élevé au plus bas. Les points seront attribués comme suit : - Soumissionnaire classé premier = 3 points - Soumissionnaire classé deuxième = 2 points - Soumissionnaire classé troisième = 1 point - Autres soumissionnaires classés (4e position et plus) = 0 point **Notation directe** Pour les éléments 10 et 11, les points seront attribués comme suit : - Oui = 1 point; - Non = 0 point.

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
		Notation directe 10. Le soumissionnaire dispose de documents définissant des mesures de latence et de rendement entre ses régions : oui ou non 11. Le soumissionnaire offre un marché pour les applications tierces : oui ou non Pour les éléments 10 et 11 : Le soumissionnaire devrait fournir les hyperliens.	

Pièce jointe 2 - Règles d’engagement

Le Canada engagera régulièrement les soumissionnaires au cours des prochains mois dans l'élaboration de la sollicitation.

En participant au processus de consultation, le soumissionnaire :

1. Reconnaît et accepte que :

- Le soumissionnaire participera activement à des événements interactifs avec le Canada (sessions de groupe interactives, sessions individuelles, sondages) tout au long du processus de consultation ;
- Une séance de groupe initiale aura lieu au cours de laquelle le Canada présentera au soumissionnaire les défis auxquels le Canada est confronté et pour lesquels il a besoin d'une solution ;
- Pendant les événements interactifs, le soumissionnaire proposera des approches innovantes au Canada pour relever ces défis ;
- Le soumissionnaire participera et partagera volontairement des idées et ces événements ne seront pas soumis à un accord de non-divulgation ;
- Le soumissionnaire aura une opportunité égale de partager des idées préliminaires, que le Canada pourrait potentiellement utiliser pour élaborer la sollicitation ; et
- chaque événement sera enregistré à des fins de documentation pour démontrer, si nécessaire, que le processus de consultation a été mené équitablement par le Canada.

2. S'engage à :

- Travailler dans les paramètres définis qui seront fournis au début du processus de consultation, tel que les délais ;
- Favoriser l'équité et la transparence lors du processus de consultation par le biais d'une communication ouverte et d'un partage d'informations avec le Canada ;
- Soulever toute préoccupation concernant l'équité ou la transparence de ce processus auprès de l'autorité contractante en temps opportun ; et
- Participer à ce processus de manière ouverte, honnête et respectueuse.